ТЕОРІЯ ТА ФІЛОСОФІЯ ДЕРЖАВНОГО УПРАВЛІННЯ

DOI: https://doi.org/10.26565/1992-2337-2023-2-01
УДК 005.2

Живило Євген Олександрович,
докторант кафедри публічної політики
навчально-наукового інституту "Інститут державного управління"
Харківського національного університету імені В. Н. Каразіна,
майдан Свободи, 4, м. Харків, 61022, Україна
e-mail: zhivilka@i.ua https://orcid.org/0000-0003-4077-7853

СУТНІСТЬ ВИСОКОТЕХНОЛОГІЧНОЇ ВІЙНИ В ОРГАНІЗАЦІЙНО-ІНСТИТУЦІОНАЛЬНОМУ ЗАБЕЗПЕЧЕННІ ТЕОРІЇ ДЕРЖАВНОГО УПРАВЛІННЯ

Анотація. На межі XX і XXI століть сталися фундаментальні зміни у сфері міжнародної безпеки. Світова спільнота зустрілася з принципово новими викликами й загрозами. У багатьох регіонах світу спостерігалось міждержавне суперництво, що призвело до спалаху локальних війн і воєнних конфліктів, які здебільш мали форму збройного протистояння.

Технічний прогрес, наявність значної воєнної сили, демонстрація рішучості та її використання трансформували суспільні відносини в більш конфліктні. Поступово у локальні війни і воєнні конфлікти втягується все більше країн світу. В цьому контексті слід зазначити, що інтенсивність та масштабність воєнних дій протягом останніх тридцяти років, які відбувалися в різних куточках земної кулі, свідчать про зростання динамічної зміни обстановки в зоні ведення бойових дій в ході застосування міжнародних коаліційних сил. При цьому жорстке виконання вимог щодо стійкого, безперервного, оперативного і скритого управління військами під час виконання ними бойових завдань спонукає провідні країни світу до розробки та впровадження нових концепцій інформаційних мереж та систем.

Необхідно зазначити, що майбутні війни будуть залежати від високотехнологічних розвідувальних засобів. Пріоритетом вбачається – першим виявити ворога, перш ніж він помітить вас; засліпити датчики противника, будь то дрони або супутники; і порушити їхні засоби та канали передачі даних, чи то через кібератаки, електронну війну чи старомодні засоби вогневого ураження. Військам доведеться розвивати нові форми і способи застосування, покладаючись на мобільність, розосередженість, маскування та заходи омани.

Як цитувати: Живило Є. О. Сутність високотехнологічної війни в організаційно-інституціональному забезпеченні теорії державного управління. *Державне будівництво.* 2023. № 2 (34). С. 8–20. DOI: https://doi.org/10.26565/1992-2337-2023-2-01

In cites: Zhyvylo, Y.O. (2023). The essence of high-tech warfare in the organizational and institutional security theory of state administration. *State Formation, no. 2 (34), 8–20.* DOI: https://doi.org/10.26565/1992-2337-2023-2-01 [in Ukrainian].

Великі армії, які не зможуть інвестувати в нові технології чи розробити нові доктрини, будуть переповнені меншими, які це зроблять. “Ми повинні визнати, що старі концепції ведення великих танкових битв на європейській суші закінчилися”, – сказав Борис Джонсон, прем’єр-міністр Великобританії, у листопаді 2021 року. “Є інші, важливіші речі, у які ми повинні інвестувати. Кібертехнології, такою буде війна майбутнього”. Через три місяці росія вторглася в Україну.

Отже, в роботі визначено проблему неповної відповідності сучасного стану і готовності сектору безпеки та оборони щодо вимог ефективної протидії загрозам національній безпеці та їхньої нейтралізації, сформульовано завдання з удосконалення цієї діяльності, щодо створення об’єднаних систем управління та зв’язку, визначено горизонтальні зв’язки цих систем та електронно-комунікаційних мереж, що в подальшому беззаперечно вплине на безпечне функціонування національного сегменту кіберпростору.

Ключові слова: інформаційні мережі, інформаційні технології, кібербезпека, кіберпростір, штучний інтелект, об’єднана мережа, система зв’язку і комунікаційна система.

Постановка проблеми. Війна в Україні є найбільшою в Європі з 1945 р. Вона формує розуміння бойових дій на наступні десятиліття. Це розвіяло будь-які ілюзії того, що сучасний конфлікт може обмежуватися кампаніями проти повстанців або розвиватися до боротьби з низьким числом жертв у кіберпросторі (далі – КП). Натомість це вказує на новий вид високо інтенсивної війни, яка поєднує передові технології з промисловими вбивствами та споживанням боєприпасів, навіть якщо вона залучає цивільних осіб, союзників і приватні компанії. Можна з впевненістю стверджувати, що автократичні режими вивчають, як отримати перевагу в будь-якому майбутньому конфлікті. Замість того, щоб відступати від смерті та руйнування, ліберальні суспільства повинні визнати, що війни між промислово розвиненими економіками є надто реальною перспективою, і необхідно почати готуватись до цього вже зараз.

