Р.В. ГУЛА, О.П. ДЗЬОБАНЬ, І.Г. ПЕРЕДЕРІЙ,
О.О. ПАВЛІЧЕНКО, Г.О. ФІЛЬ

ІНФОРМАЦІЙНА ВІЙНА:

СОЦІАЛЬНО-ОНТОЛОГІЧНИЙ ТА МІЛІТАРНИЙ АСПЕКТИ

Монографія

КИЇВ 2020

УДК 355.01+327.8

Рекомендовано до друку Вченою радою Харківського національного університету Повітряних Сил імені Івана Кожедуба Протокол № 17 від 26 листопада 2019 р.

Рецензенти:

Бєлєвцева Вікторія Вікторівна − докторка юридичних наук, старша наукова співробітниця, завідувачка наукової лабораторії права міжнародної безпеки та протидії злочинам проти миру і безпеки людства НДІ інформатики і права НАПрН України.

Степико Михайло Тимофійович **−** доктор філософських наук, професор, Заслужений діяч науки і техніки України, головний науковий співробітник відділу гуманітарної політики Національного інституту стратегічних досліджень.

І74 Інформаційна війна: соціально-онтологічний та мілітарний аспекти : монографія / Р.В. Гула, О.П. Дзьобань, І.Г. Передерій, О.О. Павліченко, Г.О. Філь. – Київ : „Каравела”, 2020. – 288 с.

ISBN 978-966-2229-53-1

Монографія розкриває особливості інформаційного протиборства у постмодерному суспільстві. Проаналізовано сучасні тенденції трансформації концепцій інформаційної війни у воєнній теорії. Розкрито особливості сучасних кіберзагроз. Висвітлені основні тенденції у військовому будівництві кібервійськ провідних держав світу. Запропоновано низку практичних рекомендацій для удосконалення системи національної безпеки в умовах інтенсифікації гібридних війн транснаціонального характеру.

УДК 355.01+327.8

Автори макету обкладинки В.Д. Гула, Р.А. Михайловський

ISBN 978-966-2229-53-1

Зміст

Перелік умовних скорочень

АІВ – акція інформаційного впливу

АЕС – атомна електростанція

ВМС – Військово-Морські Сили

ГЕС – гідроелектростанція

ГІР – глобальна інформаційна решітка

ГШ – Генеральний штаб

ЄІКП – єдиний інформаційно-комунікаційний простір

ЄС – Європейський Союз

ЗМІ – засоби масової інформації

ЗМК – засоби масової комунікації

ЗМУ – засоби масового ураження

ЗС – збройні сили

ЗСУ – Збройні Сили України

ІКТ – інформаційно-комунікаційні технології

ІПЗ – інформаційно-психологічна зброя

ІТ – інформаційні технології

ІУС – інформаційні управляючі системи

КБДІМ – командування бойових дій в інформаційних мережах

КБДКП – командування бойових дій у кіберпросторі

КСІО – командування спільних інформаційних операцій

КНР – Китайська Народна Республіка

МГП – міжнародне гуманітарне право

МО – Міністерство оборони, Міністр оборони

МОУ – Міністерство оборони України, Міністр оборони України

МП – морська піхота

МПЗ – морально-психологічне забезпечення

НАТО – Організація Північно-Атлантичного договору

НГШ – Начальник Генерального штабу

НЗФ – незаконні збройні формування

ОВТ – озброєння та військова техніка

ООН – Організація Об’єднаних Націй

ОСК – об’єднане стратегічне командування

ОФ – оперативний флот

ОЦЗЗІМ – оперативний центр забезпечення захисту інформаційних мереж

ПА – повітряна армія

ППО – протиповітряна оборона

ПС ЗСУ – Повітряні Сили Збройних Сил України

СКІЗ – сили кібероперацій та інформаційного забезпечення

РЕБ – радіоелектронна боротьба

РЛС – радіолокаційна станція

РФ – Російська Федерація

СВ ЗСУ – Сухопутні війська Збройних Сил України

СІО – спеціальна інформаційна операція

СК – стратегічні комунікації

СКбО – сили кібероперацій

СРСР – Союз Радянських Соціалістичних Республік

США – Сполучені Штати Америки

ТВД – театр воєнних дій

ТЗІ – технічний захист інформації

УНБ – управління національної безпеки

ФКІО – функціональне командування інформаційних операцій

ЦА – цільова аудиторія

ЦСР – центр спеціальних розробок

Остання війна серед людей буде війною за істину. Війна з власним невіглаством, агресією, роздратуванням. Лише докорінна зміна кожної окремої людини може стати початком мирного життя усіх людей.

М. Реріх

ВСТУП

У XXI ст. людство остаточно перейшло в нову епоху, яка характеризується зростанням обсягу інформації, телекомунікаційним розвитком, удосконаленням інформаційних технологій, вільним доступом до інформаційних ресурсів, глобалізацією, модернізацією та інформатизацією усього суспільства.

Системні протиріччя між традиційними підходами у воєнному мистецтві та сучасним трактуванням нового характеру війни є основною причиною нелінійного, суперечливого характеру розвитку драматичних подій на Сході нашої держави.

Тому дослідження інформаційних війн, процесу їх зародження та розвитку, форм прояву та методів реалізації цього надскладного соціально-політичного явища є надзвичайно актуальним. Сили і засоби інформаційної війни є основним ресурсом та інструментом досягнення геополітичного домінування на міжнародній арені. Зростаюча роль інформації у світі зумовлює актуальність захисту інформаційної безпеки як невід'ємної складової національної безпеки будь-якої високорозвиненої суверенної держави.

Процеси глобалізації та модернізації сформували унікальний феномен «віртуальної інформаційної політики» як реалізації та захисту національних інтересів у кіберпросторі, що в умовах стрімкого поширення новітніх інформаційних технологій вимагає побудови принципово нової ефективної інформаційної політики. У сучасному світі це є виключно прерогативою розвинених держав, а для інших учасників інформаційно-політичного простору існує загроза своєрідного інформаційного неоколоніалізму. Таким чином, виникає проблемна ситуація, обумовлена такими процесами: сучасний інформаційно-політичний простір одночасно в процесі глобалізації та тенденцій до інтеграції, уніфікації світу характеризується відкритою та прихованою інформаційною агресією, яка виявляється через множину форм й наслідків впливу на процес

формування нової соціальної моделі – інформаційного суспільства як основного суб'єкта здійснення інформаційного протиборства.

Перехід держави до інформаційного суспільства вимагає переосмислення, а в окремих випадках і розробки нових механізмів регулювання відносин, що виникають між громадянами, їх об'єднаннями та державою. Усі суб'єкти інформаційних комунікацій та відносин повинні усвідомлювати і виконувати свою роль у цьому процесі, але саме держава повинна активно впливати на ці трансформаційні процеси, залучати до співпраці політиків, науковців, практиків, громадськість. Світові тенденції розвитку суспільства і держави потребують не тільки удосконалення державного управління за допомогою його інформатизації, але і нової стратегії державного управління в період становлення та розвитку інформаційного суспільства.

На особливу увагу заслуговує така форма протиборства, як інформаційна війна, оскільки це явище деструктивно впливає на розвиток інформаційного суспільства та одночасно сприяє розвитку практично усіх пріоритетних сфер життя у світі. Технічний прогрес суттєво впливає на вирішення військових, торговельних, економічних конфліктів, внаслідок чого силові методи поступаються інформаційним. Усвідомлення грандіозного потенціалу впливу маніпулятивних технологій, що використовуються в інформаційних війнах, на світову політику, розвиток держав й суспільства вимагає проведення ґрунтовних досліджень цього явища.

Актуальність вивчення проблематики інформаційної політики України зумовлена завданнями наукового осмислення його як однієї з важливих детермінант зовнішньої та внутрішньої політики держави в контексті її оптимізації та ефективності. Врахування суб'єктивних чинників політики значно розширює рамки наукового аналізу й пошук нових теоретико-методологічних підходів до її аналізу. Незважаючи на надзвичайну важливість та актуальність забезпечення належного функціонування усіх сфер життєдіяльності людини, суспільства та держави, а також необхідність ефективного забезпечення інформаційної безпеки держави, зокрема через вироблення надійного механізму протидії інформаційним війнам, сьогодні, на жаль, повною мірою не визначені методологічні засади протидії інформаційним війнам. Навіть зважаючи на чималий досвід маніпуляції суспільною свідомістю в інформаційній війні, слід визнати, що наслідки застосування тих чи інших прийомів ведення ще недостатньо систематизовані. Особливо це стосується

використання для деморалізації суспільства різних ідеологій, коли їх впровадження в суспільну свідомість призводить до геноциду за етнічною, релігійною, расовою чи майновою ознакою.

Об'єкт дослідження – надскладне соціально-політичне явище «інформаційна війна» в сучасних реаліях глобалізованого світу.

Предмет дослідження – зміст, структура, особливості категорій «інформаційна війна», «інформаційна безпека», «інформаційна протидія» в їхньому розвитку та взаємодії.

Мета – комплексний теоретичний аналіз підходів до формування комплексного та інтегративного визначення досліджуваних феноменів, явищ.

Для досягнення поставленої мети необхідно вирішити комплекс ***основних наукових завдань***:

- провести порівняльний аналіз підходів, наукових концепцій до визначення сутності інформаційних війн;
- розкрити принципи, закони, закономірності, особливості, форми, методи, інструменти ведення інформаційних війн;
- визначити поняття «інформаційна зброя» та основні її види;
- визначити особливості ведення інформаційних війн різними суб'єктами та застосування ними інформаційної зброї в сучасних умовах;
- розкрити особливості трансформації форм і методів ведення інформаційної війни на сучасному етапі;
- висвітлити основні тенденції створення сил кібероперацій в провідних державах світу;
- визначити місце та роль інформаційної безпеки України в структурі національної безпеки України;
- розкрити сутність інституційного механізму протидії інформаційним війнам в Україні, визначити основні проблеми його функціонування.

Вибір методів дослідження є необхідною умовою об'єктивності ґрунтовності та комплексного характеру наукової праці. Тому ***методологія дослідження*** інформаційної війни – це систематизована сукупність принципів, підходів, категорій, методів, прийомів і процедур, використаних в процесі наукового пізнання для вивчення та аналізу основних напрямів історико-політичної та філософської, політологічної та соціологічної думки, що розкривають особливості зародження, розвитку, функціонування складових, форм, механізмів й інструментарію інформаційної війни як надскладного соціально-політичного явища.

Основою монографії є такі основні методологічні принципи:

1. *Об'єктивності*. Орієнтує на вивчення об'єктивних закономірностей, які визначають процеси розвитку. Кожне явище розглядають як багатогранне й суперечливе. При цьому вивчають всю систему чинників – позитивних і негативних. Об'єктивність передбачає, що процес дослідження відповідає дійсності та незалежним від людини законам пізнання.

2. *Діалектичності*. Визнання нелінійного розвитку сучасного інформаційного суспільства, глобального інформаційного простору, інформаційної війни та інформаційної протидії як основних якісних елементів дослідження, вивчення процесів формування цих явищ і феноменів у взаємозв'язку та взаєморозвитку, змінах, з урахуванням історичної перспективи їх трансформації.

3. Принцип *конвенціоналізму* став основою для формування системи поглядів на сучасні концепції та теорії воєн XXI ст., а також уможливив створення множини визначень понять і термінів, що становлять важливе підґрунтя для розуміння основоположних принципів та особливостей ведення воєн та протиборства у сучасному глобалізованому світі в умовах інформаційного суспільства.

Вибір **методології та методів дослідження** зумовлений складністю та міждисциплінарним характером предмета вивчення і поставленими завданнями, що потребує використання загальнонаукових, історичних, політологічних методів і підходів, а також методологічних засад філософії, соціології, психології, теорії комунікації, теорії міжнародних відносин.

Загальнонаукові підходи – ціннісний, синергетичний та концептуальний, які забезпечують взаємозв'язок філософського та спеціально-наукового знання. Це дало можливість орієнтації дослідження на вирішення широких наукових і гуманітарних завдань. Концептуальний підхід уможливив використання різногалузевих теорій до визначення предмета та об'єкта дослідження, дав можливість розглядати їх системно і комплексно.

Автори у дослідженні опиралися на *сукупність загальнонаукових методів* – дедукції та індукції, аналізу та синтезу, феноменологічної редукції, системного та логічно-семантичного, роздвоєння єдиного на протилежності, аналітичні методи контент-аналізу документів та публікацій в ЗМІ, івент-аналізу, а також ситуаційного аналізу.

Дедуктивний метод став основою дослідження для визначення загальних тенденцій діалектичного розвитку інформаційної війни як

загального, цілісного соціально-політичного явища, а також дефініції особливостей та форм його проявів.

Індуктивний метод використаний для дослідження поняття інформаційної війни як одиничного явища з притаманною йому специфікою, що впливає на його сутність.

Аналіз поняття інформаційної війни був здійснений через уявне розділення його на окремі складові при вивченні комплексу наукових підходів до вивчення цього явища.

Синтез у дослідженні передбачав об'єднання вивчених складових з метою узагальнення тенденцій їх розвитку та взаємозв'язку.

Метод феноменологічної редукції було застосовано з метою дослідження процесів впливу механізму й інструментарію інформаційної війни на формування образів держави, війни та ворога через використання інтенціональних актів свідомості.

Системний метод використано під час визначення суб'єктів ведення інформаційних воєн і вироблення ефективних механізмів боротьби з проявами інформаційних війн.

Логіко-семантичний метод, логічний метод сприяли поглибленому розкриттю сутності понятійного апарату дослідження.

Роздвоєння єдиного на протилежності. Значимим у дослідженні є методологічне дослідження протиріч та суперечностей як джерел і рушійної сили розвитку інформаційного суспільства. Через взаємодію поглядів на зміст інформаційного протиборства були визначені закони інформаційної війни.

Вибір *конструктивізму* як методологічного інструментарію для аналізу образів дає можливість розглядати інформаційну війну як основну форму суб'єктності в суспільному житті, зовнішній та внутрішній політиці; акцентувати увагу на партикуляризмі та соціальній, культурній й політичній унікальності кожної держави, які детерміновані об'єктивним історичним контекстом; на особливостях індивідуального і суспільного сприйняття образів держави, війни та ворога в ході організації й ведення інформаційної війни у глобальному інформаційному просторі.

Автори використали також *порівняльний метод* політології для порівняння ролі та місця політичних систем, режимів та ідеологій минулого і сучасності при організації та веденні інформаційних війн.

У дослідженні використано *синергетичний метод* політологічних досліджень. Синергетика визначає зміст поняття інформаційного суспільства на основі аналізу її властивостей – взаємопроникнення,

відкритості, самоорганізації, випадковості, наявності асиметричних структур, нерегулярності зв'язків і функціональної нестабільності.

За допомогою методологічного інструментарію соціології визначені основні категорії та методи дослідження інформаційного суспільства. Соціум як соціологічна категорія розглянутий у дослідженні як складна система функціонально пов'язаних між собою соціальних підсистем.

У монографії використано *спеціальні історичні методи* дослідження. *Історико-генетичний метод* дає змогу аналізувати динаміку історичних процесів. За допомогою цього методу у дослідженні розкрито логіку процесу розвитку, умови створення та удосконалення організаційно-штатної структури й трансформацію функціонального призначення сил кібероперацій ЗС США та провідних держав світу. *Метод актуалізації* на початковій стадії наукового пошуку дав можливість авторам сформулювати тему й мету дослідження. У поєднанні із загальнонауковим методом класифікації він сприяв визначенню основних напрямів вивчення теми дослідження.

Система методів *воєнних наук*, насамперед тактики, оперативного мистецтва та стратегії,, допомогла дослідникам у визначенні змісту таких фундаментальних понять, як «театр інформаційної війни» та «інформаційний театр воєнних дій».

Комп'ютерні технології сприяли використанню нових методичних прийомів дослідження джерел: оперативній систематизації усіх друкованих документів і матеріалів.

Науково-теоретичне підґрунтя монографії. У сучасних вітчизняних дослідженнях окремі теоретичні та практичні аспекти формування інформаційного суспільства і участі в цьому процесі держави розглядають В.Ю. Биков, О.В. Гриценко, В.Ф. Іванов, О.В. Литвиненко, Є.А. Макаренко, І.В. Огірко, Г.Г. Почепцов, В.П. Тронь, П.А. Цегольник, О.С. Шевчук, С.А. Чукут, В.І. Хомяков та інші. Визначенню фундаментальних понять, які характеризують інформаційне суспільство, присвячені роботи на основі концепцій постіндустріалізму закордонних авторів. Серед них слід зазначити ґрунтовний науковий внесок: Д. Бела, К. Вербаха, Р. Кана, Е. Кінга, І. Масуди, Т. Меррілла, М. Пората, Л. Робертса, К. Робінсона, Р. Реддіка, а також російських вчених І. Бачила, О. Вартанової, М. Вершиніна, В. Дрожжинова, Т. Єршової, А. Мелюхіна, А. Ракітова, А. Соколова, А. Урсула, А. Штрика, Ф. Широкова та ін.

Вивченню сутності глобального інформаційного простору

присвячені праці Р. Арона, Зб. Бжезинського, О. Тофлера, М. Кастельса. Серед вітчизняних авторів особливо слід відзначити праці В.П. Андрущенка, О.О. Базалука, О.Г. Бахтіярова, В.М. Бебика, А.Ф. Гуцала, О.В. Зернецької, В.Ф. Іванова, Є.А. Макаренка, які вивчають проблеми, пов'язані з тенденціями функціонування глобального комунікативного простору, визначенням місця й ролі вітчизняних комунікативних структур і технологій у цьому процесі. Окрім того, сучасна українська політична думка дедалі більше зближується з практикою політичного керування й управління, зосереджує увагу на дослідженнях практично значимих інформаційних аспектів національної безпеки. Тому основою монографії стали праці вітчизняних вчених, які розглядали окремі інформаційні аспекти забезпечення національної безпеки України, – О.В. Литвиненка, М.А. Ожевана, Г.Г. Почепцова, О.В. Сосніна та інших.

Наукові праці фахівців у галузі філософії, політології, загальної теорії держави та права, теорії управління, інформаційного права та безпекознавства В.П. Горбуліна, О.Г. Данільяна, О.П. Дзьобаня, О.В. Курбана, О.С. Ліпкана, Ю.Є. Максименка, В.Л. Манілова, О.В. Манойла, Н.Р. Нижник, Д.М. Овсяника, В.В. Остроухова, І.Н. Панаріна, В.М. Петрика, Г.Г. Почепцова, В.Ф. Прокоф'єва, Г.П. Ситника, О.Ф. Скакун, Ю.М. Старилова, В.А. Тихонова, М.П. Требіна, Л.С. Харченка, А.О. Фісуна, Д.Б. Фролова, Ю.С. Шемчученка, В.С. Цимбалюка, О.К. Юдіна та ін. стали науковим підґрунтям для поглибленого вивчення проблем розкриття змісту та сутності інформаційного протиборства й інформаційних воєн. Варто також виокремити низку спеціальних монографічних праць російських, європейських та американських авторів з проблематики інформаційних війн, пропаганди та спеціальних інформаційних операцій С. Зуєва, Г. Ємельянова, А. Левакова, С. П. Расторгуєва, Дж. Арквилли, Д. Кюля, Р. Моландера, Дж. Ная та інших. До джерельної бази також увійшли праці іноземних науковців, які розглядали окремі аспекти ідеї «суспільства ризику», У. Бека, К. Дейка, М. Дугласа, А. Гидденса, С. Кирша, Ф. Найта, Н. Луманна. Особливості трансформації інформаційної війни у концепції «мережецентричної», «гібридної», «консцієнтальної» та «преемптивної» воєн розкриті у працях Дж. Гарстки, Д. Альбертса, Фр. Стейна, А. Себровські, Ф. Хофмана, Ю. Громика, Ю. Крупнова, Н. Комлєвої, В. Макарова. Окремі аспекти теорії національної безпеки розроблялись Т. Шелінгом і Г. Каном (теорія міжнародних

конфліктів); Р. Лиска і Г. Снайдером (теорія блоків та коаліцій); К. Норром (теорія потенціалу держави); Зб. Бжезинським (геостратегічні моделі); Е. Люттваком і М. Портером (міжнародна економічна конкуренція) та ін.

Аналіз наукових досліджень і публікацій науковців О.Л. Морозова, В.А. Ліпкана, О.М. Тетерича, Н.М. Кострицi та інших свідчить про ґрунтовні аналітичні розробки стосовно змісту інформаційних загроз і побудови системи захисту та протидії інформаційному впливу.

Питання інформації та державного управління, взаємозв'язків держави та інформаційної сфери частково розглядали філософи, теоретики права, державознавці, економісти, соціологи, кібернетики. Особливо слід підкреслити внесок у розробку цієї проблеми вчених В.Б. Авер'янова, І.В. Арістової, Г.В. Атамчука, О.М. Бандурки, І.Л. Бачила, Д. Бела, А.І. Берга, Ю.П. Битяка, М.С. Вертузаєва, В.М. Глушкова, П. Джонстона, Ф.Є. Емері, В.В. Зуя, Р.А. Калюжного, М. Кастельса, Ю.М. Козлова, А.П. Коренєва, В.Д. Малкова, В.Г. Машликіна, Дж. Міллера, В.А. Мінаєва, В.С. Михалевича, А.М. Омарова, В.Ф. Опришко, Г.І. Петрова, Н.С. Полєвого, Г.Х. Попова, К. Прибрама, Р. Сассерінда, Е.П. Семенюка, І.В. Сергієнка, Д.Н. Узнадзе, А.Д. Урсула, М.Я. Швеця, Г.В. Щьокіна, В.В. Цвєткова, Л.П. Юзькова та інших. Теоретичні засади взаємозв'язку проблем розбудови суверенітету новоутворених пострадянських держав з питаннями інформаційної безпеки достатнім чином досліджено у працях І.Н. Панаріна, Г.Г. Почепцова, М.А. Ожевана.

Наукова новизна дослідження визначається тим, що автори виділяють у самостійний об'єкт наукового вивчення поняття інформаційної війни, яке досліджується з позицій сьогодення як комплексна категорія при нелінійному характері розвитку цього надскладного соціально-політичного явища. Запропоновано авторський теоретико-методологічний підхід до класифікації і вивчення ґенези інформаційної війни та інформаційного протиборства. Вперше введено в науковий обіг такі поняття: «театр інформаційної війни» та «інформаційний театр воєнних дій» та ін. Автори сформулювали визначення категорійного апарату предмета дослідження та запропонували нову систему його принципів, законів, закономірностей.

Науково-практичне значення полягає в тому, що отримані результати дослідження дають можливість сформувати нове, синтезоване та комплексне знання та поглиблене уявлення про

ґенезу, природу, розвиток і трансформацію соціально-духовного явища інформаційної війни. Запропонований авторами комплекс практичних рекомендацій допоможе органам військового управління в реалізації питань адміністративно-правового, ідеологічного та організаційно-розпорядчого забезпечення у процесах створення ефективної системи інформаційної протидії. Висновки служать історичним уроком необхідності своєчасного вибору напрямів і пріоритетів у формуванні системи консолідуючих концептів ідентифікації нації як носія відповідних констант патріотичної свідомості в умовах інтенсифікації процесів інформаційного впливу з боку держав-ворогів і держав-конкурентів. Комплекс практичних рекомендацій, запропонований авторами, не претендує на істину в останній інстанції та може бути предметом конструктивного дискурсу з метою досягнення конкретних результатів у підвищенні обороноздатності нашої держави. Розроблена і апробована в процесі роботи над монографією дослідницька методологія може бути використана в процесі дослідження траєкторій динамічного розвитку та трансформації інформаційних воєн у XXI ст.

РОЗДІЛ 1. ГЛОБАЛЬНИЙ ІНФОРМАЦІЙНИЙ ПРОСТІР – ПОЛЕ ГІБРИДНОГО ПРОТИБОРСТВА

Сьогодні ... світ – це швидко зникаюча ситуація.

Е. Тофлер

У другій половині XX ст. розпочалися глобальні процеси трансформації суспільства: перехід від індустріальної до інформаційної (постіндустріальної) фази організації системи суспільних відносин. Основою функціонування суспільства стала розгалужена інформаційна структура, сформована за принципами виробництва, обробки, збереження, трансформації та використання інформації. Потужний вплив інформаційних технологій на сферу соціально-політичних відносин став причиною дезінтеграції класичної класової структури суспільства. З'явилися нові критерії оцінки соціально-політичних відносин, які характеризуються відносинами щодо виробництва, передачі і використання інформації. Сьогодні людство перебуває на стадії становлення глобального інформаційного простору, формування суспільства цивілізаційних змін, революційною ознакою якого є використання інформації як засобу досягнення бажаної мети.

Фундатором концепції «інформаційного суспільства» можна вважати Ф. Махлупа, який ще у 1933 р. вводить поняття «індустрія знань»[1], яка виробляє «розумний продукт» для задоволення потреб соціуму, це акцентувало увагу на зростаючій ролі інформації і знань в економіці. Виникнення самого терміна «інформаційне суспільство» пов'язують з тенденціями в японській соціології 60-х рр. XX ст. та теорією «постіндустріального суспільства» Д. Бела[2], яку згодом вчений вже у 1980-х рр. трансформує в «інформаційне суспільство».

Необхідно зауважити, що у філософському та повсякденному дискурсі концепції постіндустріального та інформаційного суспільства вважають тотожними. Хоча окремі науковці розмежовують ці поняття за певними ознаками, Д. Бел підкреслює, що термін «постіндустріальне суспільство» більш точний, ніж «суспільство знань», тобто «інформаційне суспільство». Він відображає процес «швидкої ерозії…старих суспільних відносин (які засновані на власності), владних структур (що сконцентровані на

[1] Махлуп Ф. Производство и распространение знаний в США. – М., 1966.

[2] Daniel Bell. The Coming of Post' Industrial Society: A Venture in Social Forecasting. Harmonds worth: Penguin, Peregrine, 1973 [Електронний ресурс]. – Режим доступу: http://www.worldcat.org/title/coming-of-post-industrial-society-a-venture-in-social-forecasting/oclc/16377221

вузьких елітах) і буржуазної культури (сформованої на принципах економії та відкладеного задоволення)»[3]. Г. Блажиєвська підкреслює універсальний характер та теоретичну базу концепції постіндустріального суспільства, завдяки чому виникає підпорядкування їй концепції інформаційного суспільства[4].

Друга половина XX ст. характеризується переходом до інформаційного суспільства, що спровокувало появу потужного дискурсу в філософській, соціологічній, політологічній та економічній науках, на основі системного переходу від позитивістських, технократичних, матеріалістичних концепцій трактування суспільного поступу. Фундаментальні основи цих форм наукового пізнання обумовив комплекс визначених тенденцій – «постіндустріальне суспільство характеризується трьома основними рисами: зміщення центру тяжіння в економічній діяльності від виробництва товарів до виробництва послуг; провідна роль професій, пов'язаних з високою насиченістю знаннями та інформацією»[5].

Загалом науковці визначають «***інформаційне суспільство»*** як спільноту, в якій основним предметом праці для більшої або значної частини людей є інформація та знання, а знаряддям праці – інформаційні технології.

Існують наукові *підходи* до трактування ***сутності*** цього надскладного соціально-культурного явища й феномену, що акцентують на його окремих характеристиках.

Цивілізаційний підхід розглядає процес виникнення, становлення та розвитку інформаційного суспільства в динаміці та історично-просторовому континуумі. Інформаційне суспільство є результатом цивілізаційного розвитку, який полягає в збільшенні масштабів створення, накопичення, передачі, трансформування інформації в суспільстві, а також у впливі новітніх інформаційно-комунікаційних технологій на економіку політику, культуру та науку.

Наукове обґрунтування Д. Белом доіндустріального, індустріального, постіндустріального суспільства, С. Лешем і С. Круком – передмодерністського, модерністського, постмодерністського етапів соціального розвитку, Р. Інглегартом –

[3] Белл Д. Грядущее постиндустриальное общество: Опыт социального прогнозирования. – М., 2004.

[4] Блажиевская Г.А. Труд как социально-культурная ценность: дисс. … канд. филос. наук: 24.00.01. – Казань, 2007. – С. 89.

[5] Гриценко В.С. Труд в постиндустриальном обществе: автореф. дисс. … канд. филос. наук: 09.00.11 / [место защиты: ФГБОУ ВПО «Пермский государственный национальный исследовательский университет»]. – Пермь, 2012. – С. 3.

модернізації та постмодернізації призвело до розвитку теорії інформаційного суспільства в межах цивілізаційного підходу.
Ф. Фукуяма, А. Турси, Ж. Бодіяр, Ж. Ліотар, К. Попер вважали, що «інформаційне суспільство» – це особливий вид суспільної формації пізніх різновидів постіндустріального суспільства, нового етапу розвитку цивілізації.

На нашу думку, Е. Тофлеру належить найвагоміший внесок у розробку основ цивілізаційного підходу. Е. Тофлер розглядав історію людства як наслідок виникнення «трьох хвиль» цивілізації. Перша хвиля – «сільськогосподарська цивілізація», основою якої була взаємодія людини та природи. Друга хвиля, утвердивши взаємодію техніки та природи, започаткувала індустріальну цивілізацію. Третя хвиля порушила питання пристосування людини до потоку інформації та швидких змін техніки у взаємовідносинах «техніка – інформація – людина» постіндустріальної цивілізації. Саме Третя хвиля обумовила появу нової системи відносин, цінностей, типів комунікації, способів і механізмів збереження, трансформації та передачі інформації, нових форм взаємодії у техногенному світі. Прогнозуючи розвиток цього комплексу системних трансформацій, Е. Тофлер визначає його наслідком створення нової форми постіндустріальної цивілізації Третьої хвилі – «інформаційного суспільства»[6].

За Е. Тофлером, характерними особливостями інформаційного суспільства цього типу є: пріоритетність інформації, що є «сировиною для цивілізації Третьої хвилі»[7]; інформаційна єдність людської цивілізації, результатом якої є «можливість бачити себе частиною великої... космічної системи»[8]; здатність до «забезпечення максимальної різноманітності та персональних інформаційних запитів»[9] з вільним доступом до інформаційних ресурсів; індивідуалізація життя суспільства, що веде до «нових рівнів соціального та політичного різноманіття»[10].

У цьому контексті на особливу увагу заслуговує ідея про виникнення нових загроз для суспільно-політичних систем сучасності, що обумовлені вищенаведеними особливостями інформаційного суспільства. Небезпеку становлять сили, що активізувалися у час трансформацій: релігійний фундаменталізм;

[6] Тофлер Е. Третя Хвиля. – К., 2000.
[7] Тоффлер Э. Третья волна. – М., 1999. – С. 572.
[8] Там само. – С. 592.
[9] Там само. – С. 561.
[10] Там само. – С. 647.

екологічні екстремістські рухи («Екотеократія») і ксенофобія[11]. Нерівномірність поширення інформації та знань у глобальному просторі, а також доступу до них, фрагментують суспільства, маргіналізують окремі верстви населення, руйнують поняття громадянського суспільства та загрожують демократії загалом. Демократія опирається на масову підтримку, а сучасна «демасовізація», розділення суспільства на окремі групи за інтересами, творять нову «мозаїчну демократію», що «перетворює індивіда на «нуль» в громадському житті.

Аксіологічний (ціннісно-орієнтаційний) підхід визначає сутність інформаційного суспільства як певної моделі організації соціуму, в основі якої універсальні цінності – інформація та знання, що є формою вираження матеріального середовища життя людини та основним способом організації міжособистісних стосунків. Процес історичного розвитку суспільства від одного типу до іншого трансформує систему цінностей. За допомогою інформації як основної цінності індивіда відбувається процес соціалізації особистості та життєдіяльності суспільства, формування соціальних ідеалів і цінностей. Наука як система комунікацій також регулюється нормативно-ціннісною системою, що зорієнтована на певні зразки, критерії, оцінки та форми репрезентації креативності. Таким чином, інформаційне суспільство трактується як суб'єкт ціннісного відношення, соціальний феномен епохи глобалізації та модернізації[12].

Антропологічно-комунікативний підхід. На думку Е. Касірера, людина – символічна істота, яка живе в символічному універсумі, що сьогодні твориться в основному ЗМІ та ЗМК і формує віртуальний інформаційний соціум. Символічний універсум буття суспільства складається в системі інформаційних комунікацій газет, радіо, телебачення, Інтернету, які мають діалектично суперечливий характер[13]. У цьому підході «людина інформаційна» визначається як сукупність характеристик, які безпосередньо забезпечують її участь у процесах соціальної комунікації в системі «інформація, інформатизація – людина – суспільство» та організовують діяльність людини у соціально-інформаційних системах, інформаційно-обмінних процесах соціуму[14].

---

[11] Тоффлер Э. Метаморфозы власти. – М., 2003.

[12] Ткачова Ю. Ціннісно-комунікативні характеристики науки в умовах інформаційного суспільства // Гілея. – 2014. – № 86. – С. 216.

[13] Информационное общество: Сборник. – М.: ООО Изд-во АСТ, 2004. – С. 471.

[14] Отюцкий Г.П. Информационная антропология: предмет и проблематика // Гілея. – 2013. – № 70.

Трансформаційно-політичний підхід. Розвиток інформаційних технологій не тільки розширює можливості існуючих політичних і суспільних інститутів, але й призводить до трансформації моделей суспільно-політичних комунікацій, створює умови для нетрадиційних форм політичної участі, трансформує інституційну підсистему політичної системи суспільства[15] через гіперболізацію значущості чинника громадянського суспільства в прийнятті рішень і визначає ступінь демократичності влади у прямій залежності від її інформаційної відкритості (деліберативна теорія демократії).

Культурлогічний підхід підкреслює значущість поширення культурних сенсів й знаків у суспільстві та переважно інформативний характер сучасної культури[16]. Сучасне суспільство продукує, транслює і трансформує ідентифікаційні коди і патерни для самоідентифікації як всередині спільнот, так і у глобальному комунікативному просторі. Функціонування цих меседжів і забезпечує існування інформаційного суспільства.

Державно-елітарний підхід визначає державу та різні політичні сили основними суб'єктами становлення та подальшого розвитку інформаційного суспільства. Інформація та знання виконують функцію головного ресурсу, що забезпечує соціально-економічний розвиток держави. Незважаючи на транскордонні та транснаціональні можливості інформаційного простору, які забезпечуються наявними технологічними можливостями, процеси у сфері інформації регулюються соціально-правовими нормами відповідними державними інституціями. І хоча в процесі входження в інформаційне суспільство певні функції держави трансформуватимуться, однак ефективність цього політичного інституту залишається достатньо високою. Вона насамперед виявляється у: потребах протистояння негативним тенденціям глобалізації; необхідності захисту національної ідентичності в умовах загрози глобальної уніфікації; збереженні національних позицій на міжнародних ринках; процесах організації міжнародних інформаційних обмінів; захисті інформаційної безпеки і співробітництві у цій сфері з міжнародним співтовариством[17]. Також в межах цього підходу варто підкреслити значну роль еліт

[15] Мешкова Т.А. Социально-политические аспекты глобальной информатизации // Полис. – 2002. – № 6.

[16] Даніл'ян В.О. Інформаційне суспільство: базові концепції аналізу // Наукові записки Харківського університету Повітряних Сил. Соціальна філософія, психологія. – Х.: ХУПС, 2005. – Вип. 2.

[17] Горовий В. Національні інформаційні ресурси в контексті посилення глобальних інформаційних впливів // Наукові праці Національної бібліотеки України імені В.І. Вернадського. Вип. 36 [НАН України, Нац. б-ка України ім. В.І. Вернадського, Асоц. б-к України]. – К., 2013. – С. 14.

(політичних, духовних, «білих комірців», науковців) у процесах формування інформаційного суспільства.

Сцієнтологічний підхід. Прихильники цього підходу підкреслюють прогресивну природу інформаційного суспільства, яке в перспективі еволюціонує в «суспільство колективного інтелекту планетарного масштабу». Зокрема, М. Мойсеєв зазначає, що «інформаційне суспільство – це такий етап історії людства, коли колективний розум стає не тільки опорою для розвитку Homosapiens, а й об'єктом цілеспрямованих зусиль для його вдосконалення»[18]. У цьому підході в прогресі інформаційного суспільства простежуються елементи ідеалістично-утопічної ідеї прагнення людства в майбутньому досягти найвищого рівня розвитку, інтелекту та комфорту.

Технологічний підхід трактує інформаційне суспільство як результат якісно нового етапу соціотехнологічної революції, що сформувався на ґрунті тенденцій попереднього соціально-економічного розвитку. Інформаційно-комунікаційні технології стають каталізатором змін у суспільстві, здатні кардинально трансформувати систему взаємовідносин між «техносферою», «соціосферою» та «психосферою», що призводить до системних цивілізаційних змін в усіх сферах життя[19]. А саме – збільшення ролі інформації і знань в суспільстві, формування системи споживання інформаційних ресурсів внаслідок виникнення та розвитку інформаційно-комунікаційних технологій, що діють у глобальних масштабах[20], тобто підкреслюється «технотронна» природа суспільства. О. Дубас зазначає, що в інформаційному суспільстві «на першому місці – розвиток нових інформаційних технологій, найважливішим продуктом для більшості людей стає інформація, беззаперечною умовою є доступ до неї всіх охочих, крім випадків, які передбачені політико-правовими законами щодо інформаційної безпеки, вирішальним у цьому суспільстві стає здатність мислити, аналізувати та використовувати інформацію»[21]. Саме в такому контексті важливого значення набуває проблема подолання «неуцтва» суспільства, яка породжує відсталість та економічні загрози для держав. Наслідком є розрив між розвиненими державами

[18] Моисеев Н.Н. Информационное общество как этап новейшей истории // Свободная мысль. – 1996. – № 1.
[19] Тоффлер Э. Третья волна. – М., 1999. – С. 561.
[20] Даніл'ян В.О. Інформаційне суспільство: базові концепції аналізу // Наукові записки Харківського університету Повітряних Сил. Соціальна філософія, психологія. – Х.: ХУПС, 2005. – Вип. 2.
[21] Дубас О.П. Інформаційний розвиток сучасної України у світовому контексті: монографія. – К., 2004. – С. 62.

монополістами на використання досягнень НТР в галузі продукування інформації та знань і «країнами-паріями».

Соціально-комунікативний підхід трактує інформацію, знання й інформаційно-комунікаційні технології як «основну продуктивну силу та джерело епохальних зрушень в усіх сферах суспільного життя», вплив яких найяскравіше виявляється в політиці. В інформаційному суспільстві метаморфози політичної влади спровоковані інформацією, яка в процесах соціально-політичних комунікацій «трансформує політичні режими («е–демократія»), владні інститути («е–уряд» та «е–самоврядування»), партійні («е–партія») та виборчі системи («е–вибори» і «е–референдум»)». Саме ці зміни «прискорюють перехід від представницької демократії до демократії участі, зміцнюють правову державу і громадянське суспільство»[22]. Тобто у цьому підході наголошено на інноваційній ролі інформації та знань у процесах формування нової соціальної системи, яка здатна трансформуватись у високоінтелектуальне інформаційне суспільство.

