УДК 355.424

Юрій Григорович Даник *(д-р техн. наук, професор, начальник інституту)*
Олександр Юрійович Пермяков *(д-р техн. наук, професор, професор кафедри)*

Національний університет оборони України імені Івана Черняховського, Київ, Україна

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЗАБЕЗПЕЧЕННІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ: РЕАЛІЇ ТА ТЕНДЕНЦІЇ РОЗВИТКУ

В статті на основі аналізу сучасного стану та тенденцій розвитку інформаційних і інших високих оборонних технологій та їх впливу на забезпечення національної безпеки і оборони, з врахуванням особливостей високотехнологічного розвитку людства, виявлені основні проблемні питання їх впровадження, ефективного застосування у воєнній сфері та визначені шляхи їх вирішення. З єдиних позицій розглянуті системи оперативного управління військами (силами) та зброєю, їх роль і місце у формуванні єдиного бойового простору та практичній реалізації мережецентричних концепцій організації та ведення бойових дій, а також системо-утворююча та інтегруюча роль інформаційних технологій у вирішенні цих питань. Досліджено фактори, які впливають на зростання кількості загроз і ризиків інформаційних, кібер та когнітивних деструктивних впливів на високотехнологічні системи (комплекси, засоби), особовий склад Збройних Сил та населення через кіберпростір в сучасних умовах і їх трансформації. Запропоновані можливі шляхи щодо удосконалення системи інформаційної і кібербезпеки та кібероборони держави у воєнній сфері. Розглянуті проблемні питання наукового супроводження створення, впровадження та забезпечення ефективного застосування високотехнологічних розробок у сфері оборони, а також підготовки фахівців за високотехнологічними напрямами в інтересах забезпечення національної безпеки і оборони та запропоновані шляхи їх вирішення.

Ключові слова: *інформаційні технології, високі технології, оборонні технології, когнітивне протиборство, мережецентрична концепція організації та ведення бойових дій, гібридна війна, C4ISR.*

Вступ

Постановка проблеми. Аналіз змін геополітичної і геостратегічної обстановки демонструє наявність проявів принципово нових тенденцій у формуванні майбутньої картини світу. На її стан і розвиток істотно впливають нові явища в філософії війни, теорії воєнного мистецтва і практики війн (воєнних конфліктів), в основі яких лежать інноваційні досягнення інформаційних та інших високих технологій, а також модифіковані та трансформовані у зв'язку із вищезазначеним традиційні та кардинально нові методи, форми і способи досягнення цілей конфліктів різної інтенсивності (включно збройні).

Практика свідчить, що в більшості країн світу з метою своєчасного реагування на виклики і загрози сьогодення і майбутнього їх запобігання, стримування та нейтралізації оборонний сектор держав включає дві основні компоненти: потенціал стримування, який складається з традиційних видів збройних сил та потенціал ведення війн нового типу, основу якого складають сили і засоби спеціальних операцій, інформаційно-психологічних операцій та радіоелектронної боротьби, а також, кібервійська, органи розвідки, оперативного управління силами і засобами, зв'язку та підрозділи, які оснащені роботехнічними комплексами і засобами боротьби з ними та інші високотехнологічні сили і засоби. Їх ефективні дії відповідно до визначеної мети і задач синхронізуються, управляються та здійснюються в рамках єдиного інформаційного та бойового простору на основі використання кібернетичних систем та інформаційних технологій [1 – 6].

Тому дослідження ролі, місця, тенденцій і проблем розвитку сучасних інформаційних технологій, як невід'ємної та інтегруючої складової високих технологій в забезпеченні національної безпеки і оборони в сучасних умовах і майбутньому є актуальним і важливим.

Аналіз останніх досліджень і публікацій. Провідні країни 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 впровадженням їх в практику застосування військ (сил) [1 – 8].

Це знаходить досить чітке своє відображення в поглядах національних оборонних концепціях, стратегіях, воєнних доктринах цих країн та при трансформації і розвитку їх секторів безпеки у вигляді комплексних високотехнологічних змін на політичному, організаційному, процесуальному, кадровому рівнях.

Найбільш вагомо на забезпечення вирішення всіх зазначених питань національної безпеки і оборони впливає розвиток інформаційних технологій. Слід зазначити, що з самого початку воєнної історії людства в основі будь-яких дій в цій сфері є інформація та інформаційна діяльність. Вона включає правильно та раціонально організовану роботу з своєчасного отримання в достатніх обсягах достовірної, надійної, актуальної, пертінентної, релевантної інформації її ефективної, якісної обробки та опрацювання і

своєчасної видачі кінцевим користувачам у зручному для використання вигляді. Це було, є і буде характерним та базовим для перемоги у будь-якому конфлікті у будь-яку епоху.

У трактаті Сунь-Цзи "Воєнне мистецтво" (460 р. до н.е.) [9], стосовно значення інформаційного забезпечення було сказано: "…якщо ти знаєш своїх ворогів і знаєш себе, ти можеш перемогти в сотнях битв без жодної поразки. Якщо ти знаєш тільки себе, але не знаєш свого опонента, ти можеш як перемогти, так і отримати поразку. Якщо ти не знаєш ні себе ні свого ворога, ти завжди будеш створювати для себе небезпеки". Суть введення противника в оману та активних інформаційних і психологічних дій проти нього він сформулював так: "Війна – це шлях омани ... якщо ти і можеш що-небудь, показуй супротивнику, ніби не можеш; якщо ти і користуєшся чимось, показуй йому, ніби ти цим не користуєшся; Якщо ти близько, показуй, ніби ти далеко; Якщо ти далеко, показуй, ніби ти близько; заманюй його вигодою; приведи його в розлад і бери його; якщо у нього все повно, будь напоготові; якщо він сильний, ухиляйся від нього; викликавши в ньому гнів, приведи його в стан розладу; прийнявши смиренний вигляд, виклич в ньому зарозумілість; якщо його сили свіжі, стоми його; якщо у нього сили дружні, роз'єднай; нападай на нього, коли він не готовий; виступай, коли він не очікує".

Кардинальна зміна поглядів на характер, форми і способи підготовки та ведення дій у війнах (воєнних, збройних конфліктах) відбулася коли розвиток технологій привів до поліпшення інформаційного обміну і зростання ролі самої інформації, створення базових передумов для можливості формування єдиного бойового інформаційного простору і управління в ньому всіма наявними військами (силами) і засобами в рамках єдиної мережі та забезпечення як вертикальної, так і горизонтальної інтеграції всіх учасників операцій.

Вперше концептуальні аспекти та основи теорії мережецентричної системи управління (реалізована у воєнних доктринах США "Joint Vision 2010", "Joint Vision 2020") та кібердій, фактично розгляд воєнних дій з позицій воєнної кібернетики були сформульовані Миколою Огарковим наприкінці 70-х початку 80-х років XX століття [10].

Інформаційні аспекти взяття держави під контроль для реалізації своїх інтересів шляхом придушення волі населення і влади країни-жертви до якого-небудь опору на основі використання широкого набору інноваційних технологій, які комплексно застосовуються в війнах четвертого покоління (4GW – за західною класифікацією), були описані в статті Вільяма Лінда "Обличчя війни, яке змінюється: на шляху до четвертого покоління" (1989 р.). Основним в війнах четвертого покоління за поглядами Вільяма Лінда є війна культур, ініціація, підтримка і підживлювання ззовні та організація всередині держави психологічного та інформаційного тиску на її народ і керівництво, створення умов для виникнення та сприяння зростанню в цій країні соціально-економічному хаосу і самовиснаження військових, фінансових та інших ресурсів. Ведення з цією метою високотехнологічних психологічних дій, маніпулювання засобами масової інформації, широкого спектру акцій інформаційної війни, як усередині країни, так і в світовому медійному та Інтернет просторах, впровадження в національне законодавство норм, які шкодять національним інтересам [11–13]. Цілеспрямовані всеохоплюючі агресивні атаки на традиційні культурно-історичні та інші цінності населення, репутацію найбільш ефективних ключових керівників сфери державного та державного-воєнного управління. Створення умов для зниження рівня виховання, культури, освіти громадян. Організація компаній непокори, реалізація на території країни-жертви тактики "конфліктів низької інтенсивності" за участю будь-яких зовнішніх, внутрішніх та терористичних сил.

Впровадження та апробацію кібернетичного підходу (кібернетичний цикл Бойда) до організації дій та їх спрямованості під час проведення військових операцій для отримання максимального ефекту від впливу на три сфери (моральну, ментальну та фізичну), здійснив Джон Бойд під час проведення операції "Буря в пустелі" в 1991 році. Він розглядав війну, як поєднання трьох складових. Руйнування волі противника до досягнення перемоги шляхом його відділення від союзників (або потенційних союзників) і внутрішнього роздроблення, підриву загальної віри і спільних поглядів (moral warfare). Дії спрямовані на деформацію і спотворення сприйняття противником реальності на основі дезінформації та створення неправильних уявлень про ситуацію (mental warfare). Руйнування фізичних ресурсів противника (озброєння, жива сила, інфраструктура і предмети постачання) (physical warfare). При цьому всі дії як своїх сил, так і сил противника він запропонував розглядати в рамках кібернетичний циклу, що має в своїй структурі 4 процеси: спостереження, орієнтація, рішення, дія, (цикл або "петля Бойда"), який сам відтворюється і саморегулюється (опубліковано в 1995 р. [14]). Надалі він був покладений в основу концепції командування і управління, а також можливостей пов'язаних з ними, під кодовою назвою RTO-TR-SAS-050, яка була введена в НАТО в 2007 році в Пентагоні як модель C2 (Command and Control, тобто командування і контроль) та згодом перетворилася в C4IR (Command Control Communication Computers Intelligence And Recognition – командування, контроль, комунікації, комп'ютери, розвідка, усвідомлення), а також в інші модифікації, наприклад C4IEWS & IM (Command, Control, Communications, Computers, Intelligence, Electronic Warfare, Sensors and Information Management –

командування, контроль, комунікації, комп'ютери, розвідка, електронна війна, сенсори і інформаційне управління). В 2003 році модифікований варіант "петлі Бойда" – "Критика-Дослідження-Порівняння-Адаптація" був запропонований Девідом Брайантоном [15].

Питання системного порушення управління та функціонування держави до кризового рівня були запропоновані та реалізовані під час підготовки операції "Буря в пустелі" в 1991 році Джоном Уорденом. Він розробив системний кібернетичний підхід до сучасних бойових дій, назвавши його «операції на основі ефектів» (EBO – Effect-based-Operations), який враховував розробки Дж. Бойда та став подальшим розвитком мережецентричних дій. 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 уразливості (які отримали назви: "центри тяжіння", "центри гравітації", "критичні вузли (точки)" тощо). Їх правильне виявлення та деструкція призводить до ефекту системного, стратегічного "паралічу" держави в тих чи інших сферах або в цілому.

Генерал Девід Дептула здійснив подальший розвиток поглядів Уордена та змісту війн 4GW. Він запропонував розгляд ворога як системи на всіх національних рівнях, включаючи дипломатичний, інформаційний та економічний і вважав, що невійськові дії є невід'ємною складовою нової теорії конфлікту. В рамках цього в США були створені спецгрупи (прообраз окремих елементів стратегічних комунікацій) для роботи в Іраку і Афганістані, куди входили соціологи, етнографи, лінгвісти та інші фахівці. Команди Human Terrain спілкувалися з місцевим населенням, впливали на його свідомість, досліджували його звички, поведінку, ієрархічну структуру, слабкі і сильні сторони тієї чи іншої соціальної, етнічної і релігійної групи тощо. В 2014 Девід Дептула разом з Джоном Алленом на конференції "Нова воєнна стратегія США для нової ери: перевага, швидкість і ефективність» презентував новий концепт: "DIMET" – операцій (DIMET: дипломатія, інформація, військова сила, економіка (включно фінанси) і технології), в якому ключовою складовою є високі технології [16].

