E-mail: sviatoslav.khramov.kb.2022@lpnu.ua.
Orcid ID: 0009-0004-6486-8631.

**Опірський Іван Романович**, д.т.н., професор, завідувач кафедри захисту інформації Національного університету «Львівська політехніка».

**Ivan Opirskyy**, Doctor of Technical Sciences, Professor, Head of the Department of Information Security, National University "Lviv Polytechnic".
E-mail: ivan.r.opirskyi@lpnu.ua.
Orcid ID: 0000-0002-8461-8996.

**DOI: 10.18372/2410-7840.26.18843**
**УДК 004.415.05**

# МЕРЕЖЕВОЦЕТРИЧНІ ВІЙНИ – ВІЙНИ СУЧАСНОСТІ

***Володимир Артемов, Володимир Хорошко***

*В статті розглядається теорія мережевоцентричної війни та її вплив на сучасність. Вона була розроблена у другій половині XX сторіччі та широко використовується у війнах XXI сторіччя. Сутність концепції мережевоцентричної війни можливо переоформлювати наступним чином це війна «сліпого» проти «зрячого». Фізична сила «сліпого» - бойова міцність класичних збройних сил, які не користуються перевагами мережево-центричних підходів, що не гарантує переваги в сучасному бою. Це завідомо програшна ситуація. Мережевоцентричної війна складається з 3-х решіток–підсистем: інформаційної, сенсорної (тобто розвідувальної) і бойової. Але її основу складає інформаційна підсистема, цілями якої, виходячи з концепції є так звані кільця Уордена. Використовуючи теорію мережевоцентричної війни та застосовуючи тактику гібридної війни, РФ захопила Крим та окупувала Донбас. А 24 лютого 2024 року росія розпочала війну проти України, причому повторюючи свої дії при агресії проти Грузії у 2008 році. Тобто, починаючі з кібератак на державні установи та центри керування державою. Але рф використовуючи елементи мережевоцентричної війни, воює як воювали у Другій світовій війні. Україна застосовує перехід від управління військами та зброєю до управління збройною боротьбою. Війна росії проти України свідчить, що в сучасній війні перемагає той, хто швидше сприймає нові технології та втілює їх у життя, бере на озброєння та практично впроваджує нові воєнні доктрини та концепції, які відповідають духу часу, і уможливлюють не лише використання нових технологій та ідей, а й добре знає, які з них як і коли використовувати. Високі технології сьогодні перетворюються в системоутворюючий фактор сучасної збройної боротьби. Вони дозволяють досягнути того нового етапу розвитку воєнного мистецтва-переходу від управління військами в ході збройної боротьби до управління конфліктом у цілому.*

***Ключові слова:*** *мережевоцентрична війна, гібридна війна, кільця Уордена, теорія Бойда.*

## ВСТУП

Існування та розвиток сучасних ресурсів відбувається в тісному зв'язку з геополітичними та геостратегічними умовами і значною мірою залежить від міжнародних відносин. При цьому все більшого значення надається забезпеченню національній безпеці – стану захищеності життєво важливих інтересів особи, суспільства та держави від внутрішніх та зовнішніх загроз.

Серед багатьох факторів, що впливають на формування зовнішньої та внутрішньої політики держав, визначальна роль належить національним інтересам. Собою усвідомлюють на всіх рівнях суспільного життя, потреби народу країни у збережені та примноженні національних цінностей та національних багатств, в економічному процвітані та політичній стабільності суспільства, національні інтересам дістають своє відображення під час формування та досягнення національних цілей. Таким чином, виявляються пов'язаними національні інтереси і дії щодо їх досягнення. У міждержавних відносинах не тільки такі дії, а навіть і їх здійснення є об'єктами підвищеної уваги, ретельного вивчення та всебічної оцінки. Це особливо характерного для Європи, де переплетіння інтересів держав на перенаселеній та технологічно перенасиченій території спостерігається у найвищій мірі.

Крім того, обґрунтування національної стратегії воєнної безпеки є вважливим і відповідальним завданням. Стратегічне мислення є невід'ємним чинником ефективної політики. Як зазначив ще у 1927 році відомий теоретик воєнної науки О. Свечін: «Стратегія одна із найважливіших знарядь політики, політика й у час значною мірою має ґрунтувати свої розрахунки на військових можливостях дружніх і ворожих держав. Стратегія має заглядати у майбутнє і враховувати його у дуже широкій перспективі».

Аналіз сучасних військових конфліктів дає ключ до розуміння логіки дій учасників збройної боротьби в будь якій точці світу. Але цей арсенал передбачає не тільки вагомі матеріальні витрати, а й наявність політичній ваги держави, яка вирішу-

ла його застосувати. Актуальні тенденції в підготовці та веденні війни на сьогодні такі [1]:

- розрахунок на оснащення збройних сил засобами ведення безконтактних бойових дій. Тепер немає необхідності «йти на ви» з піднятим забралом, своє слово каже високоточна зброя, засоби електронної розвідки та радіоелектронної боротьби;
- інтенсивне нарощування сил швидкого реагування, аеромобільних військ і військ спеціального призначення. Готовність перемагати не завдяки кількісним перевагам, а майстерності і кращому оснащенню, у складних умовах, в оточенні цивільного населення, стає необхідністю. Воювати не кількістю, а вмінням в оточенні цивільного населення стає широко затребуваним умінням ( тільки не для російської армії);
- прагнення «малої кров'ю, єдиним ударом» використовуючи фактор раптовості, завдати поразки та деморалізувати противника в тилу;
- перетворити протиборство в інформаційній сфері з супровідного в домінантну сферу, перехід від прагнення заходити на територію країни до намірів цілеспрямовано впливати на думки та емоції її громадян та управління ними;
- поширення гуманітарних інтервенцій як права більш впливової у світовій табелі про ранги держави «подбати» про населення іншої країни, що опинилася у сфері інтересів «покровителя».

Теорія мережевоцетричних воєн (МЦВ), що з'явилась на межі другого та третього тисячоліть, стверджує, що збройні сили, в яких реалізовано мережеве забезпечення (горизонтальне та одночине) для всіх організаційних форм та процесів мережеві сили, мають перевагу над традиційними. Загальна інформатизація та інтелектуалізація систем управління військами якісно змінити сутність військових операцій, перетворивши їх на мережевоцентричні. Йдеться не про гуманізацію війни, вона носить тотальний характер і ведеться безперервно та у всіх сферах функціонування держави.