Соціально-економічний підхід започаткований П. Дракером, який стверджував, що сучасне суспільство формує нову економічну систему, нівелює капіталістичні відносини у соціумі через заперечення прерогатив власників на засоби виробництва над нижчими соціальними класами[23]. Капіталісти – власники матеріально-технічних засобів втрачають «владу» над людьми, що володіють інформацією і знаннями як новим капіталом, новим стратегічним ресурсом сучасності. Саме володіння цими «новими цінностями» дає реальну перевагу у формуванні влади і багатства в постіндустріальну добу.

Соціально-мережевий підхід був запропонований наприкінці 80-х початку 90-х років XX ст. іспанським соціологом М. Кастельсом, який визначив новий тип суспільства як *мережеве суспільство*[24]. Новий тип соціальної морфології суспільства визначається мережами, а «поширення «мережевої» ідеології» значною мірою позначається на процесах, які пов’язані з виробництвом, повсякденним життям, культурою. М. Кастельс наголошує, що формується нове «суспільство мережевих структур, характерною ознакою якого є

[22] Маруховський О.О. Політичні аспекти зарубіжних концепцій інформаційного суспільства: дис. … на здобуття наук. ступеня канд. політ. наук: спец. 23.00.01 «Теорія та історія політичної науки»; НАН України, Інститут політичних і етнонаціональних досліджень ім. І.Ф. Кураса. – К., 2008.

[23] Дракер П. Посткапиталистическое общество // Новая постиндустриальная волна на Западе: антология. – М., 1999.

[24] Кастельс М. Информационная эпоха: экономика, общество и культура. – М., 2000.

домінування соціальної морфології над соціальною дією»[25]. Основною рушійною силою, що творить мережеве суспільство, М. Кастельс називає суперечності між глобалізаційними процесами сучасності та ідентичностями окремих суспільств. Ці «ідентичності спротиву» виступають проти глобалізації та уніфікації світу, але через світові інформаційно-комунікативні мережі в майбутньому утворять якраз нову ідентичність, що спрямована в перспективу – «мережеве суспільство». Вчений визначає проблеми, що виникають у процесах становлення цього модерного соціуму: можливість управління мережами і цензура, нерівномірність можливостей доступу до мереж, недостатність знань окремих індивідів для «проживання в мережі», незахищеність від доступу до особистої інформації (в умовах віртуалізації економіки) та ін. Мережеве суспільство є принципово новим типом соціуму, який формується поза традиційними принципами центру та периферії, відсутності магістральних і маргінальних траєкторій розвитку, які не мають ні початку, ні кінця, при основоположній ролі інформаційно-комунікативних мережевих технологій.

Глобальний інформаційний простір є продуктом інтелектуальної діяльності інформаційного суспільства, яке намагається завдяки модернізуючим інформаційним технологіям максимально задовольнити свої потреби у спілкуванні, а також в інформаційних продуктах та послугах для політичної, економічної та інших видів діяльності. Це надскладна просторово-часова структура у якій відбуваються взаємопов'язані інформаційно-комунікаційні процеси вироблення, кодування, трансформації, передачі, декодування й зберігання інформації.

Наприкінці XX ст. категорії «глобальний», «глобалізація», «глобальні процеси», «глобалізм», «глобалістика» поширювались в науковому дискурсі настільки швидко, що наблизились до філософських категорій «єдине», «загальне», підкреслюють науковці, «глобальний не лише – планетарний,… а – всеохоплюючий, універсальний, загальний»[26]. Термін «глобалізація» виник у 1980-х рр., його вперше вжив Теодор Левітт, для позначення світового ринку товарів та послуг, виникнення якого ознаменувала економічна діяльність транснаціональних корпорацій. Адаптував це поняття для загальнонаукового використання Р. Робертсон, який визначив

[25] Кастельс М. Становление общества сетевых структур // Новая постиндустриальная волна на Западе: антология; под ред. В.Л. Иноземцева. – М., 1999.

[26] Ильин И.В. Глобалистика в контексте политических процессов : дисс. ... д-ра. полит. наук : 23.00.04 / [место защиты: Моск. гос. ун-т им. М.В. Ломоносова]. – Москва, 2011. – С. 120.

розвиток глобалізації як двоєдиний процес перетворення загального в окреме і перетворення окремого в загальне[27]. Така тенденція визначила особливості процесів обміну матеріальними та духовними цінностями між державами, націями, спільнотами, що виявлялися через не лише через інтернаціоналізацію чи універсалізацію, а й уніфікацію та нівелювання окремих ідентичностей для формування глобального чи єдиного «світового суспільства». Саме глобалізація та модернізація відображають тенденції сучасного інформаційного суспільства, стратегічною метою якого є створення цілісного світу.

Осмислення феномену глобалізації та пов'язаного з ним процесу комунікації, виявили кардинальні трансформації в сприйнятті часових і просторових відносин та географічних кордонів соціуму, які нівелюються через техногенність сучасної цивілізації, тобто почався процес «ретрайбалізації» – гомогенізації світу (комунікативного простору)[28].

У трактуванні глобалізації як феномену, процесу, тенденції немає єдиної думки, у зв'язку з тим, що глобалізація розглядається крізь призму множинності наукових парадигм з використанням різних методів й підходів.

Радикальний підхід розглядає глобалізацію як *процес*, факт та явище, які вже обумовлюють особливості функціонування усіх сфер життя суспільства. Глобалізація, на думку У. Бека «створює транснаціональні соціальні зв'язки та простори, знецінює локальні культури і сприяє виникненню третіх культур…Глобальний світ – це транснаціональна світова спільнота якій не вистачає всесвітньої держави й всесвітнього уряду»[29]. Негативні тенденції цей підхід вбачає у нівелюванні чи знищенні національних культур, а позитивним результатом глобалізації мало б стати утворення гібриду цих культур, умовної світової «суперкультури», яка б стала універсальним надбанням світового суспільства. На думку українського філософа В. Воронкової: «Глобалізація – це історичний процес … створення міжнародного культурно-інформаційного поля, інфраструктури для міжрегіональних, у тому числі й інформаційних обмінів»[30].

[27] Robertson R. Globalization: Social Theory and Global Culture. – London, 1992. – P. 25–31.

[28] Северинчик О.П. Маніпулятивний аспект діяльності ЗМІ // Філософія і соціологія в контексті сучасної культури: Збірник наукових праць – ДНУ, 2008. – С. 326–329.

[29] Бек У. Что такое глобализация? Ошибки глобализма – ответы на глобализацию. – М., 2001. – С. 26, 32.

[30] Воронкова В.Г. Філософія глобалізації: соціоантропологічні, соціоекономічні та соціокультурні виміри: монографія. – Запоріжжя, 2010. – С. 9.

Отже акцентуючи на процесах трансформації культур, радикальний підхід вказує і на нелінійний суперечливий характер змін у всіх сферах функціонування суспільства (інформаційно-комунікаційній також).

Скептичний підхід вважає глобалізацію *міфом*, який був створений ідеологами вільного ринку з метою демонтажу системи соціального забезпечення та скорочення соціальних витрат[31] і є лише відображенням процесів посилення взаємодії між національними економіками та їх інтернаціоналізацією. Причому, вказуючи на передовсім економічні аспекти процесу комунікації держав, прихильники цього підходу особливо акцентують умови цих комерційних взаємодій, а саме нерівномірність можливостей «гравців» світового ринку і їх дискретний характер. Скептики практично відкидають можливість рівноцінності та рівноправності в умовах об'єднання суспільств[32], що значно посилюється в умовах інформаційного суспільства через нерівномірність розподілу матеріальних, технологічних і кадрових ресурсів.

Реалістичний підхід розглядає глобалізацію як *тенденцію*, яка спрямована на досягнення єдності (гомогенності) усього людства у системі світу, яка забезпечує взаємодію і взаємозв'язок країн, культур, держав в економічній, політичній, культурній, технологічній та інформаційних сферах[33]. «Глобалізація – це подолання і навіть ліквідація традиційних кордонів між державами через формування єдиного технологічного, торгівельного, економічного та інформаційного простору»[34].

Комплексний підхід розглядає глобалізацію як комплекс тенденцій, форм взаємодій, фаз розвитку та об'єктивних процесів інтенсифікації транснаціональних потоків. За визначенням львівського дослідника А. Колодій, поняття глобалізації можна визначити наступним чином: «Глобалізація – це фаза сучасної поглибленої та багатоаспектної інтеграції світу в умовах новітніх інформаційних технологій, завдяки яким світ стає єдиним цілим; це також процес кількісного зростання, інтенсифікації та якісної трансформації економічних, політичних, соціальних, правових, культурних зв'язків і відносин держав та регіонів із суперечними та

[31] Валлерстайн І. Глобалізація або вік змін? Довгостроковий погляд на шлях розвитку світової системи // Глобалізація. Регіоналізація. Регіон. політика. – Луганськ, 2002. – С. 49–67.
[32] Хантингтон С. Столкновение цивилизаций. – М., 2003. – 603 с.
[33] Giddens A. The third way: the renewal of social democracy [Електронний ресурс]. – Cambridge, 1998. – 166 p. – Режим доступу: http://www.lib.miamioh.edu/multifacet/record/mu3ugb2687994
[34] Буряк В. Актуальные проблемы философии. Методологические основания экономического знания, постиндустриальное общество, глобализация. – Симферополь, 2006. – С. 85.

неоднозначними наслідками»[35]. «Глобалізація – це взаємодія груп та окремих індивідів безпосередньо один з одним через кордони, без обов'язкової, як раніше, участі в цьому процесі держави». Це об'єктивний процес, обумовлений зростаючими можливостями засобів комунікації, потребами міжнародної економічної та фінансової діяльності для вирішення загальнолюдських проблем[36].

Глобалізація, на нашу думку, є синтезованою категорією, яка розкриває процес, механізм й тенденції функціонування світового розвитку, як цілісної, взаємопов'язаної та взаємообумовленої інтегративної світосистеми, яка характеризується транснаціональними і транскордонними особливостями, що виявляються через інтенсифікацію процесів культурної, політичної, економічної та військової інтеграції та уніфікації, інноваційну діяльність та необмеженість комунікативних потенцій в епоху техногенної цивілізації. Об'єктивною передумовою глобалізації є становлення інформаційного суспільства.

Глобалізація, найхарактерніша риса сучасної епохи, значною мірою визначається експансією *інформації* як основного стратегічного ресурсу, комплексу відомостей, даних, повідомлень незалежно від форми їх презентації. Процеси модернізації, бурхливий розвиток науки та її комп'ютеризація обумовлюють трансформацію і самого поняття інформації. Модернізація способів і методів поширення та обміну інформацією радикально змінює структуру світового інформаційного простору, сприяє гомогенізації свідомості людства та універсалізації культури.

Множина підходів до визначення сутності поняття «інформація» визначається насамперед виокремленням головного чинника у її змісті в умовах стрімких процесів глобалізації та модернізації.

Діяльнісний підхід. Одне з перших визначень інформації «комп'ютерної ери» належить Н. Вінеру: «Інформація – це позначення змісту, що одержується з зовнішнього світу в процесі нашого пристосування до нього і пристосування до нього наших почуттів. Процес одержання і використання інформації є процесом нашого пристосування до мінливості зовнішнього середовища і нашої життєдіяльності в цій сфері»[37]. Тобто інформація є насамперед продуктом життєдіяльності людини.

---

[35] Основи демократії: підруч. для студ. вищ. навч. закл. ; ред. Антоніна Колодій.– Л., 2009. – С. 718.

[36] Бабаєва Н.Р. Глобалізація сучасного світу // Гілея. – 2012. – № 59. – С. 362–366.

[37] Арістова І.В. Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади [Електронний ресурс] : автореф. дис. … на здобуття наук. ступеня д-ра юрид. наук

Субстанціональний підхід. Інформація визначається як одна з трьох основних (поряд з матерією та енергією) субстанцій, що творять світ, у якому живе людина, характерними ознаками якої є те, що, по-перше, на емпіричному рівні її розглядають не як цілісність, а тільки властивість певної системи (людини, окремого суспільства), по-друге, інформація змінює і трансформує цю систему.

Військово-прикладний підхід визначає інформацію як фактологічну зброю в інформаційній війні. На думку М. Сенченка «до неї належить інформація прикладного характеру, а саме релігія, ідеологія, технологія, описова інформація часткових і узагальнених процесів. Саме фактологічною зброєю за допомогою ідеології, релігії, культурної інверсії можна дезінформувати і підпорядкувати собі супротивника»[38].

Технологічний підхід розглядає інформацію як форми знакової фіксації об'єктивної реальності, кожній із яких відповідає визначений рівень соціально-економічного та культурно-історичного розвитку в системі ціннісних смислів і орієнтацій. Концепція М. Маклюена підкреслює залежність зміни епох в історії людства від закономірностей і особливостей перетворення та кодування інформації[39]. Цей підхід називає інформацію та способи її трансляції основною рушійною силою прогресу.

Сцієнтистський підхід розглядає інформацію як об'єкт науки. Виникнення нової «інформаційно-комп'ютерної ери» обумовлене революцією в галузі інформаційних технологій, де інформація – за математичною теорією, має свої особливості, властивості та аксіоми[40].

Соціологічний підхід трактує інформацію не лише як сукупність різноманітних знань, а як елементарну соціальну функцію людської поведінки в проблемному полі комунікативних відносин[41].

Унітарно-прагматичний підхід вважає інформацію лише результатом сприйняття даних і команд, які необхідні для інтерпретації цих даних[42].

: спец. 12.00.07 „Теорія управління; адміністративне право і процес; фінансове право". – Харків, 2002. – Режим доступу: dysertaciya.org.ua

[38] Сенченко М. Четверта світова. Інформаційно-психологічна війна [Електронний ресурс]. – К., 2014. – 384 с. – Режим доступу: https://lib.rus.ec/b/241595/read

[39] Маклюэн Г.М. Галактика Гутенберга. Сотворение человека печатной культуры [Електронний ресурс]. – М., 2003 // Центр гуманитарных технологий. – Режим доступу: URL: http:// gtmarket.ru/ laboratory/basis/3568.; Маклюэн Г.М. Понимание Медиа: Внешние расширения человека. – М., 2003. – 464 с.

[40] Shannon C.E. A Mathematical Theory of Communication [Електронний ресурс]. – Режим доступу: http://cm.bell-labs.com/cm/ms/what/ shannonday/ shannon1948.pdf

[41] Ткачова Ю. Ціннісно-комунікативні характеристики науки в умовах інформаційного суспільства // Гілея. – 2014. – № 86. – С. 216.

Персоналістський підхід характерний для наукових розвідок російського дослідника С. Дятлова, який визначає поняття інформації як атрибутивну характеристику, що позначається і актуалізується через системну взаємодію та становлення свідомості вільної творчої особистості (активно управляючого суб'єкта)[43].

На нашу думку, **інформація** – це універсальна комплексна категорія, субстанціональна основа об'єктивної реальності у вигляді матеріальних й ідеальних зв'язків, що утворюють систему взаємодії компонентів структури, забезпечують процес її отримання, декодування, трансформацію і споживання.

Необхідним компонентом формування глобального інформаційного простору та глобального інформаційного суспільства є поняття «*комунікація*». Комунікаційну взаємодію, на думку В.В. Гулая, слід розглядати на основі класичної матриці міжсуб'єктної інтеракції, базовими елементами якої виступають такі поняття як «комунікатор», «комунікант», «сигнал», «шум», «канал» тощо[44]. Виділяють значну кількість моделей комунікації, які використовують в інформаційно-комунікаційному просторі в залежності від цілі, мети та завдань цього процесу[45].

У визначенні сутності комунікації як процесу, слід зазначити існування низки підходів, які принципово підкреслюють значення його ідентифікуючих ознак в трактуванні понять глобального інформаційного простору та глобального інформаційного суспільства.

Технологічний підхід називає інформацію та способи її трансляції основною рушійною силою прогресу. У межах цього підходу акцентовано на формуванні в процесі комунікації нового стилю мислення та сприйняття об'єктивної дійсності як глобального світу в системі нових глобальних цінностей, відмови від національних ідеологій та традиційних концепцій і теорій держави за допомогою інформаційно-комунікативних технологій.

Науковий підхід вважає комунікацію важливою умовою створення та оформлення нового знання на основі сукупності

---

[42]Информационная эра [Електронний ресурс]. – Режим доступу: http://www.lib.ru/SECURITY/kvn/corner.txt_with-big-pictures.html

[43] Дятлов С.А. Принципы информационного общества [Електронний ресурс]. – Режим доступу: http: // emag.iis.ru/arc/ infosoc/ emag.nsf/BPA

[44] Гулай В.В. Комунікативні механізми та масштаби пропагандистського впливу радянських партизан та підпільників на населення Львівщини в роки нацистської окупації // Військово-науковий вісник. – 2014. – Вип. 21. – С. 106.

[45] Зернецька О.В. Глобальний розвиток систем масової комунікації і міжнародні відносини. – К., 1999. – 351 с.; Goban-Klas T. Media i komunikowanie masove. Teorie i analizyprasy, radia, telewizji i Internetu. – Warszawa–Krakow, 1999. – 336 s.

інформації. Ідеали і норми наукового дослідження є виявом комунікативності науки, саме вони визначають для вченого зразки теорій, методів, фактів, аргументованості знання, способи організації знання та діяльності. В процесах інтеракцій вони можуть інституціоналізовуватися і транслюватися в пізнавальній діяльності, через комунікацію й оцінки дослідників чи наукового співтовариства соціалізуються та набувають статусу норм та ідеалів[46].

Культурологічний підхід визначає комунікацію як процес формування культурних цінностей, смислів і парадигм на основі створення нових інформаційних систем, що стають рушієм розвитку суспільства.

Орієнтаційно-цільовий підхід підкреслює важливість не характеру комунікаційного процесу, способу передачі інформації, чи особливостей кодування і її формалізації, а цільової спрямованості та задач системи, яка визначає спосіб комунікації, якість і обсяг соціально значущої інформації[47].

На нашу думку, **комунікація** – це соціальний процес, пов'язаний із спілкуванням, обміном думками, відомостями, ідеями тощо за допомогою комплексу технологічного інструментарію з метою вироблення нових системних культурних сенсів і парадигм в умовах конкретних просторово-часових характеристик.

Особливо актуальною у сучасному науковому дискурсі стають концепції масової комунікації в контексті формування глобального інформаційного простору. На увагу заслуговують такі основні:

- *Концепція тотального впливу*, основу якої становить пропаганда як інструмент формування суспільної думки ЗМІ, що транслюють зразки уніфікованої масової культури у соціум;
- *Концепція обмежених ефектів* абсолютизує роль влади та політичних еліт, які монополізують канали та засоби комунікації і використовують їх для маніпуляції свідомістю громадян (особливо у передвиборчих кампаніях);
- *Концепція глобалістської орієнтації* акцентує на позитивному впливі соціальних комунікацій на творення уніфікованих цінностей космополітичного соціуму;

[46] Микешина Л.А. Эпистемология ценностей. – М., 2007. – С. 165.

[47] Костина А.В. Тенденции развития культуры информационного общества: анализ современных информационных и постиндустриальных концепций [Електронний ресурс] // Информационный гуманитарный портал „Знание. Понимание. Умение”. – № 4. – 2009. – Культурология. – Режим доступу: http://www.zpu-journal.ru/e-zpu/2009/4/Kostina_Information_Society

- *Семіотична концепція* наголошує на виникненні універсальної знакової системи, що створена для міфологізації та інтерпретації реальності (реклама);
- *Постмодерністська концепція* проголошує «смерть реальності» через заміщення у віртуальному комунікаційному просторі реальності – «симулякром», який штучно змодельований і орієнтує реципієнта у заданому неіснуючому світі на основі сконструйованих цінностей, міфів та стереотипів.

Отже, варто підкреслити маніпулятивну природу віртуального простору в якому відбуваються інтеракції сучасного інформаційного суспільства. У науковій практиці існують спроби змоделювати глобальні системи масової комунікації. Такою спробою є системна модель Де Флера, або модель, яка ґрунтується на теорії М. Маклюена про «глобальне село» у якому «посилена тенденція до конгломерації мультимедіа-імперій з гігантами комп'ютерної сфери та індустрії телекомунікацій»[48], що «створює передумови для перерозподілу існуючої економічної і політичної влади, до нових інтеркультурних взаємодій, тобто нових глобальних процесів, що вже на початку XXI ст. можуть суттєво змінити обличчя земної цивілізації»[49]. Можна зробити висновок, що глобальні інформаційні та комунікаційні процеси стають важливим чинником міжнародних відносин на сучасному етапі та потужним інструментом трансформації могутності сучасних держав.

Коли традиційні багатства та цінності втрачають своє пріоритетне значення, інформаційно-технологічний прогрес починає визначати політичну, соціальну, економічну та інші сфери людської діяльності. Є. Макаренко підкреслив, що «інформаційний чинник здійснив у житті цивілізації за XX ст. найбільші зміни за всю її історію: він об'єднав світ в єдину систему, яка функціонує в режимі реального часу»[50]. Окрім того, взаємообумовленість цивілізаційного та інформаційного процесів у масштабах світового розвитку лаконічно підкреслено у формулі Д.С. Робертсона – «цивілізація – це інформація»[51]. Це дало можливість ввести у науковий дискурс категорію *інфосфера,* виникнення якої пов'язують з біосферою, генетичною інформацією, розумом, появою мови, писемності та інших видів інформації. Інфосфера – це середовище циркуляції

[48] Зернецька О.В. Глобальний розвиток систем масової комунікації і міжнародні відносини. – К., 1999. – С. 72.
[49] Там само. – С. 85.
[50] Макаренко Є.А. Міжнародні інформаційні відносини: монографія. – К., 2002. – С. 18.
[51] Вершинин М.С. Политическая коммуникация в информационном обществе. – СПб., 2001. – С. 10.

інформації на території Землі[52]. Тобто, *інформаційна сфера* – це сукупність суб'єктів інформаційної взаємодії та впливу, яка забезпечує можливість формування, обміну, зберігання та розповсюдження інформації.

Процеси глобалізації та модернізації сприяли суттєвим, якісним змінам у розвитку інформаційних технологій, які майже миттєво охопили всю планету комплексними віртуальними комунікативними зв'язками. Про залежність людини від техніки писав ще М. Бердяєв: «нові людські маси, які вийшли на арену історії, вимагають нових форм організації, нових знарядь»[53]. Але, технічні засоби можуть лише обслуговувати процеси інформаційного обміну в суспільстві, полегшуючи її обробку та передачу. Виробником та споживачем інформації є саме людина, тобто стає одночасно і суб'єктом і об'єктом комунікативних взаємодій.

Визначальною ознакою нової доби, на думку М. Кастельса стала інформаційно-технологічна революція, яка сприяла розвитку такого явища, як *інформаціоналізм («інформаційний капіталізм»)* – «технологічна парадигма, заснована на збільшенні людського потенціалу при обробці інформації і зв'язку, що стало можливим завдяки революції в галузі мікроелектроніки, програмного забезпечення та генної інженерії»[54].

Новітні технічні засоби не лише формують нові суспільні запити й потреби і видозмінюють спосіб життєдіяльності людини та її повсякденні звички, а й створюють умови для побудови нової моделі мислення та ціннісної орієнтації особи. М. Кастельс зазначає: «поява нової системи електронної комунікації характеризується глобальними масштабами, інтеграцією всіх засобів масової інформації, а її потенційна інтерактивність вже змінює нашу культуру й змінить її назавжди»[55]. «Нові технології та телекомунікації, – зазначають Д. Хелд, Д. Гольдблатт, Е. Макгрю та Е. Перратон, – поява міжнародних корпорацій, які володіють засобами масової інформації…породили глобальні культурні потоки, розмах яких,

[52] Иванов А.К. Глобальное информационное пространство и его место в современном международном праве // Ползуновский вестник. Барнаул: АлтГТУ – 2005. – № 1. – С. 225.

[53] Бердяев Н.А. Человек и машина (Проблема социологии и метафизики техники) // Вопросы философии. – 1989. – № 2. – С. 155.

[54] Castells M. Informationalism, Networks, and the Network Society: a Theoretical Blueprinting, The network society: a Cross–Cultural Perspective [Електронний ресурс]. – Northampton, MA: Edward Elgar, 2004. – Режим доступу: http://annenberg.usc.edu/Faculty/Communication/~/media/Faculty/ Facpdfs/ Informationalism%20pdf.ashx

[55] Кастельс М. Информационная эпоха: экономика, общество и культура. – М., 2000. – С. 315.

інтенсивність, різноманіття та швидке поширення не мають аналогів у минулому»[56].

Глобальні транснаціональні актори-корпорації створили нові форми процесу інформатизації, такі як міжнародний потік інформації – «рух повідомлень» через національні кордони, а також серед двох і більше національних та культурних систем. До засобів передачі міжнародного потоку інформації зараховують: радіо й телебачення, газети, журнали, книги, фільми, маркетинг, реклама і таке інше»[57].

Світ вступив у так звану «третю хвилю» індустріального стрибка – в фазу інформатизації. *Інформатизація* – це складний соціальний процес формування оптимальних умов для вироблення, розвитку, трансформації, використання, споживання та задоволення інформаційних потреб людства.

Процеси інформатизації та глобалізації знаходяться в діалектичній взаємозалежності: з одного боку, інформатизація є результатом глобалізації, а з іншого, її провідником. Наслідком взаємодії процесів інформатизації та глобалізації стала поява *глобального інформаційного простору,* як об'єктивної реальності інформаційного суспільства, що придатна і для вироблення та реалізації політичної стратегії усіх держав світу. Термін «глобальний інформаційний простір» почав активно використовуватися у науковому дискурсі гуманітарних і соціальних наук з початку XXI ст.

Визначення глобального інформаційного простору розглядають у таких вимірах – віртуально-політичному, технологічному, соціально-комунікативному, мережевому, військово-прикладному, науковому.

Віртуально-політичний підхід визначає *глобальний інформаційний простір* як комплекс глобальної уніфікованої інформаційної індустрії, яка розвивається на фоні зростання ролі інформації та знань у економічному та соціально-політичному контексті при кардинальних змінах в структурі інформаційного суспільства, яке будується на нових «електронних» формах демократії[58], посилюючи тенденції медіакратії, як парадигми у якій влада ЗМІ та ЗМК досягає гіперформ та загрожує існуванню політичної комунікації громадянського суспільства у сучасних

[56] Хелд Д., Гольдблатт Д., Макгрю Э., Перратон Дж. Глобальные трансформации политика, экономика, культура. – М., 2004. – С. 387.

[57] Сусська О. Право людини на інформацію як базова ознака комунікативних стосунків в інформаційному суспільстві // Комунікація. – 2012. – № 2. – С. 40.

[58] Чернов А.А. Становление глобального информационного общества: проблемы и перспективы : монографія. – М., 2003. – С. 47–48.

демократіях, суверенітету громадянина через маніпуляцію його свідомістю та нівелюванню участі в політичних процесах[59].

До віртуально-політичного підходу, на нашу думку, слід зарахувати й трактування особливостей формування та функціонування глобального інформаційного простору як «політичної віртуальної реальності», тобто створення ЗМІ та ЗМК такого іміджевого продукту, який не є адекватним відображенням об'єктивної реальності, а за допомогою новітніх інформаційно-комунікаційних технологій формує спотворену (перетворену) політичну картину світу у масовій свідомості. Виникає нетократія, як нова форма управління суспільством, в якій основною цінністю є не матеріальні об'єкти (гроші, нерухомість і т. д.), а інформація. Повноцінний доступ до достовірної інформації і маніпуляції нею гарантують владу над членами того чи іншого соціуму[60].

Технологічний підхід визначає *глобальний інформаційний простір* як сукупність інформаційних ресурсів та інфраструктур, які становлять державні та міждержавні комп'ютерні мережі, телекомунікаційні системи та мережі загального користування й інші транскордонні канали передачі інформації[61].

Соціально-комунікативний підхід звертає увагу на те, що *глобальний інформаційний простір* – це інформаційно-технологічний та соціокультурний феномен взаємодії процесів інформатизації і глобалізації, сукупність інформаційних ресурсів (джерел інформації), технологій інформаційного взаємовпливу (програмного забезпечення) та інформаційних телекомунікаційних систем (обладнання), які функціонують на основі загальних принципів та конструюють інформаційну інфраструктуру, яка забезпечує інформаційну взаємодію у суспільстві[62]. Українська дослідниця І. Арістова подає дефініцію «інформаційне суспільство» як громадянське суспільство з розвинутим інформаційним виробництвом і високим рівнем інформаційно-правової культури, в якому ефективність діяльності людей забезпечується розмаїттям

[59] Погорєлова І. Медіакратія [Електронний ресурс]. – Режим доступу: http://www.day.kiev.ua/uk/article/podrobici/mediakratiya

[60] Бард А., Зодерквист Я. Netократия. Новая правящая элита и жизнь после капитализма. – СПб, 2004. – 252 с.

[61] Гирич В.Л. Глобальное информационное пространство и проблема доступа к мировым информационным ресурсам [Електронний ресурс] / В.Л. Гирич, В.Н. Чуприна. – Режим доступу: www.rsl.ru/upload/mba2007_05

[62] Кривошееєва О.І. Громадсько-політичні рухи в глобальному інформаційному просторі // Гілея. – 2013. – № 68. – С. 883.

послуг, заснованих на інтелектуальних інформаційних технологіях та технологіях зв'язку[63].

На нашу думку, на увагу заслуговує і *мережевий* підхід. *Глобальний інформаційний простір* визначається як взаємодія нескінченної множини політичних, економічних, соціальних й інформаційно-комунікативних мереж, які за допомогою комплексу технологій формують розширений доступ до різноманітної інформації, її декодування та трансформацію, застосування безлічі форм обміну інформацією, синхронізацію процесів зворотного зв'язку та її синергетичного потенціалу. Глобальний інформаційний простір у мережевому підході стає інтегруючим атрибутом мережевих комунікацій та сприяє комплексному отриманню інформації. Одночасно, відбувається абсолютизація мережевої парадигми, як універсальної характеристики матеріального інформаційного поля, де формується свідомість глобального інформаційного суспільства.

Військово-прикладний підхід визначає глобальний інформаційний простір як сферу застосування різноманітних радіоелектронних засобів з використанням широкого електромагнітного спектру частот для прийому, передачі, обробки, зберігання, трансформації та обміну інформації за допомогою комп'ютерних мереж й інформаційно-комунікативної інфраструктури в інтересах збройних сил[64].

Науковий підхід визначає глобальний інформаційний простір як систему наукових комунікацій в просторово-часових межах де формується і поширюється наукове знання. Під впливом інтенсифікації інформаційних технологій у науковому глобальному просторі створюється нові структури комунікацій (віртуалізація), змінюється соціальний статус наукових видань, стираються національні кордони наукових співтовариств, змінюються канони викладу та презентації знань через інформаційно-комунікативні технології[65].

Отже, ці підходи визначають поняття «глобальний інформаційний простір» наголошуючи на окремих знакових

---

[63] Арістова І.В. Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади [Електронний ресурс] : автореф. дис. … на здобуття наук. ступеня д-ра юрид. наук : спец. 12.00.07 „Теорія управління; адміністративне право і процес; фінансове право". – Харків, 2002. – Режим доступу: dysertaciya.org.ua

[64] Маринин С. Подходы военных экспертов в США к разработке понятийного аппарата в сфере борьбы в киберпространстве // Зарубежное военное обозрение. – 2011. – № 10. – С. 24–30.

[65] Ткачова Ю. Ціннісно-комунікативні характеристики науки в умовах інформаційного суспільства // Гілея. – 2014. – № 86. – С. 217.

особливостях цього надскладного синтетичного динамічного явища та феномену, що свідчить про його унікальність та специфічність.

Структура глобального інформаційного простору характеризується багатоаспектністю, системністю та детермінованістю елементів.

В *організаційно-технічному* аспекті структуру глобального інформаційного простору становлять: інформаційні ресурси, інформаційно-комунікативні системи та технології інформаційного взаємовпливу в формі інформаційно-комунікаційної інфраструктури. *Інформаційний ресурс* – це сукупність текстових документів, баз даних, нерухомих й рухомих зображень, звукових і графічних матеріалів. Виокремлюють такі групи інформаційних ресурсів з окремими характерними ознаками:

– загальноцивілізаційного значення: ресурси міжнародних гуманітарних та інших організацій, міждержавних союзів, транснаціональних компаній, релігійних організацій, інших суб'єктів глобальної інформаційної діяльності, що виникають як результат вдосконалення соціальної структури суспільства. Вводяться в глобальний інформаційний простір з метою здійснення впливу окремими міжнародними суб'єктами інформаційної діяльності[66];

– державного значення: ресурси, що продукують держави з метою здійснення глобального впливу та захисту своїх інтересів, що пов'язані з реалізацією політичних, економічних, культурологічних та інших завдань, з налагодженням інформаційного взаємообміну, політичним позиціюванням, пропагандою потенційних можливостей в усіх сферах міжнародного співробітництва, національних культурних здобутків та ін.;

– матеріально-ресурсного значення: продукти для міжнародного ринку інформації. В умовах розвитку сучасного інформаційного суспільства такі ринки перебувають у процесі постійного розвитку та оптимізації. Діяльність у них набуває характерних рис традиційної ринкової діяльності з рекламними технологіями, конкурентною боротьбою та ін.;

– військово-прикладного значення: бойові інформаційні ресурси, які є основним інструментом ведення інформаційних воєн[67], нейтралізації інформаційних впливів та інформаційних атак. Характерними особливостями цього виду ресурсів є висока динаміка

[66] Скаленко А.К. Глобальные резервы роста. – К., 2002. – С. 121.
[67] Кісілевич-Чорнойван О.М. Міжнародне інформаційне право. – К., 2011. – С. 109–115.

застосування, наявність технологічних засобів, мультиваріантність форм;

– терористично-кримінального значення: ресурси кіберзлочинності[68] та протидії їм. Транскордонна кіберзлочинність та кібертероризм стали ознакою інформаційного суспільства, тому сучасні держави створюють системи захисту від хакерських атак і нормативно–правову базу для покарання злочинців[69].

Об'єднання інформаційних ресурсів у *інформаційно-комунікативних системах* та з *технологіями інформаційного взаємовпливу* відбувається у інформаційно-комунікаційній інфраструктурі. *Інформаційно-комунікаційна інфраструктура* є сукупністю територіально розподілених державних і недержавних інформаційних систем, засобів зв'язку, мереж і каналів передачі даних, засобів комунікації в управлінні інформаційними потоками.

Основними складовими глобального інформаційного простору в *синергетичному* аспекті є інформаційні поля та інформаційні потоки. *Інформаційне поле* – це комплекс зосередженої у заданому об'ємі в просторово-часових характеристиках інформації, яка існує безвідносно до об'єкта відображення та суб'єкта сприйняття. *Інформаційний потік* – це сукупність інформації, яка переміщується у інформаційному просторі по каналах комунікації.

Структурними елементами *соціальної системи* глобального інформаційного простору є:

1. Одиниці генерації інформації: воєнно-політичне керівництво держави, ЗМІ – групові комунікатори – редакції і ключові комунікатори – кореспонденти; ньюсмейкери – лідери суспільної думки; експерти – спеціалісти, які активно та професійно працюють з інформацією та визначають характер, форму, спрямованість інформаційних потоків; лідери думок – достатньо активні люди, які не пов'язані із інформаційними каналами, але мають значний вплив на середні та малі соціальні групи (блогери) в інформаційному просторі; виробники спеціальної інформації – як правило представники творчої інтелігенції, науковці, фахівці в окремих галузях.

2. Канали комунікації: електронні та друковані ЗМІ та засоби масової комунікації; канали міжособистісної комунікації;

---

[68] Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз): монографія. – К., 2010. – С. 132–148.

[69] Горовий В. Національні інформаційні ресурси в контексті посилення глобальних інформаційних впливів // Наукові праці Національної бібліотеки України імені В. І. Вернадського. Вип. 36 / НАН України, Нац. б-ка України ім. В. І. Вернадського, Асоц. б-к України. – К., 2013. – С. 7.

спеціалізовані – спрямовані на вузькопрофесійні групи; інші (товарно-грошові).

3. Області: генератори (суперноватори); новатори; центр; суперконсерватори.

Інтегрованим, комплексним поняттям в структурі глобального інформаційного простору виступає *інформаційна система* – організаційно впорядкована сукупність спеціалістів, інформаційних ресурсів, інформаційних технологій, яка реалізує інформаційні процеси.

Основними *функціями*, які виконує глобальний інформаційний простір є:

1. Інтегруюча – об'єднання в єдине просторово-комунікативне та соціально-культурне середовище окремих галузей людської діяльності, людей, міжнародних коаліцій, народів, держав.

2. Комунікативна – створення специфічного середовища інтерактивної та мобільної комунікації для інформаційного обміну.

3. Актуалізуюча – забезпечення актуалізації інтересів суб'єктів діяльності через здійснення ними інформаційної політики.

4. Геополітична – формування власних ресурсів для впливу на систему геополітичних відносин.

5. Соціальна – трансформація структури суспільства та характеру соціально-політичних відносин в усіх сферах.

Отже, аналізуючи основні елементи, особливості та функції глобального інформаційного простору, можна зробити висновок, що він стає предметом та середовищем зіткнення інтересів безпосередніх суб'єктів здійснення комунікативної діяльності, що спрямовані на одержання прибутку, переваг чи певних преференцій. Змагання за лідерство у цьому віртуальному середовищі, де маніпулюють емоціями та розумом реципієнтів інформації, призводить до зіткнення інтересів, конфліктів та стає причиною «інформаційних воєн».

Глобальний інформаційний простір є базовою категорією для поняття *інформаційної війни*, як маніпулятивної, агресивної несанкціонованої діяльності в інформаційному просторі. Основними рисами глобального інформаційного простору у співвідношенні із інформаційною війною є:

- динамічність – активне прагнення повного інформаційного домінування;

- структурованість – наявність взаємопередбачуваних та взаємовиключаючих елементів зосередження уваги й заперечення точок інформації;
- захищеність – визначення ключових компонентів, які захищаються від чужого впливу;
- універсальність – здатність впливати на усі сфери життя суспільства та буття людини;
- специфічність – використання особливостей національного менталітету при обробці та поширенні інформації;
- здатність брати непряму участь у веденні реальних бойових дій.

Особливостями глобального інформаційного простору є:

- охоплення системою глобального інформаційного простору усього цивілізованого людства;
- прозорість сучасного глобального інформаційного простору, можливість ефективного впливу на людину й суспільні групи через інформаційні сфери;
- розширення спектру можливостей та ступеню впливу інформаційного простору;
- проблемність у виявленні джерел негативного впливу інформаційних ресурсів та попередження їх руйнівних наслідків;
- відкритість доступу до джерел інформації, практичне нівелювання впливу державних політичних інститутів;
- вплив розвитку та розповсюдження засобів інформатики й нових інформаційних технологій.

Єдиний (глобальний) інформаційний простір формувався впродовж декількох останніх десятиліть, узалежнено від розвитку новітніх інформаційно-комунікаційних технологій та зростання швидкості передачі інформації. Найвизначнішим етапом формування глобального інформаційного простору стала поява та поширення *Інтернету*.