Згодом технологія може змінити умови сьогодення. Так, 30 червня 2023 р. генерал Марк Міллі, старший військовослужбовець США, зазначив, що через 10-15 років третину передових збройних сил (далі – ЗС) буде роботизовано. Він наголошує увагу керівництву США щодо переозброєння армії на безпілотну авіацію та безпілотні танки. Проте ЗС США повинні бути здатними воювати як у цьому десятилітті, так і в наступному [14]. Це означає, що необхідно провести поповнення запасів, щоб підготуватися до високих темпів виснаження, створити промислові потужності для виробництва обладнання в набагато більшому масштабі та створити відповідний людський мобілізаційний ресурс. Саміт НАТО, який було проведено 11 і 12 липня 2023 р. став перевіркою того, чи зможуть західні країни продовжувати зміцнювати свій альянс для досягнення цих цілей.

Сьогодні Україна є піонером у здатності перетворити шматок металу часів холодної війни на щось, що справді об’єднано в загальну інформаційно-комунікаційну мережу та є частиною цієї алгоритмічної війни. “Це викликає божевілля”, – зазначив Джеймс Хіппі, міністр оборони Великої Британії [1].

Відтак, нові кордони, або взагалі їх відсутність, створюють нові загрози державному устрою будь-якої країни. Зростаюча участь цивільних осіб

породжує юридичні та етичні питання. Технології не стоять на місці, фізичні та логічні процеси, елементна база (мікросхеми, чіпи) вже зараз вирішують великий масив інформаційно-аналітичних завдань, попередньо цю роботу колись можна було виконати лише на віддаленому хмарному сервері. Приватні компанії, розташовані за межами зони фізичного конфлікту, можуть стати об'єктом віртуальної або збройної атаки. У міру появи нових компаній, уряди країн повинні переконатися, що жодна з них не стане атакою "нульового" дня.

Аналіз останніх досліджень і публікацій. Аналізуючи останні дослідження та відкриті публікації з засобів масової інформації вбачається, що потреба в забезпеченні кібербезпеки (далі – КБ) та створенні засобів ведення кібервійн наразі спонукає уряди держав переглядати внутрішню політику в КП, оскільки дедалі частіше трапляються випадки використання розвідувальними службами та спеціалізованими військовими підрозділами можливостей і технічних потужностей транснаціональних кримінальних груп, що спеціалізуються у сфері кіберзлочинності.

Сьогодні реальність така, що відносна перевага Америки в КП як галузі воєнних дій оспорюється (і оспорюватиметься). США стикаються зі стратегічними загрозами у КП з боку Китаю, а також росії – двох давніх ключових суперників у цій галузі. США та їхні союзники також стикаються з тактичними загрозами з боку цілого ряду суб'єктів, включаючи дедалі активніші національні держави, такі як Північна Корея та Іран, а також широкий спектр недержавних суб'єктів, від злочинних угруповань до терористичних груп.

Стримування в КП також є ключовою стратегічною сферою уваги китайських військових вчених і стратегів. Фактичні наслідки застосування традиційної теорії стримування у КП сьогодні залишаються дещо туманними. Хоча вочевидь, що держави, які мають спроможності забезпечити реалізацію визначених військових цілей щодо активних дій у КП, такі як США, Китай і росія, в даний час не готові використовувати свої найпотужніші можливості проти тих, кого вони сприймають як рівних конкурентів, оскільки вони побоюються потенційної відповіді. Також очевидно, що інші країни готові вжити певних обмежених дій, які в інших умовах могли б розглядатися як перехід кордону щодо таких потужних гравців.

Незважаючи на широкий інтерес до зазначеного безпекового напряму, наукові дослідження (чи навіть узагальнення за цією темою) досі є поодинокими й часто несистемними.

Проблематики сучасного безпекового середовища, тенденції еволюції кіберзагроз, шляхи до безпечного використання КП, створення кібервійськ в Україні та питання пов'язані з їх забезпеченням у різних аспектах досліджувались у наукових працях (доповідях, інформаційно-аналітичних матеріалах і т. і.) О. Бакалінський, О. Баранова, А. Баровська, В. Горбуліна, В. Гурковського, О. Довганя, Д. Дубова, Г. Ємельянова, Р. Калюжного, О. Кандибіна, Р. Кирилюка, Б. Кормича, В. Лопатіна, Р. Максутова, А. Марущака, М. Ожевана, В. Остроухова, М. Панова, О. Петрошкевича,

В. Пилипчука, М. Потрубача, Г. Почепцова, М. Присяжнюка, А. Прозорова, Ю. Пунди, В. Рубана, С. Стрельцова, В. Телелима, О. Тихомирова, Н. Ткачука, В. Тютюніка, Є. Шелеста, та іншими вітчизняними дослідниками.