МЦВ робить підсумкову ставку на інформаційній боротьбі. Термін «інформаційна боротьба», який з часом переріс у поняття «інформаційної війни». Інформаційна війна – це комплексний вплив (за допомогою сукупності інформаційних операцій) на систему державного та військового управління протилежної сторони, її військово-політичне керівництво, який вже в мирний час може призвести до прийняття сприятливих для сторони-ініціатора інформаційного впливу рішень, а під час конфлікту повністю паралізує функціонування інфраструктури управління противника. Інакше метою війни XXI століття є не стільки знищення противника, стільки його деморалізація та позбавлення здатність опору.

Тому провідні держави світу свою обороноздатність, відповідно до існуючих і прогнозованих небезпек та загроз, забезпечують головним чином через розроблення та поєднання в єдину цілісну систему сучасних високотехнологічних засобів та впровадження їх у практику застосування військ [2].

## ОСНОВНА ЧАСТИНА

Розглянемо історію створення та розвитку теорії мережевоцентричних війн. Вперше концептуальні питання та основи теорії мережецентричної системи управління та організації бойових та кібердій і фактично розгляд воєнних дій та їх організації з позицій воєнної кібернетики були сформульовані М. В. Огарковим (1977-1984 роки начальник Генерального штабу ЗС СРСР) наприкінці 70-х – на початку 80-х років XX століття [3, 4]. Ці положення та висновки М. В .Огаркова були реалізовані у воєнних доктринах США "JoinVision 2010" та "JoinVision 2020".

Основні аспекти взяття держави під зовнішній контроль для реалізації своїх інтересів шляхом придушення волі населення і влади країни-жертви до опору на основі використання широкого набору інноваційних технологій, які комплексно застосовуються , були описані в 1989 році в статті Вільяма Лінда. Основним у війнах четвертого покоління, за поглядами В. Лінда, є війна культур, ініціація, підтримка та підживлювання ззовні та організація всередині країни психологічного та інформаційного тиску на її народ і керівництво, взяття їх під зовнішній контроль та управління, створення умов для виникнення та сприяння зростанню в цій країні соціально-економічного хаосу і самовиснаження військових, фінансових та інших ресурсів. Ведення з цією метою високотехнологічних психологічних дій, маніпулювання засобами масової інформації, широкий спектр акцій інформаційної війни, як у середині країни, та і в світовому медійному та Internet-просторах, впровадження в національне законодавство норм, які шкодять національним інтересам [5, 6]. Цілеспрямовані всеохоплюючі агресивні атаки на традиційні культурно-історичні та інші цінності населення, на репутацію найбільш ефективних ключових керівників сфери державного та державно-військового управління. Створення умов для зниження рівня виховання, культури, освіти громадян. Організа-

ція компаній непокори, реалізація на територій країни-жертви тактики "конфліктів низької інтенсивності" за участю зовнішніх, внутрішніх та терористичних сил.

Висловлювання великого китайського полководця Сунь-Цзи: "Війна любить перемогу і не любить тривалості. Я чув про успіх швидких військових походів і не чув про успіх затяжних. Жодна держава не отримала вигоди з тривалої війни".

Виходячи з цього американськими військовими експертами був запропонований ряд концепції бойових дій. Найбільш відома з них – концепція або теорія Бойда. У своїй концепції Бойд підрозділяє війну на три елементи [7]:

- моральну війну: руйнування волі противника до досягнення перемоги шляхом його відділення від союзників ( або потенційних союзників) і внутрішнього роздроблення, підриваючи загальну віру та загальні погляди;

- ментальну війну: деформація і перекручування сприйняття противником реальності на основі дезінформації та створення неправильної уяви про ситуацію;

- фізичну війну: руйнування фізичних ресурсів противника(озброєння, живої сили, інфраструктури).

Відповідно до ідей Бойда та його послідовників, будь-яка діяльність у військовій сфері з певним ступенем наближення може бути представлена у вигляді кібернетичної моделі ООДА (Observe – спостерігай, Orient – орієнтуйся, Decide – вирішуй, Act – дій). Зазначена модель припускає багаторазове повторення петлі дій, складеної з чотирьох послідовних взаємодіючих процесів: спостереження, орієнтація, рішення, дія. Фактично має розвиток ситуації по спіралі і на кожному етапі цієї спіралі здійснюється взаємодія із зовнішнім середовищем і має вплив на противника. Цю модель відносять до розряду кібернетичних, тому що в ній реалізується принцип " зворотного зв'язку" , відповідно до якого частина виходу з системи знову подається на його вхід, щоб уточнити, а якщо буде потрібно і скорегувати розвиток системи на наступних етапах. У ряді офіційних доктринальних документів Міністерства оборони США петля ООДА розглядається в якості єдиної типової моделі циклу прийняття рішень для систем командування і керування (C2 systems), як своїх військ, так і військ противника.

Відмінна риса циклу ООДА від інших циклічних моделей полягає в тому, що в будь-якій ситуації завжди передбачається наявність противника з яким ведеться збройна боротьба. Противник також діє та приймає рішення в рамках своєї аналогічної петлі.

На основі аналізу робіт Бойда та його послідовників виділені наступні постулати теорії ООДА:

1. Військова діяльність протиборчих сторін здійснюється в однакових кібернетичних циклах ООДА;

2. Зміст основних елементів циклу ООДА такий:

- спостереження – збір інформації від внутрішніх і зовнішніх джерел;

- орієнтація – формування множини можливих планів (варіантів) і оцінка кожного з них за сукупність критеріїв;

- рішення – вибір найкращого плану дій для практичної реалізації;

- дія – практична реалізація вибраного плану дій;

3. Цикл ООДА є моделлю військової діяльності окремих осіб і організацій для війни та конфліктів будь-якого рівня (тактичного, оперативного та стратегічного);

4. Напрямки досягнення перемоги (одержання конкурентних переваг):

- скорочення часу виконання циклу ООДА;

- поліпшення якості прийнятих у циклі рішень;

5. Збільшення швидкості всіх частинок елементів циклу ООДА – головний шліх досягнення перемоги.

Із чотирьох етапів ООДА – циклу три безпосередньо пов'язані з обробкою інформації та з комп'ютерними технологіями. Четвертий етап (дія) носить у цілому «кінематичний» характер і пов'язаний з переміщенням у просторі, захистом і поразкою противника на основі вогневої мощі.

Щоб зберегти часові рамки ООДА-циклу дій своїх сил і забезпечити більш високий ніж у противника, темп бою, необхідно прискорити всі чотири етапи циклу, які реалізуються військами. Протягом XX століття всі зусилля військових, вчених та інженерів були спрямовані на вдосконалення озброєння та технологій у частині кінематичної частини петлі ООДА. Результатом цих зусиль було збільшення мобільності, точності та вогневої міцності озброєння. Однак на сучасному стані наступила технологічна межа кінематичної частини ООДА-циклу – могутніші види зброї наносять прийнятий супутній збиток, а більш швидкісні та більш захищені платформи озброєння та засоби доставки вражаючого фактора до

цілі припускають непомірні на сучасному етапі матеріальні витрати. У зв'язку з цим з'явилася необхідність в удосконалюванні інших етапів ООДА-циклу.