Трактування поняття «Інтернет» є досить значною міжнауковою проблемою, існує множина дефініцій від утилітарного до поетизованого варіантів. Інтернет – «це ланцюг комп'ютерних мереж, які можна розглядати як найпростіший і найдешевший засіб обміну інформацією між бізнесом й іншим світом»[70]; «глобальна децентралізована мережа, яка не має органа управління. Фізичні

[70] Summer A., Dunran Gr. E-COMMERCE. Маркетинг: Пятая волна. – М., 1999.

мережі, як складові Інтернету формують ієрархію, верхній рівень якої займають високошвидкісні магістральні мережі»[71]; «це глобальна комп'ютерна мережа, що об'єднує мільйони комп'ютерів по всьому світу…глобальний засіб обміну інформацією,… «інформаційна супермагістраль»[72]; «всесвітня мережа, яка схожа на павутиння із лісових стежок, де кожен може зайти у хащі і робити там те, що захоче»[73].

В Інтернеті виникла унікальна соціальна спільнота – так зване *Інтернет-середовище*, яке може бути визначено як «особливий агент, що формує автономну реальність і впливає на специфіку взаємодії індивідів у новому соціальному просторі. Власне, Інтернет-середовище є однією зі сфер розділу суспільства на реальне і віртуальне»[74]. Позитивною рисою цього середовища є те, що сучасний Інтернет – це не просто конгломерат комп'ютерних мереж, але і (що особливо важливо) новостворена спільнота пов'язаних кібер-соціальними мережами людей, які активно діють у новому Інтернет-середовищі. Інтернет – одна з найбільш перспективних на сьогодні технічних можливостей забезпечення міжкультурної взаємодії і співробітництва»[75]. У «Інтернет-середовищі» створюються окремі об'єднання людей за інтересами чи напрямками діяльності[76], так звані «Інтернет спільноти», які мають специфічні ознаки:

1. Схожість з наднаціональними інформаційними корпораціями та здатність конкурувати з ними.

2. Масштабні віртуальні об'єднання володіють певним суверенітетом, можуть вступати в геополітичну конкуренцію за сфери впливу.

3. Здатність до мобілізації інтелектуальних ресурсів (особливо важливою є ця характеристика в умовах ведення інформаційної війни)

4. Виняткова проникаюча здатність в будь-які соціальні структури.

---

[71] Козье Д. Электронная коммерция. – М., 1999. – С. 21.

[72] Волокин А.В. Электронная коммерция: учебное пособие для служащих государственных организаций и коммерческих фирм / А.В. Волокин, А.П. Маношкин, А.В. Солдатенков. – М., 2002. – С. 64.

[73] Зуев С.Э. Измерения информационного пространства (политики, технологии, возможности) // Музей будущего: информационный менеджмент. – М., 2001. – С.230–250.

[74] Вахула Б.Я. Соціальні Інтернет-мережі з позицій інтегративної парадигми // Роль суспільних наук у забезпеченні стабільності розвитку глобальних світових процесів у XXI ст.: мат. міжнар. наук.-практ. конф. – К., 2013. – С. 58–60.

[75] Мироненко Г.В. Інтернет-психологія: напрями досліджень і перспективи розвитку / Г.В. Мироненко, Н.В. Климчук // Ученые записки Таврического національного университета им. В.И. Вернадского. Серия „Филология. Социальная коммуникация". – 2008. – Том 21 (60). – № 1. – С. 333–337.

[76] Кастельс М. Становление общества сетевых структур // Новая постиндустриальная волна на Западе: антология. – М., 1999. – С. 494–495.

5. Спроможні до модернізації та «мімікрії» в найкоротший термін.

6. Створюються для реалізації заздалегідь визначених цілей інформаційно-психологічної діяльності.

7. Наявність мотивуючої ідеології, знаків, символів.

8. В умовах інформаційного протистояння (чи навіть реальних військових конфліктів) вербують «агентів» для ведення широкомасштабної розвідувальної, диверсійної і партизанської війни в інформаційно-психологічному просторі держав-конкурентів. Усі ці спільноти та об'єднання є множинність не віртуальних, а реальних учасників. Проблема людини в інформаційному просторі розглядається у двох напрямках: по-перше, це дослідження віртуальності, по-друге, дослідження проблеми буття людини у віртуальному просторі.

За допомогою використання ефектів мультимедійних технологій віртуальний світ тісно переплітається з реальним світом. Комунікаційна система віртуальності охарактеризована Л. Земляновою як «система, в якій реальність (матеріальне та символічне існування людей) повністю захоплені, занурені у віртуальні образи, у вигаданий світ, в якому через зображення передається інформація»[77].

Глобалізація віртуальної реальності сучасної цивілізації створює передумови формування єдиного загальносвітового інформаційного простору на базі нових комп'ютерних технологій, Інтернету, ЗМІ. Зміни, що відбуваються в інформаційній сфері, обумовлюють вирішення проблем, пов'язаних із забезпеченням безпеки особистості, суспільства і держави в цілому.

Суттєвою ознакою сучасного етапу розвитку цивілізації є глобалізація віртуальної реальності, яка, як процес є частиною життя сучасного суспільства й існування світу без неї вже немислимо. На даний момент вона є невід'ємною частиною суспільних взаємин. Засоби масової інформації, мережа Інтернет активно використовують даний процес для інформування людства про проблеми, що відбуваються у світі. Уявляється, що процеси зберігаються й посилюватимуться, трансформуватимуться в інформаційну глобалізацію, що в більшій мірі знаходиться під контролем світової спільноти.

[77] Землянова Л.М. Сетевое общество, информационализм и виртуальная культура // Вестник Московского университета. Сер. 10. Журналистика. – 1999. – № 2. – С. 58–69.

Поєднання економік в єдиному ринку найчастіше приносить користь кожній країні, а з іншого боку, в результаті підйому продуктивних сил, зростання доходів і конкуренції переможці і переможені є в кожній державі. На даному етапі глобалізації віртуальної реальності не можна сказати, добре це або погано. Як і всякий процес, глобалізація віртуальної реальності має як позитивні, так і негативні сторони. На перший погляд, потрібно тільки прагнути ліквідовувати недоліки даного процесу, а його позитивні сторони використовувати на благо.

Остання третина XX ст. внесла принципово нові риси у процеси глобалізації і віртуалізації, які стали визначати долю людства: одночасна дія чинників глобалізації й віртуалізації. Вони виразно заявили про себе в різних сферах і в різних формах. Ю. Яковець виділяє 5 форм чинників глобалізації: 1) демографо-екологічні чинники; 2) глобалізація техносфери; 3) економічна глобалізація; 4) геополітична глобалізація; 5) соціокультурна глобалізація[78]. До названих чинників глобалізації слід додати й глобалізацію віртуальної реальності[79].

На наш погляд, глобалізація віртуальної реальності пронизує всі наведені чинники і в даний час уявляється найбільш складним і суперечливим компонентом розвитку глобалізації. Особливу роль глобалізація віртуальної реальності відіграє в економічній і соціальній сферах (у сфері науки, культури, освіти, етики, ідеології). З одного боку, все більш виразно виявляється глобальний характер наукового прогресу, що не знає національних меж, здійснюється обмін науковими ідеями за допомогою Інтернету; формуються загальні контури системи безперервної освіти, орієнтованої на креативну педагогіку, яка спирається на високоефективні інформаційні технології (дистанційна освіта); розвивається, обмін культурними цінностями; розповсюджується знеособлена, позбавлена національного змісту масова антикультура; руйнуються колишні етичні засади, відроджується вплив світових релігій. Одночасно спостерігаються протилежні тенденції диференціації, відродження й відособлення національних культур, різноманітності педагогічних шкіл та індивідуалізації процесу освіти.

«Інтенсивне використання технологій віртуальної реальності має певний соціальний сенс – заміщення соціальної реальності її

[78] Яковец Ю.В. Глобализация и взаимодействие цивилизаций. – М.: Экономика, 2001. – С. 238.

[79] Дзьобань О.П. Діалектика глобалізації віртуальної реальності й суспільного розвитку // Гілея: науковий вісник, 2012. – Випуск 63 (№ 8). – С. 254–260.

комп'ютерними симуляціями», – справедливо зазначає Д. Іванов[80]. Віртуалізація процесів соціального розглядається як структурна диференціація системи внаслідок появи в ній нових елементів – віртуальних аналогів реальних комунікацій. Суспільство набуває рис глобальної віртуальної реальності. Віртуалізація як технологічний процес заснована на самій віртуальності, і має соціальні наслідки як процес соціальний, але опосередкований комп'ютерами і без комп'ютерів неможливий.

Найважливішим підсумком глобалізації є формування єдиного віртуального простору як нового онтологічного і культурного рівня соціальної загальності. Віртуальний простір існує на іншому, віртуальному, онтологічному рівні буття, зв'язуючи соціум принципово новим виглядом віртуальних зв'язків і взаємодій. Віртуальні соціальні зв'язки і взаємодії, віртуальні феномени стають не тільки повсюдно поширеними, а необхідними для функціонування й розвитку сучасного соціуму. Віртуалізація суспільства виступає як глобальний процес сучасності та виявляється у віртуалізації економіки, політики, мистецтва, науки і системи освіти[81].

Формування глобального віртуального світу наближає світ віртуальної реальності до реальності дійсної. Наближення до реальності одного з віртуальних рівнів буття істотно впливає на реальне життя суспільства, змінюючи його соціальні свободи, впливає на громадську думку.

Аналізуючи сказане, можна виявити позитивні наслідки процесу глобалізації віртуальної реальності – прискорення впровадження та розповсюдження технічних нововведень і сучасних методів управління, поява нових економічних можливостей як для окремих осіб, так і для держав, можливостей забезпечення вищого рівня життя тощо.

Процес глобалізації віртуальної реальності призводить до зміни ціннісних орієнтирів суспільства, особистості й культури в цілому (легке досягнення ідеалу, віртуальна дружба тощо). У зв'язку з цим, до негативних наслідків глобалізації віртуальної реальності варто віднести збільшені загрози цілісності культур і суспільства в цілому. Суперечність полягає і в тому, що сформовані післявоєнні інститути міжнародної спільноти виявилися не готовими ефективно функціонувати в умовах глобалізації світу й віртуальної реальності. У

[80] Иванов Д.В. Виртуализация общества. – СПб.: Петербургское Востоковедение. – 2000. – С. 22.

[81] Дзьобань О.П. Діалектика глобалізації віртуальної реальності й суспільного розвитку // Гілея: науковий вісник, 2012. – Випуск 63 (№ 8). – С. 254–260.

результаті віртуалізація процесів суспільства постає радикальною трансформацією способу існування цивілізації.

Глобальне віртуальне середовище створює технологічну основу об'єднання інтелектуальних здібностей і духовних сил людства, але вона ж виступає визначальним чинником «віртуальної експансії» в суспільну й індивідуальну свідомість, у якій центральну роль відіграють нові засоби масової комунікації. Влада та вплив у віртуальному інформаційному суспільстві належить тим, хто здатний розробляти комп'ютерні програми, використовувані суспільством для відображення реальності, ухвалення рішень. Віртуальна влада є цілком реальною, оскільки трансформується у здатність окремих осіб або груп нав'язати волю суспільству (індивіду).

Міжнародна еліта, що управляє мережевим суспільством, глибоко інтегрована в простір віртуальних інформаційних потоків, які складаються перш за все з фінансової, соціально-політичної, екзистенційної інформації. Чим активніше еліта включена в простір міжнародних віртуальних потоків інформації, тим слабкішою є її залежність від певної національної культури, тим менше вона підконтрольна урядам, легітимним органам.

Технічні нововведення віртуалізації і глобалізації не означають радикальної зміни самого суспільства. Головну роль відіграє перетворення не в матерії, а у свідомості – як індивідуальній, так і суспільній.

До негативних наслідків глобалізації віртуальної реальності також слід віднести активізацію ведення інформаційних та інформаційно-психологічних воєн між окремими країнами. Ці війни відбуваються в умовах появи нових форм збройної боротьби, підйому сепаратистських рухів, посилення діяльності міжнародних терористичних організацій, зниження можливостей держав з контролю над процесами, що відбуваються в межах їх національних територій, при яких використовуються методи інформаційно-психологічного впливу. У зв'язку з формуванням загальносвітового інформаційного простору неухильно зростає роль громадської думки, яка сьогодні стала могутнім чинником управління, виховання і регулювання поведінки людей.

З наведеного видно, що проникаючи буквально у всі сфери життя, глобалізація віртуальної реальності несе в собі певний рівень небезпеки. Останніми роками спостерігається стійка світова тенденція зростання комп'ютерної злочинності. Чим більше сфер людського буття включається у глобальний простір віртуальної реальності, тим

привабливішим він стає для хакерів. До об'єктів безпеки глобальної віртуальної реальності відносяться інформаційні ресурси; системи формування, розповсюдження й використання інформаційних ресурсів; інформаційна інфраструктура; сама людина; корпоративні групи людей і суспільство в цілому.

У сучасному світі безпечний розвиток будь-якого суспільства, людини пов'язано з безпекою віртуальної реальності, оскільки системотворчим чинником цього розвитку є віртуальне середовище (Інтернет). Безпека віртуальної реальності характеризується здатністю суспільства і окремо взятої особи забезпечити з певною вірогідністю достатні і захищені інформаційні ресурси і інформаційні спроби для підтримки своєї життєдіяльності і життєздатності, протистояти негативним інформаційним впливам на індивідуальну й суспільну свідомість і психіку людей, а також на комп'ютерні мережі та інші технічні джерела інформації, здійснювати інформаційно-психологічне протиборство.

Слід відзначити, що безпека віртуальної реальності є важливим і дуже складним, різнорідним напрямом у загальній системі соціальної безпеки суспільства. Безпека віртуальної реальності торкається проблеми військової, економічної, політичної, етнічної, демографічної, ідеологічної й інших видів безпеки суспільства. У зв'язку з цим, необхідно виробити спільні підходи до вирішення проблеми боротьби з негативним впливом глобальної віртуальної реальності через створення єдиної системи безпеки віртуальної реальності. Забезпечення необхідної інформаційної безпеки як для окремої держави, так і всієї світової спільноти повинне стати одним з важливих напрямів діяльності стосовно запобігання майбутнім інформаційним впливам на людину й суспільство в цілому.

Завдання створення системи безпеки при глобалізації віртуальної реальності набуває все більш актуального характеру. Держави й інші суб'єкти міжнародного права повинні нести міжнародну відповідальність за діяльність в інформаційному просторі, здійснювану ними, під їх юрисдикцією або в рамках міжнародних організацій, членами яких вони є.

Важливе місце при розгляді поняття «глобальна безпека віртуальної реальності» займає поняття міжнародної інформаційної безпеки. Поняття «міжнародна безпека» пов'язують, зазвичай, з особливим станом світової спільноти і міждержавних відносин, при якому досягається їх стійкість до впливу дестабілізаційних чинників, загроз, що не перевищують припустимий рівень при відповідному

балансі національних і регіональних інтересів, узгодженій економічній політиці і військовій діяльності.

Основний збиток життєво важливим інтересам особи, суспільства та держави наносять інформаційні війни («віртуальні інформаційні війни» з використанням простору віртуальної реальності), здійснювані іноземними технічними розвідками і спецслужбами, промислове шпигунство тощо.

Глобалізація віртуальної реальності докорінним чином змінила прийоми ведення інформаційної війни. Сьогодні поняття «інформаційна війна» знайоме громадянам будь-якої країни. Люди асоціюють його з такими загрозами своїй безпеці, як створення перешкод, використання, псування або знищення інформації і порушення її функцій. Багато інформаційних атак націлені на враження штучних супутників, засобів управління військами, органами і силами забезпечення соціальної безпеки. Особливу небезпеку представляють віртуальні інформаційні війни, направлені на зміну свідомості людини.

В даний час розвиваються засоби і способи ведення інформаційної війни, яка включає будь-яку дію стосовно переривання, використання, спотворення або знищення інформації супротивника. Фахівці виділяють новий вид зброї – інформаційно-психологічну, яка впливає через свідомість на психіку людини в основному за допомогою засобів масової інформації, комп'ютерних ігор, системи Інтернет.

Жодна країна сьогодні не може уникнути впливу глобалізації віртуальної реальності, але перед кожною державою стають проблеми, які не мають однозначного вирішення. Усі вони вимушені шукати свої відповіді, знаходити свої рішення виникаючих проблем. Наслідки глобалізації віртуальної реальності для кожної країни значною мірою залежать від позиції політичних еліт і політики держави, які повинні виробити систему безпеки в умовах глобалізації і універсалізації віртуальної реальності.

Отже, сьогодні ми не можемо однозначно оцінити процес глобалізації віртуальної реальності як свідчення позитивного або негативного розвитку. Таким чином, ми повинні говорити про ризики глобалізації віртуальної реальності (легкість благ, що набувають на шляху неправильної експлуатації віртуальних знань і ін.), про невизначеності, пов'язані з глобалізацією віртуальної реальності, і постаратися з'ясувати хоч б у загальних рисах характер цих ризиків.

Ведучи мову про майбутнє глобалізації віртуальної реальності, про зниження її ризиків, можна виділити три значущі альтернативи.

Перша альтернатива полягає в контролі держав над соціальними процесами в суспільстві; другою альтернативою є встановлення єдиних стандартів у сфері безпеки віртуальної реальності (світовий уряд, єдині закони). Третій варіант – коли найбільш розвинені в соціальному відношенні регіони світу спільно формулюють загальні правила соціальної взаємодії і спільно вирішують питання, пов'язані із забезпеченням безпеки віртуальної реальності. Уявляється, що саме цей шлях розвитку світової спільноти найбільш вірогідний і не перешкоджає подальшому розвитку глобалізації віртуальної реальності. Він одночасно необхідний для забезпечення соціального зростання і має найбільші шанси звести до мінімуму ризики глобалізації віртуальної реальності.

Віртуальний простір, «містить інформаційну компоненту матеріальних суб'єктів», тобто інформаційний простір, як відображення в свідомості індивіда уявлень про світ через систему цифрових кібертехнологій[82].

Вперше поняття «кіберпростір» було у 1984 р. письменником У. Гібсоном для позначення сукупності інформації, що міститься в комп'ютерних мережах. У дослідженнях вчених *«глобальний кіберпростір»* (*globalcyberspace*), мережевий інформаційний простір трактується як унікальне явище, що має тенденцію до динамічної зміни параметрів, чого не відбувається з фізичними об'єктами[83].

Кіберпростір володіє низкою ознак та характеристик, визначальними серед яких є: інформаційність, комунікативність, технологічність. Тому різноманіття підходів у визначенні сутності цього явища обумовлене надшвидким розвитком як комп'ютерних технологій, так і процесами формування свідомості нового типу – віртуальної свідомості.

Віртуально-кібернетичний підхід. Відповідно до визначення командувача ВПС США М. Уінна 20 березня 2007 р. на засіданні Сенату США про створення тимчасового кіберкомандування ВПС США кіберпростір – «середовище, в якому електронний та електромагнітний спектр використовується для зберігання, модифікації та обміну даними через мережеві системи та відповідні фізичні інфраструктури»[84].

---

[82] Иванов А.К. Глобальное информационное пространство и его место в современном международном праве // Ползуновский вестник. Барнаул: АлтГТУ – 2005. – № 1. – С. 220.

[83] Bryant W.D. Cyberspacesuperiority. A conceptual model // Air & Space Power Journal. – 2013. – November – December.; Butler S.C. Refocusing cyberwarfare thought / S.C. Butler // Air & Space Power Journal. – 2013. – January – Februaty.

[84] Супрунов Ю.М. Нормативно-правове забезпечення розгортання систем кібернетичної оборони провідних країн світу // Інформаційна безпека людини, суспільства, держави. – 2011. – № 1 (5). – С. 86.

Соціотехнічний підхід розкриває сутність кіберпростору через інтегративну функцію, що об'єднує соціальну та технічну складову цього явища: «…Складовими кібернетичного простору є: інформаційний простір, комунікаційний простір, віртуально-комп'ютерний мережевий простір та соціотехнічний простір»[85].

Віртуально-інтелектуальний підхід містить спроби осмислення ідентичності кіберпростору та інфосфери, як середовищ, що акумулюючи грандіозні масиви інформації в невизначеному та безконечному простір-часі, володіють «власним інтелектом», так званим світовим розумом, може стихійно оновлюватись, подавати інформацію незалежно від запрограмованих кодів, операційних програм та алгоритмів. Тобто віртуально-технічне явище набуває ознак істоти з індивідуальним мисленням.[86].

Космополітично-соцієнтальний визначає кіберпростір як середовище у якому народжується і самореалізується космополітична свідомість, механізм якісно нового типу комунікації між суб'єктами діяльності. Цей підхід особливо наголошує на ідеологічних імперативах Інтернету про ліквідацію кордонів, утворення єдиної «світової держави», де люди зможуть реалізуватися незалежно від індивідуальних характеристик та ознак за принципом справедливості. Це новітнє середовище створює свої світові спільноти і прагне модернізації норм та суспільних законів відповідно до сучасних реалій інформаційного суспільства, рівність та рівноправність он-лайн повинно екстраполюватись у оф-лайн реальність. «Кіберпростір являє собою абсолютну модель космополісу – без кордонів, без національностей та рас, цілковита індивідуальність кожного «громадянина»[87].

Військово-прикладний підхід зараховує кіберпростір до сфери військового протиборства, як комплексне середовище для застосування сил і засобів інформаційної та збройної боротьби. За визначенням Ю. Супрунова це «мережа інфраструктури, електронні засоби та засоби розповсюдження електромагнітних випромінювань, інші фізичні інфраструктури, сполучені із соціотехнічним простором, які використовуються для створення, зберігання, модифікації та передачі інформації, управління об'єктами (системами) та зброєю

[85] Даник Ю.Г. Кібернетичний простір та забезпечення кібернетичної безпеки держави // Тези доповідей IV міжнародного науково-технічного симпозіуму „Нові технології в телекомунікаціях" (8–21 січня 2011 р.). – К.: ДУІКТ. – С. 57.

[86] Бояндин К. Инфосфера как разумная среда обитания [Електронний ресурс]. – Режим доступу: http://boyandin.name/blog/590/infosfera-kak-razumnaya- sreda-obitaniya

[87] Козуб О.О. Кіберпростір як середовище породження і самореалізації принципу космополітизму // Гуманітарний вісник ЗДІА. – 2010. – № 43. – С. 178.

впливу на об'єкти (системи) протидіючої сторони, а також інформацію яку вони містять»[88].

З перетворенням віртуальної реальності на життєве середовище сучасної людини, з розвитком цифрових технологій і пов'язаних з ними змін способів спілкування змінюються також і багато глибинних сутнісних характеристик особистості. Сучасна людина об'єктивно знаходиться у стані системної кризи ідентичності, яка спричинена комплексом протиріч між консерватизмом індустріального суспільства та творчістю і креативністю сприйняття майбутнього у прогресивному інформаційному суспільстві. Вивчення онтології віртуальності, дає можливість окреслити образ віртуальної людини: по-перше, вона є осереддям реальностей, джерелом і центром інтеграції множинних вимірювань віртуального як ідеального, втіленого в комунікативному просторі культури, який знаходить реальність у результаті дії його вольового акту; по-друге, віртуальна людина найбільш повно визначається в полі соціального і виявляється в сукупності комунікативних практик[89], по-третє, віртуальна людина повністю втрачає право на «особисте життя» та ідентифікується як «суб'єкт віртуального суспільства» у соціальному просторі безлічі електронних баз даних. Таким чином, людина стає одночасно *суб'єктом, об'єктом* інформаційного віртуального впливу та споживачем й виробником інформаційного продукту.

Суб'єкти глобального віртуального інформаційного простору характерні та унікальні:

- соціальна віртуальна спільнота;
- он-лайн спільнота;
- мережевий соціум;
- віртуальна коаліція.

Віртуальна соціальна спільнота – це соціальна система, сукупність різних соціальних систем та їх окремих елементів, сегментів інформаційного простору, джерел інтелектуальних і матеріальних ресурсів, які існують безвідносно до реального часу-простору та об'єднаних для досягнення єдиної мети єдиною ідеологією, яка є головним системоутворюючим чинником.

Он-лайн спільнота є спільнотою суб'єктів діяльності, яка ґрунтується на масовому переносі людьми, групами, організаціями інформаційної активності та взаємодій інтермереж в режим он-лайн.

---

[88] Супрунов Ю.М. Нормативно-правове забезпечення розгортання систем кібернетичної оборони провідних країн світу // Інформаційна безпека людини, суспільства, держави. – 2011. – № 1 (5). – С. 86.

[89] Лугуценко Т.В. Людина в структурі комунікативної реальності як суб'єкт віртуального простору // Гілея. – 2014. – № 81. – С. 180.

Мережевий соціум – це група людей, взаємодія яких відбувається переважно в глобальних комп'ютерних мережах.

Віртуальна коаліція – це суб'єкти геополітичної конкуренції у вигляді віртуальних союзів в складі медіа-холдингів, масштаби діяльності яких мають глобальний характер.

Гіперрозвиток сучасних інформаційно-комунікаційних технологій спровокував появу нових професій у цих галузях, а саме: IT-фахівці: програміст, системний адміністратор, perl-програміст, веб-дизайнер, системний аналітик та ін. Водночас зріс попит на «професійних комунікаторів» у мережі, що займаються деструктивно-замовною діяльністю, яка негативно впливає на якість інформаційного продукту в Інтернеті та проходить на межі легального правового поля: *розробників ботів* (спеціальних програм, що використовуються для автоматичного розповсюдження реклами (агресивний маркетинг), спаму або вірусних шкідливих програм; *хакерів*, які здійснюють DdoS-атаки на сервера та інформаційні ресурси з метою виведення систем з ладу, *тролів,* які розміщують брутальні або провокаційні повідомлення в Інтернеті. В інформаційних війнах активно використовують потенціал цих агресивних «бійців віртуального фронту» для маніпуляцій суспільною свідомістю та шантажу держав.

Інтегрованою просторово-часовою одиницею віртуальної реальності інформаційно-комунікативної мережевої інфраструктури та однією із найбільш ефективних форм організації Інтернет-середовища у глобальному інформаційному просторі є блогосфера. *Блогосфера*, на нашу думку, – сегмент глобального інформаційного простору, який утворюється і функціонує як комплекс взаємодіючих суб'єктів віртуального середовища та джерел інформації, що формують систему інформаційно-комунікаційних зв'язків, яка здатна до синергетичного оновлення, трансформації, розповсюдження та кореляції інформаційних ресурсів для маніпуляції суспільною свідомістю. Інформаційним ресурсом блогосфери є *блог* – веб-сайт або персональний сайт, який містить короткі записи тимчасової важливості та значущості, має відкритий характер і передбачає обговорення, публічну полеміку в коментарях до блогозаписів або на власних блогах у середовищі мережевого спілкування. Суб'єктом віртуального середовища є *блогер* – функціонер, який веде блог. Блог (скор. від англ. weblog – «мережевий журнал») – персональна сторінка в Інтернеті, що містить інформацію у зворотному

хронологічному порядку[90]. Сучасна блогосфера має ознаки комерціалізації (поширення реклами та просування «платних» тем чи персон), деперсоніфікації (блогер не веде блог особисто, а користується послугами професіоналів) та криміналізації (протиправний характер делінквентної поведінки) і стає простором для розгортання суспільних практик[91]. Блогосфера виконує у суспільно-політичному житті такі функції: інформаційну, експресивну, дезінформуючу, дискредитаційну, презентаційну, маркетингову і культуротворчу.

Об'єктивна реальність процесів глобалізації та модернізації спровокували появу унікального соціодуховного феномена – *віртуальної культури*, яка знаходиться зараз у процесі становлення та розвитку, але, на нашу думку, варто виокремити такі її характерні риси: плюралізм структурних компонентів культури; багатополюсність – відсутність домінуючого центру визначення ціннісних орієнтацій; домінування інформації в формі формалізованого семантичного образу; антиієрархічність та нелінейність в кодуванні інформації; інноваційність та інваріантність; персоналізація – орієнтація культури на конкретну людину; трансформація потреб і ціннісних орієнтацій людини.

Сучасна віртуальна культура виявляється через гіпертекст, який «комбінує, артикулює і виражає смисли у вигляді аудіовізуальної мозаїки, яка здатна змінювати форму залежно від цільової аудиторії»[92].

Віртуальна реальність мережевих комунікацій володіє специфічними та особливими характеристиками. Серед переваг слід відзначити: зручність; доступність; свободу вибору сфери комунікативного спілкування; величезний організаційний потенціал; оперативність; практичне зняття просторових кордонів для комунікативних зв'язків; динамічність реакції користувачів на отриману інформацію; створення унікальних передумов для всебічного розвитку особистості.

Недоліками використання Інтернету є: ймовірність технічних помилок; створення та розповсюдження комп'ютерних вірусів; інтелектуальне шахрайство та плагіат; культивація насилля, порнографії; доступність відстеження комунікацій в мережі;

[90] Bar-Ilan J. Information hub blogs // Journal of Information Science. – 2005. – Vol. 7. – No.4. – P. 297–307.
[91] Castells M. The New Public Sphere: Global Civil Society, Communication Networks, and Global Governance // The ANNALS of the American Academy of Political and Social Science. – 2008. – Vol. 616. – No.1. – P. 78–93.
[92] Кастельс М. Становление общества сетевых структур / М. Кастельс // Новая постиндустриальная волна на Западе: антология. – М., 1999. – С. 494–495.

застосування для диверсійних, терористичних актів; розвиток хакерського середовища; поширення недостовірної інформації («фейків»); порушення етики мережевого спілкування з метою штучного створення конфліктної ситуації (троллінг); кібербуллінг – приниження та переслідування у мережі Інтернет. Походить від юридичного терміну «буллінг» (від англ. bullying) яким позначається певний перелік дій, що здатні викликати переляк, принизити чи іншим чином негативно вплинути на людину.

Усе це провокує появу комплексу проблем, які можуть становити загрозу психофізичному здоров'ю та соціально-духовному стану людини: наявність надлишку інформації сучасної віртуальної особи; ґрунтовні зміни типу мислення та свідомості; зниження рівня критичного аналізу спожитої інформації[93].

Отже, тенденції до глобалізації інформатизації, пришвидшення руху інформаційних потоків та збільшення об'ємів інформації призводять також до виникнення проблеми інформаційної нестабільності. У ній слід виокремити такі основні групи:

1. Кількісна нестабільність інформації, яка пов'язана із змінами її об'ємів у соціальній системі суспільства, відображає одночасно і недостатність й надлишковість інформації.

2. Якісна нестабільність, яка виражена у поширенні та збільшенні обсягів змістовної чи беззмістовної інформації, як парадоксальність недостатності інформації в умовах її надлишку. Це виявляється у формах інформаційного шуму («інформаційне сміття») та шкідливої інформації (свідоме поширення інформації з метою негативного впливу на індивідуальну та суспільну свідомість). Відбувається своєрідне порушення *інформаційного балансу*, який обумовлює гармонійний стан інформаційного простору.

3. Нестабільність обігу інформації пов'язана з нерівномірністю інформатизації у сучасному суспільстві, оскільки різні соціальні групи та соціальні спільності мають нерівноцінні потенції доступу до інформаційних ресурсів та неоднакові можливості участі у загальному обігу інформації[94].

4. Перевантаження мережевих комунікацій, шкідливий вплив вірусів й хакерських атак.

5. Віртуалізація життя суспільства, зокрема окремих його сфер – інтернет-банкінг та комп'ютерні бази даних, зумовили ймовірність

[93] Говорухина К.А. Глобальное информационное общество и новые аспекты изучения пропаганды в контексте информационной безопасности // Человек. Общество. Управление. – 2012. – № 1. – С. 27.

[94] Писаренко О.Л. Розвиток сучасного суспільства в умовах інформаційної нестабільності // Розвиток сучасного суспільства в умовах глобальної нестабільності: мат. міжнар. наук.-практ. конф. – Одеса, 2013. – С. 46.

загрози поширення у мережі особистої інформації, яка становить таємницю приватного життя та певним чином може дестабілізувати життя суспільства.

Ця сукупність причин слугує підставою для виникнення *інформаційного колапсу* – стану мережевого інформаційного простору, який загрожує його стабільній роботі та функціонуванню, внаслідок різкого зниження перепускної здатності каналів зв'язку та неможливості передачі збільшених об'ємів трафіку.

Формування глобального інформаційного простору виявляє не лише технічні проблеми, але й, значно важливіший комплекс етичних проблем. Вчені виділяють 12 граней особистості людини, які можуть бути присутні в її образі, або компілюватися на певний час за окремих обставин, особливо це виявляється, на нашу думку, в процесі залучення людини до світового комунікативного простору Інтернет[95]. Homovirtues починає вести інший спосіб життя – віртуальний. Він характеризується принципово новою системою світоглядних, етичних, психологічних констант, що визначають нові реалії буття людини у межах глобального інформаційного простору, яке завжди виявляється на межі між реальним і віртуальним, між цивілізацією і культурою, між соціумом (рухом до соціуму) і прагненням жити власним життям (егоїзм). Така ситуація обумовлює необхідність екзистенціального вибору між віртуальним простором та неможливістю відокремлення реального від віртуального[96].

Таким чином, глобальний інформаційний простір не створює нову ідеальну модель людини майбутнього, а формує нові риси характеру, які за Е. Тофлером характеризуються наступним висловом: «Нова освіта повинна навчати індивіда, як класифікувати та перекласифіковувати інформацію, як оцінювати її достовірність, як при необхідності змінювати категорії, як переходити від конкретного до абстрактного, і, навпаки, як поглянути на проблему під новим кутом зору, як займатися самоосвітою. Неграмотною в майбутньому буде не та людина, хто не вміє читати, а та, котра не навчилася вчитися»[97].

Інтернет-технології стали символами сучасності, плюралізації та демократизації джерел інформації, дають можливість людині шукати потрібну інформацію та обмінюватися нею. Став звичним процес комунікації організований за принципом піраміди, на верхівці – джерела інформації, а в основі – безліч реципієнтів. В умовах нових інформаційних технологій, спостерігається парадоксальне явище,

---

[95] Войтенко В.П. Феномен людини: Дванадцять дзеркал; Медикодослідницьке товариство „Гіппократ". – К., 1999. – 58 с.

[96] Лугуценко Т.В. Людина в структурі комунікативної реальності як суб'єкт віртуального простору // Гілея. – 2014. – № 81. – С. 180.

[97] Тоффлер Э. Шок будущего. – М.: АСТ, 2002. – С. 451.

коли у рази збільшується кількість виробників інформації, та зменшення кількості споживачів, які розуміють її справжній зміст. Це породжує стресові стани людини, викликає так званий «інформаційний шок», що зумовлено можливістю людини отримувати більшу кількість інформації та ймовірністю одночасного «інформаційного перевантаження».

Інформаційний простір – це специфічне середовище. У ньому помітно змінюється зміст таких процесів, як взаємодія, конкуренція в процесі спільної діяльності. У процесах силового протиборства здійснюється вплив на реальні бойові дії та протистояння через засоби і методи інформаційного протиборства.

РОЗДІЛ 2
ІНФОРМАЦІЙНА ВІЙНА В КОНЦЕПТІ МОДЕЛІ АСИМЕТРИЧНОГО ПРОТИСТОЯННЯ В ЕПОХУ ПОСТМОДЕРНУ

Що мене вражає – це безсилля сили. З двох могутніх факторів – сили й розуму – сила врешті-решт завжди лишається переможеною.

Наполеон I

2.1. Особливості інформаційного протиборства в сучасних умовах

Науково-технічний прогрес у сфері інформаційно-комунікаційних технологій, розвиток засобів масової комунікації спричинили створення безпрецедентних можливостей для агресивного інформаційного впливу на соціальних суб'єктів з метою нав'язування принципів устрою та життя суспільства, знищення національних духовних цінностей, зниження економічного й військового потенціалу держав шляхом впливу на індивідуальну, групову й масову свідомість.

Процес інформатизації усіх сфер життя суспільства на сучасному етапі науково-технічної революції вплинув також і на військову справу.

Воєнна наука визнала факт краху концепції тотальної війни через усвідомлення того, що подальше широкомасштабне використання зброї масового знищення проти армій і народів у війнах неминуче призведе до забруднення навколишнього середовища, глобальної катастрофи та загибелі світової цивілізації. Адже завдяки гіперрозвитку технічного прогресу навіть поняття «ядерна війна» стає своєрідним анахронізмом у воєнному мистецтві. Це об'єктивно спровокувало потребу нагального кардинального перегляду усіх класичних концепцій ведення бойових операцій.

Сучасний світ вступає в стадію воєн нового покоління, основною метою є не стільки фізичне знищення військових сил противника, скільки досягнення політичних цілей війни без застосування масових армій. Саме інформація на тлі застосування можливостей технічних і технологічних засобів стає головним воєнним потенціалом держав та «зброєю масового знищення». Тому сучасні військові теоретики розглядають війну як складне суспільно-політичне явище, яке включає сукупність різних форм боротьби: політичної, економічної,

збройної, інформаційної, психологічної й ін., що ведуть між собою держави або їх коаліції. При цьому збройну боротьбу вже не розглядають як обов'язковий атрибут війни. На світовій політичній арені та у глобальному інформаційному просторі з'явилися потужні різновекторні сили у вигляді міжнародного тероризму, домінуючого глобалізму, антиглобалізму, неоконсерватизму та націоналізму, які певною мірою є політичними акторами й суб'єктами зовнішньої та внутрішньої політики. Інформаційна відкритість сучасного світу об'єктивно сприяє здійсненню інформаційних атак у процесах комунікацій, особливо в геополітичній сфері. Трактуючи інформаційне суспільство як нову цивілізаційну реальність, що поєднує цінності та спосіб життя локальних цивілізацій із глобальними комунікаціями, слід зазначити, що становлення та розвиток інформаційного суспільства не лише відображає позитивні тенденції цих процесів, але і є потужною причиною інформаційних катастроф. Це катастрофи як технічні й техногенні, так і гуманітарні, пов'язані з руйнуванням етичних, етнічних та соціальних ідентифікаційних кодів, що забезпечують гармонійний розвиток суспільства[98]. Використання технологічних переваг стає інструментом політики інформаційного домінування, тиску та примушення в геополітичній сфері[99].

У сучасну епоху до царин ведення протиборства окрім суші, води, повітря та космосу можна зарахувати й інформаційний простір як сферу протистояння, де зброєю є інформація, а боротьба ведеться за цілеспрямовану заздалегідь визначену трансформацію індивідуальної та суспільної свідомості членів соціуму. Інформаційний простір як базовий для розвитку інформаційної війни корелює із політичним простором, перебуває з ним у постійній взаємодії та взаємопроникненні. Політичне життя суспільства завжди розгортається в просторі й часі. Соціальний простір є розгалуженою системою суспільних зв'язків, у якій фіксується співіснування величезного різноманіття соціально-предметних об'єктів, подій з

[98] Національна безпека у філософсько-правовому дискурсі: монографія / О.Г. Данильян, О.П. Дзьобань, Є.М. Білоусов, Ю.Ю. Калиновський, І.В. Яковюк. – Харків, 2019. – 244 с.; Сучасне суспільство: філософсько-правове дослідження актуальних проблем: монографія / О.Г. Данильян, О.П. Дзьобань, С.Б. Жданенко та ін.; за ред. О.Г. Данильяна. – 2-ге видан., перероб. і допов. – Харків, 2017. – 416 с.; Інформаційне суспільство в світі та Україні: проблеми становлення та закономірності розвитку: колективна монографія / за ред. д. філософ. н., проф. В.Г. Воронкової. – Запоріжжя, 2017. – 292 с.; Інформаційна війна і національна безпека: монографія / Р.В. Гула, П.П. Ткачук, О.І. Сивак та ін. – Л., 2015. – 265с.

