Методи, засоби та заходи забезпечення інформаційно-психологічної безпеки людини, суспільства, держави

УДК 342.15

Шемаєв Володимир Миколайович
доктор військових наук, професор,
доцент кафедри інформаційної безпеки держави
Навчально-науковий інститут інформаційної безпеки
та стратегічних комунікацій НА СБ України
Shemayev Volodymyr
Doctor of Military Sciences, Professor,
Associate Professor of the Department of Information Security of the State Educational and Scientific Institute of Information Security and Strategic Communications of the National Academy of Security Service of Ukraine
ORCID: 0009-0003-2568-5587

Єрьоміна Людмила Валеріївна
старший виклад кафедри інформаційної безпеки держави
Навчально-науковий інститут інформаційної безпеки
та стратегічних комунікацій НА СБ України
Yeromina Liudmila
Senior Lecture of the Department of Information Security of the State Educational and Scientific Institute of Information Security and Strategic Communications of the Security Service of Ukraine
ORCID: 0009-0009-1656-2546

КОНЦЕПЦІЯ ЛЮДСЬКОГО ДОМЕНУ У ДОСЛІДЖЕННІ ПРОБЛЕМ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНІЙ СФЕРІ

THE CONCEPT OF THE HUMAN DOMAIN IN THE STUDY OF NATIONAL SECURITY PROBLEMS IN THE INFORMATION SPHERE

Анотація. *Вступ. В сучасних умовах в середовищі безпеки та оборони більша частина західної теорії все ще зосереджена на фізичних сферах (повітря, море, земля та космос) та кіберсфері, але у XXI столітті стратегічна перевага країни з'явиться завдяки тому, як налагоджена взаємодія з людьми та розуміння їх інтересів, а також доступ до політичних, економічних і соціальних мереж для досягнення відносної переваги, яка доповнює військову міць. Зазначені умови породжують нові загрози та можливості в різних аспектах національної безпеки. Тому актуалізується загальна проблема дослідження змісту та практики застосування в сфері національної безпеки положень інноваційної концепції людського домену.*

Мета. Метою дослідження є визначення змісту та ролі кібернетичного та людського доменів з точки зору їх взаємодії (та отримання міждоменної синергії) у вирішенні проблем та посиленні можливостей забезпечення національної безпеки в інформаційній сфері.

Матеріали і методи. Матеріалами дослідження є: нормативно-законодавчі акти США, ЄС, НАТО та України; фундаментальні праці вітчизняних і зарубіжних авторів з проблем забезпечення національної безпеки в інформаційній сфері з урахуванням людського чинника.

У процесі дослідження було використано такі методи теоретичного й емпіричного дослідження: логічне узагальнення – для визначення сутності та ролі змісту та ролі кібернетичного та людського доменів з точки зору їх взаємодії; аналіз і синтез – для дослідження сутності, змісту та особливостей людської взаємодії (людського домену) в процесах забезпечення національної безпеки, а також формулювання гіпотези щодо центральної ролі людського домену у забезпеченні національної безпеки в сучасних умовах; синергетичний підхід – при обгрунтуванні міждоменної синергії до військових проблем з точки зору багатьох доменів, комплексного

уявлення про супротивника та оточення, логічного узагальнення результатів (формулювання висновків).

Результати. У науковій статті визначено необхідність комплексного розгляду змісту та ролі кібернетичного та людського доменів з точки зору їх взаємодії (та отримання міждоменної синергії) у вирішенні проблем та посиленні можливостей забезпечення національної безпеки в інформаційній сфері. З'ясовано, що кіберпростір – це наскрізний глобальний домен в інформаційному середовищі, що складається з взаємозалежної мережі інфраструктури інформаційних технологій, включаючи Інтернет, телекомунікаційні мережі, комп'ютерні системи та вбудовані процесори та контролери.