Оскільки перші три етапи ООДА-циклу пов'язані безпосередньо із процесами збору інформації, її розподілу, осмислення, аналізу та прийняття рішень на основі отриманої інформації, то чим швидше здійснюється збір, розподіл, аналіз, сприйняття інформації, тим швидше приймається рішення. Саме швидкість і правильність прийняття рішень – найбільш важливі в сучасних реальних бойових діях. Це послужило поштовхом до розробки концепції мережевоцентричної військової діяльності, або як її ще називають мережевоцентричної війни.

Питання системного порушення управління та функціонування держави докризового рівня були запропоновані та реалізовані підчас підготовки операції «Буря в пустелі» в 1991 році Джоном Уордером. Він розробив системний кібернетичний підхід до сучасних бойових дій, назвавши його «операції на основі ефектів» (EBO), який врахував розробки Бойда та став подальшим розвитком кібернетичної концепції мережевоцентричної організації бойових дій з елементами теорії обмеження. Відповідно до цієї концепції є п'ять основних сегментів: збройні сили, виробництво, інфраструктура і комунікації, населення і уряд- життєво важливих для будь якої держави. Кожна держава має в них свої унікальні місця вразливості (які отримали назви «центри тяжіння», «критичні точки» тощо). Їх правильне виявлення, та деструктивний вплив на них призводять до ефекту системного «паралічу» держави в тих чи інших сферах або в цілому. Цю технологію і застосувала росія у 2014 році при анексії Криму та на початку агресії на Донбасі [5, 8, 9]. В 2003 році модифікований варіант «петлі Байда»-був запропонований Д. Брайтоном [10].

Генерал Дептула Д. здійснив подальший розвиток поглядів Уордена та змісту війн 4GW. Він запланував розгляд ворога як системи на всіх національних рівнях, включаючи дипломатичний, інформаційний, економічний тощо, і вважав що не воєнні дії є невід'ємною складовою нової теорії конфлікту. В рамках цього в США були створені спецгрупи для роботи в Іраку та Авганістані, туди входили соціологи, етнографи, лінгвісти та інші фахівці. Ці спецгрупи спілкування з місцевим населенням впливали на його, свідомість досліджували його звички, поведінку, ієрархічну структуру, слабкі та сильні сторони тієї чи іншої соціальної, етнічної і релігійної групи тощо. Тобто фактично формували інформаційний базис для ведення когнітивних дій. В 2014 році Дептула Д. разом з Алленом Дж. на конференції «Нова воєнна стратегія США для нової ери» презентували новий концепт DIMET-операцій (DIMET: дипломатія, інформація, військова сила, економіка (включно фінанси) і технології), в якою ключовою складовою є високі технології [3].

Вперше систему концептуального викладення теорії мережевотехнічної війни із визначенням в ній ролі і місця інформаційних та інших високотехнологічних систем здійснили в публікації «Мережево-центрична війна: її походження і майбутнє» (серпень 1998 року) Артур Середровскі та Джон Горстка.

З початку 2000-х років у США в інтересах підвищення ефективності дій сил спеціальних операцій було впроваджено інформаційно-кібернетичний цикл F3EAD (Find, Fix, Finish, Exploit, Analyze and Disseminate). Його реалізація спрямована на отримання можливостей передбачати дії противника, виявляти і визначати місцезнаходження і цілі ворожих сил. Центральним місцем у процесі F3EAD є функціональне злиття в єдиний процес розвідки і операцій. Ці наробки не залишилися без уваги в росії.

Начальник Генерального Штабу Збройних сил росії Валерій Герасимов опублікував у 2013 року статтю з промовистою назвою «Цінність науки в передбаченні». Він вже тоді, випереджаючи майбутні дії держави-агресор зазначав: «Акцент використовуваних методів протиборства змінюється в бік широкого застосування політичних, економічних, інформаційних, гуманітарних та інших не військових заходів, реалізованих із задіянням протестного потенціалу населення. Усе це доповнюється військовими заходами прихованого характеру, у тому числі реалізацією заходів інформаційного протиборства й діями сил спеціальних операцій. До відкритого застосування сили часто під виглядом миротворчої діяльності та кризового врегулювання переходять тільки на якомусь етапі, в основному для досягнення остаточного успіху в конфлікті» [1].

Цікаво, що Герасимов не згадав (швидше за все, свідомо) головну рису нової війни: її кульмінація відбувається не на полях битв, а в першу чергу в головах людей. Події останніх років в Україні свідчать що агресор прагне не тільки захопити територію, а і встановити контроль над світоглядом мільйонів громадян країни, що стала жертвою російської агресії. Мета цієї війни (як

планувалося) довести до ситуації, коли застосування військової сили стане зайвим, саме це було в Криму. Їм потрібно щоб люди самі зрадили власну державу та підтримували агресора. Але не сталося, як чекалося.

Генерал Герасимов виступив, як гадалося, буревісником агресивних планів Кремля не випадково. І в той час розгледіти в Україні потенційний об'єкт російської агресії було непросто.

Всі основні теоретичні дослідження та проекти на ведення війни нового високотехнологічного типу яскраво демонструють, що запорукою перемоги в них є забезпечення досягнення інформаційної та технологічної переваги над супротивником та високоефективне управління. При цьому інформаційна перевага передбачає створення систем отримання, обробки та аналізу інформації, надійних мереж, які свої війська і засоби, надають їм змогу покращеного обміну інформацією та забезпечують своєчасну та повну загальну ситуаційну про інформованість командирів. Загальна ситуаційна обізнаність дозволяє забезпечувати співробітництво і самосинхронізацію, підвищує стійкість і швидкість роботи команди, а це у свою чергу, підвищує ефективність місії. Апробація такої розподіленої інформаційної системи бойового керування FBCB2 (Force XXI Battle Command Brigade or Below), яка охоплювала рівень «бригада-батальйон-рота», відбулася в Іраку у 2013 році[3,9]. Разом з цим необхідно забезпечити випереджаюче виведення з ладу та придушення систем розвідувально-інформаційного забезпечення та управління у противника (засобів та систем розвідки, мережево-утворюючих вузлів, центрів обробки інформації та управління).