При цьому, теоретико-методологічні дискусії довкола термінологічної бази стикаються зі значною більш практичною проблемою, а саме застосування чинного нормативно-правового поля (особливо міжнародного) щодо КБ, КЗ, кіберзагроз, кібердій та кібероперацій і з'ясування самої можливості його застосування у відповідному контексті [4]. Серйозною проблемою міжнародного співтовариства і урядів країн є суперечки, щодо встановлення чітких кордонів національного КП держави, визначення наслідків "руйнування" її критичної інфраструктури, порядку вжиття упереджувальних заходів та законності реагування на деструктивні кібердії у відповідь [2].

Однак той факт, що ці випадки створюють значні проблеми, не є причиною уникати прийняття складних рішень на національному та транснаціональному рівні. Навпаки, той факт, що в цій галузі зберігається двозначність, а реакція США та їхніх союзників досі була обмеженою (принаймні у публічному просторі), означає, що розвідувальні органи інших країн, швидше за все, продовжуватимуть свою діяльність у КП.

Мета статті. визначення стратегічних принципів зі зв'язку та інформаційних систем (далі – ІС) сил оборони (далі – СО) України на основі вивчення змісту підходів країн-членів ЄС та НАТО, дослідження теоретико-методологічних основ функціональної сумісності та взаємодії об'єднаних мілітаризованих мереж з урахуванням адаптації позитивного зарубіжного досвіду та практичної імплементації, у досліджуваному контексті, доктрин, настанов, стандартів та публікацій країн-партнерів в рамках створення єдиного інформаційного простору.

Застосована методологія і методи: Вивчення змісту системного та структурно-функціонального підходів застосування різних сучасних інформаційних технологій (далі – ІТ) і ІС для досягнення інформаційної переваги над противником, а також принципів системності та об'єктивності відповідних ІС у сучасних війнах дозволило автору визначити методологічне забезпечення державного регулювання у досліджуваному контексті [3]. При цьому, областю проведення дослідження вбачалось за необхідне вивчити питання пов'язані з активними діями у КП та інформаційним протиборством під час ведення мережецентричних/мережевих війн. За цих умов було застосовано відповідні методи наукового пізнання, а саме абстрактно-логічний, аналіз, синтез, порівняння, узагальнення та моделювання.

Крім того, у статті визначено межі дослідження та його інформаційно-аналітичну базу, а також перспективи проведення подальшого дослідження.

Виклад основного матеріалу. Сьогодні Україна спрямовує свої пріоритети в реалізації воєнної політики держави на відсіч збройної агресії з одночасним здійсненням заходів оборонної реформи та цифрової трансформації. Першочерговим напрямком є посилення спроможностей СО,

підвищення їх готовності до виконання завдань за призначенням та участі у проведенні спільних із підрозділами НАТО бойових дій (операцій) [8].

Виконання вказаних вище пріоритетів для нашої держави неможливо без удосконалення системи зв'язку та інформаційних систем (далі – СЗІС) під час підготовки та проведення операцій СО які пов'язані з необхідністю обробки значних обсягів різнорідної інформації в стислі терміни. Це потребує застосування різних сучасних ІТ і ІС для досягнення інформаційної переваги над противником [15]. За цих умов є необхідним зробити наголос на тому, що акцент у сучасних війнах все більше і більше зміщується в інформаційну площину, де здійснюється інтенсивне інформаційне протиборство під час ведення мережецентричних/мережевих війн [10].

В умовах сьогодення є вкрай важливим для СО отримати перевагу над противником. Це, в свою чергу, може оперативно відбутись завдяки використанню єдиного інформаційного простору, побудованого на взаємосумісних мережах/системах зв'язку, які забезпечують захищений обмін інформацією між ними, що в цілому дозволить підвищити загальну ситуаційну обізнаність та управління військами (силами).

Розвиток основних спроможностей СО бойових військових частин і підрозділів зі складу СО дозволить бути боєздатними, мобільними та здатними швидко висуватися на загрозливі напрямки, зосереджувати зусилля в необхідному місці у визначений час, діяти непередбачувано та інноваційно, враховуючи загальну військову перевагу противника.

У свою чергу оснащення високотехнологічними та модернізованими зразками озброєння та військової (спеціальної) техніки спонукає виконання реалістичних та адаптивних довгострокових оборонних програм і проєктів, основою яких буде весь життєвий цикл спроможностей [2].

За цих обставин втілення цифрової трансформації органами державної влади, що беруть участь у виконанні функцій держави у відповідності до своїх повноважень, застосування сучасних технологій автоматизації управління військами та зброєю, проведення моніторингу та аналізу інформації, впровадження комплексів та засобів моделювання, експертних систем, спеціального програмного забезпечення, комунікаційних систем на тлі єдиного інформаційного середовища СО побудованого за єдиними стандартами, протоколами, архітектурою відбувається на основі принципів і стандартів НАТО.

Імплементація і взаємосумісність адаптивних комунікаційних систем та мереж СО відбувається з урахуванням національних особливостей щодо захисту суверенітету, територіальної цілісності і недоторканності України [6].