Визначена центральна роль людської взаємодії (людській домен) в усіх процесах забезпечення національної безпеки та необхідність впливу на цільових осіб і груп краще, ніж це здійснює супротивник. Обгрунтовано, що створення міждоменної синергії вимагає підходу до військових проблем з точки зору багатьох доменів, комплексного уявлення про супротивника та оточення, розуміння наявних можливостей та інтеграцію цих можливостей, зокрема: оцінки військового потенціалу супротивника, розуміння людського фактору, що випливають з культурних, ідеологічних і політичних мотивацій, які формують наміри та дії противника. Встановлено, що не менш важливим є розуміння фізичного середовища та інших факторів, що впливають на прийняття рішення в процесах забезпечення оборони та безпеки.

Визначено, що розширення меж безпекового мислення з метою охоплення міжвідомчих перспектив зміцнює довіру та спільне розуміння потреб для вирішення завдань спільних операцій у більш широкому міжвідомчому та багатонаціональному контексті.

Перспективи. В подальших наукових дослідженнях пропонується зосередити увагу на формуванні міжсистемного підходу до управління

взаємодією суб'єктів забезпечення національної безпеки в інформаційній сфері із суб'єктами зовнішнього середовища. Це є теоретичним підґрунтям розширення меж управлінського впливу, охоплення міжвідомчих перспектив, що зміцнює довіру та спільне розуміння потреб для вирішення завдань спільних операцій у більш широкому міжвідомчому та багатонаціональному контексті.

Ключові слова: *національна безпека, концепція Human Domain, кіберсфера, інформаційний простір, стратегічні комунікації, міждоменна синергія.*

Summary. *Introduction. In modern conditions in the security and defense environment, most of the Western theory is still focused on the physical spheres (air, sea, land and space) and the cyber sphere, but in the twenty-first century, the strategic advantage of the country will appear due to the way in which interaction with people and understanding of their interests is established, as well as access to political, economic and social networks to achieve relative advantage, which complements military power. These conditions give rise to new threats and opportunities in various aspects of national security. Therefore, the general problem of studying the content and practice of applying the provisions of the innovative concept of the human domain in the field of national security is actualized.*

Purpose. The purpose of the study is to determine the content and role of cybernetic and human domains in terms of their interaction (and obtaining cross-domain synergy) in solving problems and strengthening the capabilities of ensuring national security in the information sphere.

Materials and methods. The materials of the study are: normative and legislative acts of the USA, EU, NATO and Ukraine; fundamental works of domestic and foreign authors on the problems of ensuring national security in the information sphere, taking into account the human factor.

In the process of research, the following methods of theoretical and empirical research were used: logical generalization – to determine the essence and role of the content and role of the cybernetic and human domains in terms of their interaction; analysis and synthesis – to study the essence, content and features of human interaction (human domain) in the processes of ensuring national security, as well as to formulate a hypothesis about the central role of the human domain in ensuring national security in modern conditions; synergistic approach – in substantiating cross-domain synergy to military problems from the point of view of many domains, a comprehensive view of the enemy and the environment, logical generalization of results (formulation of conclusions).

Results. The scientific article identifies the need for a comprehensive consideration of the content and role of cybernetic and human domains in terms of their interaction (and obtaining cross-domain synergy) in solving problems and strengthening the capabilities of ensuring national security in the information sphere. It is found that cyberspace is an end-to-end global domain in the information environment, consisting of an interdependent network of information technology infrastructure, including the Internet, telecommunications networks, computer systems and embedded processors and controllers.

The central role of human interaction (human domain) in all processes of ensuring national security and the need to influence target individuals and groups better than it is carried out by the enemy are defined. It is substantiated that the creation of cross-domain synergy requires an approach to military problems from the point of view of many domains, a comprehensive view of the enemy and the environment, an understanding of the available capabilities and the integration of these capabilities, in particular: assessment of the enemy's military potential, understanding of the human factor, arising from cultural, ideological and political motivations that form the intentions and actions of the enemy. It has been established that it is equally important to understand the physical environment and other factors that influence decision-making in defense and security

processes.

It is determined that expanding the boundaries of security thinking to encompass interagency perspectives builds trust and shared understanding of the needs to address the challenges of joint operations in a broader interagency and multinational context.

Prospects. In further scientific research, it is proposed to focus on the formation of an intersystem approach to managing the interaction of national security entities in the information sphere with the subjects of the external environment. This is the theoretical basis for expanding the boundaries of managerial influence, covering interagency perspectives, which strengthens trust and a common understanding of the needs for solving the problems of joint operations in a broader interagency and multinational context.