Вперше системно-концептуальне викладення теорії мережецентричних війн з визначенням в ній ролі і місця інформаційних та інших високотехнологічних складових здійснили в публікації "Мережево-центрична війна: її походження і майбутнє" (січень 1998 р.) Артур Себровскі (тоді директор програми Пентагону N6 (Space, Information Warfare, Command and Control) і Джон Гарстка (тоді науковий і технічний радник Управління систем С4 Об'єднаного штабу).

З початку 2000 років в США в інтересах підвищення ефективності дій сил спеціальних операцій було впроваджено 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.

Всі основні теоретичні дослідження і практика ведення війн нового високотехнологічного типу яскраво демонструють, що запорукою перемоги в них є забезпечення досягнення інформаційної переваги над противником. При цьому інформаційна перевага передбачає створення надійних мереж, які об'єднують свої війська (сили) і засоби та надають їм змогу покращеного обміну інформацією, підвищуючи її якість та забезпечуючи своєчасну і повну загальну ситуаційну поінформованість 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 2003 році [1]. Разом з цим необхідно забезпечити випереджаюче знищення (виведення з ладу, придушення) системи розвідувально-інформаційного забезпечення та управління у противника (засобів та систем розвідки, мережоутворюючих вузлів, центрів обробки інформації та управління).

Як зазначив адмірал Вернер Кларк: "У майбутніх операціях будуть використовуватися революційні інформаційні технології і можливості розосереджених сил, об'єднаних єдиним інформаційним простором, для досягнення безпрецедентної наступальної могутності, гарантованої оборони і операбельності в складі об'єднаних з'єднань".

Таким чином, сучасні концепції передбачають організацію та ведення бойових дій за кібернетичними циклами в єдиному інформаційному просторі різнорідними силами і засобами в умовах відсутності безперервної лінії бойового зіткнення військ. Єдиний інформаційний простір надає можливість: застосовувати збройні формування у складі єдиної гнучкої просторово-розподіленої розвідувально-ударної системи; створення основи для комплексного застосування за єдиним замислом відповідно до визначеної мети і завдань наявних сил і засобів розвідки, вогневого (кінетичного) та невогневого (електронного тощо) ураження, роботизованої (безпілотної, безекіпажної) військової техніки шляхом їх модульного об'єднання для ведення узгоджених розвідувально-ударних (вогневих та невогневих) дій в реальному масштабі часу з утворенням відповідно до ситуації родових, міжродових, міжвидових і змішаних ситуаційних розвідувально-ударних комплексів (РУК) [17, 18].

Тому в багатьох країнах світу здійснюється перегляд теорії побудови і практики застосування,

як нових комплексів, так і існуючих зразків озброєння з урахуванням організації та ведення бойових дій у єдиному інформаційному та кібернетичному просторі [7, 11]. Вирішується питання, як досягти скорочення часу повного кібернетичного циклу бойового застосування комплексу озброєння для випередження противника у досягненні мети [8, 19].

Водночас провідні військові фахівці світу за останні роки все частіше відмічають як небезпечну тенденцію зростання певної невідповідності існуючих темпів розвитку органів управління оборонних структур і методів їх роботи, військ (сил), оновлення озброєння та військової техніки, організації військової освіти і науки, управління військами та зброєю реальним змінам, що відбуваються в розвитку високих оборонних технологій, теорії і практиці воєнного мистецтва [5, 6]. Так, попри постійне зростання протягом попередніх 25-30 років в провідних країнах світу кількості проектів створення нових та інноваційних зразків озброєння і військової техніки (ОВТ), бурхливий розвиток високих технологій нерідко призводив до того, що вони морально застарівали ще до прийняття на озброєння, часто не виправдовуючи величезні фінансові та матеріальні витрати на їх розробку та виробництво [8, 11, 17].

Ще одне питання, яке безпосередньо пов’язане зі зростанням високотехнологічності ОВТ та зміною форм, способів і характеру збройної боротьби – рівень професіоналізму та готовність до цього особового складу.

В провідних країнах світу (Республіка Польща, Федеративна Республіка Німеччина, Великобританія тощо) ефективність вирішення зазначених проблем досягається шляхом формування та забезпечення функціонування інтегрованих навчально-наукових, дослідно-випробувальних комплексів (високотехнологічних оборонних (кластерів)), які здійснюють на єдиній базі освітню і наукову діяльність за високотехнологічними напрямами. Наприклад, така інтеграція військової освіти і науки за високотехнологічними напрямами успішно реалізована у Військовому університеті технологій (Республіка Польща) де на одній базі зосереджені всі високотехнологічні напрями, спеціальності і спеціалізації підготовки (факультети: національної безпеки, будівництва, хімії, електроніки та телекомунікацій, енергетики, технічної фізики, геодезії і картографії, інформатики, інформатики в медицині, інженерії безпеки, інженерії матеріалів, криптології і кібербезпеки, логістики, авіації і космонавтики, механіки і машинобудування, мехатроніки, управління) [30]. Теж саме реалізовано в Університеті Бундесвера в Мюнхені (ФРН) (спеціальності: електротехніка та інформаційні технології, комп'ютерні науки, аерокосмічна інженерія, менеджмент інформаційних систем, математична інженерія, політологія та соціальні науки, розвиток людських ресурсів, медіа менеджмент, дослідження міжнародної безпеки, економіко-організаційні науки, інженерна справа та екологія, інженерна психологія, комп'ютерні технології та комунікаційні технології, машинобудування, комп'ютерна техніка, державне управління, оборонна інженерія) та в аналогічних навчальних закладах інших країн які входять до НАТО [31, 32]. За рахунок інтеграції високотехнологічних напрямів підготовки фахівців та наукових досліджень в єдиному навчальному закладі та на єдиній базі в провідних країнах світу забезпечують позбавлення їх дубляжу і розпорошення зусиль при вирішенні однотипних завдань, економію коштів на їх реалізацію, раціональне використання кадрового потенціалу, полігонної, матеріально-технічної бази, ефективне виконання замовлень на підготовку (перепідготовку) фахівців і здійснення наукових досліджень для усіх міністерств і відомств сектору безпеки та оборони держави. Такі комплекси активно взаємодіють з питань науки, інновацій та підготовки фахівців із промисловими підприємствами, військовими частинами, класичними університетами та науковими установами, що дає позитивний синергетичний ефект в оптимізації витрат, концентрації зусиль та підвищення ефективності кінцевого результату.

Забезпечення можливостей впровадження зазначених підходів у вітчизняну практику, як показує досвід провідних країн світу, потребує зосередження зусиль насамперед у галузі військової освіти, науки та підготовки військ за новими стандартами, відповідно до вимог майбутнього характеру воєнних дій, інших функцій та завдань Збройних Сил України. Як свого часу влучно зазначив Теодор фон Карман: “Наукові результати не можуть бути ефективно використані солдатами, які не розуміють їх, так само, як і науковці не можуть розробляти корисні винаходи для бойових дій, не розуміючи їх.”

Мета статті. На основі аналізу і дослідження сучасного стану і тенденцій розвитку високих і інформаційних технологій, змін які відбуваються в теорії воєнного мистецтва та практики війн (воєнних конфліктів) виявити проблемні питання впровадження інформаційних технологій в інтересах забезпечення національної безпеки і оборони та визначити раціональні шляхи їх вирішення.

Виклад основного матеріалу дослідження

Високотехнологічні війни і воєнні конфлікти. Кібер-, Інфо-, Когнітивні аспекти та особливості війн і воєнних конфліктів сучасності і майбутнього.

Провідні фахівці у галузі воєнного мистецтва зазначають, що досягнення мети в воєнних конфліктах сучасності і особливо майбутнього повною мірою залежить від розвитку в державі проривних та високих технологій і цілеспрямованого системного впровадження та використання їх продуктів в сфері національної безпеки і оборони.

В воєнних конфліктах сучасності

спостерігається стійка тенденція застосування їх учасниками як експериментальних так і серійних високотехнологічних зразків озброєння та військової техніки (які переважають за ефективністю існуючі зразки масового виробництва) та інноваційних технологій управління ними [6, 11]. При цьому, як правило, такі засоби, навіть при не масовому їх використанні, забезпечують вирішальний вплив на хід і результати конфлікту.

Це знайшло своє втілення при практичній реалізації елементів нових стратегічних концепцій: "глобальної бойової дії", "асиметричних бойових дій", "мережецентрічних війн", "стратегічного паралічу", "паралельних війн", "керованих війн", "гібридних війн", "когнітивної війни", "глобальної присутності", "глобального охоплення", "проксі війн", тощо.

Конвенційні дії у сучасних конфліктах ведуться, як правило, дистанційно із використанням високоточної, інформаційної, кібернетичної, електронної, енергетичної зброї (зброї спрямованої енергії), робототехнічних (безпілотних авіаційних та безекіпажних сухопутних і морських) комплексів та інших бойових засобів кінетичного та некінетичного впливу, які в рамках реалізації мережецентричних концепцій поєднуються системами оперативного (бойового) управління типу "С2-С5 Х…Х" (С2, С3, С4ISR тощо) в ситуаційні розвідувально-ударні комплекси.

Крім того, на цей час в результаті високотехнологічної та інформаційної діяльності людства додатково до природних: суходільного, морського повітряного та космічного, сформувався штучний п'ятий простір – кіберпростір (рис.1), (поняття вперше з'явилося в оповіданні "Burning Chrome" Вільяма Гібсона (1982 р.) та його романі "Neuromancer" (1984 р.)), який перетворився на окрему сферу боротьби між державами, включаючи збройне протиборство. Перше офіційне визначення кіберпростору було дано військовими експертами США в настанові КНШ 2006 року "Інформаційні операції": "Кіберпростір – сфера, в якій застосовуються різні радіоелектронні засоби (зв'язку, радіолокації, розвідки, навігації, автоматизації, управління і наведення), що використовують широкий діапазон електромагнітного спектра частот для прийому, передачі, обробки, зберігання, перетворення і обміну інформацією, і пов'язана з ними інформаційна інфраструктура ЗС США". За визначенням Чіпа Морнінгстара і Ф. Рендалла Фермера, кіберпростір визначається скоріше соціальними взаємодіями, а не його технічною реалізацією [11]. На їхню думку, обчислювальне середовище в кіберпросторі є доповненням каналу зв'язку між реальними людьми. Основною характеристикою кіберпростору є те, що він пропонує середовище, що складається з багатьох учасників, здатних впливати один на одного. Уряди провідних країн світу відносять взаємопов'язані інформаційні технології і взаємозалежну мережу інфраструктур інформаційних технологій кіберпростору до національної критичної інфраструктури.