Інформація – це найважливіший актив держави, а забезпечення СЗІС і послуг має важливе значення для належного управління системою консультацій, командування і управління. НАТО і союзники покладаються на використання СЗІС для ефективного обміну інформацією та ефективного функціонування [11]. Така побудова системи зв'язку і комунікаційні системи (CIS) потребує ряду принципів, які дозволять НАТО і її союзникам отримувати технологічні

переваги, а також відчути ризики пов'язані зі складнощами виконання операцій з інформаційним перевантаженням.

Врахування принципів зв'язку та ІС (en: Communication and Information Systems Principles) НАТО дозволить СО спільно використовувати інформацію в рамках єдиного інформаційного простору. Це надає право вищому воєнно-політичному керівництву держави, командирам та штабам всіх рівнів отримати значні переваги під час планування та ведення операцій (бойових дій), покращити ситуаційну обізнаність, управління військами (силами) та зброєю. Такий підхід дозволить СО отримувати переваги з використання та впровадження ІТ.

Стратегічні принципи зв'язку та ІС (en: CIS strategic principles) СО (визначені відповідно до документу Ради штабу НАТО з консультацій, командування та управління AC/322-D (2018) 0020. Alliance C3 Strategy – Part 1, 27 April 2018.) включають:

– спільне використання інформації в рамках єдиного інформаційного простору із запровадженням та супроводженням реєстру інформаційних ресурсів, електронних баз даних інформації та інформаційного менеджменту;

– забезпечення безперешкодного обміну інформацією між стаціонарними СЗІС та польовими мережами зв'язку;

– функціонування інформації в мережевому захищеному середовищі балансуючи між принципами "обов'язок щодо розповсюдження" (en: "duty to share") та "потреби в інформації" (en: "need to know");

– масштабованість СЗІС та їх сервісів (здатність динамічно адаптуватись до змін вимог), гнучкість (здатність адаптуватись до змін умов обстановки яка склалась), захищеність (здатність забезпечити політики безпеки в існуючому середовищі ризиків) та стійкість (здатність до відновлення системи після вразливості "нульового дня");

– забезпеченість СЗІС відповідними сервісами згідно методології DOTMLPFI;

Довідково: DOTMLPFI (Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities, and Interoperability) – напрями розвитку оборонних потенціалів [7] (Доктринальна база (D), Організація (O), Підготовка (T), Ресурсне забезпечення (M), Персонал (P), Якість управління та освіта (L), Військова інфраструктура (F), Взаємосумісність (I)), які є складовою процесу оборонного планування НАТО (en: NATO Defense Planning Process).

– опис та забезпеченість спроможностей СЗІС, як сервісів, сервіс-орієнтовану архітектуру та запроваджені підходи до їх життєвого циклу;

– підтримку обміну інформацією з обмеженням доступу будь-якого рівня та всіх функціональних сервісів, притаманних окремим структурним підрозділам органів державного та військового управління;

– відкритість, модульність та гнучкість для повторного використання, динамічність до розвитку і взаємосумісності та здатність до інтеграції в існуючі та майбутні спроможності архітектур СЗІС;

– відповідність пріоритету розвитку спроможностей парадигмі “ABC” “ABC” (Adopt, Buy, Create) (тобто, модернізація наявного, далі – закупівля готових ресурсів, і, як крайня міра – створення нового або їх комбінація) [12];

– заснування дисципліни з корпоративної архітектури;

– адекватну захищеність проти всіх категорій загроз, у т. ч. тих, що випливають із КП, зв’язку та ІС, їх сервісів та електронних систем;

– підтримку колективних заходів з кіберзахисту (кібероперацій) всіх складових сил безпеки і оборони;

– запровадження практик ITIL (Бібліотека інфраструктури IT (en: Information Technology Infrastructure Library, ITIL).

Розгортання об’єднаної мережі СО зі створенням єдиного інформаційного простору повинно відповідати додатково також таким принципам:

– цінова ефективність від використання;

– можливості максимального повторного використання;

– відповідність принципам єдиного інформаційного простору;

– урахування С3-таксономії;

– поетапний підхід;

– використання уніфікованих мережевих стандартів та рішень;

– підтримка угруповань СО, склад яких динамічно змінюється;

– інформаційна орієнтованість мережі.

Об’єднана мережа СО повинна використовувати гнучкі та адаптовані набори нематеріальних (політика, процеси, процедури та стандарти) та матеріальних (стаціонарна та польова мережі, сервіси та підтримуючі інфраструктури) засобів, якими забезпечуються складові СО.

Стратегічні принципи СЗІС, у контексті системи НАТО, були сформовані на вимогу Ради з питань консультацій, командування і управління (англ. C3 Board) [9], антикризового управління та з врахуванням досвіду отриманого в ході проведених операцій під керівництвом НАТО. Було сформовано покрокову концепцію, в якій визначено, що саме потрібно робити, щоб отримати розгорнуті, стійкі, надійні, функціонально сумісні і значні можливості системи (С3) і СЗІС, що лежать в основі Стратегічної концепції НАТО.