Key words: *national security, the concept of Human Domain, cybersphere, information space, strategic communications, cross-domain synergy.*

Постановка проблеми. В сучасних умовах в середовищі безпеки та оборони більша частина західної теорії все ще зосереджена на фізичних сферах (повітря, море, земля та космос) та кіберсфері, але у XXI столітті стратегічна перевага з'явиться завдяки тому, як налагоджена взаємодія з людьми та розуміння їх інтересів, а також доступ до політичних, економічних і соціальних мереж для досягнення відносної переваги, яка доповнює військову міць. Зазначені умови породжують нові загрози та можливості в різних аспектах національної безпеки. Тому актуалізується загальна проблема дослідження змісту та практики застосування в сфері національної безпеки положень інноваційної концепції людського домену.

Аналіз останніх досліджень і публікацій. Різні аспекти проблеми застосування людського чинника у безпекових дослідженнях через призму концепції людського домену останнім часом здійснювалися, переважно у закордонних дослідженнях. Американські фахівці Ф. Хофман (Frank

Hoffman), М. Девіс (Michael C. Davies) [1] досліджують фундаментальну природу війни та еволюцію характеристик сучасного конфлікту, які є під впливом людської динаміки. До американської наукової школи людського домену можна віднести також роботи Ч. Клівленда (Charles T. Cleveland), Д. Ігла (Daniel Egel) [2], якими введено поняття людського домену в сферу оборонних досліджень; О.Бранча (Austin Branch), Е. Кардона (Ed Cardon), Д. Еліса (Devin Ellis) та А. Рассела (Adam Russell) [5], які аналізують можливості врахування людського чинника у безпекових дослідженнях, а також ризики ігнорування людського надбання. В роботі Р. Чалдіні (Robert Cialdini) [6] аналізуються чинники здійснення ефективного впливу в людській сфері в контексті концепції людського домену, а в роботах В. Одома (William O. Odom) та К. Хейеса (Christopher D. Hayes) [7] вперше поставлено питання кросс-доменної синергії. Різні аспекти застосування сучасних підходів до забезпечення інформаційної безпеки проілюстровано на прикладі особливостей формування безпекових стратегій у взаємовідносинах США та Китаю в роботах Демпсі М.Е. (Dempsey M.E.) [9], Фергюсона М.П. (Ferguson M.P.) [10], Крістенсена, Т. Я. (Christensen T. J.) [11], Мазара М.Дж. (Mazarr M.J.) [12], Сімона Л. (Simón L.), Десмаеле Л. (Desmaele L.), Беккера Ж. (Becker J.) [13], Лоулесса С. (Lawless S.) [14], Сівана М. Кана (Ciwan M. Can) [15] тощо.

Виділення невирішених раніше частин загальної проблеми. Водночас, недостатньо розглянутими залишаються питання формування міждоменної синергії, зокрема взаємодії кіберсфери та людського домену, як наскрізних глобальних доменів в інформаційному середовищі національної безпеки.

Метою статті є визначення змісту та ролі кібернетичного та людського доменів з точки зору їх взаємодії (та отримання міждоменної синергії) у вирішенні проблем та посиленні можливостей забезпечення національної безпеки в інформаційній сфері.

Виклад основного матеріалу дослідження. Поняття «людський домен» уведене у 2010 році генерал-лейтенантом США у відставці Чарльзом Клівлендом [2], акцентує увагу на людях — їхніх переконаннях, їхніх мережах, їхніх цінностях — як на центрі тяжіння в сучасному світі національно-державної конкуренції. Незважаючи на те, що боротьба за когнітивний і соціальний вплив така ж давня, як історія військової думки, людська сфера знову привернула увагу вчених, політиків і оперативних спільнот.

Концепція людського домену ґрунтується на визначенні нової сфери конкуренції – людської сфери. При цьому, саме взаємодії являють собою мережу, що визначає владу та інтереси у взаємопов'язаному світі. Держава, яка найкраще розуміє місцеві контексти та будує мережу навколо відносин, використовуючи місцевий потенціал, має більше шансів виграти боротьбу у 21 столітті. У цьому взаємопов'язаному світі, навіть частіше, ніж раніше, вирішальна битва відбудеться ще до того, як пролунає перший постріл, оскільки актори змагаються, щоб посилити внутрішні розбіжності та розвинути ключові партнерства.