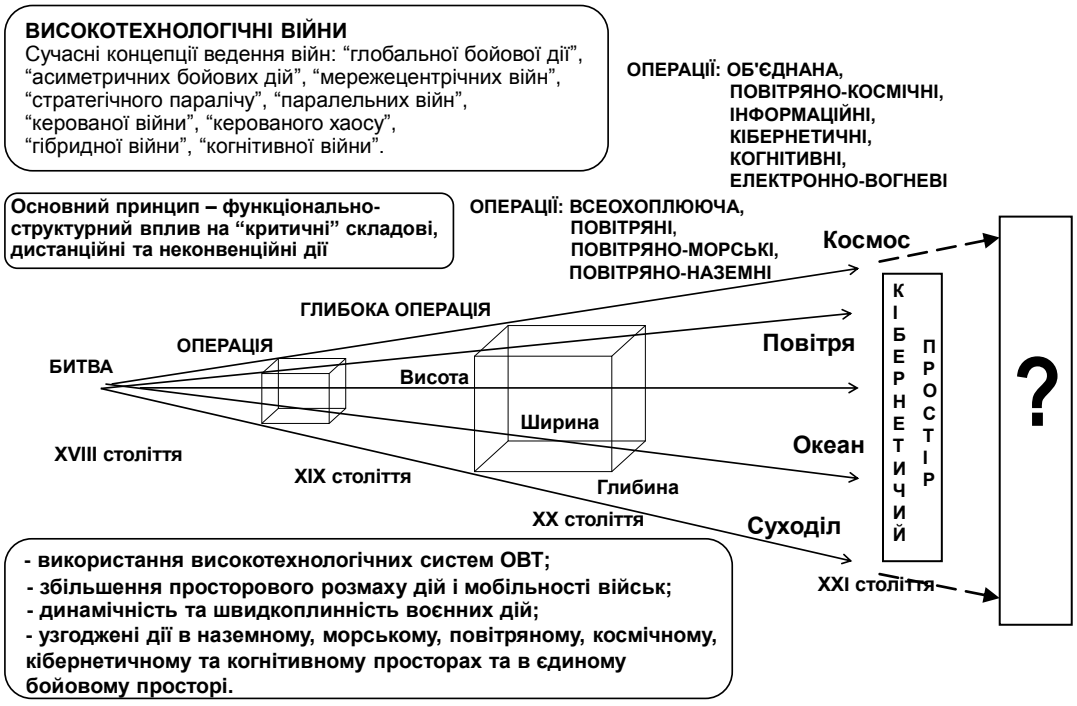

Рис. 1. Еволюція основних концепцій ведення війн

Нові вразливості національної критичної інфраструктури, які при цьому з'являються паралельно з бурхливим розвитком технологій, породжують нові небезпеки, загрози і ризики та необхідність вирішення питань їх запобігання, стримування та нейтралізації. Це привело до створення у провідних країнах світу систем кібербезпеки та кібероборони держави. Основною

тенденцією при їх формуванні стало поєднання в єдиній структурі, яка відповідає за кібероборону відповідно до мети, завдань, доцільних форм та способів забезпечення кібербезпеки у воєнній сфері різних напрямів діяльності (та відповідно, підрозділів, які її здійснюють) поєднаних відношенням до кіберпростору.

Так, в США в "National Defense Authorization Act" на 2018 рік для міністерства оборони США визначено завдання централізації керівництва всіма силами та засобами, які відповідають за кіберзахист, активні заходи дій в кіберпросторі та інші операції в комп'ютерних мережах, електромагнітному спектрі випромінювання, інформаційні та психологічні операції, дії в космічному просторі, відповідних технічних видів розвідки тощо.

Світовий досвід показує, що ефективне вирішення будь-якими військами задач за призначенням та забезпечення ними найбільш повного використання потенціалу ОВТ можливе лише за умови їх об'єднання в єдиній структурі (відповідно до простору де вони діють або ОВТ яке застосовують) та наявності раціональної системи управління від стратегічного до тактичного рівня. Як приклад – на початку XX століття масова поява авіації, танків та засобів протиповітряної оборони гостро поставила питання щодо створення відповідних структур та органів управління ними. Відомо, що до того, доки не були створені раціональні системи управління цими структурами, ефективність застосування зазначених сил та засобів була вкрай низькою.

Відповідно до цього принципу до складу Кіберкомандування США, остаточно сформованого у 2009 році, входять структури, які відповідають за: операції в комп'ютерних мережах, електромагнітному спектрі випромінювання, інформаційні та психологічні операції, організацію технічних видів розвідки, забезпечують зв'язок та криптографічний захист інформації, приймають участь у заходах введення в оману.

У відповідності до такої типової структури у 2016 році було створено Командування кібер-інформаційного простору ФРН. Нове командування має статус окремого виду збройних сил, в структурі якого об'єднані частини та підрозділи РЕР, РЕБ, інформаційно-психологічних операцій, інформаційно-технічного забезпечення (зв'язку) тощо. Аналогічним чином у теперішній час створюються кіберкомандування у багатьох країнах світу, а також Кіберкомандування НАТО.

В Україні це питання знаходиться у стадії вирішення. Відповідно до чинного законодавства підготовка держави до відбиття агресії у кіберпросторі (кібероборона) є одним із головних завдань, які покладаються на Міністерство оборони та Збройні Сили України. За виконання пов'язаних за змістом та простором завдань кібероборони на цей час відповідають різноманітні, різнопідпорядковані структурні підрозділи:

у Міністерстві оборони України: Головне управління розвідки; Департамент охорони державної таємниці; Управління інформаційних технологій;

у Генеральному штабі Збройних Сил України: Головне управління зв'язку та інформаційних систем; Центральне управління охорони державної таємниці та захисту інформації; Об'єднаний оперативний штаб; Головне оперативне управління.

З ухваленням у жовтні 2017 року Закону України "Про основні засади кібербезпеки України" на Міністерство оборони та Генеральний штаб Збройних Сил України покладено нове завдання щодо впровадження заходів із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану.

Зазначене вимагає формування такої системи кібербезпеки, яка забезпечить скоординоване управління всіма її складовими. Така система потребує наявності відповідного органу управління подібного за структурою завданнями і функціями до аналогічних органів країн-членів НАТО, призначеного для реалізації єдиної політики та стратегії дій Міністерства оборони України та Збройних Сил України в інформаційному та кіберпросторі; організації та координації заходів щодо кібербезпеки та захисту критичної інформаційної інфраструктури держави; управління силами кібербезпеки під час кризових ситуацій, в умовах особливого періоду та правового режиму воєнного стану.

Цей орган управління інформаційної та кібербезпеки повинен вирішувати такі основні задачі:

участь у формуванні та реалізації державної політики з питань кібербезпеки;

формування та реалізація політики Міністерства оборони України та Збройних Сил України щодо дій у кіберпросторі;

участь у виконанні заходів зі створення та розвитку інформаційних систем та ресурсів у Збройних Силах України;

координації дій суб'єктів кібербезпеки Міністерства оборони та Збройних Сил України;

участь у формуванні стандартів підготовки та держзамовлення на підготовку фахівців з кібербезпеки;

організації взаємодії та проведення заходів (в т.ч. щодо підготовки держави до кібероборони) зі структурними підрозділами інших центральних органів виконавчої влади та міжнародними партнерами з питань кібербезпеки;

підтримання взаємодії з системою інших відомчих команд реагування на комп'ютерні інциденти (CERT/CSIRT);

планування та узгоджене управління діяльністю суб'єктів у кіберпросторі за єдиним замислом і планом. Контроль та координація їх дій;

моніторинг та аналіз кіберінцидентів та ефективності дій системи кібербезпеки, виявлення уразливостей в інформаційних та кібер системах

своїх і противника.

З цією метою у складі органу управління інформаційної та кібербезпеки повинні бути підрозділи: моніторингу кіберпростору; захисту кіберпростору; активних дій у кіберпросторі та кібероперацій.

Наявність ефективної системи управління силами і засобами які діють в кіберпросторі забезпечить інформаційну, кібернетичну та когнітивну перевагу над противником та буде сприяти практичній реалізації прийнятої в країнах членах НАТО концепції "старт-оборони", ключовими елементами якої є високотехнологічна підготовка персоналу та збалансоване поєднання найбільш ефективних аспектів стратегій "жорсткої сили" та "м'якої сили", шляхом зваженого і узгодженого використання інструментарію стратегічних комунікацій, санкцій, переконання і застосування сили та інших впливів способом, який є найбільш рентабельним та має політичну і соціальну легітимність [20–22]. Особливістю стратегії "м'якої сили" є об'єднання трьох когнітивних компонентів: культури держави (у тому, чим вона цікавить інші держави), її політичних цінностей (чи дотримується вона їх у внутрішній і зовнішній політиці) та зовнішніх відносин (чи сприймаються вони як легітимні і морально обґрунтовані) [12, 23].

Завдяки використанню інноваційних технологій у конвенційній складовій сучасних війнах став можливим перехід від дій загальноруйнівного характеру до дій із перевагою функціонально-структурного впливу на супротивника, а найголовніше – досягнення над ним когнітивної переваги.

Проведені дослідження показали, що когнітивне протиборство стало невід'ємною складовою сучасних і майбутніх війн і воєнних конфліктів як міждержавних і внутрішньодержавних, так і між будь-якими геополітичними та регіональними акторами. Когнітивній складовій належить виняткова роль в сукупності факторів, що формують і викликають воєнний конфлікт, впливають на його хід та результат, інтенсивність і наслідки. Тому, сучасні війни, а особливо війни майбутнього ведуться за когнітивну сферу соціуму (суспільства, соціальних груп, людини, населення) і керування ним (нею).

Когнітивні впливи можуть бути навмисними і випадковими, комплексними і багатовекторними, загальної спрямованості або цільовими (цілеспрямованими), спрямованими на суспільство в цілому чи на конкретні спільноти або індивідів, на досягнення короткотривалого або довготривалого ефекту, негайно або після латентної фази, з варіацією значень або без і т. ін.

В сучасних умовах всі сторони конфлікту прагнуть взяти під контроль саме когнітивний простір, який охоплює сприйняття, усвідомлення, переконання, розуміння і цінності, інтелектуальне середовище, як індивідів, так і соціальних груп і суспільства в цілому, в якому власне і відбувається ухвалення ними рішень. Тому головний результат успішних когнітивних впливів – це зміна моделі світу та його сприйняття в людині, соціальних групах суспільства, та суспільстві в цілому, що забезпечує можливість взяття їх під контроль і здійснювати зовнішнє управління ними на емоційному, моральному, культурному, світоглядному і ментальному рівнях, з формуванням стійких стереотипів для сприйняття дійсності через їх призму. Особливе значення мають при цьому нав'язування та просування хибних наукових, суспільних, економічних, державних, військових теорій, парадигм, концепцій, стратегій, які найбільш ефективно просуваються та впроваджуються через заклади освіти та наукові установи. З цією метою використовуються всі можливості стратегічних комунікацій, ведуться інформаційні, психологічні, кібернетичні та інші дії (акції, операції тощо), які спрямовані як на безпосередніх учасників конфлікту, так і на населення країн, що беруть в ньому участь, міжнародне співтовариство. Особливістю є те, що навіть при проведенні державними акторами дій планово та узгоджено (що найчастіше це не виконується), вони проходять на тлі хаотичних цільових і випадкових впливів всіх інших акторів. Це трансформується в інформаційно-кібернетичний і когнітивний варіант війни "всіх проти всіх" (в кібернетичному та інформаційному просторах). У результаті, як показують проведені дослідження, об'єкти, на які спрямовані когнітивні дії можуть бути не просто введені в стан когнітивного резонансу або дисонансу, але і отримати інформаційні та когнітивні травми, дійти до когнітивної межі сприйняття (неможливості подальшого безпечного сприйняття когнітивних впливів), часткової або повної когнітивної дезорієнтації і навіть до когнітивного колапсу, з подальшим переходом у стан когнітивної агресії, депресії, розчарування у всьому і апатії.

Взагалі в сучасних конфліктах досягнення мети агресії здебільшого починається з несилових методів, головним чином економічних, політичних, дипломатичних, інформаційних (інформаційно-психологічних, кібернетичних).