Як зазначив адмірал В. Кларк, «у майбутніх операціях будуть випробовуватися революційні інформаційні технології і можливості розосередження сил, об'єднаних єдиним інформаційним простором для досягнення безпрецедентної наступальної могутності, гарантованої оборони і оперативності в складі об'єднаних з'єднань»

Сутність концепції МЦВ можливо переоформлювати наступним чином це війна «сліпого» проти «зрячого». Фізична сила «сліпого» - бойова міцність класичних збройних сил, які не користуються перевагами мережево-центричних підходів, що не гарантує переваги в сучасному бою. Це завідомо програшна ситуація.

МЦВ складається з 3-х решіток–підсистем: інформаційної, сенсорної (тобто розвідувальної) і бойової. Але її основу складає інформаційна підсистема, цілями якої, виходячи з концепції є так звані кільця Уордена.

Одночасно політтехнології противника ведуть масовані та скоординовані операції інформаційної війни, ціль яких-деморалізація населення, створення паніки та шоку, дезорганізація системи державного управління. У зв'язку з цим по новому проглядається співвідношення кількості та якості: можна мати у складі Сухопутних військ 90 або 550 бригад, але в умовах МЦВ, коли вони до неї не готові, ці бригади будуть неспроможні виконувати бойові завдання. Агресія з використанням принципів МЦВ буде складатися з двох етапів.

На першому етапі будуть наноситися високоточні повітряно-космічні удари на усю глибину території країни-жертви. В якості цілей для поразки вибираються критично важливі об'єкти. Списки пріоритетних об'єктів поразки складаються у мирний час, виходячи з концепції кілець Уордена. Доречи, за цією схемою будувалася атака НАТО проти Югославії у 1999 році та агресія росії проти України у 2014 році (анексія Криму та інтервенція на Донбасі). Одночасно противником будуть виконувати масові та синхроновані операції інформаційної війни:

- психологічні операції;
- електронне придушення та знищення системи державного, економічного, фінансового та воєнного управління, зв'язку, розвідки та РЕБ;
- наступальні комп'ютерні операції (кібервійна);

Метою першого етапу агресії буде:

- дезорганізація системи державного, економічного, воєнного управління;
- деморалізація населення, паніка і шок;
- дезорганізація воєнних заходів країни жертви;
- «осліплення» системи розвідки та ППО країни-жертви.

Другий етап агресії – наземне вторгнення ,яке починається тільки тоді ,коли ціль першого етапу буде досягнута, і коли це буде признано необхідним. По суті це буде вичищення місцевості.

Характерною особливістю другого етапу агресії буте те, що угрупування військ противника не будуть вести класичні військові дії. Буде виключатися сама можливість вступу в бій угрупувань противника. Характерні риси цього етапу агресії:

- противник буде випереджувати державу-жертву на усіх етапах: збору та оцінки інформації, прийняття рішень і дій;

- не буде зосередження військ, виходу військ, розгортання в бойовий порядок, безпосередньої атаки, переслідування або відходу на нові рубежі;

- не буде рубежів, полос, не буде флангів, фронтів і тилу;

- противник буде мати абсолютне інформаційне домінування на полі бою-буде бачити кожного солдата країни-жертви;

- жорстока ієрархічна система військового управління зміниться гнучкою мережевою, підлеглі війська отримають свободу у виборі методів дій, організаційно-штатна структура військ буде постійно змінюватися, пристосовуватися до вимог обстановки;

- широке використання тактичних наземних і повітряних робототехнічних комплексів, які будуть діяти в тилу, знищуючи осередки опору.

Все це корінним чином, змінює уяву про війну ,виводячи її за межі фізичної сфери у сферу інформаційну .Безконтактна війна становиться реальністю . І тут досвід Другої світової війни з організації та проведення стратегічних наступальних операцій може стати небезпечним і також шкідливим.

У концепції МЦВ є ще і психологічна складова: у того хто активно використовує переваги мережевоцентричних підходів, формується абсолютна віра до себе. Загроза життя конкретного військовослужбовця на полі бою стає мінімальною. Воєнні дії з поєдинку не за життя, а за смерть перетворюються в комп'ютерну гру за принципом: «Я тебе бачу. а ти мене – ні». Це за думками авторів концепції повинно привести до дезорганізації і деморалізації особового складу протилежної сторони ще до вступу в бій. Сторона ,яка не використовує переваг МЦВ, в короткі терміни повністю втрачає управління і, в кінцевому рахунку , отримає поразку.

МЦВ – це не міф і не фантастика .При цьому ,як рахують фахівці, концепція МЦВ універсальна та може бути застосована для боротьби з противником будь-якого типу: регулярним і нерегулярним військом, сучасним і традиційним.

Слід відзначити, що МЦВ має особливі властивості у порівнянні з традиційною війною [11]:

1. Широка могутність використання географічно розподіленої сили. Раніше за різного роду обмежень було необхідно, щоб підрозділи та елементи тилового забезпечення розташовувалися в одному районі в безпосередній близькості до противника або об'єкт який обороняється;

2. Друга відміна МЦВ в тому, що сили, які приймають в ній участь, високоінтелектуальні: користуючись знаннями, отриманими від всеохоплюючого погляду за бойовим простором і розташованого уявлення намірів командирів, ці сили будуть спроможні до самосинхронізації діяльності, стануть ефективним при автономних діях;

3. Третя відмінність – наявність ефективних комунікацій між об'єктами в бойовому просторі. Це дає можливість географічно розподіленим системам проводити сумісні дії, а також динамічно розподіляти відповідальність і весь об'єм роботи ,щоб пристосуватися до ситуації. Завдяки тому, більш чим в сім разів по відношенню до 1991 року збільшилася сумарна полоса пропускання орендованих Пентагоном каналів супутникового зв'язку для передачі інформації.

МЦВ направлена на перевід інформаційних переваг, які присутні окремим інформаційним технологіям в конкретну перевагу за рахунок об'єднання в стійку мережу інформаційно добре забезпечених, географічно розосереджених сил. Ця мережа, об'єднана з відомими технологіями, організацією процесів і людей, дозволяє застосування нових форм ведення війн. На підставі цього формуємо принципи ведення МЦВ:

1. Сили, які об'єднані надійними мережами, мають можливість покращення обміну інформацією;

2. Обмін інформацією підвищує якість інформації та загальної ситуаційної інформативності;

3. Загальна ситуаційна інформативність дозволяє забезпечувати співробітництво та самосинхронізацію, підвищує стійкість і швидкість команди;

4. Це, в свою чергу, підвищує ефективність операції.

Враховуючи особливості МЦВ по відношенню до будь-якого театру воєнних дій концепцією, цієї війни, передбачається 4 основні фази ведення бойових дій:

1. Досягнення інформаційної переваги за допомогою упереджувального знищення (виводу з ладу, подавлення) системи розвідувально-інформаційного забезпечення противника;

2. Завоювання переваги в повітрі за рахунок подавлення систем протиповітряної оборони противника;

3. Поступове знищення захищених баз управління та інформації засобів боротьби противника, в першу чергу, ракетних комплексів, авіації, артилерії, бронетехніки;

4. Кінцеве знищення або подавлення осередків опору противника.