Зокрема, у Білій книзі армії США від 2012 року стверджувалося, що «успіх майбутніх стратегічних ініціатив і здатність США формувати мирне і процвітаюче глобальне середовище все більше і більше залежатиме від нашої здатності розуміти, впливати або здійснювати контроль в рамках «людського домену» [3]. Якщо домінування в традиційних сферах ведення війни передбачає контроль над фізичним простором (забезпечення безпеки та утримання певної території; контроль морських шляхів сполучення; захист повітряного простору), то зі створенням п'ятої сфери ведення бойових дій у доктрині США – кіберсфери, домінування більше не визначається контролем тільки фізичного простору. На відміну від суші, моря, повітря і космосу, кіберсфера не є фізичною, її бойове поле значною

мірою віртуальне і тому не може бути обмежене та контрольоване, як морські шляхи, повітряний простір або конкретна місцевість.

Людська сфера все більше привертає увагу і набуває значення в контексті конкуренції великих держав протягом останнього десятиліття, особливо це стосується росії та Китаю, які дедалі активніше впливають, зокрема, на сили США, Європи, американську та європейську громадськість, безпосередньо, за допомогою тактики м'якої сили, маючи намір посіяти розбрат і підірвати демократію. Про російську концепцію інформаційної війни написано багато, в 2013 році росія створила організаційну структуру для реалізації цих концепцій, Китай також створив відповідні допоміжні організаційні структури.

Крім того, потужність дезінформації, що підживлюється штучним інтелектом (ШІ) і новими технологіями, також становить широку загрозу національній безпеці, і, отже, важливо, щоб вище керівництво країни могло представляти вимоги, відстоювати рішення, вести переговори тощо.

Значна частина зовнішніх загроз, що впливають на різні сфери національної безпеки, реалізуються через інформаційний простір, через цілеспрямовану дію на інформаційне середовище держави в цілому та сектор безпеки й оборони зокрема. Наприклад, щоб усунути конкурента з міжнародного ринку військової техніки, вдаються до поширення у світових засобах масової інформації чуток про ненадійність його як торговельного партнера, про причетність його до незаконної торгівлі зброєю, про сумнівність задекларованих ним тактико-технічних характеристик самої техніки тощо.

Умовами та чинниками, що сприятимуть формуванню ефективних механізмів протидії дезінформації та інформаційним операціям агресора/конкурентів є наступні:

- з точки зору положень підходу до людського домену, найефективнішим способом впливу на людську сферу в сучасних умовах є

побудова «мережі мереж», тому що коротка, цілеспрямована операція з впливу навряд чи матиме довготривалий вплив на спільноту. Натомість, як зауважив генерал Стенлі Маккрістал [4], потрібна мережа, щоб перемогти мережу — зокрема, супротивники США стратегічно будували мережі дезінформації в просторах стратегічного інтересу, щоб впливати на людську сферу;

- для зміни балансу сил в інформаційному просторі, держава має *залучати зацікавлені сторони за межами оборонної сфери*. Оскільки ворожі спроби вплинути на людську сферу спрямовані на соціальні розбіжності та підривають демократичні інститути, то громадські організації та лідери громадянського суспільства, які мають довіру громадськості, теж мають бути залучені;

- вкрай важливі *відносини з приватним сектором, міжнародними партнерами та впливовими неурядовими організаціями*, оскільки їхні інтереси часто перетинаються з питаннями глобальної та національної безпеки. Кампанії обміну повідомленнями з метою дискредитації джерел дезінформації мають координуватися між секторами та визначати наскрізні теми та контент, який привертає увагу ширшої глобальної аудиторії. Зрештою, щоб перемогти ворожі мережі дезінформації, націлені на людську сферу, потрібна велика, інклюзивна та глобальна мережа [5];