Але, при цьому значну роль відіграють демонстраційні заходи військового попередження і стримування. Вони, найчастіше, виступають не просто демонстрацією сили, а в першу чергу спрямовані, на економічне і морально-психологічне виснаження противника, тощо. В цілому, у гібридних конфліктах будь-якої інтенсивності бойові дії (операції) є складовою взаємоузгоджених за єдиним замислом і планом інших (несилових) дій, які превалюють на всіх їх стадіях (зародження, ескалація інтенсифікація, затухання, залагодження). Цим створюються дестабілізуючі внутрішні і зовнішні процеси в державі, яка є об'єктом агресії (стурбованість і невдоволеність населення, міграція, акції громадської непокори тощо). Надалі для

досягнення стратегічних цілей застосовуються силові методи ведення дій з широкомасштабним залученням сил і засобів розвідки, оперативного управління військами (силами) і засобами, а також традиційних засобів ураження, державних збройних формувань, некомбатантів та інших учасників (терористів, радикальних озброєних груп, рухів опору, найманців, партизан), сил спеціальних операцій і т.п. Таким чином, гібридність сучасних конфліктів базується на можливостях які є похідною високотехнологічного розвитку людства його інформатизації та (на даному етапі) цифровізації. А сама гібридна війна є високотехнологічним конфліктом, продовженням політики держав (коаліцій, політичних угруповань, транснаціональних корпорацій тощо) з метою нав'язування опонентам своєї волі за допомогою комплексних адаптивних і асиметричних синхронізованих впливів на них у різних просторах та сферах (рис. 2) з поєднанням конвенційної і неконвенційної складових, забезпеченням багатовимірності, мультиплікативності та синергетичності результатів і високого рівня невизначеності для опонентів щодо кінцевих цілей і шляхів їх досягнення. Тобто, високотехнологічний розвиток людства став основою того, що як це так і подальші покоління війн є високотехнологічними.

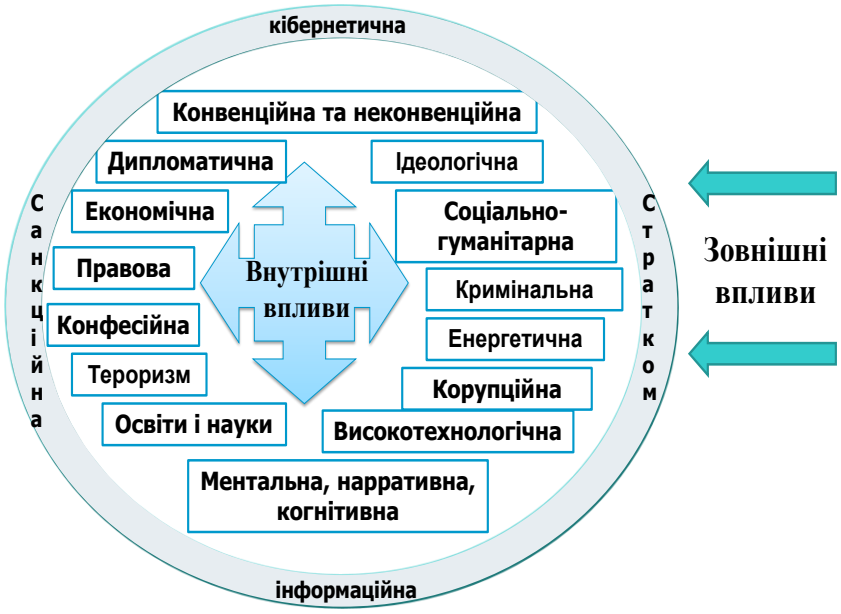

Рис. 2. Сфери гібрідних війн

Особливостями безпосередньо воєнної складової високотехнологічних війн є:

перехід від управління військами і зброєю до управління збройною боротьбою, в основі якого є кібернитично-циклічні концепції ведення дій та принцип – розвідка, прийняття рішення, ураження [11, 24];

формування та застосування в зонах (районах) де відбуваються конвенційні дії ситуаційних розвідувально-ударних комплексів, які на базі наявних систем і засобів управління і комунікацій поєднують в єдину систему наявні засоби розвідки та ураження;

виникнення єдиного бойового простору (простору ведення операцій) з новими характеристиками: нелінійність, відсутність у традиційному розумінні фронту, флангу, тилу, розподіленість одночасно з інтегрованістю та багатомірністю;

перенесення основного навантаження дій (збройної боротьби) в інформаційно-кібернетичний, когнітивний та повітряно-космічний простори;

інформаційні, психологічні, когнітивні, кібернетичні дії стають невід’ємною і превалюючою складовою воєнних дій;

доступність до всіх елементів бойового простору всіх учасників дій;

динамічність зміни просторових масштабів конфліктів, можливість швидкого їх переростання з локального на глобальний рівень з охопленням, як окремих регіонів, так всієї території держави;

зростання швидкості змін обстановки та загальної динаміки дій, маневреності дій військ (сил) на розрізнених напрямках та вимог до їх мобільності;

широкомасштабне, системне застосування високоточної керованої зброї, ефективної “нелетальної” зброї та зброї на нетрадиційних і нових фізичних принципах;

ведення бойових дій дистанційно;

роботизація засобів збройної боротьби, вивід людини з поля бою;

участь в конфлікті різнорідних сил та засобів об’єднаних в бойові модулі і системи;

створення на стратегічному рівні коаліцій, а на оперативному угруповань і на тактичному груп із заданими спроможностями і функціональністю

для ведення операцій з визначеною метою;

збільшення ролі і розширення масштабів застосування сил спеціальних операцій;

зростання кількості іррегулярних та приватних збройних формувань і їх впливу на хід і результати бойових дій;

ведення дій в зонах (районах) з високим ступенем урбанізації;

зростання асиметричності в характері бойових дій;

перехід до адаптивних форм і способів ведення воєнних дій [23].

Фізичною (технологічною) основою інформаційних технологій є результати розвитку і продукти інших високих технологій з якими вони нерозривно пов'язані. На цей час в світі існує біля 40 ключових макротехнологій, які за думкою провідних експертів визначають рівень економіки та обороноздатності країн в сучасних умовах.

До високих оборонних технологій та технологій подвійного призначення (англ. high technology, hi-tech) частіше за все відносять такі найбільш нові і прогресивні технології сучасності: штучний інтелект, космічні, робототехнічні, інформаційні та кібер технології; нано-, квантові, нейронні, біотехнології, генну інженерію, інноваційні електромеханіку, електроніку, матеріаловедення, створення нових напівпровідникових матеріалів, генерування, акумулювання та передача енергії, "чисті" (cleantech) та енергозберігаючі технології, телекомунікаційні технології та технології управління і автоматизації тощо.

Інформаційним технологіям в сфері оборони провідні країни світу приділяють першочергової та особливої уваги. При цьому, розвиток інформаційних технологій став рушієм таких тенденцій у воєнній справі:

1. Глобальної інформатизація військових формувань і створення високоінтегрованих систем управління, які є об'єктами кібернетичного впливу і розвитку відповідно до цього форм і способів ведення кібернетичного протиборства;

2. Зростанню інтенсивності конфліктів у інформаційному та кіберпросторі, за участі призначених і спеціально для цього створених спеціалізованих структур та формувань;

3. Переносу тероризму в площину інформатизації. У силу нерівномірного розвитку інформаційного простору та цифрової нерівності між різними країнами, яка формується, з одного боку та зростання уразливості при зростанні високотехнологічностів з іншого деякі держави, імовірно, або окремі терористичні угруповання можуть вдатись до будь-яких заходів для нейтралізації домінування більш розвинутих країн саме через інформаційний простір.

4. Використання світової мережі Інтернет та електронних засобів масового інформування для маніпулювання свідомістю як світової громади, так й населення окремої країни;

5. Виділення інформаційного забезпечення в самостійний вид стратегічного (оперативного) забезпечення бойових дій і формування відповідних військових структур для управління ним.

Слід зазначити, що збирання, обробка, передача і зберігання інформації здійснюється людством протягом всієї історії цивілізації. Але обсяги інформації яка продукується та потребує обробки постійно зростає. В 1983 році Е.Масуда опублікував результати досліджень, які показали, що на той час, обсяг існуючої в світі інформації, "самозростаючої, виробленої всіма і всіма інтегруємої", подвоювався кожні півтора року [25], зараз це декілька місяців. При цьому цінність інформації визначається її здатністю забезпечити суб'єкта необхідними умовами для досягнення ним поставленої мети.

Розглянемо, роль і місце інформації та інформаційних технологій у воєнній сфері в сучасних умовах, а також що є найбільш необхідним для забезпечення підвищення ефективності їх застосування в інтересах національної безпеки і оборони.

Поняття "інформація", як форма існування знання та його передачі увійшло у широкий обіг після розробки та публікації Клодом Шенноном математичної теорії інформації (1948). Теорія інформації разом із теорією керування Норберта Вінера (1948), стали основою нової галузі науки, що отримала назву "кібернетика" (наука про загальні закономірності отримання, зберігання, перетворення і передачі інформації в складних керуючих системах, будь то машини, живі організми або суспільство). У цій праці Вінер узагальнив закономірності, що відносяться до систем керування різної природи – біологічних, технічних, соціальних. Питання керування в соціальних системах були більш докладно розглянуті ним у книзі "Кібернетика й суспільство", опублікованій у 1954 році.

Стаффорд Бир назвав кібернетику наукою ефективної організації, а Гордон Паск розширив визначення, включивши в нього потоки інформації "з будь-яких джерел", починаючи від зірок і закінчуючи мозком. Вона фокусує увагу на тому, як дещо (цифрове, механічне, біологічне, або їх комбінації) для досягнення певної мети керування одержує (добуває у відповідності з отриманими завданнями), обробляє інформацію, реагує на неї й змінюється або може бути зміненим для того, щоб краще виконувати перші два завдання.

Всі чисельні визначення поняття "кібернетика" зводяться до того, що кібернетика – це наука, яка вивчає загальні закономірності будови складних систем керування й протікання в них процесів управління. А у зв'язку із тим, що будь-які процеси управління пов'язані із прийняттям рішень на основі отриманої та опрацьованої інформації, то кібернетику часто визначають ще й як науку про загальні закони одержання, зберігання, передачі й перетворення інформації в складних керуючих системах і управління технічними, біологічними й соціальними

системами. Тому виділяють такі галузі кібернетики, як технічну, біологічну, соціальну, політичну, економічну тощо. Кібернетика вводить таке поняття, як кібернетична система (КС). КС розглядаються незалежно від їхньої матеріальної природи. Прикладами КС можуть бути – автоматичні регулятори в техніці, комп'ютер, людський мозок, біологічні популяції, людське суспільство тощо. Кожна така система являє собою безліч взаємозалежних об'єктів (елементів системи), здатних сприймати, запам'ятовувати й переробляти інформацію, а також обмінюватися нею в інтересах управління.

Одночасно з потужним розвитком загальної кібернетики ця наука стала визначною системно-інтегруючою складовою у сфері воєнного мистецтва. Згідно з воєнними енциклопедичними виданнями кібернетика військова (КВ) є напрямом кібернетики, що вивчає закономірності створення і використання КС військового призначення, виробляє практичні рекомендації з управління військами та озброєнням і є основою автоматизації управління військами і засобами (зброєю). КВ розвивається на базі досягнень загальної кібернетики та воєнної науки. Вона розробляє для органів управління основні положення єдиної теорії управління збройними силами, військами та озброєнням, в тому числі з використанням автоматизованих систем управління (АСУ), включаючи передачу, зберігання, обробку, відображення, документування і використання даних обстановки (інформації) для її оцінки, вироблення рішення, постановки завдань (прямий зв'язок), отримання інформації про виконання завдань, стан, положення, характер дій своїх військ і військ противника (зворотній зв'язок). Основна мета КВ – максимальне підвищення оперативних (бойових) можливостей військ (сил), бойових засобів і ефективності їх бойового застосування [26].

Таким чином, інформаційні технології будучі по суті самостійним відгалуженням науки одночасно є ключовою складовою кібернетики.

Термін "інформаційні технології" в його сучасному розумінні вперше з'явився в статті Гарольда Дж. Лівітта і Томаса Л. Уіслера опублікованій в 1958 року в Harvard Business Review [8]. Слід зазначити, що ґрунтуючись на використовувані технології зберігання і обробки інформації, дослідники виділяють чотири етапи розвитку інформаційних технологій: попередні механічні (3000 до н. Е. – 1450 н. Е.), механічні (1450-1840), електромеханічні (1840-1940) і електронні (1940) – теперішній час).