[99] Проблема захисту національних інтересів України у сфері державної безпеки в умовах геополітичних трансформацій XXI століття: Монографія / О.П. Дзьобань, В.Я. Настюк, В.В. Бєлєвцева. – Харків, 2013. – 296 с.

точки зору їх упорядкованості, насиченості та ступеня охоплення, виражає реальний процес життєдіяльності суспільства[100].

Таким чином, інформаційний простір стає, з одного боку, ареною для запеклої геополітичної конкуренції та воєнно-політичного протистояння, з іншого – однією з найважливіших сфер життєдіяльності сучасного глобального суспільства та найважливішим інструментом впливу на формування світової громадської думки[101].

Це явище породжує цілий комплекс негативних геополітичних наслідків, найважливішими з яких, на нашу думку, є: різке прискорення поляризації світу, збільшення розриву між багатими, технологічно передовими і бідними, відсталими державами, які є головним джерелом нестабільності у світі, потенційними середовищами для виникнення конфліктів, у тому числі глобального характеру.

Процеси глобальної інформатизації та геополітичної конкуренції значно спростили доступ до інформаційно-комунікаційної інфраструктури будь-якої держави. Це призвело до того, що національні інформаційні ресурси виявилися надто вразливими об'єктами для агресивних інформаційних впливів з боку конкурентів, терористичних організацій, кримінальних угруповань та окремих зловмисників[102].

Також слід врахувати, що в інформаційному суспільстві чітко простежується тенденція до зміщення в інформаційну сферу і традиційних методів боротьби за володіння матеріальними цінностями, що, об'єктивно, призведе до загострення інформаційного протиборства[103]. Ці тенденції значно впливають на пріоритетність завдань наукових досліджень процесів і механізмів, пов'язаних з

---

[100] Ливенко В.І. Інформаційне протиборство у політичній сфері: до уточнення базових термінологічних конструкцій // Нова парадигма. – 2012. – Вип. 108. – С.137.

[101] Дзьобань О.П., Мелякова Ю.В. Комунікаційна природа інформаційного простору // Інформація і право. – 2012. – № 2 (5). – С. 81 88.

[102] Дзьобань О.П., Пилипчук В.Г. Проблема агресії і насильства: світоглядно-інформаційний вимір // Освіта регіону. – 2012. – № 2. – С. 171 – 177; Дзьобань О.П., Пилипчук В.Г. Теоретичні та державно-правові аспекти протидії інформаційному тероризму в умовах глобалізації // Стратегічні пріоритети. – 2011. – № 4 (21). – С. 12 – 17; Гула Р.В. Глобальне інформаційне суспільство: транснаціонально-громадянський науковий підхід // Соціально-правові виміри правової держави: еволюційна парадигма: зб.тез Всеукр. наук.-практ. конф. (м. Дніпро, 28 березня 2019 р.). – Дніпро, 2019. – С. 121–124.

[103] Дзьобань О.П., Данильян О.Г. Інформаційне суспільство: морально-етичний дискурс // Інформація і право. – К., 2014. – № 1 (10). – С. 16–25; Дзьобань О.П., Жданенко С.Б. Інформаційне суспільство як новий спосіб соціальної взаємодії // Правова інформатика. – № 1 (41). – 2014. – С. 3–11; Пилипчук В.Г., Дзьобань О.П. Інформаційне суспільство: філософсько-правовий вимір: Монографія. – Ужгород, 2014. – 282 с.; Інформаційне суспільство в світі та Україні: проблеми становлення та закономірності розвитку: колективна монографія / за ред. д. філософ. н., проф. В.Г.Воронкової. – Запоріжжя, 2017. – 292 с.

інформаційним протиборством, їх наслідками та загрозами у глобальному масштабі.

Інформаційне протиборство здійснювалось у всіх війнах і конфліктах людства. У останню чверть XX ст. склалася ***система інформаційного протистояння «холодної війни»,*** яку трактували як комплекс цілеспрямованих заходів техногенного та гуманітарного рівня з метою вирішення завдань для блокування чи пошкодження каналів управління і зв'язку противника, його дезінформування, створення атмосфери напруженості та паніки в тилу ворога від постійного очікування ударів, а також впливу на свідомість суперника з метою його деморалізації.

У сучасних умовах за допомогою новітніх технічних засобів і глобальних інформаційно-комунікаційних технологій значно зросли можливості для інформаційних атак на великих територіях і впливу на масову аудиторію у найкоротші терміни. Разом із позитивними явищами глобальної інформатизації чіткіше проступають контури нових міжнародних проблем сфери інформаційної безпеки держави та інформаційного протиборства[104]. Чіткіше простежується пряма залежність стабільності та легітимності політичної влади від можливостей ведення інформаційного протиборства у зовнішньо- та внутрішньополітичній сферах. Основні тенденції зміни напрямів розвитку та характеру геополітичної боротьби держав у процесі глобалізації на початку XXI ст. свідчать про те, що все активніше застосовуються інформаційні методи та засоби для досягнення воєнно-політичних цілей і вирішення завдань.

Критичне загострення протиборства в інформаційній сфері досягло таких глобальних масштабів, що витребувало необхідність створення спеціальної концепції, яка отримала назву «інформаційне протиборство». Уявляється, що в межах такої концепції інформаційне протиборство у найзагальнішому вигляді можна визначити як активне зіткнення контрсуб'єктів (держав, соціальних груп, організацій) у інформаційно-психологічній сфері, що характеризується використанням методів, способів і засобів відкритого і прихованого інформаційного (інформаційно-психологічного) впливу супротивників один на одного з метою

[104] Дзьобань О., Соснін О. Інформаційна безпека: нові виміри загроз, пов'язаних з активізацією міжнародної діяльності в інформаційно-комунікаційній сфері // Вісник Львівського університету. Серія: міжнародні відносини. – 2015. – Випуск 37. – Частина 3. – С. 35–43; Дзьобань О.П. Пилипчук В.Г. Вплив глобалізаційних процесів на державний суверенітет України // Вісник Національної юридичної академії України імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія / Редкол.: А.П.Гетьман та ін. – Х., 2010. – Вип. 3. – С. 96–103; Дзьобань О.П., Пилипчук В.Г. Теоретичні та державно-правові аспекти протидії інформаційному тероризму в умовах глобалізації // Стратегічні пріоритети. – 2011. – № 4 (21). – С. 12–17.

досягнення конкретних політичних та інших цілей, у результаті якого одні учасники протиборства отримують переваги, необхідні їм для подальшого розвитку, а інші їх втрачають (В. Ливенко)[105].

Інформаційне протиборство, як невід'ємна складова політичних відносин, є одним із основних інструментів політичного примусу в сучасних умовах. Тому, не випадково воно супроводжує всі форми політичної боротьби. Іншими словами, інформаційне протиборство вже не обмежується масштабним впливом на населення і війська, а й спрямоване на владу, еліту та суспільну свідомість держав-противників і партнерів, на системи прийняття рішень в усіх сферах життєдіяльності держави. Політичні актори, перебуваючи в стані жорсткої конкуренції (або конфлікту), безперервно обмінюються інформаційними впливами, які стають все більш витонченими та небезпечними[106].

У сучасному науковому дискурсі існує комплекс підходів до визначення суті поняття «інформаційне протиборство»:

Геополітичний підхід наголошує на пріоритетному значенні завдань міждержавного глобального протистояння й визначає інформаційне протиборство як «суперництво соціальних систем в інформаційно-психологічній сфері для впливу на ті чи інші сфери соціальних відносин й встановлення контролю над джерелами стратегічних ресурсів, в результаті якого одні учасники суперництва отримують переваги, які необхідні для подальшого розвитку, а інші їх втрачають»[107].

Державно-інструментальний підхід визначає його як «форму боротьби, сукупність спеціальних (політичних, економічних, дипломатичних, технологічних, військових та інших) методів, способів і засобів вигідного впливу на інформаційну сферу об'єкта зацікавленості та захисту власної інформаційної сфери для досягнення поставлених цілей[108].

Військово-прикладний підхід трактує інформаційне протиборство як «комплекс заходів інформаційного характеру, які здійснюють з метою захоплення й утримання стратегічної ініціативи, досягнення інформаційної переваги над противником і створення сприятливого

---

[105] Ливенко В.І. Інформаційне протиборство у політичній сфері: до уточнення базових термінологічних конструкцій / В.І.Ливенко // Нова парадигма. – 2012. – Вип. 108. – С.138.

[106] Горбенко А. СМИ в сфере информационного противоборства // Власть. – 2008. – № 11. – С. 25.

[107] Манойло А.В. Государственная информационная политика в особых условиях [Електронний ресурс]. – Режим доступу: http://razom.znaimo.com.ua/docs/45/index-18501.html

[108] Історія інформаційно-психологічного протиборства: підруч. / [Я.М. Жарков, Л.Ф. Компанцева, В.В. Остроухов, В.М. Петрик, М.М. Присяжнюк, Є.Д. Скулиш]; за заг. ред. д.ю.н., проф., засл. юриста України Є.Д. Скулиша. – К., 2012. – С. 26.

пропагандистського підґрунтя при підготовці й веденні бойової та іншої діяльності збройних сил»[109].

Соціологічний підхід визначає інформаційне протиборство як «вид соціальної протидії, інформаційний вплив на опонента (противника) з метою спотворення сприйняття та розуміння ним ситуації, що спонукає його приймати помилкові рішення»[110].

Технологічний підхід наголошує на аспекті використання усього спектра можливостей інформаційно-комунікативної інфраструктури з метою досягнення переваги над противником[111].

Психологічний підхід. На нашу думку, інформаційне протиборство є цільовим комплексним впливом на суспільну та індивідуальну свідомість для інтенсифікації процесів їх еволюції та послідовний перехід від однієї світоглядної парадигми до іншої з одночасною деформацією (або руйнуванням) символів і образів, які є основою мислення людини, тобто ідентифікаційних патернів особистості.

Отже, на нашу думку, термін «інформаційне протиборство» варто трактувати у двох смислових варіантах:

- *у широкому сенсі* – для визначення протиборства в інформаційній сфері та ЗМК для досягнення певних політичних, економічних і соціально-культурних цілей;

- *у вузькому сенсі* – для визначення комплексу воєнних дій, військове протиборство в інформаційної сфері з метою досягнення домінування при зборі, обробці й використанні інформації на полі бою та зниження ефективності відповідних дій противника.

Стратегічний рівень інформаційного протиборства визначають вищі органи влади, оперативний і тактичний – спецслужби та «великий капітал».

На нашу думку, інформаційне протиборство в безконтактних війнах – це нова стратегічна форма боротьби сторін у глобальному інформаційному просторі з використанням комплексу спеціальних технічних і психологічних способів та засобів для досягнення геополітичних цілей; сукупність спеціальних (політичних, економічних, дипломатичних, технологічних, військових та інших) методів, способів і засобів вигідного впливу на інформаційну сферу

---

[109] Там само. – С. 26–27.

[110] Война и мир в терминах и определениях [Електронний ресурс]; под общ. ред. Д. Рогозина. – М., 2004. – Режим доступу: www. royallib.ru/book/rogozin_dmitriy.html

[111] Информационное противоборство на современном этапе: анализ и тенденции [Електронний ресурс]. – Режим доступу: http://www.molych.ru/ politika/ informatsionnoe-protivoborstvo-na-sovremennom-etape-analiz-i-tendentsii.html

об’єкта, а також захисту власної інформаційної сфери в інтересах досягнення поставлених цілей.

Вищою формою інформаційного протиборства є ***інформаційна війна*** – форма ведення інформаційного протиборства різними суб’єктами (державами, неурядовими, економічними або іншими структурами), що передбачає здійснення комплексу заходів із завдання шкоди інформаційній сфері конфронтуючої сторони й захисту власної інформаційної безпеки[112].

Основними *принципами* інформаційного протиборства є: відповідність політичним цілям; зосередження зусиль на вирішальному просторі-часі; завчасна підготовка сил і засобів; постійна готовність до захисту від ураження; злагоджене комплексне використання сил і засобів; безперервність інформаційного протиборства, готовність і маневреність; всебічне забезпечення; послідовність у виконанні поставлених завдань.

О. Манойло до принципів інформаційного протиборства зараховує: інформаційну асиметрію – можливість вибіркового висвітлення подій, формування нових «видів новин»; інформаційне домінування – здатність до створення ефективної інформаційно-комунікаційної системи для акумуляції, обробки та управління безперервними потоками інформації з одночасним блокуванням аналогічних дій з боку противника; прихованість, латентність і маскування процесів інформаційного протиборства; раптовість і неочікуваність нападу; забезпечення стратегічного балансу сил в інформаційному просторі при мирному співіснуванні держав-конкурентів; використання недосконалості правової бази, міжнародних і національних юридичних норм для здійснення інформаційної агресії з метою завдати шкоди національним інтересам і ведення інформаційної війни для розв’язання збройної агресії; тотальне та грамотне використання засобів психологічного впливу при проведенні інформаційно-психологічних операцій[113].

Метою інформаційного протиборства є забезпечення домінування національних інтересів в інформаційній сфері.

Для реалізації мети інформаційного протиборства здійснюється комплекс *завдань*, а саме: досягнення воєнно-політичної переваги та

---

[112] Історія інформаційно-психологічного протиборства: підруч. / [Я.М. Жарков, Л.Ф. Компанцева, В.В. Остроухов, В.М. Петрик, М.М. Присяжнюк, Є.Д. Скулиш]; за заг. ред. д.ю.н., проф., засл. юриста України Є.Д. Скулиша. – К., 2012. – С. 27; Hula R., Perederii I., Vitrynska O. Information wars during a postmodern era // Collection of scientific papers on I International Scientific and Practical Conference «TECHNOLOGY, ENGINEERING AND SCIENCE – 2018», 24 – 25 October, 2018 – London: PoltNTU, 2018. – P. 99–101.

[113] Манойло А.В. Государственная информационная политика в особых условиях [Електронний ресурс]. – Режим доступу: http://razom.znaimo.com.ua/docs/45/index-18501.html

лідерства у міжнародних відносинах; проведення політики інформаційно-психологічної експансії в усіх сферах життя суспільства; створення необхідних умов для еволюційного переходу власної системи соціально-політичних відносин на новий високотехнологічний рівень розвитку; визначення пріоритетного вектора для трансформації структури інформаційного простору у відповідності з власними принципами формування інформаційної картини світу[114].

Основними формами інформаційного протиборства на державному рівні є: політичні, дипломатичні та економічні акції; інформаційні та психологічні операції; підривні й деморалізуючі пропагандистські дії; сприяння опозиційним і дисидентським рухам; здійснення усебічного впливу на політичне і культурне життя з метою розвалу національно-державних підвалин суспільства; проникнення в систему державного управління[115].

Видами інформаційного протиборства є інформаційно-технічне й інформаційно-психологічне.

Інформаційно-технічне протиборство – вид соціотехнічної протидії інформаційно-аналітичних комунікативних систем інформаційно-технічної інфраструктури через організацію цілеспрямованого процесу виробництва і поширення спеціального інформаційного продукту, за допомогою якого можна проникати в об'єкти інформаційно-технічної сфери суспільства і порушувати їх роботу. Головними об'єктами впливу є системи телекомунікацій і зв'язку, програмне забезпечення, радіоелектронні засоби тощо. Формою інформаційно-технічного протиборства є інформаційно-технічний вплив.

Інформаційно-психологічне протиборство – процес цілеспрямованого виробництва та поширення комплексу спеціальної інформації, яка безпосередньо впливає (позитивно чи негативно) на масову та індивідуальну свідомість, розвиток інформаційно-психологічної сфери суспільства, психіку і поведінку політичної еліти та населення країни з метою трансформації соціальних процесів у напрямку необхідному для сторони, що впливає. Головними об'єктами інформаційно-психологічного протиборства є свідомість і психіка істеблішменту, населення й особового складу збройних сил, спецслужб противника та системи формування суспільної свідомості,

[114] Там само.
[115] Думанський Д. Інформаційно-психологічна боротьба як системний виклик сучасності [Електронний ресурс]. – Режим доступу: http://moloda-naciya.smoloskyp.org.ua/?p=210

громадської думки і прийняття стратегічних державно-управлінських рішень у сфері національної безпеки[116]. Формою інформаційно-психологічного протиборства є інформаційно-психологічний вплив.

Об'єкт інформаційного протиборства – це складові форм буття, сфер суспільства, стосовно яких можливо використовувати механізми та інструменти інформаційного протиборства з метою перекодування, трансформації й модифікації їх якісних характеристик як елементів інформаційної сфери.

Таким чином, *об'єктами* інформаційного протиборства є: соціальна структура суспільства; політична система держави; сукупність духовних цінностей нації, народу; масова й індивідуальна свідомість громадян; інформаційно-комунікативна інфраструктура; інформаційні ресурси; інформаційні та психологічні процеси; психічне здоров'я нації.

Суб'єкти інформаційного протиборства – це соціально-політичні формування, які мають інтереси в інформаційному просторі, спеціальні структури для ведення інформаційного протиборства, що розробляють ефективні зразки інформаційної зброї, контролюють національні сегменти інформаційного простру та діють в правовому полі державних нормативних положень, які дозволяють брати участь в інформаційному протиборстві.

Суб'єктами інформаційного протиборства, які мають чіткі стабільні інтереси в системі глобального інформаційного простору, є:

1. Держави, союзи, коаліції – здатні сформувати, контролювати власний інформаційний простір, мають можливості для підготовки кадрів і удосконалення інформаційно-комунікативної інфраструктури, використовують політичні інститути для вироблення нормативних документів, що регламентують особливості інформаційної політики на основі власної ідеологічної доктрини.

2. *Міжнародні організації* – частково контролюють сегменти національного інформаційного простору, створюють власні і використовують національні структури (як правило, інтегровані в міжнародні організації) для ведення інформаційного протиборства, фінансують науково-технічну сферу для розробки зразків інформаційної зброї, засобів маскування та дезінформації і активно впливають на процес імплементації нормативної бази, яка

[116] Історія інформаційно-психологічного протиборства: підруч. / [Я.М. Жарков, Л.Ф. Компанцева, В.В. Остроухов, В.М. Петрик, М.М. Присяжнюк, Є.Д. Скулиш]; за заг. ред. д.ю.н., проф., засл. юриста України Є.Д. Скулиша. – К., 2012. – С. 27.

регламентує участь міжнародних організацій в інформаційному протиборстві.

3. *Незаконні збройні формування* – створюють власний (у більшості випадків закритий) сегмент інформаційного простору, акумулюють сили та засоби для ведення інформаційного протиборства, активно використовують інтелектуальний потенціал для розробки нових зразків інформаційної зброї.

4. *Транснаціональні корпорації* мають такі самі ознаки суб'єктності, як і міжнародні організації. Особливістю їх участі в інформаційному протиборстві є виключне право на використання комунікативних мереж провайдерами мережевих ресурсів.

5. *Віртуальні соціальні спільноти* – контролюють сегмент інформаційного простору шляхом підбору обмеженої кількості учасників віртуального проекту. Можуть використовувати інструменти блокування небажаних впливів на інфопростір власної спільноти. Активно протидіють процесам встановлення цензури над Інтернет-середовищем на державному законодавчому рівні.

6. *Медіа-корпорації* – активно працюють над розширенням своїх можливостей в межах інформаційного поля з використанням механізмів й інструментів інформаційного протиборства. Контролюють сегмент національного інформаційного простору.

7. *Віртуальні коаліції* – мають спільні ознаки з віртуальними соціальними спільнотами, але відрізняються мінливістю і нестабільністю[117].

Основними особливостями сучасного інформаційного протиборства є: вирішальна роль заходів інформаційного протиборства у формуванні рішучості суспільства у досягненні цілей, які поставлені воєнно-політичним керівництвом держави-лідера; висока ефективність підготовки, організації та проведення заходів інформаційного протиборства, що в ідеалі дає можливість відмовитися від застосування зброї; ретельна організація заходів інформаційного протиборства, що підвищує політичний і економічний ефект від воєнно-політичного рішення; здатність збільшувати бойову ефективність військ, берегти живу силу, зразки ОВТ при проведенні локальних збройних конфліктів, антитерористичних операцій, заходів інформаційного протиборства; вміле використання можливостей інформаційного впливу для забезпечення підтримки політичних, дипломатичних, економічних і

[117] Манойло А.В. Государственная информационная политика в особых условиях [Електронний ресурс]. – Режим доступу: http://razom.znaimo.com.ua/docs/45/index-18501.html

бойових дій усіх рівнів через зниження конкурентоздатності, технологічності та морально-психологічного стану противника; відносно низька вартість створення засобів для інформаційного протистояння; нівелювання статусу традиційних державних кордонів при підготовці й проведенні інформаційних операцій; зосередження зусиль на формуванні принципово нового суспільного світогляду, що має здатність до саморозвитку в потрібному напрямі; відсутність чітко прописаних юридичних норм міжнародного права, які регламентують принципи інформаційного протиборства; аморальність у виборі сил, засобів, інструментарію для досягнення перемоги в інформаційному протиборстві; динамічність, нерівномірність розподілу зусиль, сил, засобів інформаційного протиборства.

Активне використання цих особливостей державою обумовлює відповідний рівень її могутності та можливість *інформаційного домінування* в геополітичних відносинах як комплексного використання можливостей сучасних інформаційно-комунікативних технологій з накопичення обсягів інформації, що при відповідних методах її обробки дають змогу прогнозувати комплекс можливих сценаріїв розвитку соціальних і політичних явищ із метою визначення найбільш імовірного з них і сформувати інформаційне поле такої концентрації, яка б перевищувала інформаційний рівень структури, що має вплив на ці сценарії[118].

Основними способами досягнення інформаційного домінування є: здійснення управлінсько-фінансового впливу над ЗМІ держави-конкурента, приховане управління інформаційними процесами для зміни її системи суспільно-політичних, соціально-економічних та духовних відносин; інформаційна агресія; інформаційна війна.

У сучасних умовах значення інформаційного протиборства суттєво зросло. Це обумовлене існуванням низки *чинників*:

1. *Воєнно-політичні*:

- кардинальні зміни в системі колективної безпеки, руйнування системи політичних балансирів при забезпеченні непорушності міжнародних договорів і принципу недоторканності існуючих державних кордонів;

- невизначеність військово-політичних стратегій розвитку держав;

[118] Історія інформаційно-психологічного протиборства: підруч. / [Я.М. Жарков, Л.Ф. Компанцева, В.В. Остроухов, В.М. Петрик, М.М. Присяжнюк, Є.Д. Скулиш]; за заг. ред. д.ю.н., проф., засл. юриста України Є.Д. Скулиша. – К., 2012. – С 6.

- поява нової об’єктивної реальності у воєнному мистецтві – «гібридної війни», де інформаційна складова набуває пріоритетного значення;

- дисбаланс стратегічного ядерного потенціалу держав Європи, США і РФ й загроза поширення ядерної зброї в країнах Близького Сходу та Південно-Східної Азії, що впливає на інформаційну політику держав;

- загострення регіональних національних і релігійних конфліктів на території окремих країн, їх використання конкурентами для послаблення і розбалансування політичної системи держави й соціальної структури суспільства.

2. *Військово-технічні*:

- поява принципово нового ТВД – космічного;

- переорієнтування на якісно нові структурні підрозділи інформаційного протиборства – кібервійська;

- поява нових міжвидових зразків ОВТ із використанням елементів інформаційно-комунікативної інфраструктури;

- кардинальне зростання ролі інформації в сучасній війні;

- зниження можливостей з охорони державних кордонів внаслідок їх «розмивання» в процесах глобалізації.

3. *Соціально-економічні*:

- світові тенденції до зниження кількісного та якісного соціального складу населення у розвинених світових державах;

- зниження темпів виробництва, загрози інфляції, забруднення навколишнього середовища, виснаження світових ресурсів, виникнення національних, релігійних протиріч та ін.

Організація інформаційного протиборства є комплексом взаємопов’язаних і взаємообумовлених заходів, які спрямовані на досягнення максимально ефективної реалізації його цілей та завдань, а саме:

- цілеспрямоване планування та узгодження дій усіх елементів інформаційної інфраструктури;

- організація заходів інформаційного протиборства;

- своєчасне доведення завдань і координація дій інформаційної інфраструктури.

Принципи організації інформаційного протиборства – це найзагальніші імперативи, основоположні начала, які формуються в інтересах практики та використовуються в залежності від ситуації. Вони, на нашу думку, складаються з таких груп:

1. *Наукові:* системний підхід; передбачення дій противника; оперативна адаптації та кореляція дій в умовах швидкої зміни обстановки; формування перспектив для розвитку та удосконалення системи інформаційного протиборства.

2. *Військові*: високий фаховий рівень та єдність військово-політичного керівництва у концептуальному розумінні цілей, форм і методів організації інформаційного протиборства; наявність єдиного центру управління; закритий характер (державна таємниця) в організації та проведенні заходів інформаційного протиборства; достатнє кадрово-ресурсне забезпечення; стійкість і гнучкість управління; безперервний контроль відповідними державними органами; постійний обмін інформацією між структурними підрозділами;простота та доступність документообігу; реалістична оцінка потенціалу противника.

3. *Правові:* особливі правові преференції акторів інформаційної протидії; високий рівень повноважень військового керівництва при організації взаємодії з системою державної інформаційної інфраструктури; відповідальність органів державної влади за всебічне забезпечення та організацію взаємодії при проведенні заходів інформаційного протиборства.

Способи інформаційного протиборства – це спланована та цілеспрямована система дій державної інформаційно-комунікативної інфраструктури, яка визначає послідовність і порядок типових прийомів застосування сил й засобів для ведення інформаційного протиборства при досягненні воєнно-політичних і стратегічних завдань.

Сили та засоби інформаційного протиборства – це комплекс організованих структур й матеріальних ресурсів, інформаційно-комунікаційних систем, органів управління і забезпечення, які застосовують для ведення інформаційної війни.

Основні *сили,* які задіяні в сучасному стратегічному інформаційному протиборстві, – це невеликі групи висококласних політтехнологів, спічрайтерів та іміджмейкерів, спеціальні відділи у військових структурах, що створюють заданий сценарій, контролюють та управляють процесом розвитку суспільно-політичних подій у потрібному напрямі.

Основні *засоби* ведення інформаційного протиборства – це національні й транснаціональні ЗМІ та ЗМК, а також будь-які інші інформаційні мережі, здатні впливати як на світогляд, політичні

погляди, правосвідомість, менталітет, духовні ідеали та ціннісні установки окремої людини, так і на суспільство в цілому[119].

Інструментом ведення інформаційного протиборства є *інформаційна зброя* – комплекс засобів і методів, які дозволяють отримувати, спотворювати або знищувати інформацію; обмежувати доступ до неї законних користувачів; порушувати роботу або виводити з ладу об'єкти інформаційно-технічної інфраструктури, які використовуються у забезпеченні життєдіяльності суспільства та держави; здійснювати потужний психологічний вплив на свідомість і психіку людини, суспільства, морально-психологічний стан особового складу збройних сил за допомогою визначеного комплексу інформації.

Інформаційно-технічна зброя (ІТЗ) в масштабах геополітичного інформаційного протиборства – це інструменти та технічні засоби, що застосовують для знищення, викрадення або викривлення потоків інформації, руйнування їх систем захисту, дезорганізації роботи технічних засобів, виведення з ладу телекомунікаційних мереж, комп'ютерних систем, усіх засобів високотехнологічного забезпечення життя суспільства і функціонування держави[120]; комплекс інформаційних технологій, які забезпечують можливість системам (індивідам, організованим групам, державам) з більш високим рівнем інформатизації керувати системами з дещо нижчим рівнем інформатизації, спрямовуючи їх діяльність у своїх інтересах під постійним інформаційним контролем[121].

У масштабах інформаційного протиборства ІТЗ сукупність спеціалізованих (фізичних, інформаційних, програмних, радіоелектронних) інструментів, методів і засобів короткочасного блокування чи виведення з ладу (руйнування) потужностей служб інформаційної інфраструктури становлять комп'ютерні віруси, програмні закладки, засоби придушення інформаційного обміну в телекомунікаційних мережах і фальсифікації інформації в каналах державного та військового управління, засоби нейтралізації тестових програм, помилки, які свідомо введені у програмне забезпечення об'єкта[122].

---

[119] Історія інформаційно-психологічного протиборства: підруч. / [Я.М. Жарков, Л.Ф. Компанцева, В.В. Остроухов, В.М. Петрик, М.М. Присяжнюк, Є.Д. Скулиш]; за заг. ред. д.ю.н., проф., засл. юриста України Є.Д. Скулиша. – К., 2012. – С. 140.

[120] Лопатин В.Н. Информационная безопасность России: Человек. Общество. Государство. – Спб., 2000.

[121] Інформаційно-психологічна безпека особистості [Електронний ресурс]. – Режим доступу: https://sites.google.com/site/infobezosob/informacijno-psihologicna-bezpeka-osobistosti/ob-ektom-informacijno-psihologicnogo-zahistu-sobistosti/informacijna-zbroa---ce

[122] Расторгуев С.П. Информационная война. – М., 1998. – С.53.

На рівні інформаційного протиборства в процесі глобальної геополітичної інформаційної боротьби з метою захисту або руйнування матриць свідомості політичної еліти та населення країни використовують *інформаційно-психологічну зброю* (ІПЗ) – комплекс заходів і технологій в інфосфері, який через цілеспрямований інформаційний вплив на психіку та свідомість індивіда й суспільства формує необхідні ідеологічні та соціальні установки, помилкові стереотипи поведінки, що обумовлюють прийняття рішень, конструюють суспільні настрої та громадську думку. До складу ІПЗ входить: концептуально-методологічна, хронологічна (історична), фактологічна, лінгвістична зброя[123].

Інформаційно-психологічна зброя є дієвою як самостійний інструмент чи у комплексі із інформаційно-технічною та іншими видами зброї і застосовується для трансформації й руйнування ментально-духовних основ суспільства (мораль, традиції), інформаційного колоніалізму, конструювання меншовартісної пристосовницької ідеології, знищення національно-культурних ідентифікаційних основ спільнот для формування пристосовницької свідомості раба.

Залежно від *рівня технічного розвитку* інформаційно-комунікативної інфраструктури країни та держави-конкурента відбувається динамічний розвиток засобів інформаційно-психологічної зброї, ситуаційне коригування цілей, сил і форм управління процесами інформаційного протиборства.

Таким чином, особливості розвитку інформаційних технологій визначає характер інформаційного протиборства із застосуванням новітніх розробок інформаційно-психологічної зброї учасників конфлікту, домінуючими формами якого за умов відсутності прямого збройного протистояння є нелетальні. На останньому рівні відображено ідеалізовану модель інформаційних протистоянь майбутнього, яка мала б сприяти прояву гуманістичних якостей людини.

У рамках інформаційного протиборства проводяться заходи наступального й оборонного характеру. Відповідно, удосконалюються наявні та активно розробляються нові оборонні й наступальні засоби ведення інформаційного протиборства, які дадуть можливість досягти інформаційної переваги над противником.

---

[123] Шевченко М.М. Методологічні засади аналізу міждержавного протиборства // Нова парадигма / гол. ред. В. П. Бех. – К., 2007. – Вип. 68.

Домінування інформаційної складової в процесі сучасного цивілізаційного розвитку спричинило переміщення акцентів конфліктогенного потенціалу з мілітарної в інформаційну сферу та сферу бізнесу і комерції, що принципово змінило характер геостратегічного протиборства між провідними державами світу та транснаціональними інституціями за досягнення переваги у світовому інформаційному просторі.

Інформаційне протиборство стало аксіоматичною складовою системи сучасних міжнародних відносин і дає можливість із залученням незначних фінансових і людських ресурсів, досягати потрібних цілей. Ефективність цієї боротьби безпосередньо залежить від ступеня професіоналізму суб'єктів здійснення інформаційних атак, захиститися від яких буде спроможне лише інтелектуально розвинене суспільство.

Сутність інформаційного протиборства полягає у формуванні суспільної свідомості населення в контексті стратегічних цілей держав обумовлених завданнями оборонної/агресивної політики. Інформаційне протиборство має два види інформаційної боротьби: інформаційно-технічну та інформаційно-психологічну, що ведеться на стратегічному, оперативному та тактичному рівнях. У ході інформаційного протиборства з метою захисту або руйнування матриць свідомості політичної еліти та населення країни використовують інформаційно-психологічну зброю до складу якої входить: концептуально-методологічна, хронологічна (історична), фактологічна, лінгвістична зброя[124].

Як зазначає О. Горбенко, інформаційне протиборство, будучи невід'ємною складовою політичних відносин, виступає одним із основних інструментів політичного примушення в сучасних умовах. Тому не випадково воно пронизує всі форми політичної боротьби. Іншими словами, інформаційне протиборство вже не обмежується широкомасштабним впливом на населення і війська, а активно націлюється на вищі ешелони влади та суспільну свідомість держав супротивників і партнерів, на системи прийняття державних рішень у різних сферах життєдіяльності. Політичні актори, перебуваючи в стані жорсткої конкуренції (або конфлікту), безперервно обмінюються інформаційними впливами, які стають все більш витонченими та небезпечними[125].

[124] Лук'яненко О. Геополітичне інформаційне протиборство: сутність і варіанти захисту // Університетська кафедра. − 2016. − № 5. − С. 181.
[125] Горбенко А. СМИ в сфере информационного противоборства // Власть. − 2008. − № 11. − С. 25.

Інформаційне протиборство – це війна без лінії фронту. Проведення багатьох операцій інформаційного протиборства практично неможливо виявити. Міжнародні, юридичні та моральні норми ведення інформаційного протиборства повністю відсутні, що надає цьому феномену множину можливостей і варіантів використання будь-яких маніпулятивних технологій для досягнення мети.

Особливості розвитку інформаційного суспільства об'єктивно загострюють необхідність осмислення принципів, закономірностей, особливостей і наслідків функціонування новітніх засобів масової інформації та комунікації. З врахуванням новизни, складності та унікальності цієї тенденції існує нагальна потреба у низці диференційованих наукових досліджень сутності інформаційного протиборства, формування методичних засад його вивчення та ґрунтовних комплексних міждисциплінарних наукових розвідок.

Отже, поява нової інформаційної реальності (масштабної інформатизації, збільшення залежності воєнного сектору від сучасних інформаційних технологій, спрощення комунікацій та пришвидшення руху інформаційних потоків) суттєво трансформує глобальну реальність, а заразом і те, як саме використовуються ключові простори в інтересах геополітичних гравців. Ця реальність де-факто вже стає полем протистояння всіх великих держав. Однак, як справедливо зазначає Д. Дубов, досі залишається на завжди зрозумілим, чи дійсно новий «штучний простір» (кіберпростір) має стати частиною геополітичної теорії та чи має взагалі право на виокремлення як окремого «простору»[126].

Проблема пропагування та реалізації національних інтересів за межами держави має велике науково-прикладне значення, насамперед дослідження механізмів державного управління та розробки науково обґрунтованої стратегії й тактики забезпечення національної інформаційної безпеки, особливо в умовах динамічного розвитку сил і засобів вищої форми інформаційного протиборства – інформаційної війни.

У сучасних міжнародних відносинах інформаційна війна є одним із найефективніших інструментів реалізації зовнішньої політики. Слід також зазначити, що механізми ведення інформаційної війни проти політичної опозиції всередині держави виконують функції забезпечення суспільного балансу у внутрішній політиці.

[126] Дубов Д.В. Зрушення сфер геополітичного протиборства: від географічної експансії – до конструювання інформаційно-кібернетичних просторів // Стратегічні пріоритети. − 2014. − № 1. − С. 106−107.

Інформаційну війну можна розглядати і як один з основних чинників забезпечення національної безпеки та захисту національних інтересів у життєво важливих сферах державної й суспільно-політичної діяльності, особливо у військовій.

2.2. Інформаційна війна – вища форма інформаційного протиборства

Історичний розвиток людства свідчить про те, що поняття «інформаційна війна» завжди супроводжувало та визначало разом зі зброєю хід, характер і результат воєн, битв, операцій.

Видатний китайський військовий теоретик Сун-Цзи у VI–V ст. до н.е. вперше запропонував використовувати інформаційні заходи як альтернативу бойовим діям. Він сформулював дев'ять заповідей, дотримання яких забезпечувало такий потужний вплив на духовний світ армії противника, що вона просто «розкладалася» ще до початку битви. Сун-Цзи зазначав, що «у війні, як правило, найкраща політика зводиться до захоплення держави цілісною... Здобути сотню перемог у боях – це не вершина мистецтва. Підкорити суперника без бою – ось вінець мистецтва»[127]. Основні ідеї Сунь-Цзи активно розвивали й інші китайські мислителі. Зокрема, військовий теоретик Чжуге Лян (III ст. н.е.). вважав, що «у воєнних діях атака на психіку – головне завдання. Психологічна війна – це головне, бій – це другорядна справа»[128]. Не абсолютизував збройне насильство і відомий прусський воєнний теоретик К. Клаузевіц, автор класичного визначення поняття «війна» зазначав: «Доведеться … визнавати і такі війни, які полягають лише у погрозі супротивнику»[129].

Термін «інформаційна війна» вперше було введено в науковий обіг і практику політичного протистояння двох наддержав США і СРСР у 1967 р. колишнім директором ЦРУ А. Далесом у книзі «Таємна капітуляція». Наступного разу термін з'явився у аналітичній доповіді американського дослідника Т. Рона для компанії Boeing «Системи озброєння та інформаційна війна», де зазначалось, що інформаційна структура стає найбільш важливим елементом економіки з одного боку, та найбільш вразливою мішенню з іншого[130].

---

[127] Сун-Цзы, У-цзы. Трактаты о военном искусстве. – М., 2002. – С. 40.

[128] Цит. по: Манойло А.В. Государственная информационная политика в условиях информационно-психологической войны / А.В. Манойло, А.И. Петренко, Д.П. Фролов. – 2-е изд., стереотип. – М., 2009. – С. 231.

[129] Клаузевиц К. О войне: в 2-х т. – Т. 2. – М., 2002. – С. 449.

[130] Магда Є. В. Виклики гібридної війни: інформаційний вимір // Наукові записки Інституту законодавства Верховної Ради України. – 2014. – №5. – С.140.

У листопаді 1991 р., аналізуючи досвід досягнення інформаційної переваги після операції «Буря у пустелі», генерал Г. Отіс, колишній командувач Командування сухопутних військ США з навчання та доктрин, опублікував роботу, в який стверджував, що «природа війни повністю змінилася. Та сторона, яка виграє інформаційну війну, – переможе… інформація є ключем до сучасної війни – у стратегічному, оперативному, тактичному та технічному планах»[131]. Офіційно визначеним термін «інформаційна війна» як комплексне спільне застосування сил і засобів інформаційної боротьби та збройної боротьби (при домінуванні засобів інформаційної боротьби) вперше став у керівних документах США, зокрема в директиві МО США Т 3600.1 від 12 грудня 1992 р., під назвою «Інформаційна війна».