Виходячи з цього, слід врахувати та застосовувати такі стратегічні принципи для України:

– забезпечення безперервного обміну інформацією між стаціонарними і розгорнутими елементами СЗІС з метою супроводу операцій;

– забезпечення підтримки зміни спрямованості зусиль з надання спроможностей системі консультацій, командування і управління (С3) на надання послуг в області інформаційно-комунікаційних технологій (далі – ІКТ);

– послідовність життєвого циклу;

– об’єднання і виконання короткострокових, середньострокових і довгострокових вимог системи консультацій, командування та управління (С3) для переходу до послуг ІКТ на основі координації дій;

– оптимізація ролі і обов’язків, структури і процесів;

– зосередження уваги на необхідності діалогу між користувачами і керівниками на всіх етапах життєвого циклу і, зокрема, під час реалізації;

– сприяння співпраці між спроможностями системи консультацій, командування і управління (С3) і послугами в області ІКТ, що надаються країнами, програмами багатонаціонального або спільного фінансування, безпосередньо до розгортання;

– підтримання всіх рівнів інформаційної безпеки та КБ, а також зв'язків з громадськістю;

– забезпечення підтримки діяльності колективної безпеки в КП;

– використання найбільш пріоритетного виділення ресурсів залежно від варіанту – отримання, закупівля або створення, і, відповідно, в порядку терміновості пріоритетність присвоюється спочатку на отримання того, що вже є в наявності, потім – закупівля готової продукції і, як крайня міра – створення нового [13].

Наша держава не стоїть на місці, паралельно з бойовими діями було затверджено вагомий масив керівних документів, якими було визначено основи функціональної сумісності та взаємодії складових сил безпеки та оборони по зв'язку. Насамперед це доктрини, настанови, стандарти, публікації.

Практична імплементація цих документів у сферу застосування складових сил безпеки та оборони вже відбулась відповідно до розкритих нижче складових:

Всеосяжність інформації та доступ до неї. З отриманням можливості України експлуатації глобальної супутникової системи, розгорнутою компанією SpaceX, за допомогою групи супутників Starlink на низькій навколоземній орбіті, ознаменувала, нову еру стійкого та надійного військового зв'язку. Застосування технології Starlink дозволило ЗС організувати та розгорнути систему зв'язку яка забезпечила ведення переговорів, передачу даних та відеопотоків від кінцевих пристроїв до споживачів відеоінформації в тому числі. Розглядаючи голосові сервіси необхідно зазначити, що вони в значній мірі стандартизовані. Однак, під час розгляду відео і сервісів передачі даних слід зауважити, що технічні вимоги до передачі цих елементів розрізняються в цілому між сервісами.

Ситуаційна обізнаність поточної ситуації. Одним із суттєвих факторів, який впливає на результати бойових дій військ і ефективність вогневого ураження противника є комплексне застосування усіх можливих засобів отримання інформацій. Засоби відеоспостереження є одним із джерел отримання інформації, що змушує розглядати їх в якості одного із елементів загальної системи отримання інформації і прийняття рішення. Подальшим напрямком розвитку систем відеоспостереження вбачається їх функціонування у єдиній системі, яка складається зі стаціонарних і мобільних (машини, роботизовані платформи, БпЛА тощо) постів єдиного розвідувально-інформаційного поля.

Захищені інформаційно-телекомунікаційні послуги (сервіси зв'язку). Сервіси ІС доменів безпеки складових сектору безпеки і оборони поєднали у

собі системи та механізми передавання вибіркових даних між точками доступу або через них, відповідно до узгоджених параметрів якості та без зміни форми або змісту даних, які надсилаються і отримуються. Сервіси, орієнтовані на конкретні інтереси, забезпечують функціонал, який потрібний окремим, спеціалізованим спільнотам користувачів в підтримці операцій СО, навчань та заходів повсякденної діяльності підрозділам розвідки, планування вогневого ураження, логістики тощо.

Базові сервіси забезпечують універсальне, незалежне від груп користувачів й технічної функціональності сервіс-орієнтоване середовище з використанням інфраструктурних, архітектурних та інших необхідних складових елементів (міжміський та міжнародний зв'язок, відкрита та захищена телефонія, захищений відеоконференцзв'язок, веб доступ в автоматизованих системах управління ЗС та мережу Інтернет, електронна пошта в автоматизованих системах управління ЗС та мережі Інтернет).