- *значну роль відіграють технології та їх відношення до людей*, оскільки технології змінили спосіб, у який люди беруть участь у війнах, і відкрили нові сфери ведення бойових дій, останнім часом космічну та кіберсферу. Більше того, глобалізація, спричинена прогресом в інформаційних технологіях, об'єднала людей новими способами, у тому числі для конфліктів. Кіберсфера, зокрема, стала новою сферою ведення війни, яка не існувала б без інновацій в інформаційних технологіях. Крім того, відношення людини до інформації є ще одним важливим фактором для її динамічного впливу на людську сферу. Інформація, продукт діяльності

людини, особливо важлива для її здатності формувати сприйняття, переконань і поведінки;

- *нещодавні інновації в соціальних медіа,* що посилили вплив, який інформаційні технології мають на людське мислення та поведінку. Крім поширення інформації, створеної досягненнями в галузі інформаційних технологій, важливо також відзначити, що «низькотехнологічні» засоби поширення інформації залишаються актуальними і сьогодні. Зокрема, чутки, «пошепки», плітки та повідомлення з вуст в уста можуть бути особливо важливими в селах і районах з обмеженими технологіями, але все ще залишаються аспектом сучасного суспільства.

Для здійснення ефективного впливу в людській сфері дослідники Концепції людського домену пропонують враховувати кілька важливих міркувань:

по-перше, важливо знати, якого бажаного ефекту від своєї цільової особи або групи хотіла б сторона, що втручається. Якщо орган, що втручається, вимагає конкретних дій і обмежений у часі, то примус для досягнення відповідності може бути найкращим способом дій. Однак, якщо влада, що втручається, хоче створити тривалий вплив на групу, державу, регіон або своїх лідерів, то це займе час, тоді побудова відносин і довіри стає першорядним. Застосування сили за таких обставин, якщо воно не збалансоване в рамках ширшої мети – розбудови тривалого впливу, може бути контрпродуктивним;

по-друге, метою впливу є зміна поведінки, проте засоби, за допомогою яких це можна зробити, відрізняються. Зокрема, кампанії з дотримання вимог змінюють поведінку без зміни переконань, конформізм – змінює поведінку підсвідомо за допомогою сигналів навколишнього середовища, конверсія – змінює поведінку через зміну переконань. При конформізмі і, особливо, конверсії – зміни в поведінці мають бути довготривалими (якщо не постійними), тому що соціальні сигнали і переконання, які керують

поведінкою, були змінені. Тому зміни можуть зайняти більше часу, але вони також тривають довше;

по-третє, зміна поведінки лише в людській сфері є досяжною метою для військових, що втручаються, особливо через силову погрозу або її застосування. Однак трансформація базових переконань з метою тривалих змін у поведінці, швидше за все, вимагатиме комплексного підходу уряду. Зокрема, заохочення можуть надходити у формі допомоги, торговельних угод, військових консультацій або інших форм впливу, які вимагають від різних органів влади – не лише військових – які працюють разом для досягнення однієї мети [6].

по-четверте, у більшості випадків кампанії впливу, спрямовані на здійснення більшого, ніж тимчасові зміни, результату, вимагають часу та послідовних зусиль. Для проміжних зусиль нереалістично розраховувати на побудову надійних і довірчих відносин – вимоги до тривалого впливу – без витрат часу і послідовної взаємодії з цільовим індивідом або групою. Більше того, використання сили для впливу в короткостроковій перспективі може бути контрпродуктивним для довгострокових відносин довіри та впливу.

Таким чином, уряду і військовим може знадобитися знайдення компромісу в досягненні короткострокових і довгострокових цілей щодо зміни поведінки в людській сфері (див. рис. 1).