У традиційному розумінні технологія – послідовність дій при перетворенні матеріалів, енергії та інформації. Техніка при цьому виступає як інструментальна база реалізації технології.

Виходячи із розглянутого інформаційні технології можна визначити, як послідовність дій, методів, способів, а також засобів (електронні та інші прилади, комп'ютери, програмне забезпечення, інфокомунікаційні мережі тощо) для реалізації процесів пошуку, збору, передачі, обробки, отримання, генерування (створення), накопичення, зберігання, обміну, поширення і захисту інформації та формування інформаційних ресурсів (сукупність даних, які мають цінність в конкретних обставинах).

Мета інформаційної технології – отримання та виробництво інформації (інформаційних ресурсів, даних) для прийняття на основі її аналізу управлінських рішень та раціонального виконання дій.

На II Міжнародному конгресі ЮНЕСКО "Освіта та інформатика" до "інформаційних" були віднесені наступні технології:

введення/виведення, збору, зберігання, передачі та обробки даних;

підготовки текстових і графічних документів, технічної документації;

інтеграції та колективного використання різнорідних інформаційних ресурсів;

захисту інформації;

програмування, проектування, моделювання, навчання, діагностики, управління (об'єктами, процесами, системами).

Галузь інформаційних технологій займається створенням, розвитком і експлуатацією інформаційних систем. Інформаційні технології в сфері оборони, ґрунтуючись і раціонально використовуючи сучасні досягнення в області комп'ютерної техніки та інших високих технологій, новітніх засобів комунікації, програмного забезпечення і практичного досвіду, забезпечують вирішення завдань щодо ефективної організації інформаційних процесів, здійснення аналітичної підтримки, контролю та управління в умовах динамічного зростання мобільності, невизначеності і потреби в синхронізації процесів командування і взаємодії всіх бойових елементів і учасників дій для зниження витрат часу, зусиль, енергії і матеріальних ресурсів.

Аналіз етапів впровадження інформаційних технологій в збройну боротьбу, за досвідом провідних країн світу, свідчить про постійне зростання впливу інформаційного фактору на хід і результат воєнних дій. Встановлено, що характерними, в цьому сенсі, рисами сьогодення і тенденціями розвитку збройної боротьби є:

1. Постійне зростання кількості засобів обчислювальної техніки, що задіяна на етапах планування операцій і під час прийняття управлінських рішень у ході бойових дій. Зростання ролі імітаційного моделювання при плануванні операцій і в процесі ведення бойових дій. Подальша інтеграція засобів штучного інтелекту в системи воєнного призначення;

2. Мініатюризація обчислювальних систем, їх використання практично у всі зразках озброєння та бойової техніки (в перспективі – особистої зброї та спорядження);

3. Поступова інтеграція на основі глобальних інформаційних технологій систем розвідки та

управління в єдиний контур, що охоплює угруповання від підрозділу (одиниці бойової техніки) до командування всіх ланок управління;

4. Подальший розвиток та інтелектуалізація зразків, так званої, "керованої" зброї – якісно нових зразків високоточної зброї, заснованої на використанні інформаційних технологій, яка в сполученні з системами розвідки, управління та ураження за "модульним" принципом дозволяє знищити будь-який об'єкт у будь-якій точці планети. В перспективі такі засоби будуть відігравати провідну роль у збройній боротьбі [8].

В сучасних умовах інформаційні технології в сфері безпеки і оборони мають різні рівні та напрями застосування:

1) електронно-інформаційні, керуючі та виконавчі складові у зразках озброєння та військової техніки, як їх елементи;

2) у системах управління зброєю;

3) як зброя;

4) у системах військового управління всіх рівнів (як в автоматизованих системах управління так і для побудови єдиного інформаційного простору, надання вчасної, доступної, надійної, безпечної та доречної інформації тим хто планує, готує, забезпечує бойові дії, автоматизації інтерпретації сцен для розуміння ситуації на полі бою, а також для обробки, осмислення, розуміння та аналізу даних, підтримки у прийнятті рішень суб'єктів військового управління, для удосконалення розробки, планування, дослідження та аналізу форм та способів застосування військ (сил), воєнних концепцій, стратегій, доктрин);

5) у сфері військової освіти, науки, моделювання та підготовки військ.

Військове керівництво армій розвинутих країн світу у відповідності до нових підходів до будівництва збройних сил особливу увагу приділяє розвитку систем військового управління (СВУ) як головного фактора у досягненні воєнно-стратегічної переваги.

При цьому, при удосконаленні СВУ спостерігається таке:

1. Глобалізація СВУ. Відповідно до системно-інтегрованого підходу до форм, способів і методів ведення збройної боротьби на перший план виходить необхідність забезпечення оперативно-технологічних можливостей для організації та підтримання стійкої взаємодії і спільного бойового застосування різнорідних сил і засобів у спільних операціях. Процес інтеграції, що відбувається за багатьма напрямками, повинен забезпечувати як об'єднання в рамках єдиної інформаційно-управляючої структури збройних сил усе більшої кількості функцій і можливостей систем управління, зв'язку, розвідки різного рівня і призначення, так і забезпечення умов для їх сумісного використання.

2. Ретельне планування операцій з використанням моделювання. Зростання динамізму воєнних дій та ускладнення спеціального математичного і програмного забезпечення інформаційних систем органів управління всіх рівнів. Спостерігається подальше зростання обсягів і ваги імітаційного моделювання при плануванні операцій (бойових дій), при прийнятті управлінських рішень та у ході бойової підготовки особового складу. Кількість комп'ютерів, що задіяні в процесі моделювання, постійно зростає. Зростає також кількість варіантів розвитку подій у конфлікті, що можуть бути промодельовані. Завдяки розвитку технологій розподілених (в тому числі, мережних) обчислень, інноваційних засобів телекомунікації, в тому числі космічного базування, географічний фактор розташування інформаційно-керуючих систем перестає мати значення.

3. Зростання значення інформаційного фактору та необхідність захисту інформаційного середовища систем управління структур, що забезпечують безпеку та оборону держави. У сучасних умовах інформаційна інфраструктура держави набуває статусу критичної (життєво важливої для існування) з усіма від цього похідними: вона стає об'єктом першого удару і потребує для свого захисту збалансованої державної політики в інформаційному просторі. До критичної інформаційної інфраструктури належать, в першу чергу, інформаційні системи в сферах економіки, транспорту, енергетики, фінансової системи, систем управління структур, що забезпечують безпеку та оборону держави тощо. СВУ, канали зв'язку, системи навігації, розвідки, системи наведення зброї та інші елементи інформаційного середовища також потребують захисту від відповідних інформаційних, кібернетичних та електронних впливів.

Аналіз програм розвитку систем озброєння та систем управління озброєнням, що реалізуються в арміях розвинутих країн світу, дозволяє визначити такі основні тенденції [34]:

1. обов'язкове оснащення систем озброєння різного призначення потужними бортовими обчислювальними та телекомунікаційними системами з метою забезпечення формування інформаційної моделі обстановки, автоматизованого (автоматичного) наведення та управління зброєю в динаміці бою;

2. створення бойових платформ різного призначення за функціональним принципом на основі сумісності інформаційно-керуючих систем зразків озброєння для виконання задач, що виникають у ході бою;

3. інтеграція окремих інформаційних ресурсів інформаційно-керуючих систем зразків озброєння в інформаційний ресурс загальної інформаційно-керуючої системи озброєнням в районі конфлікту з метою сінергетичного об'єднання можливостей різнорідних засобів для виконання широкого кола завдань у бою та операції. Прикладами програм для реалізації зазначеного є:

1. FCS (BCT) – Future Combat Systems (Brigade Combat Team) (США).

2. FRES – Future Rapid Effects Systems (Велика

Британія).

3. SEP – Splitterskydded Enhets Platform (Швеція).

4. BOA – Bulle Operationnelle Aeroterrestre (Франція).

В сучасній збройній боротьбі найбільш важливим для досягнення переваги над противником є забезпечення синхронізованого виконання типового кібернетично-інформаційного циклу, який є практичною реалізацією кібернитично-циклічних концепцій ведення дій.

Перш за все, відповідно до цілей які визначені і поставлених завдань, які необхідно вирішувати здійснюються дії щодо організації та реалізації збору інформації про противника, свої сили, засоби, можливості, про місцевість (її геофізичні та інші характеристики, інфраструктуру, населення тощо). З цією метою використовуються загальні інформаційні ресурси, всі наявні бази даних, ресурси геоінформаційних систем, інформація від всіх наявних в зоні (районі) технічних засобів розвідки та інших джерел розвідувальних даних.

По-друге, здійснюється комплексна обробка у реальному масштабі часу, систематизація та всебічний аналіз інформації оцінки поточної обстановки та прогнозування на основі висновків із аналізу та результатів розрахунків і моделювання можливого характеру дій противника та розвитку ситуації.

По-третє, в інтересах підтримки прийняття рішення щодо дій для досягнення поставлених цілей виявляються найважливіші об'єкти противника та їх "критичні" складові, порушення функціонування або знищення яких позбавляє його здатності чи сенсу подальшого ведення дій та визначаються засоби для найбільш ефективного їх кінетичного (некінетичного) ураження (подавлення), розробляється декілька їх варіантів з оцінкою загроз, ризиків і переваг кожного з них, а також визначення раціонального складу угруповань військ (сил) і засобів та їх всебічного забезпечення для ефективного застосування з цією метою у різних умовах обстановки.

По-четверте, безпосереднє оперативне управління та всебічна інформаційна підтримка дій військ (сил) для забезпечення ефективності їх застосування, підвищення якості взаємодії різнорідних сил, підвищення ступеня узгодженості та цілеспрямованості їх дій.

По-п'яте, розвідувально-інформаційне супроводження дій в реальному масштабі часу, для визначення їх ефективності адаптивного реагування на зміни в обстановці (зворотній зв'язок).

Практична реалізація зазначеного типового кібернетично-інформаційного циклу може здійснюватися спеціалізованим ситуаційним центром (комплексом оперативного управління силами і засобами), який забезпечує організаційне і технічне об'єднання на час ведення дій в визначеній зоні (районі) розосереджених у просторі різнорідних засобів розвідки, наведення і ураження, військ (підрозділів) у ситуаційний розвідувально-ударний комплекс.

Необхідною умовою функціонування ситуаційного РУК є знаходження його складових в єдиному інформаційному просторі визначеної зони (району) який синтезується спеціалізованим ситуаційним центром. Спеціалізований ситуаційний центр здійснює гєоінформаційне та навігаційно-часове забезпечення, формування з наявних у визначеній зоні (районі) інфокомунікаційних засобів єдиної інформаційно-комунікаційної мережі, збір та обробку інформації, підтримку прийняття рішень, видачу цілевказівок, команд, синхронізацію та безпосереднє управління діями наявних сил та засобів.

Таким чином, інформаційні технології є основою для ефективного управління військами (силами) та засобами, збільшення ефективності їх застосування та отримання нових можливостей озброєння та військової техніки.

Проте ефективність сучасних систем військового управління та застосування військ (сил) оснащених сучасними високотехнологічними засобами ОВТ, в найбільшому ступені залежить від якості підготовки особового складу та потребує відповідного удосконалення системи військової освіти і науки.

Шляхи вирішення проблеми організації наукових досліджень та підготовки фахівців із застосування високотехнологічних систем (комплексів, засобів) в інтересах національної безпеки та оборони.

Останнім часом підвищена увага до проблем військової освіти і науки спостерігається майже у всіх провідних країнах світу. Це обумовлено зниженням рівня професійної підготовки випускників військових закладів вищої освіти і, насамперед, у сфері отримання практичних навичок ефективної діяльності під час впровадження та застосування інноваційних оборонних технологій, про що свідчить практика діяльності вищих органів управління оборонних структур, повсякденної та бойової діяльності військ у більшості країн

Експлуатація дорогих високотехнологічних зразків та комплексів ОВТ особовим складом, який не має необхідної підготовки, не дозволяє ефективно їх застосовувати (повністю реалізовувати їх можливості). При цьому, дуже часто у зв'язку з непрофесійним застосуванням такі комплекси (засоби) виходять з ладу. Тобто завдання не виконуються, а держава несе значні збитки.