Успішне виконання кожної з фаз будується на значно меншій протяжності бойового циклу «виявлення – розпізнавання – ураження» по відношенню з противником, на очних і повних відомостях про угрупування противника.

В військово-практичному сенсі МЦВ дозволяє перейти від війни на виснаження до більш короткотривалої та більш ефективної форми, для якої характерні дві основні характеристики: швидкість управління та принцип самосинхронізації.

Швидкість управління в уявленні експертів має такі аспекти:

1. Війська досягають інформаційної переваги, до якої відносяться не надходження інформації в великій кількості, а більш високі ступені уявлення і більш глибоке розуміння ситуації на полі бою. В технологічному плані все це припускає впровадження нових систем управління, розвідки, контролю ,комп'ютерного моделювання;

2. Війська мають інформаційну перевагу впроваджують в життя принципи маскування результатів, а не маскування сил;

3. В результаті таких дій противник втрачає можливість проводити будь-який курс дій і впадає в стан шоку.

Принцип самосинхронізації прийшов з теорії складних систем. У відповідності з цією теорією, складні явища та структура в найкращому ступені організовується за принципом знизу вгору.

Іншими словами, під самосинхронізацією фахівці розуміють спроможність військової структури самосинхронізуватися знизу, а не змінюватися у відповідності за вказівками з гори. Організаційна структура частин і підрозділів, норми та методи виконання ними бойових задач будуть видозмінюватися за рішенням командира на полі бою, але у відповідності з потребами вище стоячого командування.

Цей принцип входить в протиріччя з традиційними основами централізованої ієрархічної воєнної організації, яка основана на підлеглості директивним вказівкам з гори. Зламати таку систему важко, так як це потребує змін не тільки в організаційних формах і методах управління, але і в менталітеті начальників та підлеглих. Але принцип самосинхронізації вже реалізований збройними силами України.

Застосування систем самосинхронізації дозволяє досягти переваги над противником в швидкості та раптовості дій. Зникають тактичні та оперативні паузи, якими супротивник міг би скористатися, усі процеси управління і самі бойові дії становляться більш динамічними, активними та результативними. Воєнні дії набувають не форму послідовних боїв і операцій з відповідними паузами між ними. а форму безперервних високошвидкісних дій з рішучими цілями.

На основі цих принципів та фаз МЦВ в Україні була сформульована система забезпечення воєнної безпеки України пов'язане як із зовнішньою. так і внутрішньою сферами діяльності держави. Зовнішній аспект полягає в стабілізації воєнно-політичної обстановки в регіоні та в світі, в зменшенні рівня воєнної небезпеки для України з боку інших держав і в першу чергу від росії. Внутрішня сфера охоплює питання, пов'язані з вирішенням соціально-економічних проблем, підтримання на належному рівні обороноздатності держави в тому числі бойового потенціалу Збройних Сил, мобілізаційних можливостей тощо.

У основу забезпечення воєнної безпеки України як без'ядерної держави покладені три базові концепції.

По-перше це концепція воєнно-політичного партнерства, що опирається на розвинену економіку з раціональною інфраструктурою, стабільну сферу та обґрунтовану воєнну політику, спрямовану на підвищення стратегічної стабільності в регіоні та зменшення рівня воєнної небезпеки політичними та економічними засобами.

По-друге, це концепція оборонного стримування, за якого в мережах оборонної доцільності створюється воєнна організація держави, яка здатна звести до мінімуму ймовірності виникнення воєнного конфлікту за рахунок загрози завдання можливому агресору неприйнятної шкоди, внаслідок чого він втрачає стимул до нападу.

По-третє, це концепція відбиття можливої агресії, яка опирається на мобілізацію усіх можливостей та ресурсів країни для протидії воєнному нападу, завдання агресору поразки та придушення його до припинення воєнних дій. Але ця система забезпечення безпеки не спрацювала так як була сформульована у мирний час.

Основний зміст забезпечення воєнної безпеки України складають за мирного часу у загрозливий період із початком відбиття збройної агресії. У даний час нас більше цікавить відбиття агресії, яку Росія здійснила проти України [13]:

- своєчасне введення воєнного або надзвичайного стану в Україні або в окремих її місцевостях, здійснення наявного або часткового стратегічного розгортання Збройних Сил України, приведення їх та інших військових формувань до

готовності щодо виконань завдань локалізації воєнного конфлікту та відбиття збройної агресії;

- переведення національної економіки України, підприємств, транспорт і комунікацій на роботу за умови воєнного стану;

- розгортання відповідно до вимог воєнного часу систем стратегічного керівництва Збройних Сил України та іншими військовими формуваннями, систем оперативного, тилового, технічного та медичного забезпечення, сил і засобів територіальної та цивільної оборони;

- зосередження зусиль органів державної влади та органів військового управління, органів місцевого самоврядування, громадських організацій і громадян на виконання завдань оборони держави;

- повне використання можливостей міжнародних організацій з безпеки для припинення воєнного конфлікту, його локалізації та недопущення переростання його в локальну (регіональну) війну;

- відбиття збройного нападу, завдання ударів військам та найважливішим об'єктам агресора з метою примушення його до відмови від подальшого ведення (бойових) дій на початковій стадії збройної агресії та на укладання миру на умовах , які відповідають національним інтересам України.

Для оборони України поняття, зміст і характеристики загрозливого періоду мали надзвичайно важливе значення. Зусилля України у сфері оборони принципи ведення переговорів та укладання угод з воєнно-політичних питань були спрямовані на забезпечення таких умов, за яких спроба агресії Росії проти України не відчувалася та цей період мав бути більш тривалим. Це б надало Україні змогу вирішити завдання своєї оборони, враховуючи що ЗС України мали меншу чисельність [12, 13].