Функціональні сервіси орієнтовані на конкретні інтереси, що забезпечують функціонал, окремих спеціалізованих спільнот користувачів в підтримці операцій СО, навчань та заходів повсякденної діяльності (захищена СЕДО, інтеграційна платформа "ДЕЛЬТА" – об'єднання інформації з дронів, соціальних мереж, геопросторової розвідки, радіочастотних супутників; спеціального програмного забезпечення "Віраж-планшет" – реалізує інформаційно-розрахункові задачі збору, обробки та видачі інформації про повітряну і надводну обстановку; відеоспостереження; інтеграційні інформаційні ресурси різнотипних інформаційних та автоматизованих систем; єдине геоінформаційне та інформаційно-аналітичне середовище з розмежуванням прав доступу користувачів до всіх зазначених ресурсів).

Технічні сервіси. Представляють собою набір сервісів з вимогами до програмних і апаратних функціональних можливостей та можуть бути повторно використані для різних цілей разом із політиками по їх застосуванню. При цьому клієнтські програми використовують і самі технічні сервіси для забезпечення спроможностей, орієнтованих на користувача. Клієнтські програми надають інтерфейс користувачу, який об'єднує технічні сервіси в підтримку визначеного процесу.

Підсумовуючи зазначене необхідно зауважити що глобальний розвиток ІТ та засобів електронної комунікації започаткували нові технології впливу для вирішення різноманітних конфліктів. Наше суспільство і держава зіткнулось з новою загрозою, яка має величезний військовий і геополітичний потенціал. За короткий проміжок часу вразливості які мали/ють єдині системи електронних комунікацій, системи управління технологічними процесами, перетворились на ефективний імовірний набір реальних і потенційних загроз національній безпеці України у КП [5]. Окреслені вище загрози та стійкий та неухильний прогрес в сфері ІТ комунікаційних засобів здатні порушити штатний режим функціонування таких систем (у тому числі зрив та/або блокування їх роботи, та/або несанкціоноване управління їх ресурсами).

Отже, сьогоднішнє становище відображає нове оперативне середовище протистояння інтернаціональних інтересів, а саме міждержавне протиборство, війну у кіберпросторі – кібервійну. Розуміння загроз, особливо на її початковій стадії, забезпечує вирішальну роль у виборі пропорційності та адекватності заходів КЗ на реальні та потенційні ризики, надає змогу реалізувати невід'ємні права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у КП.

З огляду на оцінки та переконливі думки провідних експертів, зарубіжних і вітчизняних науковців можна твердо стверджувати, що у сучасному цифровому світі важливість КБ зросла в рази. Кібервійна – це нова сфера ведення війни, до якої країни повинні готуватися. Кібервійська – це спеціалізовані військові підрозділи, завданням яких є захист від кібератак і проведення кібероперацій [7]. Ці війська є невід'ємною частиною стратегії національної оборони будь-якої країни в сучасному світі.

Висновки з даного дослідження і перспективи подальших досліджень. Отже, динамічність та оперативність сьогоднішніх подій які відбуваються на "полях смерті" нашої країни дозволяють зробити три важливі висновки.

По-перше, поле бою стає прозорим. Оптичні прилади та паперові топографічні карти – це вже минуле, необхідно розвивати та впроваджувати "всевидючу" мережу датчиків на супутниках і приймати на озброєння парки дронів. Цінова політика, здебільшого цієї продукції доволі низька в порівнянні з життям людини, при цьому ті дані які вони надають мають дедалі вдосконалені алгоритми обробки тих чи інших видів сигналу, які дозволяють в режимі реального часу "витягнуть голку зі стогу сіна", чи розпізнати сигнал мобільного телефону з прив'язкою до його власника, або розпізнати обриси замаскованого танка на місцевості. Здебільшого ця інформація може бути передана супутниковими каналами зв'язку солдату або використана центрами прийняття рішень для наведення артилерії та ракет із безпрецедентною точністю та дальністю.

Навіть в епоху штучного інтелекту другий висновок полягає в тому, що війна все ще може залучати величезну фізичну кількість в сотні тисяч людей, мільйони машин і боєприпасів. Втрати в Україні серйозні: здатність бачити цілі та точно вражати їх змушує керівництво держави постійно проводити підрахунок кількості загиблих. Щоб адаптуватись, війська перекопали безмежну кількість багнюки, щоб вирити траншеї, гідні Вердена чи Пашендейля. Витрата боєприпасів і техніки вражає: росія випустила 10 мільйонів снарядів за рік. Україна втрачає 10 тисяч дронів на місяць. Вона просить у своїх союзників касетні боєприпаси старої школи, щоб провести контрнаступ.