Тому серед загроз своїй національній безпеці у воєнній сфері багато країн уже зараз вбачають не тільки відставання в розробленні та прийнятті на озброєння нових високотехнологічних засобів озброєння і військової техніки. Ще більшою мірою це стосується якості підготовки військових кадрів, які повинні на високому рівні виконувати завдання з управління військами (силами) і засобами та забезпечити їх раціональне застосування у війнах і збройних конфліктах сьогодення та майбутнього.

Аналіз розвитку воєнної науки і військової освіти на основі історико-хронологічного підходу з точки зору визначення напрямів їх трансформації яскраво демонструє безперспективність і згубність підготовки до війн минулого та ігнорування тенденцій еволюції воєнної справи. Основною тенденцією в цій сфері завжди була орієнтація на інноваційні досягнення та забезпечення готовності до творчого використання їх можливостей.

На підставі визначених в Стратегічному оборонному бюлетені [27] пріоритетних напрямів розвитку Збройних Сил України з урахуванням досвіду бойових дій на Сході України та кращих світових практик у зв'язку з відсутністю раціональної, чітко структурованої системи підготовки військових кадрів за високотехнологічними напрямами від тактичного до стратегічного рівня доцільно реалізувати варіант подібний до кращих практик країн членів НАТО.

Відповідно світовому досвіду основні зусилля на тактичному рівні підготовки фахівців за високотехнологічними напрямами необхідно зосередити на інтеграції наукового, науково-педагогічного та матеріально-технічного потенціалів на єдиній базі, шляхом формування об'єднаного військового закладу вищої освіти для комплексного проведення наукових досліджень та підготовки фахівців за високотехнологічними напрямами, спеціальностями, спеціалізаціями. А саме: інформаційної та кібернетичної безпеки, технічних видів розвідки, радіоелектронної боротьби, захисту інформації, криптології та криптоаналізу, космічних систем забезпечення, автоматизованої обробки розвідувальної інформації, інформаційно-аналітичної роботи, інформаційно-психологічної протидії, автоматизованих систем управління, систем оперативного управління силами та засобами, інформаційно-комунікаційних систем, геоінформаційних систем, експлуатації та застосування робототехнічних (безпілотних, безекіпажних) систем (комплексів) і комплексів боротьби з ними, спеціальної метрології, енергетики, сил спеціальних операцій, квантово-оптичних систем, впровадження квантових і нанотехнологій у військовій сфері, зброї, побудованої на нетрадиційних і новітніх принципах тощо [28].

Це дозволить:

запобігти дублювання функцій різними структурами;

забезпечити раціональне використання фінансів, кадрових та інших ресурсів;

підвищити якість підготовки фахівців з високотехнологічних напрямків для всіх видів збройних сил і інших центральних органів виконавчої влади національного сектора безпеки і оборони держави;

суттєво підвищити ефективність здійснення досліджень, розробки, створення, випробування і застосування інноваційних високотехнологічних систем (зразків) ОВТ;

З цією метою, відповідно досвіду провідних країн світу він в своєму складі повинен мати:

потужну систему воєнно-наукових досліджень з науково-організаційною структурою;

освітню складову за високотехнологічними напрямами;

навчально-наукову, дослідницьку та випробувальну бази (науково-випробувальний комплекс високих оборонних технологій) зі стаціонарними та мобільними зразками озброєння і військової техніки, командними пунктами та лабораторіями;

експериментально-бойові та бойові підрозділи за високотехнологічними напрямами, які забезпечують їх становлення і розвиток, із супроводом навчально-наукової складової (рис. 3).

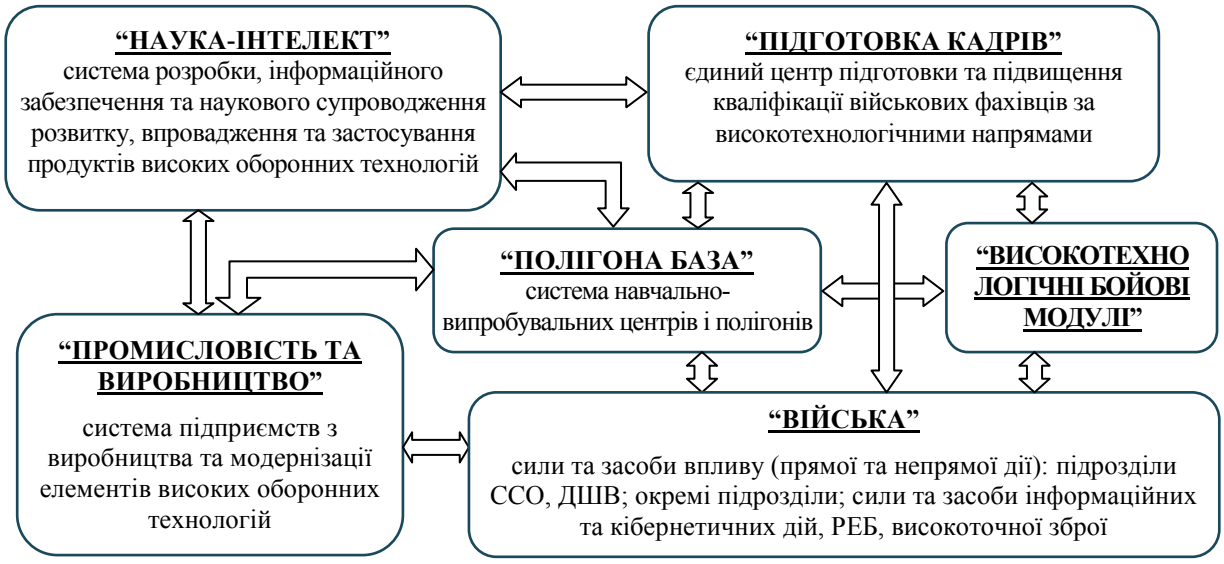

Рис. 3. Система підготовки військових фахівців та наукових досліджень за високотехнологічними напрямами

Науково-випробувальний комплекс високих оборонних технологій в першу чергу має концентрувати свою діяльність на дослідженні:

концепцій, стратегій, проблем і особливостей гібридних війн, технологій їх ведення, своєчасного виявлення гібридних впливів у всіх сферах і протидії їм, а також подолання їх наслідків;

проблем превентивної оборони, як виду стратегічних дій в сучасних умовах [33];

проблем виявлення деструктивних інформаційно-психологічних впливів на військовослужбовців і цивільне населення та протидії їм;

методів підвищення психофізичної стійкості та психологічної готовності військовослужбовців до виконання бойових завдань в умовах гібридної війни;

проблем забезпечення інформаційної (інформаційно-психологічної та кібернетичної) безпеки держави з урахуванням особливостей гібридних війн;

проблем формування та розвитку стратегічних комунікацій;

проблем розвитку та застосування технічних систем розвідки;

проблем розробки і застосування засобів радіоелектронного придушення та ведення радіоелектронної боротьби;

проблем створення та бойового застосування систем оперативного управління силами і засобами та автоматизованих систем управління зброєю;

проблем формування, підготовки та застосування сил спеціальних операцій;

проблем розвитку та застосування когнітивних технологій і нанотехнологій в інтересах оборони;

проблем застосування космічних систем в інтересах оборони;

проблем створення захищених безпілотних авіаційних комплексів та їх бойового застосування;

проблем боротьби з безпілотними літальними апаратами (дронами) [29];

проблем організації та проведення наукових досліджень, випробувань в сфері високих оборонних технологій і підготовки висококваліфікованих військових фахівців для цієї сфери.

Підготовка фахівців оперативно-тактичного рівня за зазначеними високотехнологічними напрямами, спеціальностями, спеціалізаціями повинна здійснюватися в відповідному спеціалізованому структурному підрозділі Національного університету оборони України.

При цьому всі офіцери які отримують освіту оперативно-тактичного та оперативно-стратегічного рівня незалежно від напрямів, спеціальностей, спеціалізацій підготовки повинні набути компетенції та володіти знаннями щодо:

високих та інформаційних технологій і їх застосування в сфері оборони;

інформаційно-аналітичної діяльності в сфері оборони (яка відіграє визначальну роль в арміях країн-членів НАТО);

організації застосування автоматизованих систем управління військами (силами) (АСУВ (с)) та систем типу С4ISR;

організації та застосування технічних систем моніторингу операційного (бойового) простору в інтересах військ (сил);

застосування сучасних геоінформаційних технологій та систем в інтересах військ (сил);

скритого управління військами та комплексної протидії технічним розвідкам;

основ інформаційної безпеки держави у воєнній сфері та захисту інформації;

основ кібернетичної безпеки та кібероборони у воєнній сфері.

стратегічних комунікацій в сфері оборони.

Особливості створення системи для розвитку передових високотехнологічних розробок для безпеки і оборони.

Окремої уваги потребує вирішення питання організації та здійснення наукових досліджень за високотехнологічними напрямами.

Дослідження показали, що основними факторами, які впливають на розвиток і впровадження високотехнологічних розробок в інтересах національної безпеки і оборони в Україні є:

відсутність незалежної, дієвої та ефективної системи пошуку, аналізу та всебічної експертної оцінки можливості реалізації та ефекту від впровадження перспективних, передових, проривних ідей і високотехнологічних проектів, та їх впливу на забезпечення обороноздатності;

відсутність або/та неузгодженість, незакінченість, безсистемність ряду законодавчих та нормативно-правових актів, доктрин, концепцій, програм щодо гармонізації розвитку фундаментальної і прикладної науки та передових розробок для безпеки і оборони;

відсутність єдиного державного органу (у тому числі з функціями управління і контролю), відповідального за формування та реалізацію політики пошуку, здійснення відбору, фінансування та реалізації розробок в сфері високих та проривних інноваційних технологій для забезпечення обороноздатності держави;

катастрофічне зниження спроможності наукових шкіл, технологічності виробничих підприємств, відставання вітчизняної науки та промисловості в практичних і технологічних аспектах розробки і впровадження високотехнологічних проектів;

розпорошеність зусиль, повноважень, ресурсів (економічних, технічних, часових) та наукового і науково-педагогічного потенціалу за територіальним розміщенням і цільовим призначенням;

системне недофінансування фундаментальної науки, проектів в сфері високих та проривних інноваційних технологій, глибока комерціалізація оборонно-промислового комплексу, недостатній розвиток державно-приватного партнерства.

Таке становище в сфері розвитку високих та проривних інноваційних технологій в Україні в

сучасних умовах вимагає створення системи пошуку, здійснення відбору та реалізації тих розробок, які за умови їх реалізації здатні забезпечити стратегічні переваги в сфері безпеки і оборони держави на основі принципово інноваційних рішень.

Таку систему доцільно створити дворівневою.

І рівень: Національне (державне) агентство передових розробок для безпеки і оборони (прим.: назва умовна) (аналог DARPA (DARPA – Defense Advanced Research Projects Agency – агентство передових оборонних дослідницьких проектів США)), яке повинно мати статус спеціально уповноваженого державного органу, відповідального за визначення політики розвитку, супроводження розробки високотехнологічних систем озброєння і військової техніки для забезпечення обороноздатності держави. Воно має бути підпорядкованим Уряду (профільному віце-прем'єру; Міністру оборони, якщо будуть переглянуті його повноваження) та підзвітним РНБО. Основний напрямок його діяльності – займатися проектами в критичних високотехнологічних сферах та галузях які, за умови їх реалізації надають державі стратегічні переваги.