У сучасному науковому дискурсі проблемі вивчення надскладного соціально-політичного явища «інформаційна війна» надається достатньо уваги. Різноманітність підходів до визначення основного змісту, відсутність єдиної системи класифікації призвели до унеможливлення створення уніфікованої дефініції понять інформаційної війни та інформаційно-політичного простору, відсутність методологічного осмислення співвідношення цих понять та ін.

Наприклад, А. Манойло зміст поняття інформаційної війни розглядає на різних рівнях пізнання як соціальне явище; як поле політичних конфліктів; як особлива форма політичного конфлікту; як інструмент інформаційної політики[132]. А. Фісун до цього додає ще й форму психологічного впливу[133].

Варіантами визначення сутності поняття «інформаційна війна» є комплекс наукових гіпотез, які активно використовують у сучасному науковому дискурсі.

1. Соціологічна гіпотеза: визначає інформаційну війну як соціальне явище і нову форму суспільних відносин, що утворені інформаційним суспільством (В.Г. Крисько, Г.Г. Почепцов).

2. Системна гіпотеза: інформаційна війна трактується як поле для політичних конфліктів, які перебувають у взаємозв'язку і взаємодії. Кожен політичний конфлікт розглядається як одинична реалізація

[131] Див.: James Adams. The Next World War. Computers Are the Weapons and the Front Line Is Everywhere / Adams James. – NewYork, 1998. – P. 55.

[132] Манойло А.В. Управление психологической войной [Електронний ресурс]. – Режим доступу: http ://andreymanoylo. vov. ru/ uprpsiv.html

[133] Фісун А.О. Ґенеза поняття «інформаційна війна» // Гілея. – 2011. – № 49. – С. 534.

множини конфліктних ситуацій, згенерованих інформаційно-політичним полем (І.М. Панарін, С.П. Расторгуєв).

3. Конфліктологічна гіпотеза: інформаційна війна є різновидом політичного конфлікту, що виникає в процесах управління суспільством і здійснення влади, в якому зіткнення сторін здійснюється у формі інформаційних операцій із застосуванням інформаційної зброї (О.Г. Караяні, В.П. Петров).

4. Системно-функціональна або *інструментальна гіпотеза*: інформаційна війна є складовою системи політичного регулювання, інструментом інформаційної політики (А.В. Манойло, І.М. Панарін, П.Г. Панаріна).

5. Психологічна гіпотеза: інформаційно-психологічна війна – це вплив на масову та індивідуальну свідомість, метою якого є формування громадської думки в заданому маніпулятором напрямі, закладання ерзац поведінки (С.А. Зелінський, В.Є. Лепський).

6. *Гіпотеза «світового заколоту»:* інформаційна війна – форма мережевої війни, тотального інформаційно-психологічного впливу глобальних світових (у більшості випадків – таємних) структур з метою створення керованого мережевого суспільства, прошарку «агентів впливу» та перекодування свідомості владної еліти в інтересах «світового уряду» (О.Г. Дугін, Д.Є. Галковський, Милослав Князєв, М.І. Сенченко, В.І. Філатов).

У залежності від основних аспектів дослідження об’єкта, які вирізняють науковці, та від гіпотез щодо сутності явища, виділяється *шість основних підходів* до поняття «інформаційна війна»[134]:

Соціально-комунікативний підхід – трактує поняття інформаційної війни як сукупність окремих інформаційних заходів, інформаційних способів і засобів корпоративної конкуренції, що є продуктом еволюційного розвитку способів і засобів комунікації між людьми, суспільствами, державами та світом загалом. В межах цього підходу український дослідник Г.Г. Почепцов визначає «інформаційну війну» як всеосяжну, цілісну стратегію, яка надає значущості та цінності інформації в процесах командування, управління і виконання наказів збройними силами й реалізації національної політики[135]. П. Шпига та Р. Рудник сутність інформаційної війни бачать як сукупність політико-правових, соціально-економічних, психологічних дій, що передбачають захоплення інформаційного простору, витіснення

[134] Фісун А.О. Ґенеза поняття «інформаційна війна» // Гілея. – 2011. – № 49. – С. 534–538.
[135] Почепцов Г.Г. Информационные войны. – М., К., 2000. – С. 3.

ворога з інформаційної сфери, знищення його комунікацій, позбавлення засобів передачі повідомлень та інше[136].

Особливостями соціально-комунікативного підходу є:

- відображення сутності досліджуваного явища лише як закономірного розвитку людського суспільства у рамках біологічної еволюції з домінуванням принципів природного відбору, боротьби за існування й виживання найбільш пристосованих як визначальних факторів громадського життя;
- визначення природи соціального конфлікту як вічного та непереборного;
- трактування інформаційної агресії як нової трансформованої форми природної агресії людини.

Інформаційно-комунікаційний. Інформаційна війна розглядається в площині протистояння інформаційно-комунікаційних систем.

Американський дослідник інформаційної війни У. Швартоу трактує інформаційну війну як електронне протистояння, у якому головною ціллю є інформація, яку треба захопити та знищити[137].

За визначенням Я. Малика «інформаційна війна – форма ведення інформаційного протистояння між різними суб'єктами (державами, неурядовими, економічними та іншими структурами), яка передбачає проведення комплексу з нанесення шкоди інформаційній сфері конкуруючої сторони і захисту власної інформаційної сфери, конкуруючої сторони і захисту власної інформаційної безпеки»[138].

Особливостями цього підходу є:

- розгляд суб'єктів феномену війни як комплексу структур;
- акцентування уваги на понятті «інформаційна сфера»;
- відносно загальний характер визначення сутності інформаційного протистояння.

Також Я. Малик виділяє інформаційні війни першого та другого покоління. Форми інформаційного протиборства першого покоління спрямовані переважно на дезорганізацію інформаційно-комунікаційної системи держави-супротивника та включали (і включають сьогодні) наступні елементи:

- вогневе придушення (у воєнний час) елементів інфраструктури державного та військового управління;
- ведення радіоелектронної боротьби;

[136] Шпига П.С. Основні технології та закономірності інформаційної війни [Текст] // Проблеми міжнародних відносин. – 2014. – Вип. 8. – С. 328.
[137] Там само.
[138] Малик Я. Інформаційна війна і Україна // "Демократичне врядування" Науковий вісник. – 2015. – Вип. 15. – Режим доступу: http://nbuv.gov.ua/UJRN/DeVr_2015_15_3

- одержання розвідувальної інформації шляхом перехоплення й розшифровки інформаційних потоків;

- здійснення несанкціонованого доступу до інформаційних ресурсів із наступною їх фальсифікацією чи викраденням;

- масове подання в інформаційних каналах супротивника чи глобальних мережах дезінформації для впливу на особи, які приймають рішення;

- одержання інформації від перехоплення відкритих джерел інформації[139].

Маніпулятивно-психологічний підхід визначає суть інформаційної війни як системи способів і засобів психологічного впливу на індивідуальну та масову свідомість з метою спрямування її у вигідному для суб'єкта впливу напрямі. Експерт з питань інформаційної війни М. Лібікі дає наступне визначення цьому соціально-політичному явищу: «Інформаційна війна – це засоби, які включають збір, передачу, захист, маніпулювання, спростування, заперечення та знищення інформації, завдяки яким можна встановити перевагу над противником. Маніпулювання інформацією в контексті інформаційної війни – це зміна інформації з метою викривлення сприйняття дійсності противником. Інформаційна війна, як і традиційна, передбачає застосування різноманітних стратегій, засобів впливу, зброї та оборонних технологій. У сучасному світі, де панують глобалізаційні процеси, всеохоплююча інформатизація призводить до створення єдиного інформаційного простору»[140].

Р. Чирва стверджує, що головне завдання інформаційних воєн полягає в маніпулюванні масами, дезорієнтації та дезінформації громадян, залякуванні супротивника своєю могутністю[141].

П. Померанцев зазначає, що російська теорія інформаційної війни тяжіє до інформаційної та психологічної війни; ядром інформаційної війни є людська свідомість, психологічна сфера[142].

Формами інформаційної війни у даному підході є використання психотропної зброї, побудова віртуального світу, підміна реальності та ін. Представники цього підходу вважають, що інформаційно-

---

[139] Малик Я. Інформаційна війна і Україна // «Демократичне врядування» Науковий вісник. – 2015. – Вип. 15. – Режим доступу: http://nbuv.gov.ua/UJRN/DeVr_2015_15_3

[140] Лібікі М. Що таке інформаційна війна? http:// viysko.com.ua/texnologiji-voyen/martin-libiki-shhotake-informacijna-vijna/

[141] Чирва Р. Інформаційна війна – зброя, страшніша за ядерну [Текст] // Профспілкові вісті. – 2014. – № 13. – С. 9.

[142] Семен Н.Ф. Російські інтернет-ресурси як чинник інформаційної війни проти України (на прикладі сайтів «Правда.ру» та «Российский диалог») / автореф. … здобуття наукового ступеня кандидата наук із соціальних комунікацій. – спец. 27.00.01 – теорія та історія соціальних комунікацій. – Дніпро, 2018. – С. 6.

психологічна війна – це вплив на суперника через засоби масового психологічного впливу для зміни світогляду чи ініціювання процесу самознищення, добровільної здачі території, ресурсів і т.п.[143]

Інформаційна боротьба другого покоління за поглядами вищецитованого Я. Малика передбачає переважно використання інструментарію психологічного впливу на індивідуальну та суспільну свідомість. Це:

- створення системи бездуховності й аморальності, негативного відношення до культурної спадщини противника;
- маніпулювання суспільною свідомістю соціальних груп населення країни з метою створення політичної напруженості та хаосу;
- дестабілізація політичних відносин між партіями, об'єднаннями й рухами з метою провокації конфліктів, розпалювання недовіри, підозрілості, загострення політичної боротьби, провокування репресій проти опозиції і навіть громадянської війни;
- зниження рівня інформаційного забезпечення органів влади й управління, інспірація помилкових управлінських рішень;
- дезінформація населення про роботу державних органів, підрив їхнього авторитету, дискредитація органів управління;
- підрив міжнародного авторитету держави, його співробітництва з іншими країнами;
- нанесення збитку життєво важливим інтересам держав у політичній, економічній, оборонній та інших сферах[144].

Особливостями цього підходу є:

- розкриття психологічного впливу феномену;
- комплексне розкриття психологічного аспекту і маніпулятивної природи інформаційної війни;
- ігнорування оборонного (захисного) характеру інформаційної війни;
- нівелювання технічного аспекту, матеріальних засобів інформаційного протиборства;
- недостатнє прогнозування наслідків впливу економічної складової.

Військово-прикладний підхід зараховує інформаційну агресію до сфери військового протиборства й розглядає її у комплексі спільного застосування сил і засобів інформаційної та збройної боротьби. При

[143] Морозов А.М. От физической к психологической войне. Эволюция форм войны в процессе развития цивилизации [Електронний ресурс]. – Режим доступу: http://psyfactor.org/biowar.htm

[144] Малик Я. Інформаційна війна і Україна // "Демократичне врядування" Науковий вісник. – 2015. – Вип. 15. – Режим доступу: http://nbuv.gov.ua/UJRN/DeVr_2015_15_3

цьому представники військово-прикладного підходу не вважають інформаційну війну окремим методом ведення війни. На їх думку, існує множина форм інформаційної війни, кожна з яких претендує на різні концепції, зокрема: командно-контрольні, розвідувальні війни; радіоелектронна боротьба; психологічні операції; хакерська війна, програмні атаки на інформаційні системи; інформаційно-економічна війна; кібервійни[145].

У цьому випадку характер інформаційної війни визначається як найгостріша форма протистояння в інформаційному просторі, де першочергового значення набувають такі якості взаємодії, як безкомпромісність, висока інтенсивність суперечки та короткотривалість гострого суперництва[146].

Кібервійну розглядають як процес розвитку та поширення інформаційних технологій. При цьому відбувається процес ототожнення інформаційних війн з кібернетичними війнами (протистояння між технічними системами). Кібервійна – елемент інформаційної війни, що здійснюється з використанням засобів всесвітньої мережі у формі кібератак. Сутність інформаційної війни полягає у застосуванні прихованих цілеспрямованих інформаційних впливів інформаційних систем одна на одну з метою одержання певного прибутку в матеріальній сфері[147]. Наголошено на тому, що інформаційно-блогова або мережева війна – це внутрішньо-середовищна особливість Інтернету, яка виявляється у формах жорсткої дискусії, цілковитого свавілля із взаємними образами, атаками на ресурси противника, зламами особистої інформації та ресурсів. Блоги стають потужним інструментом формування громадської думки[148]. «Інформаційна війна, на думку американських теоретиків Дж. Аркуіла та Д. Ронфельдта, може бути частиною широкого та всеохоплюючого поняття ворожих дій – мережевої війни або кібер-війни»[149].

У військовій сфері – як комплексне використання високоточної зброї, технологій «Стелс», бойових і розвідувальних засобів з урахуванням футуристичних розробок у галузі роботизації й

[145] Libicki M. What is Information Warfare? [Електронний ресурс]. – Режим доступу: http:// www.iwar. org.uk/iwar/resources/ndu/infowar/a003cont.html

[146] Шпига П.С. Основні технології та закономірності інформаційної війни [Текст] // Проблеми міжнародних відносин. – 2014. – Вип. 8. – С. 328.

[147] Расторгуев С.П. Информационная война. – М., 1998. – С. 51.

[148] Жаров М. Хроники информационной войны. – М., 2009. – С. 3.

[149] John Arquilla and David Ronfeldt. Cyber war is Coming! Comparative Strategy 2 (April-June 1993) [Електронний ресурс]. – Режим доступу: http:// www.rand.org/ pubs/reprints/RP223.html

автоматизації[150]. Тобто, інформаційна війна інтерпретується як форма забезпечення та ведення військово-силових дій за допомогою найсучасніших електронних засобів (цифрових випромінювачів, супутникових передавачів та інших аналогічних засобів, які застосовуються для виконання військових завдань)[151].

У форматі кібервійни визначаються такі види діяльності[152]: 1) вандалізм – псування інтернет-сторінок, зміна змісту негативними або пропагандистськими матеріалами; 2) пропаганда – поширення звернень, що закликають до певних дій, або розміщення відповідної інформації на чужих інтернет-майданчиках; 3) збирання інформації – зламування сторінок приватних осіб або окремих організацій для отримання закритої інформації; 4) втручання в роботу програмно-апаратного забезпечення – dDoss атаки на комп'ютери, що виконують адміністративно-контрольні функції у державних, громадських, військових та комерційних організаціях; 5) атаки на комп'ютерну мережу об'єктів критичної інфраструктури – напад на комп'ютери, що контролюють життєдіяльність міст, зокрема телефонних ліній, водопостачання, електропостачання, пожежної безпеки, транспортного сполучення та ін.

Особливостями цього підходу є:

- системність, дає можливість охопити політичний, економічний, психологічний та інший аспекти;
- «агресивний характер», зорієнтований на швидке досягнення бажаного тактичного результату з одночасною втратою стратегічної перспективи;
- ігнорування прогнозування наслідків для іншої сторони конфлікту;
- нівелювання соціального аспекту при домінуванні політичної складової конфлікту.

Державно-інструментальний підхід називає інформаційну війну інструментом зовнішньої та внутрішньої політики, «можливістю для збору, обробки та розповсюдження безперервного потоку інформації…у відповідь на дії противника»[153]. Особливістю цього підходу є абсолютизація ролі політичних інститутів і організації

[150] Климчук О.О. Кібервійна у сучасних умовах // Інформаційна безпека. Людина. Суспільство. Держава. – 2011. – № 1 (5). – С. 79.
[151] Шпига П.С. Основні технології та закономірності інформаційної війни... – С. 328.
[152] Зеленін В.В. По той бік правди: нейролінгвістичне програмування як зброя інформаційно-пропагандиської війни. – Вінниця, 2014. – С. 38.
[153] Yoshihara T. Chinese Information Warfare: A Phantom Menace or Emerging Threat? – Strategic Studies Institute, U.S. Army War College. – P. 3–4.

держави у веденні інформаційної війни та нівелювання впливу соціальних, економічних і психологічних чинників.

Геополітичний підхід. Дослідники вважають інформаційну війну явищем латентно мирного періоду міждержавного протиборства, що дозволяє вирішувати зовнішньополітичні завдання несиловими методами. Інформаційна війна стосується сфери геополітичного протиборства, її трактують як особливий вид відносин між державами, при якому для вирішення існуючих протиріч використовують методи, засоби й технології впливу на інформаційну сферу функціонування цих держав. Під інформаційною війною дослідники цього напряму розуміють дії, які спрямовані на завдання противнику конкретного, відчутного збитку в окремих галузях його діяльності[154]. І.М. Панарін інформаційну війну визначає як цілеспрямоване вироблення та поширення спеціальної інформації, яка безпосередньо впливає на функціонування та розвиток інформаційно-психологічної сфери суспільства, психіку і поведінку політичної еліти й населення певної території чи держави[155].

Близьким до визначення І.М. Панаріна слід вважати дефініцію Дж. Стейна, який вважав, що метою інформаційної війни є вплив на розум еліти – людей, які визначають доцільність війни та миру і окреслюють місце та час застосування потенціалу та можливостей, якими оперують їхні стратегічні структури[156].

Особливостями цього підходу є:

- охоплення геополітичних суб'єктів інформаційно-політичного простору;
- трактування інформаційної війни як певного природного закону;
- ігнорування значимості особистості як окремого об'єкта для впливу;
- недостатнє вивчення причин інформаційної війни.

Віртуально-кібернетичний підхід. Інформаційна війна розглядається як сукупність технічних, програмних та інших засобів, які використовують у віртуальному просторі, з метою ураження інформаційних систем і органів військового управління супротивника (комп'ютерні віруси та ін.).

Особливостями віртуально-кібернетичного підходу є:

---

[154] Манойло А.В. Государственная информационная политика в условиях информационно-психологической войны. – М., 2009. – С. 481.

[155] Панарин И.Н. Информационная война и мир. – М., 2003. – С. 38.

[156] Семен Н.Ф. Російські інтернет-ресурси як чинник інформаційної війни проти України (на прикладі сайтів «Правда.ру» та «Российский диалог») / автореф. … здобуття наукового ступеня кандидата наук із соціальних комунікацій. – спец. 27.00.01 – теорія та історія соціальних комунікацій. – Дніпро, 2018. – С. 6.

- розкриття суті інформаційної війни крізь площину математичного виміру;

- виокремлення тенденцій сучасного інформаційного простору та розвитку інформаційних технологій (особливо в контексті інформаційно-блогових процесів);

- ігнорування психологічного аспекту явища;

- невизначеність ролі держави в цьому процесі;

- домінування теоретичного, а не практичного значення, відсутність рекомендацій та прийомів, які б дали змогу виявити інформаційну агресію і захиститись від неї.

Комплексний підхід. Український дослідник А. Фісун констатує, що жоден із підходів не розкриває сутність інформаційної війни комплексно ні як політичного конфлікту, ні як соціального явища, ні як соціокультурного феномену та дає власне бачення розкриття її сутності: «Інформаційна війна це комплексний відкритий чи прихований цілеспрямований інформаційний вплив однієї сторони, чи взаємний вплив сторін одна на одну, який містить систему методів і засобів впливу на людей, їх психіку та поведінку, на інформаційні ресурси та інформаційні системи, з метою досягнення інформаційної переваги (в забезпеченні національної стратегії), що обумовлює прийняття сприятливих для ініціатора впливу рішень або знищення інформаційної інфраструктури противника, з одночасним зміцненням і захистом власної інформації та інформаційних систем»[157].

На нашу думку, до комплексного підходу слід зарахувати й дефініцію В. Ліпкана, Ю. Максименко, В. Желіховського: «Інформаційна війна – це 1) дії, розпочаті для досягнення інформаційної переваги шляхом завдання шкоди інформації, процесам, що базуються на інформації і інформаційних системах супротивника при одночасному захисті власної інформації, процесів, що базуються на інформації і інформаційних системах; 2) нефізична атака на інформацію, інформаційні процеси та інформаційну інфраструктуру; 3) найвищий ступінь інформаційного протиборства, спрямований на розв'язання суспільно-політичних, ідеологічних, національних, територіальних та інших конфліктів між державами, народами, націями, класами й соціальними групами шляхом широкомасштабної реалізації засобів і методів інформаційного насильства (інформаційної зброї)»[158].

---

[157] Фісун А. О. Генеза поняття «інформаційна війна» // Гілея. Історичні науки. Філософські науки. Політичні науки. – К. – 2011. – Вип. 49 (№ 7).

[158] Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції: навч. посібник. – К., 2006. – С. 270.

У ідеологіях маргінальних політичних формувань екстремістського та окультистського напрямів став популярним так званий *конспірологічний* підхід. Найбільш послідовним апологетом цього напрямку можна вважати О.Г. Дугіна. Інформаційну війну він розглядає як форму тотального впливу глобальних політичних, економічних, терористичних, сектантських мережевих структур (хасидсько-парамасонська група, Захід на чолі з США, країни «золотого мільярду»), з метою контролювання політичної, соціальної, економічної ситуації та інтенсифікації трансформаційних тенденцій духовності світового суспільства через спрямування інформаційних процесів в інтересах США, які одночасно створюють систему захисту власного мережевого коду, який ці процеси дешифрує та структурує.

Сегментами глобальної мережі у цьому підході є:

- пряме проамериканське лобі експертів, політологів, аналітиків, технологів, контролюють владу та претендують на роль інтелектуальної еліти суспільства;
- представники великого бізнесу та політичної еліти, які орієнтовані на фінансово-економічну діяльність за кордоном;
- ЗМІ та ЗМК, які виконують функцію масованого інформаційного впливу за допомогою потоків візуальної та смислової інформації.

Тобто, «інформаційну війну ведуть ідейні кілери — найманці з числа політиків, духівництва, інтелектуалів, які зраджують інтереси народу, проституюючи совість і розум»[159].

Характерною рисою «мережевої війни», за О.Г. Дугіним, є тотальний інформаційний вплив «мережевої п'ятої колони» «агентів впливу» – рушійної сили світового заколоту з метою десуверенізації країни[160].

Особливостями цього підходу є:

- дослідження мережевого характеру сучасного світового бізнесу, політичних проектів, терористичних формувань і сектантських організацій;
- розкриття сутності діяльності «агентів впливу»;
- надмірна абсолютизація поняття «мережі», ігнорування психологічних особливостей людини як самостійного індивіда;

[159] Сенченко М. Четверта світова. Інформаційно-психологічна війна [Електронний ресурс]. – К., 2014. – Режим доступу: https://lib.rus.ec/b/241595/read

[160] Дугин А.Г. Сетевые войны. Доклад на заседании Изборского клуба 08.07.2013 [Електронний ресурс]. – Режим доступу: http://dynacon.ru/content/articles/2318/

- містично-конспірологічний погляд на роль світових глобальних структур, демонізація західного світу, захоплення ідеєю «світового єврейського заколоту», окультизм і расовий фактор.

Інформаційна війна здійснюється у формі *інформаційного протиборства* як системи цілеспрямованих дії для створення інформаційної переваги, за допомогою руйнування інформації, інформаційних систем протилежної сторони, при цьому одночасно відбувається процес захисту власної інформації і інформаційних систем[161].

Отже, на нашу думку, **інформаційна війна** – це *суспільно-політичне явище*, яке у *політичному аспекті* є продовженням домінуючих ідеологічних засад державної політики, що здійснюється за допомогою комплексу засобів інформаційно-технологічної індустрії, механізмів інформаційно-психологічного впливу на суспільство всередині держави чи населення країн-конкурентів в умовах політичного (воєнно-політичного, економічного) конфлікту з метою формування у *соціальному аспекті* єдності суспільства, визначення його ідентичності та інформаційного захисту світоглядних цінностей, а також – деморалізації та фрагментації населення та силової компоненти держав-противників у межах глобального інформаційного простору.

Як будь-яке соціально-політичне явище інформаційна війна має свої *характерні риси*, що відрізняють її від звичайної війни. До них відносяться:

- відсутність видимих фізичних руйнувань, через що оборонна реакція країни може бути запізнілою;
- засоби ведення інформаційної війни є майже непередбачуваними та постійно змінюються в оперативному плані, тому варіанти протидії таким засобам мають спиратися на високий інтелектуальний потенціал, зокрема аналітичні здібності, всіх ланок управління країни, що є досить складним в умовах сьогодення;
- під час ведення інформаційної війни не обов'язково відбувається фізичне захоплення людських ресурсів, але встановлюється контроль над їх свідомістю;
- вибірковість за принципом досягнення найбільшого ефекту, тобто інформаційна війна буде результативною, коли досягатиме реального ефекту у впливі на суб'єктів прийняття рішень в країні, щодо якої відбувається атака;

[161] Любарський С.В. Місце та роль мережевої розвідки в моделях інформаційного протиборства // Збірник наукових праць ВІТІ НТУУ «КПІ». – 2013. – № 1. – С. 38.

- короткострокова інформаційна війна є малоефективною у випадку слабкої інформаційної інфраструктури країни впливу;

- розуміння правди нівелюється, дискусії зводяться до абсурду, здійснюється саботаж здорового глузду;

- вплив на хід думок супротивника з метою прийняття останнім вигідного для атакуючого рішення;

- переведення переваг супротивника в його недоліки;

- гра на емоціях, відволікання розуму на негідний об'єкт[162].

Особливостями інформаційної війни є:

- використання її як частини ідеологічної боротьби;

- відсутність безпосереднього фізичного контакту з противником, що не призводить безпосередньо до жертв й руйнувань;

- вплив на свідомість людини та її психоемоційний стан.

На нашу думку, фундаментальними *принципами* інформаційної війни є такі:

- *кореляції цілей та завдань інформаційної війни з політичними*, тобто визначальна роль політики, її основоположне значення та вплив на процеси ведення інформаційної війни;

- *завчасної готовності сил і засобів*, залежність перебігу та результату інформаційної війни від співвідношення бойового, економічного та духовно-культурного потенціалу держави;

- *планування та узгодження*, наголошує на системному характері організації та проведення інформаційно-пропагандистських кампаній, координації та узгодженості дій різних за кількістю та якістю сил і засобів;

- *активності та рішучості*, відображає спрямованість та наступальний характер інформаційної війни, обумовлені її цілями;

- *неочікуваності та раптовості дій*, тобто збереження таємниці, прихована підготовка до використання сил, маскування та дезінформація, виявлення слабких місць в організації інформаційної протидії противника, нанесення несподіваних ударів по інформаційному середовищу противника та дезорганізація його системи управління інформаційними каналами і потоками;

- *оперативності та гнучкості,* творчий характер управління процесами організації інформаційної війни та застосування новітніх форм і методів за умов зміни обстановки;

[162] Павліченко О.О. Сутнісні характеристики сучасної інформаційної війни // Науковий семінар «Інформаційна агресія Російської Федерації проти України»: тези доповідей, 25 жовтня 2018 року. – Х., 2018. – С. 43–44.

- *системної взаємодії з елементами інформаційно-комунікативної інфраструктури та підтримка взаємодії між ними* для узгодження дій у конкретному просторі-часі;

- *безперервності та потужності ведення операцій*, забезпечує діалектичний взаємозв'язок і розвиток процесів інформаційної війни та ефективність управління процесами ведення інформаційної війни;

- *своєчасності та маневреності сил та засобів інформаційної війни,* передбачає координацію та зосередження на визначальних напрямах і об'єктах інформаційного впливу для максимального нівелювання нерівномірності сил і засобів;

- *постійного відновлення сил і засобів* інформаційної війни для відновлення процесу управління та зв'язку, пошкодженої техніки для забезпечення потенційних можливостей реалізації поставлених цілей й завдань;

- *непохитності у досягненні цілей* інформаційної війни, що визначає напрям розвитку та способи досягнення ухвалених рішень і завдань.

Організація та ведення інформаційної війни, яка ґрунтується на цих принципах, передбачає дотримання законів і закономірностей інформаційної війни. *Закон інформаційної війни*, на нашу думку, може бути визначений як необхідний, стійкий та загальний об'єктивний зв'язок, що розкриває сутність функціонування елементів інформаційної війни у траєкторіях їхнього розвитку, модернізації та трансформації в інформаційному просторі. *Закономірності* відображають комплексну дію множини законів інформаційної війни.

Український дослідник М. Требін виокремлює такі закони інформаційної війни:

1. *Закон визначальної ролі політичних цілей* – об'єктивує ступінь використання сил і засобів інформаційної сфери, масштабів й інтенсивності ведення інформаційної війни (узалежнено від економічного потенціалу держав), кінцеву мету війни та заходи для зміцнення союзницьких відносин у коаліції союзників.

2. *Закон залежності перебігу та результатів інформаційної війни від стану соціально-політичного, економічного, військового і духовного потенціалів держави* демонструє упорядкованість й розвиток системи співвідношення форм буття, що розкривають

потенційні можливості держави та суспільства для ведення інформаційної війни[163].

Визначено такі закономірності ведення інформаційної війни узалежнено від:

1. *Організаційно-управлінські*:

- форм і способів ведення інформаційної війни, її ефективності від кількості та якості засобів інформаційного впливу, способів їх застосування, а також рівня професійної підготовки персоналу для спецпропаганди та контрпропаганди;

- досягнення цілей інформаційної війни від рівня координації інформаційних дій різних суб'єктів інформаційної діяльності в часі і просторі;

- нерівнозначності впливу різних сил та засобів на інфосферу протиборчої сторони від нерівномірності розподілу сил і засобів у інфосфері.

2. *Технологічні*:

- ефективності впливу сил і засобів інформаційної війни від технічного стану інформаційно-комунікаційної інфраструктури;

- використання нових тактичних прийомів, механізмів реалізації завдань інформаційної війни від впровадження в практику новітніх інформаційних технологій.

3. *Суспільно-політичні*:

- масштабів війни, обумовлених особливостями військово-політичної та економічної обстановки, цілями політики національної безпеки держави, структур і підрозділів, що ведуть інформаційну війну;

- відповідності змісту, масштабів і засобів інформаційної війни характеристикам суспільного та державного устрою;

- побудови сил і засобів інформаційної війни на основі матеріального і духовного потенціалу держави (інших суспільних і економічних структур)[164].

Головними об'єктами для деструктивного впливу інформаційної війни у межах глобального інформаційного простору є свідомість окремої людини, громадянське суспільство та інформаційна інфраструктура держави.

Об'єкти інформаційної війни поділяються на загальні, спеціальні та об'єкти розвідувальних спрямувань.

---

[163] Требін М.П. Феномен інформаційної війни в світі, що глобалізується // Вісник Національного університету «Юридична академія імені Ярослава Мудрого». – 2014. – № 2 (16). – С. 191.

[164] Там само. – С. 192.

До *загальних об'єктів* належать стан правопорядку в державі; органи влади й управління; мобілізаційна готовність і боєздатність силових структур; зовнішньополітичні зв'язки, міжнародний авторитет держави.

С*пеціальні об'єкти*: суспільство загалом і окремі елементи його суспільно-політичної та соціально-класової структури.

До об'єктів *розвідувальних спрямувань* зараховують:

- засоби масової інформації та комунікації, інформаційні агентства, незалежні аналітичні центри й дослідні центри, які безпосередньо займаються збором, аналізом і прогнозуванням перспектив розвитку подій, тенденцій суспільно-політичних і геополітичних процесів у регіоні та світі;
- відповідні структурні підрозділи міністерств, відомств чи інших органів державного управління, які забезпечують налагодження й підтримання зв'язків із громадськістю та інформування суспільства щодо діяльності зазначених установ, а також інші об'єднання громадян, які виступають від імені своїх членів (політичні партії та блоки, громадські організації, профспілки й т. ін.).

Основними об'єктами для деструктивного впливу інформаційної війни є:

- ідеологічно-психологічне середовище суспільства, пов'язане з використанням інформації, інформаційних ресурсів та інформаційної інфраструктури для здійснення впливу на психіку й поведінку людей;
- інформаційні ресурси, які транслюють систему цінностей, традицій у різних сферах життя суспільства;
- інформаційна інфраструктура як сукупність проміжних комунікативних ланок між інформацією та людиною;
- система формування суспільної свідомості (світоглядні, етичні, політичні патерни суспільства);
- система формування та розвитку громадської думки;
- система розробки та прийняття політичних рішень вищим керівництвом держави;
- індивідуальна свідомість та поведінка людини[165].

Мета інформаційної війни може бути визначена як комплекс організаційно-управлінських, агітаційно-пропагандистських рішень та дій органів державного управління, спеціальних соціальних

[165] Історія інформаційно-психологічного протиборства: підруч. / [Я.М. Жарков, Л.Ф. Компанцева, В.В. Остроухов, В.М. Петрик, М.М. Присяжнюк, Є.Д. Скулиш]; за заг. ред. д.ю.н., проф., засл. юриста України Є.Д. Скулиша. – К., 2012. – С. 28–29.

інститутів і суб'єктів інформаційно-технологічної інфраструктури, метою діяльності яких є:

- забезпечення тотального контролю над інформаційним простором для захисту військово-інформаційних комунікацій та здійснення інформаційних атак на ворога;
- максимальне послаблення морально-психологічного стану та підриву, дезорганізації усіх сфер життя противника чи конкурента з одночасним посиленням свого політичного, соціального, духовного, військового, економічного потенціалу;
- підвищення загальної ефективності збройних сил при виконанні військових інформаційних функцій.

Основне завдання інформаційної війни (між державами) – здійснення безпосереднього негативного впливу на могутність держави-конкурента (чи противника) через послаблення її реальних і потенційних можливостей із забезпечення безпеки, створення перешкод для активної внутрішньої та зовнішньополітичної діяльності; руйнування іміджу, послаблення владної еліти, загроза стабільності соціально-політичного режиму, конституційному устрою чи територіальній цілісності держави.

До *основних маніпулятивних технологій* інформаційної війни належать:

1. Обґрунтування «справедливого характеру» війни через створення «образу ворога» в інформаційному просторі, погроз використання ЗМУ, підтримки міжнародного тероризму та загроза «молодим демократіям».
2. Провокування конфліктів на соціальному, релігійному та національному ґрунті у соціумі противника.
3. Активне використання (як реальних, так і сфальсифікованих) фактів порушень міжнародного гуманітарного права, поширення інформації про «звірства проти мирного населення» у глобальному інформаційному просторі з метою формування абсолютно негативного сприйняття противника світовою спільнотою[166].

Окрім того, важливим є і такий аспект маніпулювання, як вплив на психоемоційний стан військовослужбовців, які безпосередньо беруть участь у бойових діях у зоні конфлікту, а також на свідомість населення, через трансляцію у ЗМК та ЗМІ фальсифікованої інформації про недієздатність уряду країни, підкуп істеблішменту ворогом, щоб створити «образ жертви» для соціуму, що може

[166] Серов А. О роли дезинформации в современных конфликтах и войнах // Зарубежное военное обозрение. – 2011. – № 7. – С. 16–17.

негативно вплинути на довіру між суспільством, армією та владними інституціями, деструктивно відобразитися на національній безпеці держави і патріотичній налаштованості нації.

Основними цілями інформаційної війни є:

- дискредитація історичних фактів і національної самобутності народу, підміна системи цінностей, які визначають його національну ідентичність, нівелювання визнаних світових досягнень у науці, техніці й інших галузях, перебільшення значення помилок, недоліків, наслідків хибних дій рішень уряду;
- створення стану політичного напруження та нестабільності в державі за допомогою маніпулятивних технологій «керованого хаосу»;
- загострення антагоністичних протиріч у таборах політичних партій та рухів з метою провокування конфліктів, ворожнечі, недовіри, підозри для дестабілізації політичної системи держави;
- свідоме спонукання до надмірного застосування сили (терору) владою стосовно політичних опонентів;
- зниження рівня інформаційного забезпечення та блокування інформаційної ініціативи влади, монополія в інформаційному просторі політичного опонента, конкурента, ворога;
- акцентуація негативних рис політичної еліти (корупція, нетрадиційна сексуальна орієнтація, кримінал) для зруйнування авторитету та дискредитації органів державної влади;
- провокації та розпалювання соціальних, політичних, національно-етнічних і релігійно-конфесійних зіткнень;
- перманентний процес ініціювання акцій протесту та громадянської непокори;
- підрив авторитету та дискредитація іміджу держави, створення передумов для її міжнародної ізоляції;
- створення чи посилення активності опозиційних угруповань або рухів;
- формування підґрунтя для економічної, духовної чи військової поразки, втрати волі до боротьби та перемоги; підрив морального духу населення і, як наслідок, зниження обороноздатності та бойового потенціалу;
- пропаганда моделі певного способу життя як еталонного зразку світоглядних і поведінкових парадигм майбутнього;

- завдання шкоди безпеці інформаційно-технічної інфраструктури[167].

Основним механізмом реалізації завдань інформаційної війни є *маніпулювання масами*.

Оксфордський словник англійської мови трактує *маніпуляцію* як «акт впливу на людей... майстерне управління …або обробка». Об'єктом дій маніпулятора є духовна, психологічна складова, психоемоційні патерни людської особистості[168].

Основними видами маніпуляцій є міжособистісні, масові, політичні.

На нашу думку, політичні маніпуляції найбільше впливають на масову свідомість у добу інформаційного суспільства, як приховане управління політичною свідомістю та поведінкою людей з метою примусити їх до дії або бездіяльності всупереч їх потребам чи інтересам. Для здійснення цього маніпулювання використовують: пряму підтасовку фактів, замовчування невигідної інформації, недостовірну інтерпретацію фактів, поширення сфальсифікованої інформації та ін. Основними засобами маніпуляції суспільною свідомістю є:

- мовні – використання штампів, термінів, ідеологічних та політичних кліше;
- немовні – блокування чи нівелювання «невигідної» інформації, висвітлення інформації у сприятливому для себе контексті;
- активні – насадження стереотипів і цінностей;
- пасивні – подання фрагментованої інформації.

Сучасні інформаційні технології, глобалізація інформаційно-комунікативного середовища та інтерсуб'єктно-суспільні обміни в Інтернеті суттєво розширюють спектр й потенціал застосування маніпулятивних стратегій і тактик.

Мета маніпулювання свідомістю полягає у поширенні ворожих, шкідливих ідей та поглядів; дезорієнтації та дезінформації мас; послабленні архетипів та стереотипів суспільства для нівелювання його національної ідентичності; створення образу ворога як зовнішнього так і внутрішнього; залякуванні противника своєю (реальною чи псевдо) могутністю.

Виділяють такі основні рівні маніпулятивного впливу:

---

[167] Основні поняття маніпулятивного впливу [Електронний ресурс]. – Режим доступу: http://psychlib.com.ua/osnovni-ponyattya-manipulyativnogo-vplivu.htm

[168] Oxford English Dictionary, second edition, edited by John Simpson and Edmund Weiner, Clarendon Press, 1989, twenty volumes, hardcover [Електронний ресурс]. – Режим доступу: http://www.oed.com/

- посилення існуючих у свідомості людей ціннісних установок, стійких стереотипних конструктів, що сформовані у минулому та містять ціннісно-орієнтаційні патерни;

- часткова трансформація поглядів при акцентуванні уваги на ту або іншу подію;

- кардинальна зміна життєвих установок[169].

Для маніпулювання суспільною свідомістю використовують методи перекручування, приховування та способу подання інформації.