Третій висновок – той, який також застосовувався протягом більшої частини XX століття полягає в тому, що межі великої війни широкі й нечіткі. Конфлікти Заходу в Афганістані та Іраку велись невеликими професійними арміями і були легким тягарем для цивільного населення (але часто завдавали багато страждань місцевим жителям). В Україні мирні жителі були втягнуті у війну як жертви, так понад 9000 людей загинуло. При цьому провінційна бабуся не дивлячись на

загрози допомагала керувати артилерійським вогнем через додаток на смартфоні. Радянський оборонно-промисловий комплекс нашої держави, разом з новою когортою приватних компаній виявився надзвичайно потужним альянсом в умовах війни. Українське бойове програмне забезпечення, розміщене за кордоном на хмарних серверах великих платформ, разом з розгалуженою мережею партнерів обробляє та надає дані для наведення вогневих засобів, також в цих умовах важливу роль відтворив – супутниковий зв'язок.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Війна в Україні показує, як технології змінюють поле бою. *The Economist*, 2023-07-05. URL: https://texty.org.ua/fragments/110086/vijna-v-ukrayini-pokazuye-yak-tehnolohiyi-zminyuyut-pole-boyu-the-economist/

2. Живило Є. О., Орлов О. В. Сутність кібербезпеки національного сегменту кіберпростору держави в умовах кризового управління // Збірник наукових матеріалів XXII Міжнародного наукового конгресу "*Публічне управління XXI століття в умовах гібридних загроз*" 27 квітня 2022 р. Харків : Харківський національний університет імені В. Н. Каразіна, 2022. С. 248–254.

3. Живило Є. О., Шевченко Д. Г. Оцінка ризиків кібербезпеки та контролю конфіденційності в інформаційних системах державного управління // Науковий журнал "*Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*" Київ : Військовий інститут Київського національного університету імені Тараса Шевченка, 2022. № 75. С. 66–76.

4. Розпорядження Кабінету міністрів України від 10 березня 2017 р. № 155-р. "Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України". URL: https://zakon.rada.gov.ua/laws/show/155-2017-%D1%80#Text

5. Постанова Кабінету міністрів України від 11 листопада 2020 р. № 1176 "Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом". URL: https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#Text.

6. Закон України "Про критичну інфраструктуру" (документ 1882-IX, від 16 листоп. 2021 р.). URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

7. Указ Президента України № 96/2016р. в ред. від 28 серпня 2021 року "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України". URL: https://www.rnbo.gov.ua/ua/Ukazy/417.html

8. Указ Президента України від 17 вересня 2021 року № 473/2021 "Стратегічний оборонний бюлетень України". URL: https://законодавство.com/laws/file/text/93/f509164n72.docx

9. Assessing Security and Privacy Controls in Information Systems and Organizations, August 2021. URL: https://csrc.nist.gov/pubs/sp/800/53/a/r5/ipd

10. Koval M., Sova O., Orlov O., Zhyvylo Y., Zhyvylo I. Improvement of complex resource management of special-purpose communication systems. *Eastern-European Journal of Enterprise Technologies*. 2022. 5 (9–119). С. 34–44.

11. Special Publication 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS). URL: https://csrc.nist.gov/pubs/sp/800/94/final

12. Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight, September 2022. URL: https://csrc.nist.gov/pubs/ir/8286/c/final

13. Svitlana Onyshchenko, Yevhen Zhyvylo, Anna Cherviak, Stanislav Bilko Determining the patterns of using information protection systems at financial institutions in order to improve the level of financial security. *Eastern-European Journal of Enterprise Technologies*. 2023. Vol. 5 (13 (125)). С. 65–76.

14. The Economist: A new era of high-tech warfare began in Ukraine 07 July, 2023. URL: https:// zn.ua/ukr/WORLD/the-economist-v-ukrajini-pochalasja-nova-era-visokotekhnolohichnikh- vijn.html

15. Yevhen Zhyvylo, Vladyslav Kuz Risk Management of Critical Information Infrastructure: Threats-Vulnerabilities-Consequences. *Theoretical and Applied Cyber Security.* 2023. Vol. 5 No. 2. C. 68–80.

Стаття надійшла до редакції 11.10.2023 р.
Стаття рекомендована до друку 13.11.2023 р.

Zhyvylo Y. O.,
Doctoral candidate of the Department of Economic Policy and Management,
Educational and Scientific Institute «Institute of Public Administration»,
V. N. Karazin Kharkiv National University,
4, Svobody Sq., Kharkiv, 61022, Ukraine
e-mail: zhivilka@i.ua *https://orcid.org/0000-0003-4077-7853*

THE ESSENCE OF HIGH-TECH WARFARE IN THE ORGANIZATIONAL AND INSTITUTIONAL SECURITY THEORY OF STATE ADMINISTRATION

Annotation. At the turn of the 20th and 21st centuries, fundamental changes occurred in the field of international security. The world community faced fundamentally new challenges and threats. In many regions of the world, interstate rivalry was observed, which led to the outbreak of local wars and military conflicts, which mostly took the form of armed confrontation.

Technological progress, the presence of significant military power, the demonstration of determination and its use transformed social relations into more conflictual ones. Gradually, more and more countries of the world are involved in local wars and military conflicts. In this context, it should be noted that the intensity and scale of hostilities during the last thirty years, which took place in different corners of the globe, testify to the growth of dynamic changes in the situation in the combat zone during the use of international coalition forces. At the same time, the strict implementation of the requirements for stable, continuous, operational and covert management of troops during their performance of combat missions prompts the world's leading countries to develop and implement new concepts of information networks and systems.