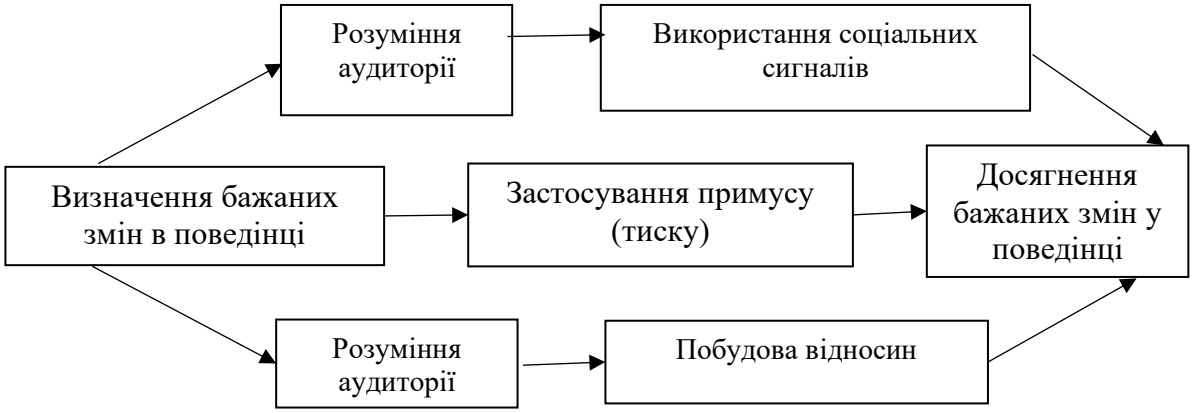

Рис. 1. Три шляхи інформаційного впливу для зміни поведінки людини

Джерело: складено авторами на основі [7]

Здійснення впливу для зміни поведінки, що є метою в людській сфері, потребує ресурсів. Одним із найкорисніших та ефективних інструментів збройних сил країни є ресурси, спрямовані на формування та поширення інформації. Інформаційні операції та ІПСО, за умов їх правильного використання, можуть допомогти у створенні відповідних інструкцій, що формують поведінку, зокрема:

по-перше, як і у випадку з усіма кампаніями впливу, інтервенційні сили мають знати, якого типу поведінки вони хочуть від своєї цільової аудиторії для створення ефективної програми;

по-друге, всі форми повідомлень від різних відомств уряду повинні надсилати одне й те саме повідомлення, щоб запобігти плутанині;

по-третє, повідомлення також повинні мати культурний сенс, месенджеру потрібно довіряти. Зокрема, в країнах, де державам, що втручаються, не довіряють, може бути краще і навіть необхідно працювати через месенджерів на місцях для формування потрібної поведінки.

В сучасних умовах, коли багато із загроз неможливо стримати і надзвичайно важко від них захиститись, підвищується цінність винахідливого формування, на свою користь, стратегічного середовища на випередження, нав'язуючи супротивнику дилеми і ризик ескалації. Інструментарій для цього має охоплювати заходи із комплексного застосування військ, включно з планами розвитку, навчання і демонстрації сили, *стратегічними комунікаціями,* розробкою концепцій, фінансуванням розвитку сил і засобів, моделюванням і тренуванням, а також штабними навчаннями. Для цього потрібно використовувати широку і розмаїту мережу партнерів (країн, промисловості, академічних кіл), мережу науковців, а також центрів передового досвіду з питань трансформації.

Покращення цієї співпраці залежить від розгляду безпекових проблем із всеосяжної междоменної перспективи, а не тільки через призму окремої

служби. Щоб здійснити цю зміну фокусу, в роботі [8] визначається міждоменний синергізм як центральна ідея в сучасних умовах.

У безпековому застосуванні міждоменна синергія досягається, коли інтегроване використання можливостей землі, моря, повітря, космосу, кіберпростору, та/або людської взаємодії (використання двох або більше доменів для досягнення переваги) дає сукупний ефект, більший, ніж сума окремих ефектів [8]. Це часто передбачає застосування можливостей з однієї сфери до іншої з головною метою покращення оперативної продуктивності та зменшення непотрібного резервування об'єднаних сил безпеки та оборони.

Висновки і перспективи подальших напрацювань. Отже, міжнародний досвід у сфері безпеки та оборони свідчить про застосування таких областей (доменів), як: суша, море, повітря, космос, кіберпростір та людина. Фізичний простір розмежовує сухопутний, морський, повітряний і космічний домени з фізичними характеристиками кожного, що визначає відносні можливості та вразливість дій, що відбуваються в них. Кіберпростір – це наскрізний глобальний домен в інформаційному середовищі, що складається з взаємозалежної мережі інфраструктур інформаційних технологій, включаючи Інтернет, телекомунікаційні мережі, комп'ютерні системи та вбудовані процесори та контролери.