Перекручування інформації – діяльність суб'єктів маніпулятивного впливу від відвертої брехні до часткових деформацій (підтасовування фактів або зміщення в семантичному полі поняття).

Приховування інформації виявляється у замовчуванні або приховуванні важливих якісних чи кількісних ознак інформації у кожному конкретному просторі-часі. Частіше використовують метод часткового висвітлення, дисперсного чи вибіркового подання матеріалу.

Спосіб подання інформації відіграє вирішальну роль у тому, щоб зміст, який передається, був сприйнятий так, як необхідно його відправнику[170]. У способі подання інформації важливого значення набуває комплексний вплив уваги та емоційної пам'яті на процес активації образів, які здатні запустити процес формування поглядів у свідомості в заданому напрямі. З цією метою відбувається руйнування бар'єрів історичної та короткотривалої пам'яті для створення сприятливої атмосфери навіювання[171].

Формами маніпулятивного впливу є *фальсифікації, дезінформація та негативна міфологізація.*

Фальсифікація – свідоме викривлення фактів і подій з метою перекодування колективної свідомості народу.

Методи фальсифікації – це насамперед підробка документів, замовчування, вигадування і довільне тлумачення фактів, що унеможливлює створення реальної картини та негативно впливає на громадську думку, суспільно-політичну позицію й діяльність як окремої особистості, так і усього суспільства.

---

[169] Серов А. О роли дезинформации в современных конфликтах и войнах // Зарубежное военное обозрение. – 2011. – № 7. – С. 15.

[170] Історія інформаційно-психологічного протиборства: підруч. / [Я.М. Жарков, Л.Ф. Компанцева, В.В. Остроухов, В.М. Петрик, М.М. Присяжнюк, Є.Д. Скулиш]; за заг. ред. д.ю.н., проф., засл. юриста України Є.Д. Скулиша. – К., 2012. – С. 13.

[171] Серов А. О роли дезинформации в … С.15.

Дезінформація – це хибна інформація, яка свідомо надається противнику для більш ефективного ведення бойових дій власними збройними силами, ускладнення перевірки можливих каналів і джерел витоків інформації, процес маніпулювання інформацією з метою введення противника в оману шляхом надання неповної або повної, але застарілої інформації, чи спекулятивного використання її частин у спотвореному вигляді.

Різновидами дезінформації є напівправда або «брехня на замовчування» та «інформаційний шум». Напівправду використовують в інформаційній війні з метою створення ілюзії про успіхи та досягнення з одночасним замовчуванням невдач і провалів. *«Інформаційний шум»* – своєрідна «димова завіса», диверсифікація негативної інформації через «занурення» у комплекс версій, які «підтверджуються» набором штучно сконструйованих фактів, для творення у свідомості спотвореної інформаційної «картинки»[172].

Обов'язковим елементом процесів фальсифікації та дезінформації соціуму у добу сучасного інформаційного суспільства є міфологізація як множина поглядів, уявлень, відчуттів, що існують у підсвідомості для осмислення історичних подій та постатей, основоположних світоглядних, культурних, духовних характеристик народу, які мають для нього пріоритетне значення.

Міфологізація здійснюється через маніпуляцію історичними даними для досягнення мети сучасної етнополітики; створення жорсткої конструкції догматів, які ігнорують критичне сприйняття та вимагають лише сліпої віри; ігнорування наукової методології та використання псевдонаук.

Основними ознаками здійснення інформаційно-комунікативного впливу є :

1) ігнорування матеріалів, що містять альтернативні відомості;

2) штучне звуження теми і тотальне ігнорування множини фактів;

3) спрощена система доказів;

4) свідома дискредитація опонентів будь-якими методами;

5) ігнорування плюралістичних теорій науковців, посилання на псевдо авторитетні джерела, які поширюють заздалегідь заплановані моделі міфу;

6) надмірна екзальтація та емоційність, безапеляційне ствердження основних ідей та постулатів;

7) псевдоерудиція, нагромадження факт без їх поглибленого аналізу;

[172] Там само.

8) маніпуляторне цитування;

9) відсутність наукової критики джерел;

10) етноцентризм[173].

Слід зазначити, що маніпулятивні технології у процесах реалізації цілей і завдань інформаційної війни здійснюють методами ідеологічної пропаганди.

Ідеологія – система концептуально оформлених уявлень та ідей, яка виражає інтереси, світогляд та ідеали різних суб'єктів політики – класів, націй, суспільства, політичних партій, громадських рухів і виступає формою санкціонування або існуючих в суспільстві панування та влади, або радикального їх перетворення[174].

Пропаганду ж можна розглядати як поширення та утвердження в масовій свідомості систематизованих форм логічного мислення, що відображають світоглядні орієнтири особи та суспільства в цілому[175].

Особливостями пропаганди є визнання її як інформаційного процесу, визначення інтерпретаційного характеру пропагандистських акцій, використання емоційного забарвлення пропагандистського повідомлення.

Політична пропаганда – це комунікативна діяльність, яка зорієнтована на формування у свідомості або трансформацію певних установок, переконань, стереотипів цільової аудиторії за допомогою інформаційних та/або маніпулятивних прийомів, технік, методів для досягнення поставлених цілей і завдань[176]. Тобто, це діяльність, що передбачає «системне поширення, поглиблене роз'яснення соціально-політичних, економічних, правових поглядів, ідей, теорій та забезпечує формування у суспільстві певних настроїв, закріплення у свідомості громадян тих чи інших цінностей, орієнтацій, уявлень з метою максимального розширення кола прибічників відповідної ціннісної системи»[177].

Таким чином, «основна психологічна мета пропаганди – вплив на систему ідейних, суспільних і політичних установок людей», де установка – «це сформована під впливом пропаганди, виховання та досвіду відносно стійка організація знань, почуттів і мотивів, які

---

[173] Гула Р.В. Патриотизм и национализм. Опыт историософского анализа. – Д., 2014. – С. 66.

[174] Новая философская энциклопедия: в 4 т. / Ин-т философии РАН, Нац. общ-науч. фонд. – Т. II. – М., 2010. – С. 81.

[175] Скуленко М.І. Логічні засади пропаганди: монографія. – Запоріжжя, 2010. – С. 5.

[176] Яковлева Н.І. Пропаганда як складова політичної комунікації: автореф. дис. … канд. політ. наук: спец. 23.00.02 «Політичні інститути та процеси». – К., 2010. – С. 3.

[177] Політологічний енциклопедичний словник [Упор. В.П. Горбатенко; за ред. Ю.С. Шемшученка та ін.]. – 2-ге вид., доп. і перероб. – К., 2004. – С. 544–545.

провокують відповідне ставлення людини до ідейних, політичних і суспільних явищ дійсності»[178].

До *загальних і спеціальних методів пропаганди* Н.І. Яковлева зараховує спрощення, замовчування, вигаданий факт, пряме коментування, непряме коментування, двосторонню аргументацію, напівправду, інсинуацію, інформаційне перевантаження, інформаційно-пропагандистську індукцію, семантичне маніпулювання, політичний евфемізм, дифамацію (розголошення інформації, що може зіпсувати імідж певної особи, але відповідає істині)[179].

На нашу думку, в сучасному глобалізованому світі загальні та спеціальні методики пропаганди здійснюються та реалізовуються через спеціальну пропаганду (спецпропаганду) й контрпропаганду.

Спеціальна пропаганда (спецпропаганда) – комплекс технологій військово-психологічної інженерії під час війни або локального конфлікту, що здійснюються через маніпуляції суспільною свідомістю (переконання та навіювання) для деморалізації мирного населення і військ противника та досягнення політичних (військових, економічних) перемог.

Особливостями спецпропаганди є:

- зміщення акцентів з теоретичного рівня світобачення на рівень емпіричного сприйняття;
- домінування у доказовій базі ірраціональних явищ (міфів, інстинктів, штампів);
- нав'язування потрібних хибних стереотипів сприйняття та мислення, викривлених уявлень про події у світі та країні.

Слід зазначити, що у сучасному науковому дискурсі поняття спецпропаганди часто ототожнюють із поняттям психологічна війна. На нашу думку, ці поняття суттєво різняться. ***Психологічна війна*** – цілеспрямоване застосування прямих і опосередкованих психологічних та інших (дипломатичних, пропагандистських, економічних) впливів на ідеї, настрої, психіку ворога (конкурента) з метою створення необхідних ідеологічних і соціальних установок свідомості, формування стереотипів його поведінки та прийняття рішень, необхідних для деморалізації противника. Отже, психологічна війна ширше поняття, яке стає складовою частиною інформаційної війни у мирний та воєнний час. Спецпропаганда –

[178] Войтасик Л. Использование психологии в системе пропаганды // Реклама: внушение и манипуляция. Медиа-ориентированный подход. – М., 2001. – С. 257–260.

[179] Яковлева Н.І. Пропаганда як складова політичної комунікації: автореф. дис. … канд. політ. наук: спец. 23.00.02 «Політичні інститути та процеси» / Н.І. Яковлева. – К., 2010. – С. 11.

необхідний компонент будь-якої війни або збройного конфлікту та має специфічну військову спрямованість.

Контрпропаганда – створення модифікованого інформаційного потоку, проведення інформаційних і психологічних операцій зі зниження ефективності інформаційно-психологічних заходів противника для послаблення, а в ідеалі – повної ліквідації ефекту від пропаганди ворога.

Особливостями контрпропаганди є:

- наявність апріорної інформації про цільову аудиторію;
- спрямування контрпропагандистських акцій проти конкретних ідей, які потрібно нейтралізувати;
- скерованість акцій проти потенційних джерел генераторів ідей.

Типами контрпропаганди є: цензура, пряма та непряма контрпропаганда. У мережі Інтернет – це безпосередньо атаки на сайти і тролінг[180].

Політичне маніпулювання можна визначити як «систему засобів ідеологічного та духовно-психологічного впливу на масову свідомість з метою нав'язування певних ідей, цінностей та цілеспрямований вплив на громадську думку і політичну поведінку задля скерування їх у заданому напрямку»[181].

Основними *маніпулятивними інструментами пропаганди* є: анонімний авторитет, буденна розповідь, прийом «тримай злодія», емоційний резонанс, ефект бумеранга, ефект ореолу, ефект присутності, інформаційна блокада, коментарі, констатація фактів, помилкова аналогія, відволікання уваги[182].

Практична реалізація завдань ідеологічно-пропагандистського маніпулятивного впливу під час ведення інформаційної війни має такі характерні риси:

- жорстке підпорядкування інформаційних потоків ідеологічно-пропагандистським завданням влади і національним інтересам;
- максимальна централізація пропагандистської діяльності та створення спеціалізованих структур контр- і спецпропаганди;
- тотальне обмеження альтернативних джерел інформації;
- примусова участь у пропагандистських маніпулятивних акціях «публічного каяття» ідеологічного (військового) противника;

---

[180] Почепцов Г.Г. Пропаганда и контрпропаганда. – М., 2004. – 256 с.

[181] Кучма Л. Аксіологічний вимір політичного маніпулювання [Електронний ресурс]. – Режим доступу: http // www. ena.lp.edu.ua: 8080/bitstream/ ntb/7862/7862/1/21/pdfn2

[182] Присяжнюк М.М. Прийоми маніпулювання свідомістю людей через засоби масової інформації [Електронний ресурс]. – Режим доступу: http//www.nbuv.gov.ua /portal/natural/sitsbo/01-18/01-18.pdf

- індивідуальна підготовка пропагандистського апарату, опора на еліту чи публічних осіб.

У сучасному інформаційному суспільстві у добу глобалізації маніпуляції суспільною свідомістю здійснюються передовсім через інформаційний вплив.

Інформаційний вплив – це організоване цілеспрямоване застосування спеціальних інформаційних засобів і технологій для внесення деструктивних змін у свідомість та психіку особистості, соціальних груп чи населення (корекція поведінки), а також в інформаційно-технічну інфраструктуру об'єкта впливу та (чи) фізичний стан людини.

Процес інформаційного впливу умовно можна розділити на такі етапи:

- генерація джерелом впливу даних, інформаційних елементів та інформаційних сукупностей;
- передача інформації джерелом впливу;
- прийом інформації реципієнтом;
- акумулювання даних, інформаційних елементів об'єкта впливу;
- активні дії об'єкта впливу[183].

Інформаційний вплив поділяється на інформаційно-технічний та інформаційно-психологічний.

Інформаційно-технічний вплив – це система заходів інструментального впливу на інформаційно-технічну інфраструктуру об'єкта з метою забезпечення реалізації необхідних негативних змін у її функціонуванні, а також вплив на фізичний стан людини. «Ворожа нація або група можуть скористатися слабким місцем для проникнення у погано захищені комп'ютерні мережі та порушити або вивести з ладу їх критичні функції»[184].

Інформаційно-психологічний вплив – комплекс заходів цілеспрямованого виробництва та поширення спеціальної інформації в середовищі політичної еліти та суспільства, формування певних соціальних ідей, уявлень, переконань, нав'язування цілей, які не входять до числа їх інтересів і безпосередньо впливають на системні зміни світоглядних орієнтирів суспільства, його свідомості, психіки і поведінки. «Акції інформаційної війни повинні бути спрямовані

[183] Фурашев В.М. Інформаційні операції крізь призму системи моніторингу та інтеграції Інтернет-ресурсів // Правова інформатика. – 2009. – № 2 (22).

[184] Lewis J.A. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies. – December – 2002. – P. 9.

проти системи знань і переконань противника», – зазначає полковник армії США Р. Сафранські[185].

Вчені класифікують сучасне суспільство, сформоване на пострадянському просторі, як об'єкт інформаційно-психологічного впливу таким чином:

1. «Явні паразити», які свідомо і цілеспрямовано ведуть захоплення території і ресурсів країни (1–2%).

2. «Мародери» – спільників ворога, які поспішають нажитися в умовах безладу і хаосу (5–7%).

3. Основна маса населення (80–85%) – «живі трупи», жертви інформаційно-психологічної війни, які фізично ще виживають, але моральних сил для опору вже не мають. Це основні об'єкти маніпуляції, яка діє на них як своєрідний допінг, «доза» якого зростає у визначені моменти, особливо під час виборів.

4. «Контужені» в інформаційній війні (5–7%). Вони усвідомлюють процеси, що відбуваються, але втішають себе ілюзіями, готові до боротьби, але не здатні бачити її способи та методи, стають заручниками псевдо-ідеологій та псевдолідерів.

5. «Передовий загін» (1–2%), це саме ті бійці, які не тільки розуміють, що триває Четверта світова війна, а й ведуть боротьбу за свободу й незалежність Батьківщини[186].

Основними *складовими інформаційної війни* в межах інформаційного протиборства, на думку українських дослідників, можна вважати:

- *психологічні операції* – це планова пропагандистська і психологічна діяльність, яку здійснюють у мирний або воєнний час, спрямована на іноземні ворожі, дружні або нейтральні аудиторії з метою впливу на їх свідомість та поведінку в потрібному напрямку для досягнення як політичних, так і військових цілей держави;

- *дезінформація* – комплекс недостовірної інформації, що створює у противника помилкове уявлення про власні сили та наміри;

- *фізичне руйнування* – частина інформаційного протиборства, цілями якої є руйнування інформаційних систем противника;

- *інформаційна розвідка* – комплекс заходів з отримання та обробки даних про дійсного або ймовірного противника, його

[185] Szafranski R. A Theory of Information Warfare. Preparing For 2020 [Електронний ресурс]. – Режим доступу: http:// www.airpower. maxwell.af. mil/ airchronicles/apj/apj95/spr95_files/szfran.htm

[186] Сенченко М. Четверта світова. Інформаційно-психологічна війна [Електронний ресурс]. – К., 2014. – Режим доступу: https://lib.rus.ec/b/241595/read

військові ресурси, реальні бойові можливості, а також про потенційний театр воєнних дій[187];

- *інформаційні атаки* – комплексні акції інформаційно-технічного та інформаційно-психологічного впливу в інформаційно-комунікаційній сфері з використанням протоколів міжмережевої взаємодії, ЗМІ та ЗМК з метою управління, спостереження та деструкції (знищення) об'єкта впливу через нанесення йому прямої чи опосередкованої шкоди з використанням його слабких сторін.

Складовими інформаційної війни, за оцінками Інституту національно-стратегічних досліджень США, є:

1. Командна війна – визначення стратегії й тактики нейтралізації органів управління противника, порушення систем управління військами, знищення його комунікаційних мереж на стратегічному, оперативному та тактичному рівнях через здійснення комплексу інформаційних операцій. Інформаційні операції визначаються як «акції, цільовий вплив на інформацію та інформаційні системи противника, а також захист власної інформації та інформаційних систем»[188].

2. Розвідувальна війна – несанкціоноване отримання та обробка даних про віддалену інформаційну систему, її ресурси, засоби захисту, пристрої та програмне забезпечення для здобування стратегічно важливих знань про потенціал противника.

3. Електронна війна – створення системи тотального контролю за інформаційними ресурсами ворога, його системами управління та зв'язку і способи їх знищення.

4. *Психологічна війна* – застосування інформаційних впливів на психіку ворога з метою створення необхідних ідеологічних і соціальних установок, формування стереотипів поведінки та прийняття рішень, необхідних для деморалізації противника.

У доктрині інформаційних операцій США виділяють чотири основні категорії інформації, що використовуються проти людського інтелекту, психіки, менталітету нації. Це операції проти волі нації, проти командування суперника, ворожих військ та національних культур[189].

---

[187] Любарський С.В. Місце та роль мережевої розвідки в моделях інформаційного протиборства // Збірник наукових праць ВІТІ НТУУ «КПІ». – 2013. – № 1. – С. 32.

[188] Information Operations Roadmap – Do DUS. – 30 October 2003. – 78 p. [Електронний ресурс]. – Режим доступу: http://www.information-retrieval. info/ docs/info_ops_roadmap.pdf

[189] Гуріна Н. Інформаційне протиборство – один з головних напрямків політики сучасних міжнародних відносин [Електронний ресурс]. – Режим доступу: ukrlife.org/main/cxid/gurina.doc; http: // www.dtic.mil/ doctrine/ jel/new_pabs/jp 3_13.pdf

5. *Комп'ютерна війна (кібервійна)* – використання комп'ютерних технологій та Інтернету однією державою, або за її безпосередньої підтримки, проти іншої держави, спрямоване проте її безпеки та оборони, яке є настільки інтенсивним і серйозним, що становить реальну загрозу безпеці та суверенітету цієї держави[190].

М. Лібікі виокремлює наступні види інформаційної війни:

- «командно-управлінський» спрямований на знищення каналів зв'язку між командуванням та виконавцями;
- «розвідувальний» передбачає збір важливої та захист власної інформації;
- «психологічний» характеризується пропагандою, інформаційною обробкою населення, деморалізацією, дезінформацією;
- «хакерський» реалізується через диверсійні дії та атаки проти ворога шляхом створення спеціальних програм;
- «економічний» втілюється у інформаційній блокаді та інформаційному імперіалізмі;
- «електронний» спрямований проти засобів електронних комунікацій: радіозв'язку, радарів, комп'ютерних мереж;
- «кібервійна» відрізняється від хакерської тим, що в даному випадку мова йде про вірус, яким заражується система[191].

Український дослідник Я. Малик пропонує власну класифікацію інформаційних війн: психологічна війна, кібервійна, мережева війна (мережа – інформаційний простір, де і розгортаються основні стратегічні операції – як розвідувального, так і військового характеру, а також відбувається їхнє медійне, дипломатичне, економічне і технічне забезпечення), ідеологічна війна, радіоелектронна боротьба, яка може проявитися такими способами як подавлення телебачення і радіомовлення, ресурси телебачення і радіомовлення можуть бути захоплені/підкорені для здійснення дезінформації, мережі комунікацій можуть бути заблоковані або недоступні, операції фондової біржі можуть саботуватися електронним втручанням, даючи витік чутливої інформації або поширюючи дезінформацію[192].

Експерти Пентагону з початку XXI ст. поділяють арену військових дій на традиційний простір і кіберпростір, який у війнах

---

[190] Супрунов Ю.М. Нормативно-правове забезпечення розгортання систем кібернетичної оборони провідних країн світу // Інформаційна безпека людини, суспільства, держави. – 2011. – № 1 (5). – С. 86.

[191] Рудницька У.І. Інформаційні війни як засіб геополітичного протистояння // Гуманітарний журнал. – 2015. – № 1-2. – С. 137.

[192] Малик Я. Інформаційна війна і Україна // "Демократичне врядування" Науковий вісник. – 2015. – Вип. 15. – Режим доступу: http://nbuv.gov.ua/UJRN/DeVr_2015_15_3

нового покоління буде відігравати вирішальну роль[193]. Тому, у червні 2011 р. МО США в «Стратегії дій Міністерства оборони США у кіберпросторі» офіційно визначив статус кіберпростору як сфери ведення бойових дій.

Війна у кіберпросторі *(кібервійна)* в сучасному науковому дискурсі розглядається як форма розвитку та поширення інформаційних технологій у воєнній сфері, складова частина інформаційних війн, що здійснюється із використанням всесвітньої мережі[194], і як «інформаційна війна, яка ведеться в кіберпросторі шляхом здійснення кібератак і захисту власної інфосфери»[195].

На нашу думку, ***кібератака*** – це цілеспрямована та спланована інформаційно-технічна акція, яка характеризується невпинністю, стрімкістю, рішучістю дій проникнення і активного впливу на систему державного та військового управління, інформаційно-комунікаційні мережі й ресурси системи національної безпеки супротивника з метою їх дезорганізації та знищення. За визначенням індійського дослідника Р. Патьяла, кібератака є «одним із методів кібервійни», який ставить за мету «злам комп'ютерних мереж противника… спрямований на носії, у яких зберігається інформація або знищення елементів …структури командування та контролю противника в режимі реального часу, щоб знизити його бойові потужності»[196].

Американські дослідники вважають, що за спрямованістю на об'єкт, кібератаки можна поділити кібератаки на дані та кібератаки на об'єкти інфраструктури.

Кібератака на дані є порушення цілісності (модифікація, видалення, ін'єкція) або доступності даних (інформації, що міститься в обчислювальних системах), або процесів їх обробки, яка містить економічні втрати в 1 млрд. доларів і більш. Тут не береться до уваги порушення конфіденційності (крадіжка) даних.

Кібератака на об'єкти інфраструктури є інформаційно-технічна дія на об'єкти інфраструктури, що завдає збитку в 100 млн. доларів і

[193] Гриняев С.Н. Концепции ведения информационной войны в некоторых странах мира // Зарубежное военное обозрение. – 2002. – № 2. – С. 25.
[194] Польских Л. О применении глобальной компъютерной сети Интернет в интересах информационного противоборства // Зарубежное военное обозрение. – 2005. – № 7. – С. 20–23.
[195] Климчук О.О. Кібервійна в сучасних умовах // Інформаційна безпека людини, суспільства, держави. – 2011. – № 1(5). – С. 80.
[196] Патьял Р. Принципы войны: необходимость переосмысления // Геополитика. Информационно-аналитическое издание. Тема выпуска: Война. – Вып. XXI. – М. – С. 40.

більше або веде до загибелі від однієї і більше осіб. Даний вид дії виходить за межі лише інформаційних систем[197].

Бойові операції в кіберпросторі – це організовані акти відповідних частин і з'єднань, які скоординовані та взаємопов'язані за цілями, завданням, місцем і часом здійснюються одночасно й послідовно, а також маневри сил, що здійснюються за єдиним задумом і планом стратегічних, оперативно-стратегічних, оперативних й оперативно-тактичних завдань у кіберпросторі, які проводяться для перемоги у цій сфері та забезпечення інформаційної переваги над противником, дезорганізації та виводу з ладу його систем державного, військового та цивільного управління, а також порушення функціонування або знищення об'єктів критичної інфраструктури[198].

Кібероперації ЗС США класифікуються за певними ознаками на:

а) мережеві операції забезпечення: кіберзахист – захист інформації, комп'ютерних мереж, реагування на несанкціоновану активність; управління мережевою інфраструктурою – планування, проектування, установка та обслуговування мереж; діагностика мережевої інфраструктури – виявлення та усунення технічних недоліків мережевого обладнання.

б) кібероперації забезпечення: моніторинг надійності системи кіберзахисту; оцінка безпеки «методом від загроз» та усунення виявлених недоліків; моделювання діяльності супротивника; контррозвідка; розвідка кіберзагроз і кіберрозслідування; НДДКР з засвоєння кіберпростору.

в) спільні операції: радіоелектронна розвідка; операції в ЕМ-спектрі; операції в інших доменах.

г) бойові кібероперації: кібератака; кіберрозвідка комп'ютерних мереж супротивника; превентивна оборона; виявлення джерел атаки; вивчення та прогнозування кіберзагроз; вивчення мережевих параметрів.

д) додаткові можливості: взаємодія з приватним сектором; взаємодія з правоохоронними органами та спецслужбами; захист критично важливих об'єктів інфраструктури[199].

---

[197] Башкиров Н. Взгляды военного и политического руководства США на защиту инфраструктуры от киберугроз // Зарубежное военное обозрение. – 2018. – №12. – С. 13–17.

[198] Тулин С. Органы управления ВС США боевыми действиями в кибернетическом пространстве // Зарубежное военное обозрение. – 2012. – № 2. – С. 10.

[199] Олегин А. Силы кибероперацій сухопутных войск США. Взгляды американского командования на их применение // Зарубежное военное обозрение. – 2014. – № 1. – С. 44.

6. Інформаційна війна в *економічній сфері* – умисне створення негативного іміджу конкурента і несприятливих умов ведення бізнесу для захоплення ринків збуту. На сучасному етапі формою інформаційної війни в економічній сфері є також і промислове шпигунство як діяльність із незаконного одержання конфіденційної інформації (комерційна таємниця) про стратегічні й тактичні бізнес-плани для конкурентної переваги на ринку, а також «знищення» конкурента.

7. *Інформаційний тероризм* – особливий різновид психологічного терору, синтезована форма інформаційно-психологічного насильницького впливу на суспільну свідомість та злочинне використання його інформаційно-комунікативних систем, мереж і їхніх компонентів, фізичного або технологічного порушення роботи критичних телекомунікаційних вузлів для здійснення терористичних дій та інших акцій, що прирівнюються до них.

Формами інформаційної війни в залежності від комплексу завдань є оборонна та наступальна. Однак, на практиці більшість інформаційних заходів є комплексними, адже більшість інформаційних впливів одночасно поєднують елементи наступальних та оборонних процедур.

Оборонна інформаційна війна – це сплановані та цілеспрямовані дії органів державного і військового управління, соціальних інститутів суспільства для досягнення повного інформаційного контролю над противником з одночасним захистом своїх інформаційних комунікацій й ресурсів, що здійснюються як всередині держави, так і у міжнародному середовищі. Д. Альбертс зазначає: «Термін «оборонна інформаційна війна» застосовується для визначення будь-яких дій, що спрямовані на захист від інформаційних атак…на осіб, які приймають рішення, інформації й інформаційних процесів …і комунікаційні засоби передачі рішень у війська»[200].

Наступальна інформаційна війна – це спланована та цілеспрямована діяльність органів державного і військового управління, соціальних інститутів суспільства, яка передбачає рішучі дії з проникнення та активного впливу на інформаційні мережі та ресурси противника з метою їх дезорганізації та повного знищення. За висловом Д. Коала: «Наступальна інформаційна війна наносить

[200] Alberts David S. Defensive Information Warfare. National Defense University Press, 1996 [Електронний ресурс]. – Режим доступу: http:// www. dodccrp.org/ files/Alberts_Defensive.pdf

удар противнику в голову, замість того, щоб вести війну… силою проти сили»[201].

Основним видом оборонних і наступальних інформаційних війн є *інформаційні операції.*

Інформаційні операції – комплексний термін, який об'єднує поняття електронної війни, комп'ютерних мережевих операцій (радіоелектронної боротьби), психологічних операцій, воєнної дезінформації для здійснення впливу, управління інформаційними потоками та контролю за ними, руйнування діяльності інформаційної системи, пошкодження чи захоплення засобів підтримки прийняття рішень командним складом противника, а також заходи, що спрямовані на підвищення захищеності від відповідної діяльності противника.

Інформаційні операції здійснюються як на глобальному рівні автоматизованих систем (технотронний підхід), так і на локальному з метою впливу на особовий склад ЗС противника, населення регіону чи соціальну групу (психологічний підхід).

У *технотронному підході* метою при проведенні інформаційних операцій є зруйнування інформаційно-технічної інфраструктури і технічної компоненти інформаційно-аналітичних систем суб'єкта впливу[202].

Психологічний підхід. За визначенням українських дослідників В.П. Горбуліна, О.Г. Додонова, Д.В. Ланде, термін «інформаційна операція» як вид інформаційного протистояння насамперед спрямований на здійснення маніпуляції суспільною свідомістю з такими основними цілями:

- дезорієнтація людей та їхня дезінформація;
- послаблення переконань людей, основ суспільства;
- залякування мас (психологічний терор).

Особливостями інформаційних операцій (з врахуванням обох підходів) є:

1. Комплексність. Інформаційні операції – це міждисциплінарна система методів і технологій в інформатиці, соціології, психології, міжнародних відносинах, теорії комунікації, воєнній науці.

2. Нестандартність. Дотепер не існує єдиних визначених стандартів проведення інформаційних операцій.

---

[201] Coale John C. Fighting Cybercrime // Military Review. – March-April. – 1998. – P. 77–82.

[202] Додонов О.Г. Захист інформації в інформаційно-аналітичних системах державних органів управління // Реєстрація, зберігання і обробка даних. – 2000. – Т. 2. – № 2.

3. Загальнодержавний рівень. У розвитку технологій інформаційних операцій зацікавлені оборонні відомства, інститути громадянського суспільства, комерційні організації.

4. Науковий підхід. Задачі формування наукового підходу до інформаційних операцій є нагальними та актуальними[203] у сучасному глобалізованому середовищі в добу інформаційного суспільства.

Інформаційні операції *на державному рівні* виконують такі завдання:

- захист національних інтересів;
- попередження міжнародних конфліктів;
- припинення провокаційних і терористичних акцій;
- забезпечення національної безпеки і захисту національних інформаційних ресурсів.

При виконанні *військових завдань* інформаційні операції здійснюються як комплекс заходів у масштабах ЗС країни, їх видів, об'єднаних командувань у зонах відповідальності і є складовою частиною військових кампаній (операцій). Завданнями інформаційних операцій є:

- досягнення інформаційної переваги над противником;
- захист своїх систем управління[204].

Інформаційні операції реалізуються в *формі* акцій інформаційного впливу та спеціальних інформаційних операцій.

Акція інформаційного впливу (АІВ) – одноразова акція інформаційно-психологічного та інформаційно-технічного впливу, яка передбачає спланований вплив на свідомість і поведінку людей через поширення упередженої, неповної чи недостовірної інформації та (або) інформаційно-технічну інфраструктуру об'єкта (об'єктів).

Спеціальна інформаційна операція (СІО) – це сплановані дії, спрямовані на ворожу, дружню чи нейтральну аудиторію з метою спонукання до прийняття управлінських рішень або (та) вчинення дій, вигідних для суб'єкта інформаційного впливу. СІО можуть передбачати також вплив на інформаційно-технічну інфраструктуру для більш ефективного контролю свідомості і поведінки людей[205].

Інструментом інформаційної війни є *інформаційна зброя* – сукупність організаційно-психологічних та організаційно-технічних

---

[203] Горбулін В.П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. – К., 2009. – С. 12–16, 153–162.

[204] Климчук О.О. Кібервійна у сучасних умовах // Інформаційна безпека. Людина. Суспільство. Держава. – 2011. – № 1 (5). – С. 79.

[205] Історія інформаційно-психологічного протиборства: підруч. / [Я.М. Жарков, Л.Ф. Компанцева, В.В. Остроухов, В.М. Петрик, М.М. Присяжнюк, Є.Д. Скулиш]; за заг. ред. д.ю.н., проф., засл. юриста України Є.Д. Скулиша. – К., 2012. – С. 20.

впливів на суспільну та індивідуальну свідомість політичної еліти, населення, особовий склад збройних сил, інформаційні системи, комплекси автоматизованого і автоматичного керування, системи та мережі зв'язку, тощо здійснених з використанням таких інструментів й засобів:

- знищення, спотворення, розкриття, крадіжки чи створення хибної інформації;
- подолання систем захисту;
- обмеження або розширення доступу до інформації та ресурсів законних користувачів;
- протидії та дезорганізації роботи технічних засобів, комп'ютерних систем;
- управління ресурсами інформаційних систем[206].

Основними *принципами використання інформаційної зброї* є:

- цілеспрямованість – конкретне визначення об'єкта впливу;
- вибірковість – зосередження основних зусиль на визначеному (стратегічному) напрямку дій;
- розосередженість – вміле використання маневру сил і засобів;
- масштабність впливу, швидкість доставки компонентів зброї за допомогою сучасних інформаційних технологій, що дає можливість для нанесення руйнівного удару, незалежно від національних кордонів та суверенітетів;
- комплексність впливу на людей, технічні засоби і системи, можливість регулювання (дозування) «потужності» впливу тощо;
- прихованість – здатність досягти мети без завчасної підготовки до ведення бойових дій;
- універсальність – можливість поліваріантного використання як військовими, так і цивільними структурами держави-агресора, проти військових і цивільних об'єктів;
- економність – вигідне для атакуючої сторони співвідношення витрат та запланованого ефекту катастрофи для країни-об'єкта військової агресії.

У оборонній сфері інформаційна зброя спрямована на:

- інформаційні ресурси стратегічного управління, науково-дослідні підрозділи, оборонно-промисловий комплекс;
- системи зв'язку й управління військами та зброєю, їх інформаційне забезпечення;

---

[206] Горбенко І.Д. Інформаційна війна – сутність, методи та засоби ведення // Ювілейна науково-технічна конференція «Правове, нормативне та метрологічне забезпечення захисту інформації в Україні». – К., 1998. – С. 11.

- інформаційну інфраструктуру, зокрема центри обробки й аналізу інформації штабів, пункти управління, вузли та лінії зв'язку силових структур;

- морально-психологічний стан військ.

За об'єктами впливу інформаційна зброя поділяється на два основних класи:

1. Інформаційно-технічна зброя, що впливає на інформаційні ресурси, інформаційно-технічну та інформаційну інфраструктуру збройних сил, держави в цілому. За принципом дії можна виділити такі види ІТЗ:

- фізична – засоби вогневого ураження і фізичного знищення основних компонентів інформаційно-технічної інфраструктури держави, систем управління економікою та воєнною організацією;

- радіоелектронна зброя – засоби радіоелектронної боротьби і радіоелектронної розвідки для контролю інформаційних ресурсів потенційного противника, прихованого чи відкритого втручання в роботу його систем зв'язку та управління;

- програмно-технічна зброя – засоби несанкціонованого доступу до інформаційних ресурсів з метою їх викрадення, викривлення або знищення для дезорганізації роботи комп'ютерно-комунікаційних мереж[207].

2. Інформаційно-психологічна зброя впливає на морально-психологічний стан людини, окремих груп населення, суспільства в цілому. За принципом дії її поділяють на пропагандистську, нейролінгвістичну, психоаналітичну, психотропну, психогенну:

- пропагандистська – сукупність друкованих й електронних засобів впливу на свідомість, психіку об'єкта через процеси опосередкованого спілкування з допомогою комплексу спеціалізованої інформації для формування у нього потрібних ідей, поглядів, переконань;

- нейролінгвістична – комплекс вербальних і технологічних операцій, за допомогою яких досягаються принципові зміни мотивації об'єкта через дію на їх свідомість спеціальних лінгвістичних програм;

- психоаналітична – засоби психокорекційного впливу на особистість за допомогою терапевтичних маніпуляцій (особливо в стані гіпнозу);

[207] Панін В.Г. Різновиди та тенденції розвитку інформаційної зброї // Вісник Київського національного університету імені Т. Шевченка. – 2012. – Вип. 28. – С. 4.

- психотропна – комплекс медичних препаратів, хімічних і біологічних засобів, які безпосередньо впливають на психіку людини;

- психогенна – використання комплексу фізичних подразників (шумових ефектів, освітлення, температури) і спеціальної інформації (масові жертви, зруйнування), внаслідок чого відбуваються деструктивні зміни фізіологічних реакцій та знижується здатність до раціонального аналізу оточуючої дійсності;

- психотронна – спеціальні технічні засоби (психогенератори), що використовують вплив енергоінформаційних полів[208].

За метою використання інформаційна зброя буває атакуючою та забезпечувальною.

Атакуюча активно впливає на інформацію, яка зберігається, обробляється та передається в системі управління. Комплексом цільових завдань застосування даної зброї є системне порушення:

- конфіденційності;
- цілісності інформації;
- доступності інформації;
- психологічного балансу абонентів інформаційної війни.

Забезпечувальна зброя – це комплекс засобів комп'ютерної розвідки та засобів подолання систем захисту, який застосовують в атаках проти дії інформаційних систем противника[209].

За принципами бойового застосування, видами інформаційної зброї є:

1. Психотронна (психофізична) зброя – сукупність інтелектуальних і технологічних можливостей та знань психотроніки, її засобів, методів, приладів, конструкцій, генераторів, які застосовуються у дистанційних психотропних атаках на людину з метою корекції та програмування її поведінки чи фізіологічних функцій. Психотронний (парапсихологічний, екстрасенсорний) вплив здійснюється через позачуттєве (неусвідомлюване) сприйняття, здійснюється дистанційно за допомогою різних пристроїв, що випромінюють періодичні коливання в різних діапазонах електромагнітних, акустичних хвиль; періодичних коливань магнітних, електричних полів, які діють на психіку завдяки резонансу

[208] Информационная цивилизация – XXI век [Електронний ресурс] / Нелетальное оружие уже убивает. – Режим доступу: http // info21.ru/second.php?id=53

[209] Климчук О.О. Кібервійна у сучасних умовах // Інформаційна безпека. Людина. Суспільство. Держава. – 2011. – № 1 (5). – С. 81–82.

з частотами організму для стимулювання певних психологічних реакцій[210].

2. Засоби здійснення програмно-математичного впливу на державні, цивільні й військові інформаційні системи та мережі для керування ними на відстані поділяються на:

- нейтралізатори тестових програм, що забезпечують приховування випадкових і навмисних «недоліків» програмного забезпечення;
- засоби придушення інформаційного обміну в телекомунікаційних мережах, фальсифікації інформації в каналах державного та військового управління;
- засоби ретрансляції «потрібної» для іншої сторони «правдоподібної» інформації.

Об'єктами для мережевих атак цих засобів можуть бути мережеві вузли, мережеві служби, операційні системи, засоби захисту, користувачі мережі.

3. Інформаційні матеріали – це сукупність джерел та систем, що містять інформацію, призначену для передачі.

За формою вони бувають:

- текстові інформаційні матеріали: документи, книги, журнали, газети, довідники, каталоги, рукописи;
- графічні або образотворчі: графіки, креслення, плани, схеми, карти;
- аудіовізуальні: звуко- та відеозапис, кінофільм, діапозитив, фотографія[211].

Основні види інформаційної зброї можна поділити на такі типи:

1) засоби розвідки, отримання інформації з інформаційних й телекомунікаційних систем;

2) засоби впливу на інформацію, яка обробляється в інформаційних системах, наприклад, на програмно-математичне забезпечення цих систем;

3) засоби впливу на інформаційну інфраструктуру;

4) засоби впливу на людину та суспільну свідомість у цілому[212].