It should be noted that future wars will depend on high-tech intelligence. The priority is to identify the enemy first, before he notices you; blind the enemy's sensors, be it drones or satellites; and disrupt their means and data channels, whether through cyberattacks, electronic warfare, or old-fashioned firepower. Armies will have to develop new forms and methods of application, relying on mobility, dispersion, camouflage and deception measures. Large armies that fail to invest in new technology or develop new doctrine will be overwhelmed by smaller ones that do. "We have to recognize that the old concepts of fighting large tank battles on European land are over," said Boris Johnson, the UK's prime minister, in November 2021. "There are other, more important things in which we should invest. Cyber technologies, this will be the war of the future." Three months later, Russia invaded Ukraine.

So, the work defines the problem of incomplete compliance of the current state and readiness of the security and defense sector with regard to the requirements of effective countermeasures against threats to national security and their neutralization, the task of improving this activity, regarding the creation of unified management and communication systems, and horizontal connections are defined connections of these systems and electronic communication networks, which in the future will undoubtedly affect the safe functioning of the national segment of cyberspace.

Keywords: information networks, information technology, cyber security, cyberspace, artificial intelligence, unified network, communication system and communication system.

REFERENCES

1. The war in Ukraine shows how technology is changing the battlefield. *The Economist, 2023-07-05.* URL: https://texty.org.ua/fragments/110086/vijna-v-ukrayini-pokazuye-yak-tehnolohiyi-zminyuyut-pole-boyu-the-economist/

2. Zhyvylo, Ye.O., Orlov, O.V. (2022). Sutnist kiberbezpeky natsionalnoho sehmentu kiberprostoru derzhavy v umovakh kryzovoho upravlinnia. *Collected of scientific materials of the XXIIth International Scientific Congress "Public Administration of the XXIst Century: in Conditions of Hybrid Threats", 27 April 2022, Kharkiv, 248–254* [in Ukrainian].

3. Zhyvylo, Y.O., Shevchenko, D.G. (2022). Assessment of cyber security risks and privacy control in information systems of state administration. *Scientific journal "Collection of Scientific Works of the Military Institute of Taras Shevchenko Kyiv National University", no. 75, 66–76* [in Ukrainian].

4. Decree of the Cabinet of Ministers of Ukraine dated March 10, 2017, No.155-r. (2017). "On the approval of the plan of measures for the year 2017 for the implementation of the Cybersecurity Strategy of Ukraine". URL: https://zakon.rada.gov.ua/laws/show/155-2017-%D1%80#Text

5. Decree of the Cabinet of Ministers of Ukraine dated November 11, 2020, No.1176 (2020). "On approval of the Procedure for conducting a review of the state of cyber protection of critical information infrastructure, state information resources and information, the requirement for the protection of which is established by law". URL: https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#Text

6. Law of Ukraine "On Critical Infrastructure" (document 1882-IX, dated November 16, 2021). (2021). URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

7. Decree of the President of Ukraine No. 96/2016 ed. dated August 28, 2021 On the decision of the National Security and Defense Council of Ukraine dated January 27, 2016 (2021). "On the Cyber Security Strategy of Ukraine". URL: https://www.rnbo.gov.ua/ua/Ukazy/417.html

8. Decree of the President of Ukraine dated September 17, 2021 No. 473/2021 (2021). "Strategic Defense Bulletin of Ukraine". URL: https://zakonodavstvo.com/laws/file/text/93/f509164n72.docx

9. Assessing Security and Privacy Controls in Information Systems and Organizations, August 2021. (2021). URL: https://csrc.nist.gov/pubs/sp/800/53/a/r5/ipd

10. Koval M., Sova O., Orlov O., Zhyvylo Y., Zhyvylo I. (2022). Improvement of complex resource management of special-purpose communication systems. *Eastern-European Journal of Enterprise Technologies, No. 5(9-119), 34–44.*

11. Special Publication 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS) URL:// https://csrc.nist.gov/pubs/sp/800/94/final

12. Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight, September 2022. (2022). URL: https://csrc.nist.gov/pubs/ir/8286/c/final

13. Svitlana Onyshchenko, Yevhen Zhyvylo, Anna Cherviak, Stanislav Bilko (2023). Determining the patterns of using information protection systems at financial institutions in order to improve the level of financial security. *Eastern-European Journal of Enterprise Technologies, vol. 5 (13 (125)), 65–76.*

14. The Economist: A new era of high-tech warfare began in Ukraine 07 July, 2023. (2023). URL: https://zn.ua/ukr/WORLD/the-economist-v-ukrajini-pochalasja-nova-era-visokotekhnolohichnikh-vijn.html

15. Yevhen Zhyvylo, Vladyslav Kuz (2023). Risk Management of Critical Information Infrastructure:Threats-Vulnerabilities-Consequences. *Theoretical and Applied Cyber Security, vol. 5, no. 2, 68–80.*

The article was received by the editors 11.10.2023.
The article is recommended for printing 13.11.2023.