Центральну роль у діяльності в сфері безпеки та оборони відіграє людська взаємодія (людській домен). Подібно до кіберсфери, людська сфера також містить виклики для виявлення та вимірювання безпекових цілей. Тому безпековою метою в людській сфері має бути вплив на неї, а домінуванням у людській сфері є набуття здатності впливати на цільових осіб і груп краще, ніж супротивник.

Створення міждоменної синергії вимагає підходу до безпекових проблем з точки зору використання багатьох доменів. Це передбачає формування комплексного уявлення про супротивника та оточення,

розуміння наявних можливостей та інтеграцію цих можливостей. У військовій сфері знання ворога стає необхідною умовою ефективних військових дій і досягнення синергії в діях проти нього. На додаток до оцінки військового потенціалу супротивника, оборонний істеблішмент повинен краще розуміти людські фактори, що випливають з культурних, ідеологічних і політичних мотивацій, які формують наміри та дії противника. Не менш важливим є розуміння фізичного середовища та факторів, які впливають на рішення учасника бойових дій.

Подальше розширення безпекового мислення з метою охоплення міжвідомчих перспектив, що зміцнює довіру та спільне розуміння потреб для вирішення завдань спільних операцій у більш широкому міжвідомчому та багатонаціональному контексті з використанням міжсистемного підходу є **напрямом подальших досліджень** у цієї сфері.

Література

1. Hoffman F., Davies M.C. Joint Force 2020 and the Human Domain: Time for a New Conceptual Framework? URL: https://www.academia.edu/6105175/Joint_Force_2020_and_the_Human_Domain_Time_for_a_New_Conceptual_Framework? (дата звернення: 21.11.2024).
2. Cleveland Ch.T., Egel D. The American Way of Irregular War. An Analytical Memoir. RAND Corporation, Santa Monica, Calif. USA, 2020. 245 p.
3. Army White Paper-2012. The Army Civilian Corps – A Vital Component of the Army Profession. URL: https://dml.armywarcollege.edu/wp-content/uploads/2023/01/Army-Civilian-Corps-A-Vital-Component-of-the-Prof-2012.pdf (дата звернення: 21.11.2024).
4. Маккрістал С., Коллінз Т., Сильверман Д., Фассел К. Команда команд. Нові правила взаємодії у складному світі; пер. з англ. А. Жищинської. 4-те вид. Харків: Моноліт, 2024. 384 с.

5. Branch A., Cardon E., Ellis D., Russell A. We ignore the human domain at our own peril. URL: https://mwi.westpoint.edu/we-ignore-the-human-domain-at-our-own-peril/ (дата звернення: 21.11.2024).

6. Cialdini R. Influence: The psychology of persuasion. New York, NY: Harper Collins. 2006. 81 p.

7. Gregg H.S. The Human Domain and Influence Operations in the 21st Century. *Special Operations Journal*. 2016. 2. P. 92–105, URL: https://core.ac.uk/download/pdf/81224395.pdf (дата звернення: 21.11.2024).

8. Odom W.O., Hayes Ch.D. Cross-Domain Synergy. Advancing Jointness. Joint Force Quarterly. *National Defense University Press*. URL: https://ndupress.ndu.edu/Media/News/News-Article-View/Article/577517/cross-domain-synergy-advancing-jointness/. (дата звернення: 21.11.2024).

9. Dempsey M.E. The Future of Joint Operations: Real Cooperation for Real Threats. *Foreign Affairs*. June 20, 2013. URL: https://www.foreignaffairs.com/articles/united-states/2013-06-20/future-joint-operations (дата звернення: 25.11.2024).

10. Ferguson M.P. Strategic Imperative: A Competitive Framework for US-Sino Relations. *Strategic Studies Quarterly*. FALL 2021. Vol. 15, No. 3. P. 48-68.URL: https://www.jstor.org/stable/48618296 (дата звернення: 25.11.2024).

11. Christensen T. J. No New Cold War Why US-China Strategic Competition will not be like the US-Soviet Cold War. *Asan Institute for Policy Studies.* 2020. URL: https://www.jstor.org/stable/resrep26078 (дата звернення: 25.11.2024).