Результати аналізу можливої війни для України та оцінки стану воєнної безпеки України, які були зроблені в 2010 році, давали змогу визначити такі основні шляхи удосконалення підготовки оборони держави в інтересах збільшення загрозливого періоду воєнного конфлікту:

1. Створення ефективної системи раннього попередження про воєнну загрозу. Основу такої системи мали складати інформаційні сили та засоби Генерального штабу Збройних Сил, Служби безпеки України, Прикордонних військ, сили розвідки видів Збройних Сил та штабів оперативного командування. Перш за все це стосується агентурних, радіо – та радіотехнічних каналів розвідки. Об`єднані в єдину систему під безпосереднім керівництвом Генерального штабу ЗСУ, ці сили та засоби можуть надати надійну і своєчасну інформацію щодо ознак підготовки противником до агресії та імовірні терміни початку бойових дій з упередженням, необхідним для відповідного розгортання військ і виконання інших заходів підготовки до відбиття агресії;

2. Відмову від утримання в складі ЗС та інших військових формувань мирного часу значної кількості скадрованих частин та з'єднань. Доцільно мати добре укомплектовані і повністю боєздатні частини та з`єднання, які у разі агресії зможуть забезпечити відбиття агресії. У такому разі потенційний противник не зможе сподіватися на успіх раптового воєнного нападу без попереднього розгортання своїх збройних сил;

3. Підвищення уваги до захисту найважливіших угруповань військ і об`єктів від ударів з повітря. Це також знижує ймовірність спроб раптового воєнного нападу на Україну;

4.Збільшення уваги до завчасної підготовки країни до війни, перш за все, до її оперативного улаштування. Це також примушуватиме потенційного агресора збільшувати обсяги приготувань до збройного нападу, тим самим втрачається час і фактор раптовості.

Однак ці задачі не були виконанні тому , що на початку 2013 року ніщо не віщувало відставку В. Януковича. У Верховній Раді панувала президентська більшість на основі Партії регіонів, що легко ламала через коліно законодавчий процес у власних інтересах .Україна виглядала цілком підконтрольною та покірною росії і ніщо не віщувало масштабних соціальних потрясінь, а вже тим паче – військової агресії. Ще не було виступу Герасимова щодо майбутніх дій російського керівництва, хоча вони вже планувались.

Анексія Криму планувалась рф відповідно до поглядів Герасимова та системної моделі МЦВ на основі теорії Уордена. Як вже зазначалося, об'єкт з критичною кібернетичною інфраструктурою центр тяжіння за Уорденом – це та точка де об`єкт або суб`єкт впливу є найбільш вразливим [4, 5, 8]. Модель Уордена реалізовується за схемою «війна з середній зони». Слід врахувати, що ця модель добре працює в зонах конфліктів, коли збройні сили розглядаються місцевим населенням як зовнішній агресор.

На відміну від цієї моделі, росія тривалий час мала на території Криму підтримку з боку місцевого населення та значні військові формування Чорноморського флоту, які не сприймалися у ролі агресора або ворога [8, 9]. Росія здійснювала

тривалий попередній вплив на населення Криму з метою сприйняття військовослужбовців російської федерації як захисників населення та виправлення "історичної помилки" щодо підпорядкуванню Криму Україні. Потім почав здійснюватись вплив на керівництво Автономної Республіки Крим і міста Севастополь, а після цього інформаційно-психологічний вплив (згідно з теорією МЦВ) на особовий склад ЗС України. Були взяті під контроль основні об'єкти транспортної інфраструктури та системи життєдіяльності. Дії росії при проведенні компанії з введення Збройних Сил до Криму супроводжувались діями, які мали всі ознаки підготовленої та продуманої за цілями, заходами й наслідками операції, спрямованої перед усім на російську спільноту, а з іншого боку – на Українське та західне суспільство.

Тактика гібридної війни застосована росією в Криму, була з певними змінами, поширена і на Донбасі. Там, при агресії у південно-східному регіоні України, основний вплив був зосереджений на населенні регіону, наступними об'єктами впливу були державна інфраструктура та система життєзабезпечення відповідно. Четвертим та п'ятим об'єктами впливу стали ЗС та воєнно-політичне курівництво України.

Особливістю гібридної війни росії на Донбасі та в Україні, на той час, було і є зараз постійний пошук і використання актуальних інформаційних приводів, здатних сформувати необхідну громадську думку. Також спостерігалась та спостерігається тенденція (розширення) виливу на сфери, які раніше були непритаманні для інформаційного протиборства, а саме: перегляд історії державності України та росії та міжконфесійні відносини.

Для досягнення політичних цілей росії, та з метою дестабілізації обстановки значне поширення отримали терористичні акти, котрі проводились диверсійно-розвідувальними групами не лише в зоні проведення операцій об'єднаних сил (раніше антитерористичній операції), а й в інших регіонах України. З метою залякування населення та зниження морально-психологічного стану особового складу підрозділів операцій об'єднаних сил. Незаконні збройні формування використовували демонстраційні та провокаційні бойові дії.

Слід зазначити, що війна у кіберпросторі розпочалась 14 лютого 2022 року. У цей день російські хакери нанесли потужну кібератаку по державним установам та банківській системі України. З цього дня почались постійні кібератаки на Українські системи. А 24 лютого 2022 року росія почала спеціальну операцію проти України, тобто широкомасштабну агресію проти суверенної держави. Слід зазначити, що гібридна війна при цьому вийшла на новий рівень. Крім того російські СМІ , головними своїми темами акцентували: захист Луганської та Донецької народних республік від нападу України, денацифікацію та демілітаризацію України, а саме головне захист російськомовного населення українського суспільства.

Також слід зазначити, що у ніч з 23 на 24 лютого (відповідно до концепції МЦВ) російські хакерські групи здійснили, ряд додаткових кібератак на сайти державних установ та ЗМІ України.

Ці дії повторюють дії російського агресора у війні з Грузією у 2008 році [9], коли вони здійснили кібератаки на державні сайти Грузії перед початком агресії. Але кіберзахист України спрацював потужно, що дало можливість захистити більшість сайтів.

За російськими планами, які були озвучені в їх СМІ, вони повинні були за 3 дні захопити Київ, а за 9 днів повністю окупувати Україну. Але не сталося, як гадалося.

Слід зазначити, що найбільш важливішим з точки зору теорії воєнної стратегії, є початковий період війни (ППВ). Під ним розуміють такий період воєнних дій, коли протиборчі сторони, здійснювали перші операції збройних сил у вигляді створених угрупувань військ і сил, діють відповідно до завчасно розроблених планів, намагаються захопити стратегічну ініціативу, завдати супротивнику максимальних втрат та створити сприятливі умови для досягнення цілей війни [12].

Це загальне визначення можна розповсюдити на поняття ППВ для України. Вивчення досвіду МЦВ дає змогу стверджувати, що для ППВ характерні [1, 14]:

- висока напруга та динаміка бойових дій;
- рішуча боротьба за панування в повітрі та вогневу перевагу;
- невизначеність обстановки та швидкість її змін;
- одночасне діяння вогневими та ударними засобами, повітряними десантами на всю глибину оперативної побудови противника із зосередженням основних зусиль на головних напрямках і найважливіших об'єктах;
- масове застосування розвідувально-диверсійних груп, аеромобільних та повітряно-десантних військ;

- підвищення ролі всіх видів розвідки та прихованого управління військами;

- залежність успіху бойових дій військ від всебічності та рівня їх оперативної та бойової підготовки.