З цією метою агентство повинно здійснювати:

пошук, аналіз і оцінку ідей, проектів;

всебічну оцінку спроможностей держави (технологічних, економічних, фінансових, політичних, безпекових) для їх реалізації;

всебічну оцінку ризиків та загроз проекту (фінансових, політичних, безпекових, технологічних);

оцінку (прогноз) ефекту (впливу) від впровадження результатів проекту (політичного, економічного, воєнного, інформаційного);

здійснення функцій державної експертизи розробок з питань таємниць;

підготовку висновків та рекомендацій щодо подальшої розробки проекту;

формування вимог і завдань центрам компетенції (ІІ рівня), координація їх діяльності і контроль реалізації проектів;

формування спроможностей і сприяння державно-приватному та міжнародному партнерству (у разі можливості та доцільності);

відбір та ліцензування експертів.

Має складатися з керівництва Агентства, керівників проектів (за напрямами), державних експертів (за кластерами і напрямками), підрозділів, що забезпечують діяльність.

ІІ рівень: система Центрів компетенції за профільними напрямками. Може складатися з відповідних підрозділів організацій, установ, закладів вищої освіти, ВВНЗ, НАНУ, НЦ, НДІ, НДЛ, КБ, за необхідності з дослідним виробництвом або лабораторіями, які забезпечують можливість практичної оцінки і перевірки розробок і пропозицій. Кожен центр відповідає за свої напрями, які іншими центрами не дублюються.

Основні завдання Центрів компетенції:

моніторинг знань в т.ч. спецінформації у визначеній предметній галузі;

формування, утримання і оновлення науково-технічної бази інформаційного ресурсу за кластерами та напрямками в т.ч. страхового фонду документації;

збір, систематизація, поширення й примноження знань та ефективних практик за напрямами, забезпечення ефективного доступу до експертного інформаційного ресурсу;

підтримка формування та розвитку наукових шкіл;

розробка відповідних стандартів і впровадженням отриманого досвіду;

поглиблення рівня підготовки та розвиток науковців та висококваліфікованих інженерів-дослідників;

оптимізація та концентрація на єдиній базі наукового, конструкторського, технологічного та виробничого потенціалу, фінансових, та інтелектуальних ресурсів;

супроводження та координація науково-виробничої діяльності через інститут генеральних (головних) конструкторів;

виготовлення і дослідження макетів, дослідних зразків.

Додаткові обов'язкові вимоги (умови). Повинна бути сформованою дієва система контролю і відповідальності. Всі безпосередньо пов'язані з прийняттям рішень керівники і виконавці юридичних осіб в складі яких створені центри компетенції мають нести відповідальність за результати роботи згідно із законом (дисциплінарну, адміністративну, кримінальну, матеріальну). Державні експерти – за висновки, керівники проекту – за рішення, і т.ін.

Висновки й перспективи подальших досліджень

Практика збройних конфліктів останніх десятиліть не без підстав свідчить, що в сучасній війні перемагає той, хто швидше сприймає нові технології та втілює їх у життя, бере на озброєння нові воєнні доктрини і концепції, які відповідають духу часу, і, врешті-решт, у кого командири не тільки самі використовують нові технології та ідеї, а й добре знають, які з них і коли може використовувати противник.

Новітні інформаційні технології сьогодні перетворюються в системоутворюючий фактор сучасної збройної боротьби. Завдяки їх використанню суттєво зростає кількість можливих сценаріїв розв'язування і ведення збройних конфліктів, забезпечується детальне планування і прогнозування їх наслідків у всіх галузях (політичній, економічній, воєнній тощо). Вони дозволяють досягнути якісно нового етапу розвитку воєнного мистецтва – переходу від управління військами в ході збройного конфлікту до управління конфліктом у цілому.

Військові фахівці розвинутих країн світу наполегливо працюють над розробленням та впровадженням нових концепцій ведення операцій.

Застосування сучасних інформаційних технологій дозволяє суттєво поширити можливості з розроблення таких концепцій.

Серед концепцій, що засновані на застосуванні "жорсткої сили", найбільш показовими є так звані "мережецентричні концепції ведення бойових дій", що розроблена американськими фахівцями, та "концепція інтегрованого бойового простору", що запропонована військовими фахівцями Великої Британії.

Взагалі, інтеграція інформаційних та телекомунікаційних ресурсів угрупування військ в районі конфлікту в єдиний інформаційний простір забезпечує можливість адаптивного реагування на ситуації шляхом корегування рішень фактично у реальному часі та є базовою основою практичної реалізації мережецентричної концепції ведення бойових дій. Своєчасно отримані від різних джерел та якісно проаналізовані дані розвідки забезпечують маневрування військ (частин, підрозділів), їх всебічне забезпечення та оперативне адаптивне управління їх діями відповідно обстановці.

Високий ступінь інтегрованості та сінергії дій сил та засобів, який досягається за рахунок створення єдиного інформаційного простору угрупування військ в районі конфлікту значно підвищує ефективність їх застосування.

Зростання високотехнологічності воєнних конфліктів, ролі систем оперативного управління військами та засобами і охоплення ними всіх рівнів управління, підвищує вразливість сектору безпеки і оборони держави від деструктивних інформаційних та кібер- дій противника.

На сьогоднішній день кіберпростір перетворився на окрему сферу боротьби, де постійно відбуваються різнопланові інциденти. Відповідно до мети, завдань, форм та способів забезпечення кібербезпеки у воєнній сфері, задіяних у цьому сил та засобів, у світі на теперішній час сформувалися типові структури органів управління. Особливістю при їх формуванні у провідних країнах світу стало поєднання в одній структурі різних напрямів діяльності, пов'язаних між собою кінцевою метою.

Таким чином, постійне зростання кількості загроз, інцидентів та посилення впливу на особовий склад Збройних Сил та населення через кіберпростір вимагає об'єднання зусиль щодо інформаційної та кібербезпеки, у тому числі і шляхом формування системи кібербезпеки у воєнній сфері та кібероборони з відповідною структурою управління, яка забезпечить скоординоване управління всіма її складовими.

Сучасні високі технології також як і технології попередніх епох змінюють процеси організації бойових дій (операцій) та методи управління ними, і тому вимагають відповідної підготовки та перепідготовки фахівців. Відповідно до цього відбувається удосконалення систем військової освіти в арміях провідних країн світу. Практично кожна з таких країн має військові навчальні заклади, в яких проводиться підготовка фахівців всіх рівнів та проводяться наукові дослідження з питань застосування високих технологій в інтересах національної безпеки і оборони.

Література

1. Мережево-центрична війна. Матеріал з Вікіпедії. URL: https://uk.wikipedia.org/wiki/Мережево-центрична_війна. (дата звернення 27.04.2018). **2. The Implementation** of Network-Centric Warfare. URL: http://www.iwar.org.uk/rma/resources/ncw/implementation-of-NCW.pdf. (дата звернення 27.04.2018). **3. Війна** четвертого покоління. Матеріал з Вікіпедії. URL: https://uk.wikipedia.org/wiki/Війна_четвертого_покоління. (дата звернення 27.04.2018).**4. Киреев С**. 4GW – технология войн XXI века. URL: http://falcon-security.ru/falcon-news/news-860.html. (дата звернення 27.04.2018). **5. Вильям С. Линд,** полковник Кит Найтингейл (Армия США), капитан Джон Ф. Шмитт (Корпус морской пехоты США), полковник Джозеф У. Саттон (Армия США), подполковник Гэри И. Уилсон (Корпус морской пехоты США, резерв). Меняющееся лицо войны: четвертое поколение. *Marine Corps Gazette*, 1989, pp. 22–26. URL: http://pentagonus.ru/publ/23-1-0-1094. (дата звернення 27.04.2018). **6. Defending** the borderland Ukrainian Military Experiences with IO, Cyber, and EW, 2017. URL: https://www.researchgate.net/publication/322869859_Defending_The_Borderland_Ukrainian_Military_Experiences_with_IO_Cyber_and_EW. (дата звернення 27.04.2018). **7. Куликов А.** Война в едином информационном пространстве. 2008. URL: http://www.vko.ru/koncepcii/voyna-v-edinom-informacionnom-prostranstve. **8. Пермяков О. Ю.,** Сбітнєв А. І. Інформаційні технології і сучасна збройна боротьба. Луганськ: Знання, 2008. 204 с. **9. Сунь-Цзи** Містецтво війни; переклад Г. Латника. К.: Арій, 2014. 128 с. **10. Политов В.** Доктрина маршала Огаркова. *Умное производство*. URL: http://www.umpro.ru/index.php?page_id=17&art_id_1=292&group_id_4=49. (дата звернення 27.04.2018). **11. Даник Ю. Г.,** Грищук Р. В. Основи кібернетичної безпеки: монографія; за заг. ред. проф. Ю. Г. Даника. Житомир: ЖНАЕУ, 2016. 636 с. **12. Даник Ю. Г.,** Бойченко О. С. Пріоритетні високотехнологічні напрями забезпечення обороноздатності держави в умовах загрози та ведення "гібридних війн". *Наука і оборона*. 2016. № 2. С. 19–27. **13. Світова** гібридна війна: український фронт : монографія / за заг. ред. В.П. Горбуліна. К.: НІСД, 2017. 496 с. **14. The d-n-i echo**: The Essence of Winning and Losing, by John R. Boyd, 1996 URL: https://danford.net/boyd/essence.htm. (дата звернення 27.04.2018). **15. Bryant D.J.** Critique, Explore, Compare and Adapt (CECA): A New Model for Command Decisionmaking. Defence R&D Toronto Technical Report, DFDC, Toronto TR, 2003. 63 p. **16. Deptula, David A.** Effects-Based Operations: Change in the Nature of Warfare, Arlington, VA: Aerospace Education Foundation, 2001. 40 p. **17. Даник Ю. Г.,** Бойченко О. С. Формування основ забезпечення оперативного управління силами та засобами в умовах сучасних військових конфліктів *Наука і оборона*, 2016. № 1. С. 4–10. **18. Даник Ю. Г.,** Шестаков В. І. Особливості розвитку та удосконалена класифікація розвідувально-ударних комплексів. *Сучасні інформаційні технології у сфері безпеки та оборони*, 2017. № 3(30). С. 126–136. **19. Даник Ю. Г.,** Писарчук О. О., Соколов К. О. та ін. Багатокритеріальні математичні моделі ситуаційного управління та самоорганізації у складних інформаційних системах: монографія. Житомир: ПП "Рута", 2016. 232 с. **20. Dr. Phillip A Peterson**, Nicholas Myers (2018), The Baltic Security Net Assessment. *The Potomac Foundation and the Baltic Defence College*. URL:

https://www.baltdefcol.org/files/files/publications/BalticSecurityNetAssessment2018.pdf. (дата звернення 27.04.2018). **21. Danyk Y.,** Maliarchuk T., Kokhreidze G. Hybrid highly technological synergy of modern wars and military conflicts. *Proceedings of the David Agmashenebeli National Defense Academy of Georgia*. 2017. pp. 14–21. URL: http://www.academia.edu/35491547/Synergy_of_Modern_Wars.pdf. (дата звернення 27.04.2018). **22. Danyk Y.,** Maliarchuk T., Briggs Ch. Hybrid War: High-tech, Information and Cyber Conflicts, Connections. *The Quarterly Journal*. Vol. 16, No. 2 (Spring 2017), pp. 5–24. URL: http://www.jstor.org/stable/26326478. (дата звернення 27.04.2018). **23. Special operations** for disruption of state and military control system. *Security and Defence Quarterly*, published by War Studies University, Warsaw, Poland. 2015. № 4(9). URL: https://securityanddefence.pl/resources/html/article/details?id=124640. (дата звернення 27.04.2018). **24. State Cyber** Defense Formation and Development in Conditions of Hybrid Challenges and Threats. *International Conference on Information and Telecommunication Technologies and Radio Electronics*. September.11-15, 2017 DOI: https://doi.org/10.1109/UkrMiCo.2017.8095427. (дата звернення 27.04.2018). **25. Masuda Y.** The information society as post – industrial society. Washington: *World Future Society*, 1983. 171 p. **26. Военный** Энциклопедический Словарь (ВЭС). М.: *Воениздат*, 1986. 922 с. **27. Про Стратегічний** оборонний бюлетень України: Указ Президента України від 20.05.2016 р. №240/2016. URL: http://www.president.gov.ua/documents/2402016-20137. (дата звернення 27.04.2018). **28. Вдовенко С. Г.,** Даник Ю. Г. Концептуальні напрями комплексного вирішення проблеми захисту інформації в системі скритого управління збройних сил. *Сучасні інформаційні технології у сфері безпеки та оборони* 2017. №2(29). С. 98–107. **29. Korobiichuk I.,** Nowicki M., Danik Y.G., Dupelich S., Oleksyj S. The Selection Methods for Multisensor System Elements of Drone Detection. *Recent Advances in Systems, Control and Information Technology*. Proceedings of the International Conference SCIT 2016, (May 20–21, 2016) Warsaw, Poland. pp. 20–26. DOI: https://doi.org/10.1007/978-3-319-48923-0_3. **30. Військова** Технічна Академія імені Ярослава Домбровського. URL: http://www.wat.edu.pl. (дата звернення 27.04.2018). **31. Королівський** військовий коледж Канади. URL: https://www.rmc-cmr.ca/en. (дата звернення 27.04.2018). **32. Universität** der Bundeswehr München. URL: https://www.unibw.de/home. (дата звернення 27.04.2018). **33. Даник Ю. Г.,** Дупелич С. О. Стратегічні аспекти боротьби з робототехнічними комплексами. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2017. № 2(29). С. 16–25. **34. Benjamin Schreer:** "Die Transformation der US-Streitkräfte im Zuge des Irakkriegs", Seite 7. *Stiftung Wissenschaft und Politik* vom Dezember 2003. 28 p.

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБЕСПЕЧЕНИИ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ И ОБОРОНЫ: РЕАЛИИ И ТЕНДЕНЦИИ РАЗВИТИЯ

Юрий Григорьевич Даник *(д-р техн. наук, профессор, начальник института)*
Александр Юрьевич Пермяков *(д-р техн. наук, профессор, профессор кафедры)*

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

В статье на основе анализа современного состояния и тенденций развития информационных и других высоких оборонных технологий и их влияния на обеспечение национальной безопасности и обороны, с учетом особенностей высокотехнологичного развития человечества, выявлены основные проблемные вопросы их внедрения, эффективного применения в военной сфере и определены пути их решения. С единых позиций рассмотрены системы оперативного управления войсками (силами) и оружием, их роль и место в формировании единого боевого пространства и практической реализации сетецентрической концепции организации и ведения боевых действий, а также система-образующая и интегрирующая роль информационных технологий в решении этих вопросов. Исследованы факторы, которые влияют на рост числа угроз и рисков информационных, кибер и когнитивных деструктивных воздействий на высокотехнологичные системы (комплексы, средства), личный состав Вооруженных Сил и население через киберпространство в современных условиях и их трансформации. Предложены возможные пути по совершенствованию системы информационной и кибербезопасности государства в военной сфере, а также кибероборонны. Рассмотрены проблемные вопросы научного сопровождения создания, внедрения и обеспечения эффективного применения высокотехнологичных разработок в сфере обороны, а также подготовки специалистов по высокотехнологичным направлениям в интересах обеспечения национальной безопасности и обороны, предложены пути их решения.

Ключевые слова: *информационные технологии, высокие технологии, оборонные технологии, когнитивное противостояние, сетецентрическая концепция организации и ведения боевых действий, гибридная война, C4ISR.*

Modern information technologies in providing national security and defence: current state and development trends

Yurii Gryhorovych Danyk *(Doctor of Technical Science, Professor, Head of the Institute)*
Alexander Yuryevich Permyakov *(Doctor of Engineering, professor of the department)*

National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine

In the article has been analys of the current state and trends in the development defence tecnologys. Accomplished impact the high-tech on national security and defense. And accomplished problems of their implementation in the military field and ways of their solution. Viewd the systems of operational troops (forces) and weapons control, their role and place in the formation of total combat space and the practical implementation of a network-centric concept of organizing and conducting military operations are considered. System and integrated role of information technologies in solving these issues. Investigated the influence factors

grow of the numbers of threats and risks at information and cyber fields, destructive influences on high-tech systems (complexes, facilities), the Armed Forces personnel and the civilian population through cyberspace in modern conditions. Offered ways to improve the information and cybersecurity system, and cyber-defense in the military field. Considered the problems of scientific creation and effective maintenance application of high-tech developments in the defense field. Considered problems of specialists training in high-tech directionals of national security and defense and offered ways of their solution.

Key words: *information technologies, high technologies, defense technologys, cognitive confrontation, network-centric concept of organization and conduct a combat operations, hybrid war, C4ISR.*

References

1. Network-centric warfare**.** From Wikipedia. URL: https://en.wikipedia.org/wiki/Network-centric_warfare. **2. The Implementation** of Network-Centric Warfare. URL: http://www.iwar.org.uk/rma/resources/ncw/implementation-of-NCW.pdf. **3. Fourth-**generation warfare**.** From Wikipedia. URL: https://en.wikipedia.org/wiki/Fourth-generation_warfare. **4. Kireev S.** 4GW – tehnologiya voyn XXI veka. URL: http://falcon-security.ru/falcon-news/news-860.html. **5. William S. Lind**, Colonel Keith Nightengale (USA), Captain John F. Schmitt (USMC), Colonel Joseph W. Sutton (USA), and Lieutenant Colonel Gary I. Wilson (USMCR). The Changing Face of War: Into the Fourth Generation. *Marine Corps Gazette*, (1989), pp. 22–26. URL: http://globalguerrillas.typepad.com/lind/the-changing-face-of-war-into-the-fourth-generation.html. **6. Defending** the borderland Ukrainian Military Experiences with IO, Cyber, and EW, (2017). URL: https://www.researchgate.net/publication/322869859_Defending_The_Borderland_Ukrainian_Military_Experiences_with_IO_Cyber_and_EW. **7. Kulikov A**. Voyna v edinom informatsionnom prostranstve. (2008). URL: http://www.vko.ru/koncepcii/voyna-v-edinom-informacionnom-prostranstve. **8. Permjakov O. Ju.,** Sbitnjev A. I. Informacijni tekhnologhiji i suchasna zbrojna borotjba: Lughansjk: *Znannja*, (2008). p.204. **9. Sunj-Czy** Mistectvo vijny. K.: Arij, 2014. 128 p. **10. Politov V.** Doktrina marshala Ogarkova. *Umnoe proizvodstvo*. URL: http://www.umpro.ru/index.php?page_id=17&art_id_1=292&group_id_4=49. **11. Danyk Ju. Gh.,** Ghryshhuk R. V. (2016). Osnovy kibernetychnoji bezpeky: monoghrafija. Zhytomyr: ZhNAEU. 636 p. **12. Danyk Y. G.,** Bojchenko O. S., (2016). Priorytetni vysokotekhnologhichni naprjamy zabezpechennja oboronozdatnosti derzhavy v umovakh zaghrozy ta vedennja "ghibrydnykh vijn". *Nauka i oborona*. № 2. pp.19–27. **13. Svitova** ghibridna vijna: ukrajinsjkyj front: monoghrafija / za zagh. red. V.P. Ghorbulina. (2017). K.: *NISD*. 496 p. **14. The d-n-i echo**: The Essence of Winning and Losing, (1996). John R. Boyd, URL: https://danford.net/boyd/essence.htm. **15. Bryant D.J.** (2003). Critique, Explore, Compare and Adapt (CECA): A New Model for Command Decisionmaking. Defence R&D Toronto Technical Report, DFDC, Toronto TR. 63 p. **16. Deptula, David A.** (2001). Effects-Based Operations: Change in the Nature of Warfare, Arlington, VA: *Aerospace Education Foundation*. 40 p. **17. Danyk Y. G.,** Bojchenko O. S., (2016). Formuvannja osnov zabezpechennja operatyvnogho upravlinnja sylamy ta zasobamy v umovakh suchasnykh vijsjkovykh konfliktiv *Nauka i oborona*, № 1. pp. 4–10. **18. Danyk Y. G.,** Shestakov V. I. (2017). Development features and improved classification of situational surveillance and attack systems. *Modern information technologies in the sphere of security and defence*. № 3(30). pp.126–136. **19. Danyk Y.G.,** Pysarchuk O.O., Sokolov K.O., et al. (2016), The multi-criteria mathematical model s for the situational control and self-organization under complex information systems. Zhytomyr, 232 p. **20. Dr. Phillip A Peterson**, Nicholas Myers (2018), The Baltic Security Net Assessment. *The Potomac Foundation and the Baltic Defence College*. URL: https://www.baltdefcol.org/files/files/publications/BalticSecurityNetAssessment2018.pdf. **21. Danyk Y.,** Maliarchuk T., Kokhreidze G. (2017). Hybrid highly technological synergy of modern wars and military conflicts. *Proceedings of the David Agmashenebeli National Defense Academy of Georgia*. pp. 14–21. URL: http://www.academia.edu/35491547/Synergy_of_Modern_Wars.pdf. **22. Danyk Y.,** Maliarchuk T., Briggs Ch. (2017). Hybrid War: High-tech, Information and Cyber Conflicts, Connections. *The Quarterly Journal*. Vol. 16, No. 2, pp. 5–24. URL: http://www.jstor.org/stable/26326478. **23. Special** operations for disruption of state and military control system. (2015). *Security and Defence Quarterly*, published by War Studies University, Warsaw, Poland. № 4(9). URL: https://securityanddefence.pl/resources/html/article/details?id=124640. **24. State** Cyber Defense Formation and Development in Conditions of Hybrid Challenges and Threats. (September.11-15, 2017). *International Conference on Information and Telecommunication Technologies and Radio Electronics*. DOI: https://doi.org/10.1109/UkrMiCo.2017.8095427. **25. Masuda Y.** (1983). The information society as post – industrial society. Washington: *World Future Society*, 171 p. **26. Voennyiy** Entsiklopedicheskiy Slovar (VES). (1986). M.: Voenizdat. 922 p. **27. Pro Strateghichnyj** oboronnyj bjuletenj Ukrajiny: Ukaz Prezydenta Ukrajiny vid 20.05.2016 p. №240/2016. URL: http://www.president.gov.ua/documents/2402016-20137. **28. *Vdovenko S. G.,*** *Danik Y. G.* (2017). Conceptual approaches for complex solution of information security in the code C2 of the Armed Forces. *Modern information technologies in the sphere of security and defence*. №2(29). pp. 98–107. **29. Korobiichuk I.,** Nowicki M., Danik Y.G., Dupelich S., Oleksyj S. (May 20–21, 2016) The Selection Methods for Multisensor System Elements of Drone Detection. *Recent Advances in Systems, Control and Information Technology*. Proceedings of the International Conference SCIT 2016. Warsaw, Poland. pp. 20–26. DOI: https://doi.org/10.1007/978-3-319-48923-0_3. **30. Wojskowa** akademia techniczna im. Jarosława Dąbrowskiego. URL: http://www.wat.edu.pl. **31. Royal** Military College of Canada URL: https://www.rmc-cmr.ca/en. **32. Universität** der Bundeswehr München. URL: https://www.unibw.de/home. **33. Danyk Y. G.,** Dupelich S. O. (2017). Strategic aspects of fight against robot systems. *Modern information technologies in the sphere of security and defence*. № 2(29). pp. 16–25. **34. Benjamin Schreer:** "Die Transformation der US-Streitkräfte im Zuge des Irakkriegs", Seite 7. *Stiftung Wissenschaft und Politik* vom Dezember, 2003. 28 p.