12. Mazarr M.J. The Essence of the Strategic Competition with China. *PRISM*. 2020. Vol. 9, No. 1. P. 2-21. URL: https://www.jstor.org/stable/26940156 (дата звернення: 25.11.2024).

13. Simón L., Desmaele L., Becker J. Europe as a Secondary Theater? Competition with China and the Future of America's European Strategy. *Strategic Studies Quarterly*. SPRING 2021. Vol. 15, No. 1. P. 90-115.

14. Lawless S. American Grand Strategy for an Emerging World Order. *Strategic Studies Quarterly*. SUMMER 2020. Vol. 14, No. 2. P. 127-147.

15. Ciwan M. Can. Temporal Theory and US-China Relations. *Journal of Strategic Security.* 2022. Vol. 15, No. 2. P. 1-16. URL: https://www.jstor.org/stable/48682655 (дата звернення: 25.11.2024).

References

1. Hoffman F., Davies M.C. Joint Force 2020 and the Human Domain: Time for a New Conceptual Framework? URL: https://www.academia.edu/6105175/Joint_Force_2020_and_the_Human_Domain_Time_for_a_New_Conceptual_Framework?.

2. Cleveland Ch.T., Egel D. The American Way of Irregular War. An Analytical Memoir. RAND Corporation, Santa Monica, Calif. USA, 2020. 245 p.

3. Army White Paper-2012. The Army Civilian Corps – A Vital Component of the Army Profession. URL: https://dml.armywarcollege.edu/wp-content/uploads/2023/01/Army-Civilian-Corps-A-Vital-Component-of-the-Prof-2012.pdf.

4. Makkristal S., Kollinz T., Sylverman D., Fassel K. Komanda komand. Novi pravyla vzaiemodii u skladnomu sviti; per. z anhl. A. Zhyshchynskoi. 4-te vyd. Kharkiv: Monolit, 2024. 384 s. [in Ukrainian].

5. Branch A., Cardon E., Ellis D., Russell A. We ignore the human domain at our own peril. URL: https://mwi.westpoint.edu/we-ignore-the-human-domain-at-our-own-peril/.

6. Cialdini R. Influence: The psychology of persuasion. New York, NY: Harper Collins. 2006. 81 r.

7. Gregg H.S. The Human Domain and Influence Operations in the 21st Century. *Special Operations Journal.* 2016. 2. P. 92–105, URL: https://core.ac.uk/download/pdf/81224395.pdf.

8. Odom W.O., Hayes Ch.D. Cross-Domain Synergy. Advancing Jointness. Joint Force Quarterly. *National Defense University Press*. URL: https://ndupress.ndu.edu/Media/News/News-Article-View/Article/577517/cross-domain-synergy-advancing-jointness/.

9. Dempsey M.E. The Future of Joint Operations: Real Cooperation for Real Threats. *Foreign Affairs.* June 20, 2013. URL: https://www.foreignaffairs.com/articles/united-states/2013-06-20/future-joint-operations.

10. Ferguson M.P. Strategic Imperative: A Competitive Framework for US-Sino Relations. *Strategic Studies Quarterly.* FALL 2021. Vol. 15, No. 3. P. 48-68.URL: https://www.jstor.org/stable/48618296.

11. Christensen T. J. No New Cold War Why US-China Strategic Competition will not be like the US-Soviet Cold War. *Asan Institute for Policy Studies.* 2020. URL: https://www.jstor.org/stable/resrep26078.

12. Mazarr M.J. The Essence of the Strategic Competition with China. *PRISM.* 2020. Vol. 9, No. 1. P. 2-21. URL: https://www.jstor.org/stable/26940156.

13. Simón L., Desmaele L., Becker J. Europe as a Secondary Theater? Competition with China and the Future of Americas European Strategy. *Strategic Studies Quarterly.* SPRING 2021. Vol. 15, No. 1. P. 90-115.

14. Lawless S. American Grand Strategy for an Emerging World Order. *Strategic Studies Quarterly.* SUMMER 2020. Vol. 14, No. 2. P. 127-147.

15. Ciwan M. Can. Temporal Theory and US-China Relations. *Journal of Strategic Security.* 2022. Vol. 15, No. 2. P. 1-16. URL: https://www.jstor.org/stable/48682655.