Конкретними цілями війни росії проти України є ліквідація або зміна існуючого політичного устрою, позбавлення суверенітету та територіальної цілісності тощо.

Виходячи з цього агресор під час ППВ застосував різноманітні форми воєнних дій, у тому числі терористичні, диверсійні, інформаційні тощо.

Оскільки найважливішою визначальною рисою ППВ є боротьба за стратегічну ініціативу, його можна розділити на такі дві фази:

- по-перше, фази вогневого та іншого взаємного діяння угрупувань військ сторін з метою створення умов для захоплення панування в повітрі та досягнення вогневої переваги, підняття морально-психологічного стану особливого складу збройних сил та населення;
- по-друге, фази використання результатів ураження противника та діяння на нього шляхом розгрому його ударних угрупувань, захоплення ключових рубежів з метою оволодіння стратегічною ініціативою.

Аналізуючи фази ППВ можна зробити висновок, що Україна отримала перемогу у цьому етапі війни. На початку війни росії проти України склалась дуже складна ситуація. Агресор підійшов до Києва, Харкова, захопив Херсон та частину Запорізької області, окопував Чернігівську та Сумську області. Але ще у березні 2022 року ЗСУ змогли відкинути ворога від Києва та Харкова, а далі звільнити Чернігівську та Сумську області. Сили оборони змогли переломити хід бойових дій. Переваги у повітрі, у повному розумінні, росіяни не змогли домогтися. Моральний дух наших воїнів та цивільного населення вони не змогли зламати, а тільки зміцнили. Захопити ключові трубежі їм також не вдалося. Навпаки, у вересні-жовтні ЗСУ звільнило Харківську область, а потім і Херсон. Тому можна стверджувати, що ППВ росіяни програли.

Сучасні війни за способами та засобами ведення суттєво відрізняється від воїн середини XX сторіччя. Це підкреслюється і теорією МЦВ. Україна за допомогою своїх західних партнерів це опанувала, а росія воює так як вона воювала у Другій світовій війні. Україна застосовує:

- перехід від управління військами та зброєю до управління збройною боротьбою;

- формування та застосування в зонах, де відбуваються бойові дії, ситуаційних розвідувально-ударних комплексів, які на базі наявних систем і засобів управління та комунікації поєднують в єдину систему наявні засоби розвідки та управління;

- перенесення основного навантаження дій у інформаційно-кібернетичний, когнітивний простір;

- інформаційні, психологічні, когнітивні, кібернетичні дії стають невід'ємною та переважаючою складовою воєнних дій;

- доступність до всіх елементів бойового простору всіх учасників дій;

- широкомасштабне, системне застосування інноваційних високотехнологічних засобів озброєння та військової техніки, гіперзвукової, високоточної та керованої зброї;

- ведення бойових дій дистанційно (при можливості);

- роботизація збройної боротьби;

- збільшення ролі та розширення масштабів застосування сил спеціальних операцій та кібервійськ;

- зростання асиметричності в характері бойових дій.

В той же час росія воює тільки кількістю військових, а не технікою. І при цьому вона несе дуже великі людські втрати.

Слід зазначити, що велику роль відіграє російська пропаганда.

Згадати хоча б нинішню російсько-українську війну. На початку повномасштабного вторгнення російська пропаганда кричала: «Київ за три дні», «Зранку взяття Києва, а в вечорі парад на Хрещатику» та інше.

Окупанти були впевнені, що українці їх зустрічатимуть, як визволителів і з квітами, і були здивовані, побачивши шалений опір українців.

Якщо згадати історію то перед битвою за Грозний (1994 року) російський генерал Грачов говорив, що йому треба дві години та силами одного парашутно-десантного полку, щоб узяти столицю Чечні. Та через дві доби чеченці спалили усі російські танки та БТР-и, які зайшли в Грозний, а росіян частково знищили або взяли в полон.

Найбільшим мінусом російської армії є недооцінка супротивника. У кожній війні росіяни чомусь були впевнені, що вони дуже легко переможуть. Так, на приклад, ще до початку Другої світової війни 1938-1939 років радянське командування запевняло, що війна буде на чужій тери-

торії, воювати Союз буде «малою кров'ю», що противники Радянського Союзу не зможуть гідно протистояти, адже немає такої ж «потужної» армії.

## ВИСНОВКИ

Армія будь якої країни світу має свої традиції, які формувалися сторіччями. Сучасна російська армія вважає себе спадкоємицею радянської армії і частково царської. Для усіх трьох армій характер підготовки офіцерського складу та ведення війни за понад 100 років майже не змінився.

Як відмічають фахівці, росіяни дуже самовпевнені. Їхня улюблена фраза – «Мы русские. С нами Бог!» Тому вони вважають, що програти війну вони просто не можуть. Таке собі окозамилювання.

Загалом росіяни дуже люблять апелювати до колишніх перемог. Проте чомусь не згадують, що то були часи російської імперії чи Радянського Союзу і воювали там не лише росіяни.

Війна росії проти України свідчить, що в сучасній війні перемагає той, хто швидше сприймає нові технології та втілює їх у життя, бере на озброєння та практично впроваджує нові воєнні доктрини та концепції, які відповідають духу часу, і уможливлюють не лише використання нових технологій та ідей, а й добре знає, які з них як і коли використовувати.

Високі технології сьогодні перетворюються в системоутворюючий фактор сучасної збройної боротьби. Вони дозволяють досягнути того нового етапу розвитку воєнного мистецтва-переходу від управління військами в ході збройної боротьби до управління конфліктом у цілому.

## ЛІТЕРАТУРА


[1]. Магда Е. Гібридна агресія Росії: уроки для Європи. К: Вид. «KALAMAR», 2017. 268 с.

[2]. Пермяков О.Ю., Збітнєв А.І. Інформаційні технології і сучасна збройна боротьба Луганськ: Знання, 2008. 204 с.

[3]. Даник Ю.Г. Високотехнологічні аспекти забезпечення національної безпеки і оборони // Коммуникации и сети. Телеком. 2018, октябрь, спец. выпуск. С. 58-69.

[4]. Пирцхалава Л. Г., Хорошко В. А., Хохлачева Ю. Е., Шелест М.Е. Информационно-аналитическое обеспечение безопасности. К: ФОП Янчинский А.В., 2021. 470 с.

[5]. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки. Житомир: ЖНАЕУ, 2016. 636 с.

[6]. Світова гібридна війна: український фронт / За ред. В.П. Горбуліна. Л: НІСД, 2017. 496 с.