---

[210] Баранівський В.Ф. Основні напрямки застосування психологічних знань під час виконання бойових завдань в умовах збройних конфліктів [Електронний ресурс]. – Режим доступу: http://www. ekmair.ukma.kiev.ua/bitstream/123456789/1055/1/Bodnar_Osnovni_napriamky.pdf

[211] Українські підручники он-лайн. Психофізична зброя [Електронний ресурс]. – Режим доступу: http:// pidruchniki. ws/ 1334020336973/ politologiya/ psihotronna_psihofizichna_zbroya

[212] Присяжнюк М. Аналіз засобів ведення інформаційної боротьби з використанням інформаційних технологій, форм і способів їх застосування [Електронний ресурс]. – Режим доступу: http:// defpol.org.ua/site/index.php/uk/component/content/article/51-kolonkaavtora/56-10082009

За оцінками експертів інформаційна зброя є основною загрозою не лише інформаційній, але й національній безпеці у глобалізованому інформаційному просторі. Усі розвинені світові держави використовують сили та засоби інформаційної зброї, сумарні витрати на розробки в цій галузі у 2012 р. вже перевищили 120 млрд дол. на рік[213].

Використання переваг ІТ технологій у сучасних інформаційних війнах стає важливою складовою забезпечення національної безпеки держави у добу глобалізації. Метою війни все більш стає не знищення збройних сил та населення противника, захоплення його території, а управління ними через маніпулювання потоками інформації та суспільною свідомістю. Зброєю у цій боротьбі є пристрої та технології, які використовуються для широкомасштабного, цілеспрямованого, швидкого і прихованого впливу на цивільні та військові інформаційні системи противника. Але, основним завданням інформаційної війни в умовах глобалізації та модернізації сучасного світу, стає досягнення тотального контролю над індивідуальною та колективною свідомістю людини та спільнот у межах глобального інформаційного простору.

Інформаційна війна як агресивна взаємодія протиборчих сторін в інформаційній сфері впливає на процеси політичних комунікацій суспільства в цілому. Застосування таких кампаній політичними акторами пов’язане зі зростанням ризиків, результатом чого є швидка зміна статусів і позицій у відносинах влади, розмивання чи втрата смислів національного менталітету, перекодування свідомості, світоглядних позицій, а також національної ідентичності народу. Через високу інтенсивність і динамічність змін інформаційні війни стають некерованими, важко піддаються управлінню та свідомому регулюванню, тому можуть нести потенційну загрозу для протиборчих сторін. Це провокує посилення політичної конфронтації, підвищує конфліктогенний потенціал у соціумі, знижує можливість поширення консенсусної культури, загрожує стабільності у суспільстві.

Сучасна суспільно-політична практика свідчить про те, що політичні, суспільні та бізнес-конфлікти переходять у площину інформаційних протиборств, які без перебільшення можна назвати інформаційними війнами. У класичному розумінні інформаційна війна – це одна з форм інформаційного протиборства, предметніше –

[213] Панін В.Г. Різновиди та тенденції розвитку інформаційної зброї // Вісник Київського національного університету імені Т. Шевченка. – 2012. – Вип. 28. – С. 6.

комплекс заходів інформаційного тиску на масову свідомість для зміни поведінки людей і нав'язування цілей, які не відповідають їхнім інтересам, а також захист від подібних впливів.

Ідеологія інформаційних воєн ґрунтується на символічному сприйнятті світу, тому інформація володіє здатністю перетворюватись з віртуальної субстанції на матеріальну. Процес моделювання потрібної інформації (або дезінформації) для здійснення маніпулятивних технологій у свідомості суспільства перетворює її потоки на форму матеріального активного дієвого впливу при цілеспрямованому використанні за допомогою ЗМІ та ЗМК.

На сьогодні дослідження явища та феномену інформаційних війн, процесу їх зародження та розвитку, форм прояву та методів реалізації є максимально актуальними. Знання про арсенал сил, засобів інформаційної війни є основним інструментом для досягнення геополітичного домінування на міжнародній арені. Крім того, зростаюча роль інформації в світі, зумовлює актуальність забезпечення інформаційної безпеки як невід'ємної складової національної безпеки розвиненої держави.

Інформаційна війна в умовах сучасного глобалізованого світу – це основна форма протиборства між державами. У XXI ст. інформаційні війни будуть використовуватися як головний інструмент впливу на міжнародні відносини, економічну, культурну політику, духовно-культурне середовище суспільства. Захищати свої інтереси в інформаційному протиборстві у глобальному середовищі буде набагато легше державам з гармонійно розвинутим, а, тому й захищеним інформаційним суспільством, яке побудоване на засадах пріоритетності та визначної ролі індивідуальної свідомості та суспільної значимості окремої особистості.

РОЗДІЛ 3
МОДЕРНІЗАЦІЯ ТА ТРАНСФОРМАЦІЯ ФОРМ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА У СУЧАСНОМУ СВІТІ

Прогрес цивілізації заперечувати не можна:в кожній новій війні нас вбивають по-новому.

У. Роджерс

3.1. Еволюція концепцій інформаційних воєн в реаліях сучасності

Динамічні зміни сучасного світу набули глобального характеру, що процес аналізу ситуації і прогнозування не завжди здатний ефективно враховувати системні зрушення у структурі та тенденціях вибору напряму розвитку. Тенденції до уніфікації національних культур, кризовість сучасних систем управління суспільством, посилення економічного та «цифрового» розриву між країнами, недостатня впливовість міжнародних організацій із захисту інтересів у міждержавних взаємодіях в глобальному інформаційно-комунікаційному просторі актуалізують переосмислення концепцій національної безпеки держави та системи міжнародної безпеки загалом. У цих умовах, особливістю інформаційних війн сучасності є їх яскраво виражена траєкторія розвитку,активних розробок нових концепцій теоретичного і практичного застосування, а також трансформації у принципово нові множини форм.

Концептуальні зміни у військових доктринах, в багатьох галузях воєнного мистецтва з’явилися внаслідок домінування двох тенденцій, що сформувалися ще з кінця 90-х рр. XX ст.

Перша тенденція пов’язана із зростанням «інформаційної озброєності» ОВТ в системах виявлення, бойового управління, зв’язку, розвідки, комп’ютерних і космічних системах. Це призвело до удосконалення ефективності ядерних і звичайних зразків ОВТ за рахунок підвищення точності, скорочення підлітного часу, якісного зростання можливостей виявлення та супроводження цілей.

Друга тенденція наголосила на підвищеній вразливості інформаційно-комунікативних систем до зовнішнього, ворожого впливу, помилок в програмному забезпеченні, технічних збоїв і підкреслила особливу важливість та значення «людського чинника» у проведенні військових операцій проти інформаційних систем.

Таким чином, з одного боку, швидкими темпами зросла бойова ефективність ОВТ за рахунок якості інформаційного озброєння, а з

іншого – проявився рівень низької (недостатньої) захищеності цих систем від зовнішніх впливів в умовах гіперрозвитку технологій, інформаційної зброї та способів їх застосування. Сфера традиційного протиборства між наступальними й оборонними системами була перенесена у кіберпростір й перетворилася у глобальну сферу протиборства.

Особливостями цього протиборства є:

- необмеженість в часі й просторі. Область інформаційного протиборства не може бути обмежена ні окремим ТВД, ні часом, ні простором, ні системою ОВТ;
- неконтрольованість та відсутність міжнародних домовленостей з цього приводу (крім обмежень по розгортанню РЛС);
- безконечність конфігурацій. Область інформаційного протиборства не має визначених форм і способів застосування;
- необмежені можливості практичного застосування ІТ у системі стратегічних ядерних засобів, повітряно-космічної, протиповітряної оборони.

Нове розуміння інформаційної могутності держави в сучасному світі відображене множиною дефініцій терміну «війна», що з'явилися у воєнній науці «мережево-центрична», «інформаційно-центрична», «знаннє-центрична», «гібридна», «преемптивна», «консцієнтальна», «інформаційна війна стратегічних комунікацій», «інформаційно-мережева», «мережева». Основною ознакою сучасних війн стало комплексне поєднання протиборства в інформаційній сфері з веденням реальних бойових дій. Російський дослідник В. Сліпченко на основі аналізу основних форм і методів збройної боротьби, запропонував класифікацію поколінь воєн:

перше покоління – часів античних, аграрних та кочових суспільств;

друге покоління – епохи мануфактурного виробництва;

третє покоління – ранніх індустріальних суспільств;

четверте покоління – розвинутих індустріальних суспільств;

п'яте покоління – локальні конфлікти і «холодна війна» ядерної епохи;

шосте покоління – неконтактні, дистанційні війни із застосуванням високоточної зброї;

сьоме покоління – інформаційно-мережеві[214].

[214] Слипченко В. Природа войны: вчера, сегодня, завтра. – М., 2004. – С. 22.

Існує і класифікація воєн XX–XXI ст.ст., як надскладного соціально-політичного явища, які залежно від основних характеристик поділяються на:

1. Війни великих мас населення (I Світова війна) – 1914–1918 рр.
2. Війну моторів (II Світова війна) – 1939–1945 рр.
3. Війну з абсолютизацією ролі ЗЗМУ («холодна війна») – 1945–1991 рр.
4. Когнітивну війну з опорою на інформацію як основний засіб ведення бойових дій – 1992–2010 рр.
5. Війну Керованого Хаосу – сукупності роз'єднаних у просторі, але об'єднаних єдиною метою військових конфліктів – з 2010 р.[215].

Український дослідник М. Сенченко запропонував так класифікувати світові війни XX–XXI ст.ст. На його думку, «холодна війна» була Третьою Світовою (1946–1991 рр.), а з 1992 р. людство вступило у Четверту Світову. «Особливість сучасної війни в тому, що більшість людей не відчувають воєнних дій, не здогадуються, що вона перманентна і відбувається щоденно, щогодини і щохвилини. Вона невидима і її бойові дії відчуває тільки та частина людства, яка добре поінформована. Сучасна війна має три театри воєнних дій: геополітичний або фізичний, інформаційний чи психологічний, духовний або цивілізаційний»[216]. На наш погляд, досить спрощена класифікація, яка не передбачає поліваративного, комбінованого застосування усіх трьох видів театрів воєнних дій.

Р. Багіров правомірно зауважує, що під впливом сучасних політичних комунікацій відбуваються фундаментальні зрушення в соціокультурних характеристиках воєн і збройних конфліктів. «Образ війни, як запеклого збройного протиборства, тьмяніє на тлі образів нанотехнологічної, психологічної, інформаційної, консцієнтальної (війна свідомості) і преемптивної («перероблення націй») воєн. Світ вступає в новий етап боротьби як конкуренції форм організації свідомості, де предметом поразки та знищення є певні типи свідомості. Найважливішим об'єктом сучасних, і, особливо, майбутніх воєн стають менталітет націй, духовні основи армій, віра, ідеологія, історія, патріотизм, культура, національна ідентичність. Звідси зрозуміла та увага, яку розвинені держави приділяють

[215] Балуевский Ю. Глобализация и военное дело [Електронний ресурс] // Независимое военное обозрение. – 08.08.2014. – Режим доступу: http://nvo.ng.ru/concepts/2014-08-08/1_globalisation.html

[216] Сенченко М. Четверта світова. Інформаційно-психологічна війна [Електронний ресурс]. – К., 2014. – 384 с. – Режим доступу: https://lib.rus.ec/b/241595/read

питанням забезпеченню інформаційної складової військової безпеки, захисту свого способу життя»[217].

Таким чином, зміни в воєнних доктринах зумовлені появою системи нових оцінок характеру війн сучасності, що обумовлені:

- швидкими темпами росту ефективності озброєнь (передусім якості інформаційного продукту). Інформація за ефективністю свого впливу перевершила матеріальні ресурси;

- удосконаленням способів впливу на сучасні зразки озброєнь засобами обчислювальної техніки і комунікації;

- успіхами психології у сфері вивчення поведінки та маніпуляції свідомістю великих груп людей.

Слід зазначити, що існує низка підходів до трактування сутності нових концепцій війн:

Військово-прикладний зараховує інформаційну агресію до сфери військового протиборства і розглядає її у комплексному застосуванні сил і засобів інформаційної та збройної боротьби. Інформаційна складова є лише необхідним компонентом в організації та проведенні військових операцій. Передовсім, це концепції «мережево-центричної», «інформаційно-центричної», «знаннє-центричної», «гібридної» воєн та з відповідною долею умовності «преемптивної» війни.

Воєнні теоретики сучасності визначають «***мережево-центричну війну***» як *принцип* бойового застосування комплексу взаємопов'язаних і взаємодіючих підсистем, які використовують для створення нової ефективної моделі управління процесами збору, обробки та використання усіх видів інформації в кіберпросторі з метою досягнення цілей і завдань військової компанії у формі збройного, а в ідеалі, – незбройного конфлікту.

Концепція «мережево-центричної війни» була розроблена у США наприкінці 90-х рр. XX ст. Сучасні російські дослідники вважають, що вперше ідея мережево-центричного принципу війни була запропонована начальником ГШ ЗС СРСР (1977–1984) Маршалом Радянського Союзу М. Огарковим[218], але масштабне застосування інформаційних технологій у воєнній сфері розпочалося в США. Вперше термін «мережево-центричний» (NetworkCentric) був використаний віце-адміралом ВМС США А. Себровскі та

[217] Багиров Р.З. Политическая коммуникация в обеспечении военной безопасности Российской Федерации: автореф. дис. … на соискание науч. степени канд. полит. наук : спец. 23.00.02 „Политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии". – М., 2009. – С. 10.

[218] Кондратьев А. Будущее сетецентрических войн [Електронний ресурс] // Независимое военное обозрение. – 07.09.2012. – Режим доступу: http://nvo.ng.ru/concepts/2012-09-07/1_web_war.html

Дж. Гарстка у статті «Мережево-центрична війна: її походження та майбутнє», яка була опублікована в журналі «Proceedings» у січні 1998 р. Мережево-центрична війна, як цілісна концепція була дороблена та запропонована суспільству у книзі Дж. Гарстка, Д. Альбертса та Фр. Стейна[219]. Автори концепції вважали зміни, що відбуваються у сучасному світі глобальними: «Ми переживаємо епоху революції у воєнній сфері, якої не було з епохи наполеонівських війн, коли Франція вперше реалізувала концепцію масової армії»[220]. Сутність цих трансформацій, за словами начальника штабу ВМС США адмірала Дж. Джонсона, полягає у «фундаментальному зсуві від того, що ми називаємо платформо-центричною війною, до того, що ми називаємо мережево-центричною війною»[221].

Концепція «мережево-центричної війни» активно розробляється окрім США й у інших державах, а також інститутами забезпечення колективної безпеки у глобальному міжнародному середовищі. Зокрема, в НАТО – це програма «Комплексні мережеві можливості» (NATO Network Enabled Capability), Франції – «Інформаційно-центрична війна» (Guerre In focentre), Нідерландах – «Мережево-центричні операції» (Network Centric Operation), КНР – «Система бойового управління, зв'язку, обчислювальної техніки, розвідки, спостереження та вогневого ураження» (Command,Control, Communication, Computers, Intelligence, Surveillance and Kill), РФ – Концепція «Ведення бойових дій в єдиному інформаційно-комунікаційному просторі»[222].

З розвитком даної концепції поняття «мережі» набуло інтегрованого системного характеру та визначалося як сукупність єдиного комплексу комп'ютерів в просторі інформаційно-технічних і соціальних мереж, які забезпечують функціонування військового організму в системі організованих контактів і зв'язків між різними категоріями військовослужбовців: воєнно-політичним керівництвом, що приймає рішення, начальниками та підлеглими, бойовими частинами та підрозділами забезпечення, солдатами на полі бою з

[219] Alberts D.S., Garstka J.J., Stein F.P. Network Centric Warfare: Developing and Leveraging Information Superiority // CCRP Publ., 2nd Edition (Revised). Aug 1999, Second Print Feb. – 2000. – P. 284 [Електронний ресурс]. – Режим доступу: http://www.dodccrp.org/files/Alberts_NCW.pdf

[220] Цит. по: Попов И. Сетецентрическая война. Готова ли к ней Россия? // Красная звезда. – 13.09.2012 [Електронний ресурс]. – Режим доступу: http://www. redstar. ru/index.php/news-menu/ino-military-menu/usarmy/item/4659-setetsentricheskaya-voyna

[221] Там само.

[222] Кондратьев А. Исследование «сетецентрических» концепций в вооруженных силах ведущих зарубежных стран // Зарубежное военное обозрение. – 2010. – № 12. – С. 3.

урахуванням міжвидового, міжвідомчого та міжнародного (коаліційного) характеру цих військових «соціальних» мереж.

Модель «мережевої центричної війни» є системою, що складається із інформаційної, сенсорної та бойової підсистем. Причому, інформаційна підсистема – основна.

Слід наголосити, що концепція мережево-центричної війни не є новий її типом, а проголошує модерні принципи та підходи до організації та ведення бойових дій, де основним об'єктом уваги стає поняття «мережа» у вигляді глобальної інформаційної решітки (мережі, підсистеми) (ГІР) (GIG), глобальна, взаємопов'язана множина інформації, яку можна накопичувати, зберігати, розповсюджувати та управляти нею на вимогу військових, економічних і політичних суб'єктів. До складу ГІР входять власні та орендовані комунікації, комп'ютерні системи та сервіси, програмне забезпечення (з додатками), база даних, сервіси безпеки та Національні Системи Безпеки[223].

Елементами сенсорної решітки (мережі, підсистеми) є «сенсори» – засоби розвідки, а складові бойової решітки (мережі, підсистеми) виконують функції бойового придушення супротивника за допомогою засобів ураження. Ці підсистеми об'єднані єдиним органом управління. Система взаємовідношень між цими двома підсистемами досить складна й поліваріантна, але дає реальну можливість ефективного застосування бойової підсистеми при отриманні інформації одразу від «сенсорів», від наказів командування та самостійно[224].

Таким чином, головними компонентами моделі «мережевої центричної війни» є:

1. Високоефективна «інформаційна решітка» (підсистема, мережа), яка забезпечує безперебійний доступ до комплексу інформації.
2. Високоточна зброя у «бойової решітці» (підсистемі, мережі) з великою дальністю поразки цілей та високою мобільністю.
3. Інтегрована «сенсорна решітка» (підсистема, мережа), яка об'єднана у єдину мережу з «бойовою решіткою» та високоефективною «інформаційною решіткою».

«Мережево-центрична війна» повинна утворити мережу сил з високим рівнем інформованості, необмеженим доступом до

[223] DoDD 8000.01. Management of the Department of Defense Information Enterprise, dated February 10. – 2009. – P. 11. [Електронний ресурс]. – Режим доступу: http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf

[224] Попов И. Сетецентрическая война. Готова ли к ней Россия? // Красная звезда. – 13.09.2012 [Електронний ресурс]. – Режим доступу: http://www. redstar. ru/index.php/news-menu/ino-military-menu/usarmy/item/4659-setetsentricheskaya-voyna

комплексу необхідної інформації, елементи якої розміщені у різних географічних ареалах. Основними принципами її функціонування є швидкість та оперативність управління, самосинхронізації та самоорганізації структури[225].

Самоорганізація, на думку американських фахівців, це здатність військової структури до організації за принципом знизу вверх, а не змінюватися згідно вказівок згори.

Самосинхронізація визначається як процес самостійної зміни організаційної структури частин і підрозділів, форм і методів самостійно, на основі принципу доцільності, але у відповідності із стратегічними поглядами воєнно-політичного керівництва[226]. Тобто, жорстка ієрархічна система військово-адміністративного управління змінюється гнучкою мережевою: війська отримають свободу у виборі форм і методів ведення бойових дій, а організаційно-штатна структура буде постійно змінюватися, «пристосовуватися» до вимог особливостей військово-політичної обстановки[227].

У американській військовій доктрині мережевих війн підкреслено: «…Самосинхронізація – це головний елемент мережевої війни. Фактично, це і є та консолідація сил, яку ми шукаємо. Коли групи людей,окремі особистості, суспільні рухи, без попередньої домовленості (спонтанно), реагують на якусь подію. Самосинхронізація усуває всі відмінності між дійовими особами, акції стають знеособленими і спільними одночасно. Ті, хто вперше відгукується на подію – задають тон і спрямованість реакції. На цьому їх роль закінчується. Решта підхоплюють акцію в заданому ключі і створюють її інформаційне тло, залишаючись безіменними. Це дає можливість спланувати і провести акцію у зручному форматі, скоординувати її за місцем і часом, де командир вкаже кінцеву мету операції»[228].

У ідеалі, самосинхронізація повинна забезпечити можливість базових бойових підрозділів, частин в з'єднань діяти практично в автономному режимі, формулювати та вирішувати комплекс оперативно-тактичних завдань на основі всебічної інформації та розуміння задуму командира на ведення бойових дій. Результатом такої взаємодії стає:

---

[225] Попов И.М. Сетецентрическая война Пентагона [Електронний ресурс] // Независимое военное обозрение. – 2004. – № 9 (369). – Режим доступу: http://nvong.ru/concepts/2004-03-12/1_pentagonhtml

[226] Там само.

[227] Там само.

[228] Коровин В. Главная военная тайна США. Сетевые войны. – М., 2009. – С. 53.

- підвищення значення ініціативи для інтенсифікації ведення бойової операції;
- розуміння фінального замислу операції та наміру командира, що нівелює значення формального наказу;
- швидку адаптацію до змін в реальній бойовій обстановці та позбавлення від штампів та стандартів «покрокових» операцій традиційної військової стратегії[229].

Таким чином застосування концепції мережево-центричної війни буде вносити необхідні корективи в організаційно-штатну структуру, вибір форм і методів виконання бойових завдань за рішенням командира на полі бою, але у відповідності з поглядами вищестоящого командування. Це змінює традиційний погляд на централізовану ієрархічну військову структуру, яка побудована згори та об'єктивно провокує суперечності між керівниками і підлеглими[230]. Дотримання цих принципів забезпечить: досягнення інформаційної переваги завдяки знанню більшого обсягу інформації, розумінню бойової обстановки; покращення результату на основі інформаційних переваг; повний параліч системи управління супротивника[231].

Характерною умовою ефективного використання та практичної реалізації основних принципів мережево-центричної війни є наявність розвиненого демократичного суспільства та механізмів участі громадян у процесах прийняття політичних рішень. За оцінкою англійського спеціаліста з інформації С. Слейда: «можливість обмінів інформацією, передачі даних і забезпечення вільного безперешкодного потоку інформації по мережі, дає людям можливості для збору тактичної картини». У іншому випадку, С. Слейд називає досвід операції «Буря в пустелі»: «Країни, де заморожені потоки інформації, ідей і даних будуть не здатні використати ці системи…Іракська система – деревовидна, й в корені її – Саддам Хусейн. Розрив системи у будь-якому ланцюгу призведе до катастрофи, особливо якщо командир дивізії, який відрізаний від

[229] Hutchins S.G., Kleinman D.L., Hocevar S.P., Kemple W.G. and Porter G.R. Enablers of Self-synchronization for Network-Centric Operations: Designof a Complex Command and Control Experiment //Proceedings of the 6 the international command and control research and technology symposium, CCRP, Annapolis, MD, USA, 2001 [Електронний ресурс]. – Режим доступу: www.dtic.mil/cgi-bin/ GetTRDoc?AD

[230] Попов И.М. Сетецентрическая война Пентагона [Електронний ресурс] // Независимое военное обозрение. – 2004. – № 9 (369). – Режим доступу: http://nvong.ru/concepts/2004-03-12/1_pentagonhtml

[231] Cebrovski A. Network Centric Warfare and information Superiority. RUSI. Whitehall, London, 2000; Garstka J. Network Centric Warfare: An Overview of Emerging Theory// PHALANX. – Vol. 33. – No. 4. – December. – 2000.

кореня, знає, що нагородою за ініціативу йому буде куля у потилицю»[232].

Основними принципами технічної реалізації концепції мережево-центричної війни є стандартизація, уніфікація та комплексне застосування новітніх інформаційних технологій з метою створення єдиного інформаційно-комунікаційного простору. Таким чином, єдина мережа засобів розвідки, зв'язку, органів управління органічно входить в систему взаємодії з мережею засобів вогневої поразки, мережами видів забезпечення бойових дій. Зведення цих мереж в єдиний інформаційно-комунікаційний простір, який функціонує в режимі реального часу дозволяє військам діяти ефективно, швидко та досягати поставлених завдань.

Реалізація мережево-центричного принципу закріплена у програмі FCS (Future Combat System) в США, прийняття якої було критично обумовлене необхідністю створення принципово нової єдиної системи прийому, обробки, трансформації та передачі інформації через суттєве зростання її потоків. Значна кількість операційних систем і додатків, які використовувалися в системах управління були не в змозі забезпечити безперебійний обмін інформацією між засобами розвідки і пунктами управління (т.зв. «вертикальна» мережа) та унеможливлювали «горизонтальну» взаємодію між засобами розвідки й носіями зброї[233].

Основними завданнями з реорганізації ЗС США були визначені такі:

- об'єднання усіх систем управління та ведення бойових дій;
- максимальна заміна живої сили процесів управління в армійської мережі на автоматизовані й роботизовано еквіваленти;
- удосконалення техніки та озброєння для узгодження процесів їх комплексного використання в єдиній системі армійської мережі[234].

Максимально ефективна реалізація цих завдань повинна призвести до створення «адаптивної системи», яка забезпечить:

- скорочення органів і центрів передового розгортання інформаційних систем;
- кардинальне зменшення часу на збір, обробку та трансформацію розвідувальної інформації;

---

[232] Тоффлер Э. Война и антивойна. Что такое война и как с ней бороться. Как выжить на рассвете XXI века. – М., 2005. – С. 207–212, 219.

[233] Балахонцев Н. Влияние концепции „сетецентрическая война" на эффективность разведывательного обеспечения вооруженных сил США // Зарубежное военное обозрение. – 2011. – № 2. – С. 16.

[234] Кузьмин И. Future Combat System – революция или эволюция? [Електронний ресурс]. – Режим доступу: http://www. 3dnewsru/ editorial/ future_combat_system

- зниження потреби у кількості апаратури та фахівців, що дислокуються безпосередньо в зоні конфлікту.

Разом з розробкою нової моделі організації та ведення бойових дій, мережево-центричний принцип застосовується у проектуванні мережево-центричних інформаційних управляючих систем (ІУС) спеціального призначення. У основі ІУС використана також глобальна інформаційна решітка, яка забезпечує перехресну («вертикально-горизонтальну») взаємодію між вузлами прийняття рішення, виконавчими органами, постачальниками, обробниками та споживачами циркулюючої в ІУС інформації[235].

Створена мережево-центрична система управління повинна відповідати наступним вимогам:

- відповідності єдиному простору станів у системі єдиного координатно-часового поля;
- своєчасності і безперебійності надання інформації за допомогою застосування уніфікованих форматів для сумісного використання;
- адаптації усіх систем збору, обробки та розподілу інформації до параметрів нового мережевого та інформаційного простору;
- реалізації принципу «підключив і працюй», з допомогою якого відбувається удосконалення систем та засобів розвідки з мінімальними вимогами до модернізації апаратних, програмних компонентів й формування комплексної системи розвідки;
- підвищення ефективності управління інформаційними потоками та їх систематизації (тегування, сортування, каталогізація);
- синергії системи, здатності максимально швидко адаптуватися до нових умов, стійкості до можливих часткових відмов вузлів мережі та ліній зв’язку;
- постійної відкритості обміну ресурсами оптико-електронної, радіоелектронної, радіо- та радіотехнічної розвідок у масштабі часу близькому до реального для конструювання єдиної картини бою;
- побудови прямих каналів зв’язку та передачі даних від сенсорної до бойової підсистеми;
- здатності до ініціації цілей у свідомості військовослужбовця;
- децентралізований, максимально неієрархічний характер прийняття рішень.

Аналізуючи досвіду збройних конфліктів сучасності (як локальних, так і міждержавних), можна сформулювати найбільш

[235] Макаренко А. Введение в сетецентрические информационно-управляющие системы [Електронний ресурс]. – 2010. – Режим доступу: http://www.rdcn.ru/estimation/2010/03042010.shtml

вірогідний алгоритм застосування принципу «мережево-центричної війни» у два етапи.

На першому етапі ударам високоточної зброї («бойової решітки») буде передувати комплекс розвідувальних дій збору та обробки інформації («інформаційна решітка») для визначення критично важливих об'єктів держави-жертви. Класичною схемою визначення пріоритетів для здійснення інформаційних агресій слугують т.зв. «п'ять кілець» полковника Д. Уордена, що визначають послідовність нанесення ударів по військово-політичному керівництву держави, системі життєзабезпечення, об'єктам інфраструктури, населенню та лише наприкінці по збройним силам. За такою схемою була побудована стратегія операцій НАТО у Югославії в 1999 р.[236].

Одночасно, за допомогою «сенсорної» решітки буде вестися інформаційна війна: комплекс психологічних операцій, електронне придушення засобів РЕБ, розвідки, засобів зв'язку, мереж державного управління та наступальні комп'ютерні (мережеві хакерські атаки) операції.

Метою першого етапу є повна дезорганізація системи державного, економічного, військового управління, розвідки та ППО, деморалізація населення, паніка, шок і зрив військових заходів держави-жертви.

Другий етап розпочинається наземним вторгненням (своєрідним «зачищенням» місцевості) лише після досягнення цілей першого етапу. Особливістю цього етапу є максимальне уникнення прямих (класичних) бойових зіткнень з деморалізованим противником.

Головна мета реалізації мережево-центричного принципу війни – досягнення зміни правлячого режиму через зруйнування основ державної влади за допомогою масованого інформаційного впливу на морально-психологічний стан її керівництва, населення, особовий склад ЗС без знищення (в ідеалі) військового та економічного потенціалів.

Таким чином, сучасні тенденції розвитку засобів організації бойових дій в рамках концепції мережево-центричної війни, а також мережевих інформаційно-управляючих систем дають можливість зробити висновок про такі її основні характерні ознаки: відкритість, самоорганізація, незначна ієрархічність системи прийняття рішень та здатність продукувати ідеї в межах даної системи.

[236] Морозов Ю.В. Балканы сегодня и завтра: военно-политические аспекты миротворчества. – М., 2001. – 376 с.

Революційний характер та новітні технології мережево-центричної війни сприяли її трансформації у нові форми ефективного використання та застосування. Наступним періодом в еволюційному розвитку військової теорії стала поява концепцій «інформаційно-центричної» та «знаннє-центричної» воєн.

Усвідомлення надважливого значення інформації у сучасному глобалізованому інформаційному суспільстві, кореляція інформаційних і мережевих технологій створили передумови для переходу на наступну стадію еволюційного розвитку військової теорії – виникнення концепції інформаційно-центричних війн. «Крихітна частинка інформації може дати колосальну стратегічну або тактичну перевагу…нестача цієї частинки може призвести до катастрофи…Комп'ютерні програми змінюють баланс воєнних сил у всьому світі…»[237].

«Інформаційно-центрична війна» – це принцип ведення бойових дій з метою досягнення інформаційної переваги над супротивником на основі комплексу високотехнологічних інформаційних систем збору, обробки, моделювання, візуалізації даних та підтримки прийняття рішень в режимі реального часу.

На думку багатьох воєнних експертів, ця концепція вже реалізується у військових конфліктах сучасності.

Прикладом реалізації завдань інформаційно-центричної війни можна вважати російську стратегію так званого «рефлексивного управління». Як пише американський аналітик Т. Томас, його зміст полягає в тому, щоб переконати противника прийняти добровільно необхідне ініціатору рішення, тобто настільки добре знати його поведінку, щоб спровокувати на будь-яку потрібну дію[238].

Наступним логічним кроком розвитку теорії інформаційних воєн стала концепція «знаннє-центричної війни», яку зараз активно розробляють у науковому та воєнно-науковому середовищі. Блискуче наукове передбачення Е. Тофлера та Х. Тофлер про новітню воєнну «стратегію знань», визначення необхідних компонентів «війни знань», досліджень складної системи їхніх взаємовідношень та побудови «моделі знань» розширює стратегічні можливості використання цього перспективного напрямку розвитку воєнного мистецтва[239].

---

[237] Тоффлер Э. Война и антивойна. Что такое война и как с ней бороться. Как выжить на рассвете XXI века. – М., 2005. – С. 223.

[238] Рудницька У.І. Інформаційні війни як засіб геополітичного протистояння // Гуманітарний журнал. – 2015. – №1-2. зима-весна. – С. 135.

[239] Там само. – С. 207–262.

«Знаннє-центрична війна» – це принцип ведення бойових дій, який на основі комплексу інформації використовує інноваційні методики прогнозування розвитку військово-політичної обстановки та характеру ведення бойових дій за допомогою «штучного інтелекту» та новітніх технологій отримання знань.

Головним функціональним завданням «знаннє-центричної війни» є не передача інформації, а передача знань. Сутність цієї концепції полягає в тому, що комплекс даних про оперативну обстановку, який був раніше доступний лише командуванню, буде переданий кожному солдату майбутнього, щоб забезпечити реалізацію принципу децентралізації управління силами та засобами. Слід зазначити, що цей крок, хоча й логічний, але зовсім не обов'язковий. Враховуючи динамічний розвиток інформаційно-комунікативних технологій, головним завданням майбутньої «знаннє-центричної війни» буде не передача знань своїм військам, а знищення та деформація системи знань супротивника або комбіноване виконання цих двох завдань[240]. Як слушно зазначають науковці «Можна розповсюджувати і хибну інформацію, дезінформацію, правду (коли вона корисна), пропаганду – знання разом з антизнанням»[241].

Формами прояву спроб деформації системи знань конкурентів і супротивників на сучасному етапі слід вважати «експорт мізків» із країн-об'єктів і знищення інтелектуального потенціалу держави, а методом, що був використаний для запобігання цій ситуації – створення умов, які ускладнять такі «міграції знань». Наприклад, заборона еміграції російських вчених в Іран і Північну Корею на початку 2000-их рр. для надання допомоги цим країнам у створенні ядерної зброї.

До військово-прикладного підходу, на нашу думку, слід зарахувати й поняття ***«гібридна війна»***.

Історія розвитку людства свідчить про те, що гібридна війна не є ексклюзивним явищем і феноменом епохи модерну та постмодерну. Історія війн і військового мистецтва знає багато прикладів ведення асиметричних воєн із використанням нелінійної тактики та нерегулярних збройних формувань, комбінацій інформаційно-психологічного, економічного та військового протиборства, які є аналогами сучасної гібридної війни. Аспекти гібридної форми

[240] Буренок В.М. Курс – на сетецентрическую систему вооружения [Електронний ресурс]. – ВКО. – 2009. – № 5. – Режим доступу: www. vko.ru/koncepcii/kurs-na-setectntrscyeskuyu-sistemu-vooruzhenia# d-comments

[241] Тоффлер Э. Война и антивойна. Что такое война и как с ней бороться. Как выжить на рассвете XXI века. – М., 2005. – С. 221.

протистояння можна знайти у Пелопоннеській війні, де римськими полководцями були ефективно використані нерегулярні варварські формування. Інструментарій асиметричних дій ми бачимо у війні за незалежність США, американо-в'єтнамській війні, концепції «затяжної революційної війни» Мао Цзедуна, боротьбі Хезболла проти ізраїльських сил оборони і безпеки, чеченських бойових угрупувань проти російської армії. Принципи гібридної війни були активно застосовані Росією у війні проти Грузії в 2008 р. У цьому локальному конфлікті Росії вдалося відносно вдало поєднати безпосередню військовий компонент з використанням в комплексі забезпечення бойових дій інформаційно-психологічного, економічного складників та елементів кібервійни. Хрестоматійним є приклад використання принципів гібридної війни у конфлікті між Хезболлою та Ізраїлем. Починаючи з 2006 р. арабські терористи діють в рамках нової моделі бойових дій, яка поєднує регулярні та нерегулярні форми боротьби. Поряд з використанням регулярних військових терористичних підрозділів та традиційних озброєнь (протитанкові і протиповітряні ракети, безпілотні літальні апарати), Хезболла активно впроваджує тактику точкових індивідуальних терористичних актів за допомогою саморобних вибухових пристроїв.

Отже, теорію гібридних війн можна вважати моделлю воєнної стратегії епохи постмодерну.

У сучасному науковому дискурсі не існує однозначного визначення дефініції «гібридна війна». Більш того, існує суперечливі думки про пріоритетність застосування цього терміну. Український дослідник А.С. Дорошкевич[242] стверджує, що поняття «гібридна війна» було введено в науковий обіг американським дослідником М. Маклюеном, який детально аналізував роль інформації в сучасному світі. Учений дійшов парадоксального висновку, що засоби комунікації є новими «природними ресурсами» які збільшують багатство суспільства. Він аргументував цей висновок наступною тезою: «Істинно тотальна війна — це війна за допомогою інформації». Також на основі ґрунтовних досліджень він довів, що сучасні війни зазвичай ведуться в інформаційному просторі та за допомогою інформаційних видів озброєнь. Вперше широко розтиражованим було згадування цього терміну у промові генерал-

[242] Дорошкевич А.С. Гібридна війна в інформаційному суспільстві // Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». – 2015. – № 2 (25). – С. 23.

лейтенанта Дж. Меттіса 8 вересня 2005 р.[243]. Але більшість дослідників сходяться в тому, що вперше використав цей термін Ф. Хофман, автор книги «Конфлікт в XXI столітті. Повстання гібридних воєн». Він визначав цей тип війн, як принцип комбінованого використання ворогом дозволеної зброї, партизанської війни, тероризму, злочинної поведінки та пропаганди для досягнення політичних цілей[244]. В досліджені «Hybrid vs compound war» він схарактеризував цей тип війни як «повний арсенал різних видів бойових дій, враховуючи конвенціональні можливості, іррегулярну тактику і формування, терористичні акти, що містять насилля та кримінальні безлади»[245].

Гібридна війна насамперед, передбачала використання принципу асиметрії при веденні бойових дій, що дозволяє нівелювати перевагу противника у збройній боротьбі. Дослідник з питань національної безпеки Ф. Хофман звернув увагу на те, що: «Ця теорія готова подолати вузький традиціоналістський підхід до розуміння військових дій у XXI столітті. Підготовка до епохи асиметричних війн – не дурниця, не стратегічний чи імперський вибір, це просто необхідність в епоху постійних нелінійних конфліктів»[246].

Асиметричні воєнні дії набули особливого значення після терактів «Аль-Каїди» 11 вересня 2001 р. у США. Терористичні атаки у Нью-Йорку і Вашингтоні підтвердили факт того, що традиційні форми та методи ведення бойових дій не здатні протистояти новим викликам. Для ефективної нейтралізації «нового» противника необхідно використовувати особливості діяльності спецслужб, нові засоби технічного контролю та спостереження.

Характер сучасного гібридного політичного насилля Ф. Хофман розкрив за допомогою такого визначення: «Гібридна війна – це суміш летальності міждержавного конфлікту з фанатизмом і люттю партизанської війни. У таких конфліктах держави, або підтримані ними бойовики та терористи, будуть використовувати переваги сучасного озброєння, систем зв'язку, кіберзлочинності, інформаційної пропаганди і масового насилля проти цивільних»[247].