[7]. Самойлов І.В., Конотов О.В., Концепція Байза // Коммуникации и сети. Телеком, 2016, сентябрь, спец. выпуск. С. 66-67.

[8]. Пєвцов Г.В., Залкін С.В., Сіденко С.О., Хударковський К.І. Інформаційно – психологічні операції Російської Федерації в Україні: моделі впливу та напрями протидії // Наука і оборона. № 2. 2015. С. 28-32.

[9]. Artemov V., Khoroshko V., Brailovsky M., Khokhlachova Y., Pirtskhalava T. Methoods of Preparing and Conducting Modern Hybrid Wars // SPCSI, v. 6, № 3. 2022. pp. 1-12.

[10]. Bryant D. I. Critique, Compare and Adapt: A New Model of Command Decisionmaking. Defend R&D Toronto Technical Repost, DFDC, Toronto TR, 2003. p. 63.

[11]. Бірюков В.О., Єсаулов М.Ю., Жук П.В., Міночкін А.І., Павлов І.М. Теоретичні основи інформаційної боротьби в сучасних війнах, воєнних конфліктах та у війнах майбутнього – К: ВІТІ ДУТ, 2013. 322 с.

[12]. Борискин В.Д., Военно-политическая и военно-стратегическая оценка возможности и характера локальных воин и конфликтов для Украины // Наука и оборона, №1, 1995. С. 52-56.

[13]. Шкідченко В.П., Кохно В.Д. Елементи теорії воєнної безпеки. К: БФ «Миротворець», 2001. 194 с.

[14]. Хорошко В., Хохлачова Ю., Іванченко І., Пірцхалава Т. Інформаційна зброя як інструмент інформаційної війни // Захист інформації, Т. 24, №2, 2022. С. 50-85.

[15]. Толубко В.Б. Інформаційна боротьба: концептуальні, теоретичні, технологічні аспекти. К: НАОУ, 2003. 320с.


## NETWORK WARS – MODERN WARS


The article examines the theory of network-centric warfare and its impact on the present. It was developed in the second half of the twentieth century and is widely used in the wars of the twenty-first century. The essence of the concept of network-centric warfare can be redefined as follows: it is a war of the "blind" against the "sighted". The physical strength of the "blind man" is the combat strength of classical armed forces that do not take advantage of network-centric approaches, which does not guarantee an advantage in modern combat. This is a losing situation. Network-centric warfare consists of 3 lattice subsystems: information, sensor (i.e., intelligence) and combat. But its basis is the information subsystem, the goals of which, according to the concept, are the so-called Warden rings. Using the theory of network-centric warfare and hybrid warfare tactics, Russia seized Crimea and occupied Donbas. And on 24 February 2024, Russia launched a war against Ukraine, repeating its actions during the aggression against Georgia in 2008. That is, it started with cyberattacks on government agencies and government control centers. But the Russian Federation, using elements of network-centric warfare, is fighting as it did in World War II. Ukraine is making a transition from managing troops and weapons to managing armed struggle. Russia's war against Ukraine shows that in mo-

dern warfare, the winner is the one who is quicker to perceive new technologies and implement them, adopts and implements new military doctrines and concepts that are in line with the spirit of the times and enable not only the use of new technologies and ideas, but also knows well which ones to use and when. High technologies are now turning into a systemic factor in modern armed struggle. They make it possible to reach that new stage in the development of military art – the transition from command and control of troops in the course of armed struggle to conflict management in general.
**Keywords**: network-centric warfare, hybrid warfare, Warden rings, Boyd's theory.

**Артемов Володимир Юрійович**, доктор педагогічних наук, професор, професор спеціальної кафедри Національної академії СБУ.

**Volodymyr Artemov**, doctor of pedagogical sciences, professor, professor of the special department of the National Academy of SBU.
E-mail: Vuk_karadzic@ukr.net.
Orcid ID: 0000-0002-5290-4496.

**Хорошко Володимир Олексійович**, доктор технічних наук, професор, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.

**Volodymyr Khoroshko**, doctor of technical sciences, professor, professor of the department of security of information technologies of the National Aviation University.
E-mail: professor_va@ukr.net.
Orcid ID: 0000-0001-6213-7086.

**DOI: 10.18372/2410-7840.26.18844**
**УДК 004.056.5**

# O HARNESSING BLOCKCHAIN AND EBPF FOR IMMUTABLE AUDIT OF SYSTEM EVENTS: A TECHNOLOGICAL CONVERGENCE APPROACH

***Pavlo Hlushchenko, Valerii Dudykevych***

*The importance of secure and reliable system event auditing has grown significantly in today's complex IT environments, where data integrity and security are paramount. Traditional auditing methods, which rely on centralized systems and are vulnerable to tampering and performance bottlenecks, are no longer sufficient. This article addresses these challenges by proposing a novel framework that combines blockchain and eBPF technologies to create an immutable, transparent, and efficient system for event auditing. The proposed solution leverages eBPF's real-time monitoring capabilities and blockchain's tamper-proof ledger to ensure the integrity and verifiability of audit logs. Through a detailed exploration of the conceptual framework and an analysis of potential challenges and solutions, this approach has proven to be effective in enhancing the reliability and security of system event auditing. The results of this study provide a foundation for future implementations, research and robust solutioning for organizations seeking to improve their auditing processes.*
***Keywords**: event auditing, blockchain, eBPF, immutability, monitoring.*

## INTRODUCTION

The primary objective of this article is to explore the innovative application of blockchain technology coupled with eBPF (Extended Berkeley Packet Filter) in the domain of system event auditing. Given the growing complexity and security requirements of modern computing environments, traditional auditing methods often fall short in providing the necessary transparency and integrity. This article proposes a novel approach that harnesses the immutable and decentralized nature of blockchain along with the powerful monitoring capabilities of eBPF to enhance the reliability and efficiency of auditing processes.

Auditing system events is critical in ensuring the security and compliance of information systems. It involves tracking and analyzing operations on the system to detect anomalies, unauthorized changes, and potential breaches. As systems grow in complexity, the volume of events increases exponentially, making it increasingly challenging to manage and secure these logs against tampering. Effective auditing helps organizations not only to comply with regulatory requirements but also to maintain the integrity and confidentiality of their data.

This article delves into two pivotal technologies: blockchain and eBPF. Blockchain is renowned for its robustness in managing data in a tamper-resistant manner across a distributed network, making it a valuable tool for enhancing the security and transparency of audit trails. On the other hand, eBPF provides a highly flexible and efficient framework for monitoring system events directly from the kernel space, offering precise visibility and control over system operations. The convergence of these technologies presents a promising avenue for redefining traditional system event auditing frameworks, promising enhanced security features and operational efficiencies.