---

[243] Там само.

[244] Цит. по Гарбуз Л. Неужели Европа еще представляет, что есть возможность отстранения от драматических событий в Украине? [Електронний ресурс] // День. – 06.05.2014. – Режим доступу: http:// m.day.kiev.ua/ ru/article/mirovye-diskussii/gibridnaya-voyna-putina

[245] Hoffman F. G. Hybrid vs. compound war // Armed Forces Journal, Oct. 2009.

[246] Хоффман Ф. Гибридные угрозы: переосмысление изменяющегося характера современных конфликтов // Геополитика. Информационно-аналитическое издание. Тема выпуска: Война. – Вып. XXI. – М., 2013. – С. 49.

[247] Hoffman F. Further Thoughts on Hybrid Threats [Electronic resource] / F. Hoffman // Small Wars Journal. – Access mode: www.smallwarsjournal.com/blog/2009/03/further-thoughts-onhybrid-thr/. (Accessed 20 Febrary 2015).

Також, на думку Ф. Хофмана, гібридні війни є формою використання мультивузлових суб'єктів, тобто здійснюватися, державними і недержавними акторами[248].

Ф. Хофман вважає, що зміст гібридних воєн будуть визначати комплекс причин: «замість супротивників, які застосовують фундаментально різні підходи до ведення військових дій, нам слід очікувати таких, які будуть використовувати усі форми війни і, можливо, одночасно. Такі змішані загрози називають гібридними загрозами. Комбіноване застосування різнорідних засобів супротивниками використовують для отримання асиметричної переваги»[249]. До них зараховують загрози:

- гібридного співіснування форм традиційних і нерегулярних тактик;
- децентралізованого планування та виконання;
- участі держав (союзу держав) і недержавних акторів з одночасним використання простих і складних технологій інноваційного розвитку;
- комплексного використання комбатантів і нерегулярних формувань;
- заміни стандартних військових формувань нерегулярними «добровольчими» загонами;
- застосування терору та кримінального безладу;
- симбіозу державного конфлікту з фанатичним затяжним характером нерегулярної війни;
- комбінованого використання ОВТ сучасного військового потенціалу та саморобних вибухових і вогнепальних засобів;
- інформаційних, фінансових, економічних кібервійн[250].

Дослідник стверджує, що гібридна війна містить п'ять елементів: модальність проти структури, одночасність, злиття, комплексність, злочинність[251].

На думку генерала Франка ван Каппена, «…гібридна війна – це мішанина класичного ведення війни з використанням нерегулярних збройних формувань. Держава, яка веде гібридну війну, укладає оборудку з недержавними виконавцями – бойовиками, групами місцевого населення, організаціями, зв'язок із якими формально повністю заперечується. Ці виконавці можуть робити такі речі, які

[248] Хоффман Ф. Гибридные угрозы: переосмысление изменяющегося характера современных конфликтов // Геополитика. Информационно-аналитическое издание. Тема выпуска: Война. – Вып. XXI. – М. – С. 56.
[249] Там само – С. 45.
[250] Там само. – С. 55–56.
[251] Hoffman F. G. Future Threats and Strategic Thinking / Hoffman F. G. // Infinity Journal, No Fall 2011. – P. 17.

сама держава робити не може, тому що будь-яка держава зобов'язана дотримуватися Женевської конвенції та Гаазької конвенції про закони сухопутної війни, домовленості з іншими країнами. Всю брудну роботу можна перекласти на плечі недержавних формувань»[252].

Американський дослідник Дж. Мак Куєн визначає гібридну війну як комплексне застосування традиційних і асиметричних форм насилля з одночасним використанням протестного потенціалу місцевого населення до участі у конфлікті і маніпулюванням думкою міжнародної спільноти, або нівелюванням її впливу. Ця форма протистояння розглядається як один з із сучасних проявів асиметричної війни у трьох вимірах: серед громадян зони конфлікту; серед громадян агресора; серед міжнародної спільноти[253].

Американський аналітик Р. Уілкі робить наголос у визначенні гібридної війни на використання власне недержавних, нелегітимних акторів та пропонує розглядати війну як конфлікт під час якого держава, або недержавне угрупування використовує терористичне насилля, нерегулярних військових, невибіркове насилля, злочинців і найманців, з метою дестабілізації політико-економічного статусу опонента[254].

Колишній начальник управління розвідки військового штабу ЄС, екс-начальник військової розвідки сил оборони Фінляндії адмірал Г. Алафузов сутністю гібридної війни вважає комплексне використання воєнних і невоєнних методів ведення війни. На його думку «невоєнні способи доповнюються воєнними мірами прихованого характеру, включаючи дії сил спеціальних операцій, а також економічними санкціями, використанням протестного потенціалу населення. Важливе місце відводиться заходам інформаційного протиборства, які здатні в деяких випадках навіть змінити головний геополітичний потенціал держави – національний менталітет, культуру, моральний стан людей»[255].

Власна характеристика нового виду асиметричного протистояння належить високопосадовцю ізраїльських спецслужб Й. Купервассеру. У праці «10 уроків для реформи ізраїльської розвідки» (2007) він стверджував, що принаймні з 1982 протистояння з

[252] Радіо Свобода. Путін веде в Україні гібридну війну – генерал Каппен [Електронний ресурс]. – Режим доступу: ww.radiosvoboda.org/ content/ article/ 25363591.html

[253] McCuen J. Hybrid Wars / John McCuen // Military rewiew. – 2008. – March-April. – P. 108.

[254] Wilkie R. Hybrid Warfare. Something Old, Not Something New / Robert Wilkie // Air & Space Power Journal. – 2009. – Vol. 23, № 4. – P. 4.

[255] Экс-глава военной разведки ЄС о влиянии гибридных угроз на оценку ситуации в мире // Зарубежное военное обозрение. – 2018. – № 12. – С. 92.

арабськими терористичними угрупуваннями стає майже безперервним, з короткотривалими високоінтенсивними діями. При цьому противник намагається діяти малими формуваннями, часто без визначення військової форми одягу та атрибутики. Бойові дії відбувається в багатовимірному просторі. Поняття захисту кордонів набуває умовного характеру, оскільки точкове проникнення терористів, які проходять через кордони або є громадянами тієї країни, де відбуваються дії набуває масового характеру[256].

М. Бонд зазначила, що майбутні війни будуть мати вид гібридної війни. Водночас вона визначає гібридну війну як парадигму операцій по стабілізації в несформованих державах[257].

В. Мурей та П. Менсур визначають гібридну війну як конфлікт, де беруть участь звичайні збройні сили та іррегулярні формування (партизанські, повстанські, терористичні), які включають як державних, так і недержавних акторів та діють синхронно, з метою досягнення спільної політичної мети[258].

Цікаве визначення гібридної війни належить Р. Ньювсону. Цей вид протистояння він визначив як комбінація конвенційних, іррегулярних та асиметричних засобів, що включають постійну маніпуляцію політичним та ідеологічним конфліктом, а також залучення сил спеціальних операцій та конвенційних збройних сил, агентів розвідки, політичних провокаторів, представників медіа, економічний шантаж; кібератаки; проксі-сервери і сурогати, пара-військові, терористичні і кримінальні елементи[259].

Ґрунтовно розглядаються питання гібридної війни у сучасній вітчизняній науковій думці. Наприклад, М. Требін визначає гібридну війну, як: «комбінацію з партизанської і громадянської війни, заколоту і тероризму, головними дійовими особами яких є нерегулярні військові формування, бойовики, кримінальні банди, міжнародні терористичні мережі, спецслужби іноземних держав, приватні військові компанії, військові контингенти міжнародних організацій»[260].

---

[256] Kuperwasser, Yosef. Lessons from Israel's Intelligence Reforms. The Saban Center for Middle East Policy at the Brookings Institute, 2007. – ANALYSIS PAPER. – № 14. – P. 7–9.

[257] Bond, Margaret. Hybrid War: A New Paradigm for Stability Operations in Failing States, Carlisle arracks, PA: U.S. Army War College, March 30, 2007.

[258] Williamson, Murray, and Peter Mansoor. Hybrid warfare: fighting complex opponents from the ancient world to the present. Cambridge University Press, 2012. – P. 3.

[259] Newson, Robert A. Counter-Unconventional Warfare Is the Way of the Future. How Can We Get There? In Janine Davidson Blogspot: Defense in Depth. October 23, 2014. http://blogs.cfr.org/davidson/2014/10/23/counterunconventional-warfare-is-the-way-of-the-future-how-can-we-get-there/

[260] Требін М. Феномен «гібридної» війни // Гілея. – 2014. – Випуск 87 (8). – С. 366.

Характерними рисами цих суб'єктів війни є недисциплінованість, прагнення до збагачення, індивідуалізм, зневага до правил війни і використання насилля проти цивільних громадян. Прагматичне використання цих біосоціальних якостей людини дозволяє державам зняти з себе відповідальність за військове втручання, порушення норм міжнародного права і підтримку нерегулярних військових формувань. Аналогічні термінологічні дефініції дають експерти українського центру суспільних відносин. Вони визначають гібридну війну, як сукупність підготовлених і оперативно реалізованих державою дій військового, дипломатичного, інформаційного, економічного характеру, спрямованих на досягнення стратегічних цілей[261]. Отже, акценти робляться на досягнення перемоги не в формах збройного протистояння, а в дипломатичному, психологічно-інформаційному та економічному вимірах.

У цих же змістових характеристиках визначають гібридну війну В. Телелим, Д. Музиченко та Ю. Пунда. Вони трактують її як «загострення протиріч між державами, які вирішуються не лише військовими методами боротьби, а й застосуванням широкого спектру економічних, інформаційних та політичних методів боротьби»[262]. Отже, утилітарно-прагматичне використання переваг гібридної війни надає державі-агресору комплекс преференцій, які дозволяють йому уникнути відповідальності за розв'язання збройного конфлікту, військові злочини, порушення міжнародного права та знаходити інформаційні приводи для виправдання власної агресії.

Аналіз наявної інформації дає можливість визначити такі характерні риси цього принципу ведення бойових дій, насамперед:

- відсутність юридично визначеного стану війни на тлі активного ведення бойових дій сторонами конфлікту;
- інтуїтивне (підсвідоме) використання «мережево-центричного» принципу організації бойових дій регулярними військовими формуваннями;
- інформаційна війна як між учасниками конфлікту, так і в межах глобального інформаційного простору з використанням множини форм і методів із залученням потенцій та ресурсів інформаційно-комунікаційної інфраструктури сторін – учасників конфлікту;
- використання методів економічної війни (блокади, санкцій);

[261] Гібридна війна: як це працює [електронний ресурс]. – Режим доступу : www.csr.org. ua/index.php/uk/aktsenti-dnya/318-gibridna-vijna-yak-tse-ratsyue. (дата звернення 20.02.2015) – Назва з екрану.
[262] Телелим В. Планування сил для виконання бойових завдань у «гібридній війні» // Наука і оборона. – 2014. – № 3. – С. 30.

- активна дипломатична пропаганда дій держави-агресора у міжнародних інституціях;

- підтримка сторонами конфлікту радикальних незаконних збройних формувань озброєнням і військовою технікою з метою «утилізації» застарілих а також бойовим випробуванням новітніх зразків ОВТ;

- створення іміджів «борців зі злочинною владою (хунтою, диктатурою, сепаратистами, бандитами, карателями та інш.)» усім учасникам конфлікту;

- проголошення «миротворчих ініціатив» з одночасною активізацією бойових дій з метою «глорифікації» чи «демонізації» сторін учасників конфлікту;

- примусове нав'язування власного інформаційного продукту місцевому населенню за допомогою блокування ЗМІ супротивника на захоплених територіях.

Незважаючи на визначне значення в гібридної війні інформаційного складника було б помилковим зводити гібридну війну тільки до цього компонента, можливостей оперувати гігантськими масивами даних, здатністю побудови безструктурних суб'єктів. Гібридна війна має свої особливості, а саме: різнорівневий цивілізаційний розвиток супротивників, де використовуються не тільки і не стільки воєнні засоби, а й легальні інструменти управління, демократії, культури, ЗМІ, освіти, що не відокремлює їх від повсякденного життя і робить ефективним засобом маніпулювання. Друга особливість – тотальність. Гібридна війна ведеться і проти ворогів, і проти друзів. Руйнівні наслідки впливу на мислення та поведінку сприяють тому, що люди самі руйнують свою державу та владу всередині. І нарешті, гібридна війна є комплексним явищем, яке враховує в організації бойових і не бойових дій розвиток цивілізації, демократію, особисті свободи, світогляд та спосіб життя людей.

Полем застосування інструментів гібридної/асиметричної війни є: населення зони конфлікту, тилове населення, міжнародна спільнота. До форм ведення такого виду війни слід віднести: 1) громадські заворушення – акції громадської непокори, демонстрації, блокування, вуличні зіткнення; 2) повстання – відкритий військовий виступ проти офіційної влади; 3) партизанський рух – прихований збройний опір офіційній владі; 4) тероризм – організація та здійснення гучних вбивств, підривання транспортних засобів, споруд, місць масових соціальних контактів; 5) громадянська війна – воєнні

дії між прихильниками різних ідеологічних, територіальних або національних груп у межах однієї держави[263]. Здобутком XX ст. стало виникнення нового формату інформаційно-комунікаційних протистоянь, який дістав назву кібервійна. Останню розуміють як боротьбу сторін на рівні програмного забезпечення шляхом видобування закритої інформації та виведення з ладу програмно-апаратних засобів супротивника з метою здобуття суттєвих переваг в економічних, політичних та воєнних протистояннях[264]. Головними дійовими особами в такій війні є спеціальні фахівці: хакери (ті, що видобувають інформацію) та кракери (ті, що псують програмноапаратні засоби).

Таким чином, на нашу думку, ***гібридна війна*** – це форма збройного конфлікту, яка передбачає використання як традиційних засобів збройної боротьби так і змішаних форм тактичного застосування регулярних та нерегулярних військових формувань в умовах неоголошеного військового (надзвичайного) стану на обмеженій території на тлі інтенсифікації інформаційної війни у глобальному інформаційному просторі, економічної війни в системі світової економічно-торгової інтеграції, дипломатичної війни, як засобу тиску на супротивника через глобальні міжнародні інституції сторонами конфлікту і «державами-спонсорами», або коаліціями держав, які мають геополітичні інтереси в регіоні конфлікту[265].

Концепція ***«преемптивної війни»*** знаходиться на зрізі військово-прикладного та психологічного підходу. Але, визначальне значення збройного компонента у ході ведення бойових дій,дає можливість зарахувати її передовсім до військово-прикладного підходу. Слід підкреслити і її стійкий логічний та діалектичний зв'язок з концепціями «мережево-центричної» і «гібридної» воєн. Концепція преемптивної війни є органічною синтезованою формою ведення бойових дій сучасності на основі розвитку концепцій «мережево-центричної», «консцієнтальної» та «гібридної» воєн.

Поняття «преемптивна війна», як термін в офіційному документі, вперше був застосований в Національной стратегії

[263] Кравченко В.Ю. Теорія «Гібридної війни»: український вимір // Вісник Дніпропетровського університету. – 2015. – № 2. – С. 139–148.

[264] Зеленін В.В. По той бік правди: нейролінгвістичне програмування як зброя інформаційно-пропагандиської війни [Текст]. – Вінниця, 2014. – С. 38.

[265] Гула Р.В., Передерій І.Г. Концепт гібридної війни Ф. Хоффмана як модель форми асиметричного протистояння в епоху постмодерну // Тези 71-ої наукової конференції професорів, викладачів, наукових працівників. Аспіратнів та студентів університету. Том 2. (Полтава, 22 квітня – 17 травня 2019 р.). – Полтава, 2019. – С. 252–254.

забезпечення безпеки США (National Security Strategy of the United States) у 2002 р.

Концепцію преемптивної війни визначає сутність терміну «преемпція» – сукупності системних превентивних силових дій та масованого інформаційного впливу на правлячий політичний режиму держави-парії (терористичної держави, посібника міжнародних терористичних організацій), як носія потенційної загрози державного та недержавного тероризму. Здійснюється з метою зміни політичного керівництва, знищення національного суверенітету, побудови нової «правильної» нації. Алгоритм реалізації даної концепції передбачає насамперед збройну агресію з метою зміни політичного режиму та захоплення його ресурсної бази для створенням системи тотального контролю над суспільством, переформатування особистісної свідомості за допомогою інформаційно-психологічних технологій в своєрідний кібер-продукт з мінімумом соціальних потреб. «Творення нації» передбачає знищення решток «невдалих» державно-політичних «проектів», здійснення процесу створення нових «модернових» націй та націй-держав за допомогою «демократичних» виборів і формування нового «елітарного» прошарку. Цей процес супроводжується масованим інформаційним впливом в межах глобального інформаційного простору[266].

Спільними з «гібридною» війною рисами є такі:

- ведення за допомогою не лише збройних сил, але й найманців, бандитів, приватних військових компаній на яких не розповсюджуються дія норм міжнародного гуманітарного права (МГП);
- неможливість застосування поняття «військова агресія» до держав-агресорів, оскільки вони формально не приймають участь у них;
- незаконні збройні формування (НЗФ) застосовують тактичні прийоми у бойових діях, що заборонені міжнародними нормативно-правовими документами (захоплення заручників, загрози використання зброї масового ураження у місцях скупчення цивільного населення та ін.);
- внаслідок специфіки формування та функціонування НЗФ не підпадають під дію громадського цивільного контролю, що не дає

[266] Крупнов Ю. Преэмптивная война [Електронний ресурс]. – Режим доступу: http: www. kroupnov. ru /5/30 1shtml; Комлева Н.А. Преэмптивная война как технология ресурсного передела мира [Електронний ресурс]. – Режим доступу: komleva@yandex.ru

можливості об'єктивно оцінити їх рівень забезпечення, матеріальних і людських втрат[267];

- використання інформаційного впливу та механізмів тиску державою-агресором на міжнародній арені із застосуванням форм економічної та політичної блокади.

Відмінністю преемптивної війни від гібридної є те, що гібридна війна визначає принципи ведення збройної боротьби безпосередньо у ході ведення бойових дій. Преемптивна війна формує сукупність підготовчих, превентивних дій, які забезпечують механізм і форми збройного застосування та комплекс заходів, які спрямовані на закріплення результатів перемоги у війні.

На підготовчому етапі визначається держава – об'єкт агресії з одночасним створенням іміджу «ізгою», «терористичної» держави, «фашистського» («нацистського») режиму за допомогою тотального інформаційного тиску – потужного цільового спрямування інформаційних ресурсів на об'єкт впливу для досягнення системних змін та руйнування ціннісно-інформаційних констант. Відбуваються зрушення в традиційних інформаційних наративах – суб'єктивно-ідеалістичних структурованих описах об'єктивної дійсності через вплив заданого обсягу інформації у жорстко окреслених рамках інтерпретацій. Наратив, як інституціонально-системне структурування дійсності на цьому етапі характеризується неоднозначністю отриманого комплексу суперечливої інформації та вступає у антогоністичну суперечність із встановленою системою ціннісних констант[268].

На першому етапі відбувається створення в соціумі держави-об'єкта опозиційного до влади прошарку, через ескалацію національних, релігійних і соціальних протиріч, який виявляє свій «політичний спротив» через мирні «демократичні» протестні акції. Політичний спротив – це ненасильницька боротьба (протест, втручання або відмова від співпраці), яку ведуть демонстративно й активно для досягнення політичних цілей[269]. Головною метою використання інформаційних технологій на цьому етапі є надання через світові ЗМІ, ЗМК чи дипломатичні канали «запрограмованому»

[267] Кочнев И.П. Концепция преэмптивной войны и пограничная безопасность государства // XII Всероссийское совещание по проблемам управления ВСПУ-2014, Москва, 16 – 19 июня 2014. – С. 6215.

[268] Почепцов Г. Революция. com. Основы протестной инженерии [Електронний ресурс]. – Москва, 2005. – Режим доступу: http://www.litres.ru/pages/biblio_book/?art=3006095

[269] Шарп Дж. Від диктатури до демократії: концептуальні засади здобуття свободи / Пер. з англ. ін-т ім. Альберта Ейнштейна. − Львів, 2004. – 83 с.

натовпу іміджу «авангарду народу, який вийшов на сцену історії з метою зміни режиму»[270].

На другому етапі мирні демонстрації перетворюються на збройне зіткнення опозиції із владою. Класик політтехнологій «кольорових революцій» Дж. Шарп, так характеризує цей розвиток подій «Реагуючи на жорстокість, тортури, зникнення та вбивства, люди вважають насильство єдиним засобом повалення диктатури. Розлючені жертви іноді об'єднувалися для боротьби з жорстокими диктаторами, вдаючись до будь-яких можливих насильницьких і військових засобів, не зважаючи на очевидну нерівність сил»[271]. В цей період відбувається захоплення складів зі зброєю, нейтралізація військових і правоохоронних формувань, провокування міжнаціональних зіткнень та передислокація НЗФ через державний кордон з метою загострення напруженості та безладу.

Третій етап характеризується активізацією діяльності НЗФ у формі бойових зіткнень з регулярними військами, знищенням місцевих мешканців, які нелояльні до «повстанців», криміналізацією та маргіналізацією суспільного життя. Для підтримки «повстанців» через державний кордон зорганізується постачання зброї, видів бойового, тилового, технічного та медичного забезпечення.

На заключному етапі агресії відбувається (як правило за допомогою міжнародних організацій або при ігноруванні цих інституцій) зміна законного уряду на «демократичний» («легітимний», «антифашистський», «народної довіри», «національної згоди»). Держава-об'єкт позбавляється права на володіння власними природними ресурсами, втрачає суверенітет і статус самостійного суб'єкта міжнародних відносин.

Таким чином, на нашу думку, ***преемптивна війна*** – це комплексна форма збройного конфлікту, компонентами якої є цілеспрямована інформаційна війна, мережево-центричний принцип ведення бойових дій, «гібридний» характер застосування регулярних і нерегулярних формувань з метою досягнення політичних цілей та трансгуманітарна перебудова в формах консцієнтальної війни індивідуальної та суспільної свідомості, перекодування національних ментальних рис (національної ідентичності) переможеного народу.

---

[270] Ремизов М. Неоколониальная революция: осмысление вызова // Стратегический журнал. – 2005. – № 1. – С. 85.

[271] Шарп Дж. Від диктатури до демократії: концептуальні засади здобуття свободи / Пер. з англ. ін-т ім. Альберта Ейнштейна. — Львів, 2004. – 83 с.

На нашу думку, до військово-прикладного підходу слід зарахувати й так звану ***«доктрину Герасимова»,*** в якій викладені основні константи воєнної політики Російської Федерації**.** У сучасних умовах ця доктрина акумулювала традиції російської військової історії, світовий досвід воєн XX –XXI ст. і новітні теоретичні дослідження концепцій війни.

Датою офіційного проголошення «доктрини Герасимова» слід вважати виступ її автора – начальника Генерального штабу ЗС РФ генерала армії В. Герасимова – на засіданні Академії воєнних наук (АВН) у січні 2013 р. Слід звернути увагу на дату першого офіційного проголошення цілей доктрини – кінець січня 2013 р., тобто до подій у Криму залишався ще рік і розвиток внутрішньо-політичної ситуації в Україні не передбачав ескалації соціальної напруги, якою характеризувалися драматичні події на Майдані в листопаді 2013 – лютому 2014 рр. Разом із тим, характер викладених теоретичних положень не залишає сумнівів у передбаченні перспектив застосування цієї доктрини в Україні, що підтверджується подальшою логікою розвитку та трансформації воєнно-політичної обстановки, починаючи з лютого 2014 р.

Друкована версія доповіді В. Герасимова була оприлюднена в лютому 2013 р. на сторінках видання «Воєнно-промисловий кур'єр»[272]. Характерно, що повний зміст доповіді В. Герасимова в АВН відсутній, але навіть аналіз його скороченого викладу на сторінках указаного друкованого джерела дає достатньо матеріалу для концептуальних висновків.

На нашу думку, «доктрина Герасимова», насамперед, може бути визначена як:

- *система поглядів політичного керівництва РФ* на сутність і перспективи розвитку міждержавного конфлікту для досягнення потрібних геополітичних, стратегічних результатів;
- *воєнно-політична теорія*, яка систематизує основи воєнної науки з урахуванням положень філософської парадигми постмодерну;
- *керівний теоретичний воєнно-політичний принцип*, вихідним началом якого є поєднання в єдину систему нетрадиційних (нелінійних) військових дій із політичними, економічними, інформаційними, гуманітарними та іншими невійськовими заходами.

Науково-теоретичними та світоглядними основами «доктрини» є:

[272] Герасимов В.В. Ценность науки в предвидении // Военно-промышленный курьер. – 2013, 27 февраля. – № 8 (476). – С. 1–2.

1. *Дискретність ідеї війни*, яка закладена в романі Л. Толстого «Війна й мир», тобто використання соціальних протестів населення проти ворога, оперування зміною настроїв суспільства, акцентування уваги населення на ворожому характері політичної влади країни-супротивника[273].

2. *Концепція «необмеженої війни»* Національно-визвольної армії Китаю, основним змістом якої є гасло «кращий спосіб – не воювати, а контролювати», тобто використання проросійськи налаштованої частини суспільства, політичних сил, які поділяють ідеї «Русского мира», з метою впливу на воєнно-політичне керівництво країни-супротивника та застосування механізму економічного тиску російського бізнесу на політичні рішення влади держави-супротивника[274].

3. *Доктрина М.В. Огаркова,* використана В. Герасимовим в частині пріоритетності бойового застосування мобільних бойових груп і відмови від масштабних фронтальних бойових зіткнень оперативних об'єднань. Звідси – підвищення ролі міжвидових мобільних угрупувань військ. Більшість ідей М. Огаркова знайшли розвиток у концепції мережево-центричної війни[275].

4. *Концепція «трьох кварталів»* ізраїльського полемолога М. ван Кревельда. У межах «доктрини Герасимова» вона передбачала можливість використання в бойових діях політично мотивованих кримінальних і маргінальних елементів соціуму[276]. Крім того, за поглядами полемолога, солдат майбутнього повинен бути готовим до виконання трьох основних завдань: ведення загальновійськового бою, поліцейських функцій і виконання гуманітарної місії, що (за винятком загальновійськового бою) було застосовано ЗС РФ під час анексії Криму в лютому 2014 р.

5. *Теорія гібридної війни.*

У доповіді Командування спеціальних операцій США наголошується, що у конфлікті з Україною «Росія використовує такі елементи гібридної війни, як участь регулярних військових формувань, економічне залякування України, демонстрація сили на

[273] Narr S.J. Expanding Tolstoy and Shrinking Dostoyevsky // Military Review. – 2017. – September-October (т. 97, № 5). – P. 39.

[274] Гула Р.В. «Русский мир» – концепція імперського фантому в геополітичній реальності // Науковий семінар «Інформаційна агресія Російської Федерації проти України»: тези доповідей, 25 жовтня 2018 року. – Х., 2018. – С. 31–33; Коттер Брайн П. Русский мир // Concordiam. Журнал по проблемам безопасности и обороны в Европе. – 2016. – Специальный выпуск: «Противодействие российской пропаганде». – С. 31–35.

[275] Garstka J. Network Centric Warfare: An Overview of Emerging Theory / J. Garstka. – PHALANX. – December. – 2000. – № 4. – P. 28–33.

[276] Van Creveld M. The Transformation of War: The Most Radical Reinterpretation of Armed Conflict Since Clausewitz. – Free Press, 1991. – P. 18.

кордоні з НАТО, дипломатичний тиск, транснаціональні злочинні угрупування, політичні провокації та інформаційна пропаганда»[277].

«Доктрина Герасимова та російська нелінійна війна» стали предметом ретельного аналізу британського політолога М. Галеотті. При вивченні агресивних дій Москви, він оперує дефініцією «нелінійна війна», хоча визнає право на використання визначень «гібридна війна» або «спеціальна війна». Вчений розглядає їх в парадигмі більш широкої, в його розумінні «російської партизанської геополітики», де Кремль застосовує нову стратегію, що сфокусована на пошуку слабких місць противника та тактики уникнення прямих та явних зіткнень з ним[278].

До *концептуальних новацій доктрини* слід віднести нове бачення самої сутності війни. Якщо, за класичним визначенням К. Клаузевіца, «війна є продовженням політики насильницькими засобами із використанням зброї», то згідно з поглядами сучасного керівництва РФ власне політика є продовженнями війни із широким використанням невоєнних методів. Також ставиться під сумнів постулат К. Клаузевіца про використання «центру» концентрації зусиль на головному операційному напрямку. В умовах гібридної війни вирішальне значення має використання комплексного різновекторного застосування воєнних і невоєнних методів[279].

У узагальненому вигляді, *погляди сучасного воєнно-політичного керівництва РФ на сутність і характер війн XXI ст*. можна розкрити в наступних положеннях:

1. «Кольорові революції» – типова форма війни XXI ст., оскільки за масштабами руйнувань і катастрофічними наслідками в усіх сферах життя суспільства вони можуть вважатися новою формою збройного протиборства.

2. Зростання ролі невоєнних способів у досягненні політичних цілей, до яких належить широке застосування політичних, економічних, інформаційних, гуманітарних засобів із використанням протестного потенціалу населення.

3. Використання форм прихованого військового характеру шляхом реалізації заходів інформаційного протиборства та дій Сил спеціальних операцій. Інформаційна війна, як дистанційний

[277] Gertz B. Russia, China, Iran Waging Political Warfare, Report Says [Electronic resource] // The Washington Free Beacon. – Access mode: http://freebeacon.com/national-security/ russia-china-iran-waging-unconventional-warfare-report-says/. (Accessed 20 Febrary 2015).

[278] Galeotti, Mark. The ‘Gerasimov doctrine’ and Russian Non-Linear War. In Moscow’s shadows. 6 July 2014, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimovdoctrine-and-russian-non-linear-war/

[279] Monaghan A. The «War» in Rusian's «Hybrid Warfare» // Parameters. – 2015–2016. – Winter (т. 45, № 4). – С. 65–74.

безконтактний вплив на супротивника, є головним способом досягнення цілей[280].

4. Миротворча діяльність – маніпулятивна форма відкритого застосування сили, в умовах декларативного проголошення «нейтральності».

Отже, *основними складниками «доктрини Герасимова»* є воєнні та невоєнні компоненти[281]. До воєнних слід віднести стратегічне стримування, стратегічне розгортання військ, безпосереднє ведення бойових дій та миротворчу діяльність. До невоєнних – формування політичних союзів і коаліцій, економічні санкції та економічна блокада, дипломатичний тиск і розрив дипломатичних відносин, формування політичної опозиції та активізацію її дій проти політичної влади держави-ворога (держави-конкурента), змушення ворога до переведення економіки на воєнний стан, технології зміни політичного керівництва та проведення наступного комплексу заходів щодо зниження напруженості у відносинах після такої зміни. Загалом, доктрина передбачає співвідношення невоєнних і воєнних дій як 4:1[282].

Першу спробу опису механізму практичного застосування «доктрини Герасимова» на основі аналізу російсько-українського гібридного конфлікту зробив Я. Берзиньш – директор Центру з питань безпеки і стратегічних досліджень (Center for Security and Strategic Research, CSSR) при Національній академії оборони Латвії. Він ідентифікував вісім взаємопов’язаних між собою фаз розвитку. На досягненнях кожної попередньої фази ґрунтується наступний етап, тому вона є обов'язковою передумовою для успіху чергової фази.

У перших п'яти некінетичних фазах представлені лише невоєнні засоби й методи, в останніх трьох (кінетичних) – лише етапи та методи з використанням зброї. Проте, в п'яти некінетичних фазах визначені військові засоби залякування противника у вигляді помилкових атак з повітря, тимчасових військових навчань і крупних маневрів поблизу кордонів території противника зі Східної Європи і країн Балтії[283].

---

[280] Hula R., Perederii I. Information Wars Concepts in Present Social and Communication Technologies Realities // International journal of Engineering and Technology. – 7 (4/8) (2018). – P. 741–744.

[281] McDermott R. Does Russia Have a Gerasimov Doctrine? // Parameters : журнал. – 2016. – Spring (т. 46, № 1). – P. 97–105.

[282] Гула Р.В. Доктрина Герасимова – теорія «організованого хаосу» в філософській парадигмі постмодерну // Збірник наукових праць XI Міжнародної науково-практичної конференції «Проблеми й перспективи розвитку академічної та університетської науки», 20–21 грудня 2018 року – Полтава, 2018. – С. 91–93.

[283] Radin A. Hybrid Warfare in the Baltics. Threats and Potential Responses. – RAND Corporation, 2017. – (Project Air Force). – 48 p.

Фаза 1. Створення сприятливих політичних, економічних і військових умов для внутрішньої дестабілізації через ідеологічні, дипломатичні й економічні операції, а також дії та методи психологічної війни з використанням масиву дезінформації.

Фаза 2. Уведення в оману політичного та військового керівництва противника через поширення помилкових даних через дипломатичні канали, ЗМІ.

Фаза 3. Акції, які призводять до того, що урядовці та посадові особи противника покидають свої пости, будучи заляканими, обдуреними чи дискредитованими.

Фаза 4. Наростання незадоволення населення шляхом активізації «п'ятої колони», проникнення бойових груп і посилення підривних дій.

Фаза 5. Підготовка військових дій, у ході якої в країні, що атакується, створюються різного роду проблеми та закидаються окремі бойові групи («зелені чоловічки»), які взаємодіють з озброєною опозицією.

Фаза 6. Початок військових дій після ретельної розвідки та підривної діяльності. Усі (російські) війська, включаючи спеціальні сили, повинні зайняти свої позиції.

Фаза 7. Знищення основних сил оборони противника скоординованими діями всіх сил і засобів, включаючи ведення «електронної війни».

Фаза 8. Розгром осередків опору, що залишилися, і знищення частин, які чинять опір, шляхом проведення спеціальних операцій.

Хоча з російської точки зору анексія Криму в березні 2014 р. успішно завершилася фазою 5, але атаки підтримуваних Росією сепаратистів на Донбасі застрягли на фазі 6[284].

Отже, В. Герасимов поєднав радянську військову стратегію з її ідеєю тотальної війни з новітніми концепціями воєнного мистецтва. Його теорія ведення сучасної війни більш схожа на мілітаризований хакерський булінг суспільства ворога, ніж на пряму відкриту атаку. Американський політолог К. Моллі так коментує сутність доктрини В. Герасимова: «Краще розколоти суспільство ворога, ніж атакувати його в лоб»[285].

[284] Цит. за: Гибридная война и доктрина Герасимова [Електронний ресурс] // ИнВоенInfo. – 2018, 22 июня. – Режим доступу: https://invoen.ru/analitika/doktrina-gerasimova/

[285] McKew Molly K. The Gerasimov Doctrine [Електронний ресурс] / Molly K. McKew // Politico Magazine, September/October 2017. – Режим доступу: https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538

Опосередковано думку американського політолога підтверджує й сам В. Герасимов, наголошуючи: «Самі правила війни змінилися. Роль невоєнних засобів досягнення політичних і стратегічних цілей зросла, у багатьох випадках за ефективністю вона значно перевищує навіть силу зброї. Усе це доповнюється прихованими військовими заходами»[286].

«Доктрина Герасимова» створює основу для ефективного функціювання нового інструментарію впливу на індивідуальну та колективну свідомість з метою деформації суспільної психології. До цих засобів належать кібероперації, а також інформаційні та пропагандистські кампанії, які проводяться міжнародним телевізійним новинним каналом «Росія сьогодні» (Russia Today) та його агентами. Такими є також фінансова й ідеологічна підтримка правих або лівих популістських рухів і партій, особливо в засобах масової інформації та комунікації адресно визначених цільових країн.

Згідно з доктриною, невоєнні тактики – це не допоміжні засоби, які забезпечують бойові дії, а пріоритетний механізм перемоги. У комплексному поєднанні з точковим використанням дрібномасштабних військових операцій і застосуванням багаточисельних політичних, економічних, соціальних важелів і кіберінструментів, таке домінування та диктат в інформаційній сфері можуть кардинально змінити сприйняття поля бойових дій, створюючи при цьому ілюзію повної відсутності збройного протистояння. Фактично, саме невоєнні дії і є справжньою війною, стратегією керованого хаосу, якої наразі дотримується Кремль. В. Герасимов стверджує, що кінцевою метою реалізації його доктрини є формування в суспільстві ворожої країни атмосфери постійного занепокоєння та ескалації конфліктогенної обстановки.

Разом з тим, проголошення В. Герасимовим 2 березня 2019 р. нової Воєнної доктрини РФ на засіданні все той же Академії воєнних наук кардинально змінила акценти воєнної політики. Проголошення пріоритетності воєнних методів перед будь-яким супротивником одночасно не знизило важливість ассиметричних форм гібридної війни. Тобто, В. Герасимов наголошує на необхідності зосередження уваги на підготовці до ведення бойових дій власне збройного компоненту[287].

---

[286] Герасимов В.В. Ценность науки в предвидении // Военно-промышленный курьер. – 2013, 27 февраля. – № 8 (476). – С. 2.

[287] Новая военная доктрина РФ: подготовка к масштабной войне // Українська правда. – 9 марта 2019. – Режим доступу: https://www.pravda.com.ua/rus/news/2019/03/9/7208764/

Психологічний підхід визначає суть інформаційної війни як системи способів та засобів психологічного впливу на індивідуальну та масову свідомість з метою спрямування її у вигідному для суб'єкта впливу напрямку. До цього підходу зараховують концепції «консцієнтальної» війни та «стратегічних комунікацій».

Концепція ***консцієнтальної війни*** ґрунтується на принципах побудови мережевого суспільства та логічно пов'язана з принципами мережево-центричної та преемптивної воєн і теорією «зіткнення цивілізацій» С. Хантінгтона. Сутність концепції розкривається через визначення змісту поняття «самоідентифікація індивіда», як основного суб'єкту впливу консцієнтальної війни, тобто за допомогою активного інформаційно-психологічного тиску інформаційно-комунікативних мереж формується задана етнорелігійна ідентичність індивіда, його ціннісні орієнтири, стиль життя, культурні уподобання[288]. Тобто, окремі типи свідомості «витісняються» за межі цивілізаційних норм[289].

На думку білоруського дослідника В. Макарова: «під ***консцієнтальною війною***, у сфері смислів, слід розуміти війну психологічну за формою, цивілізаційну за змістом та інформаційну за засобами, у якій об'єктом впливу є знищення або деструкція інтелектуального ресурсу нації та руйнування універсальних установок населення»[290]. Таким чином, враховуючи тісний зв'язок ціннісних установок людини з культурою, можна вважати головним об'єктом знищення у консцієнтальній війні культуру, історію, менталітет та ідентичність народу. Основна мета консціентальної війни: діаспоризація нації, фрагментація регіональних та соціально-стратових спільнот через крах існуючих ідентичностей.

У збройних силах НАТО, особливо США, значна увага приділяється ролі «несмертельної зброї» і технологій, перш за все інформаційної зброї та психолого-пропагандистським операціям у війнах XXI ст., які суттєво змінюють характер застосування сухопутних, військово-повітряних і військово-морських сил на ТВД і геополітичного та цивілізаційного протиборства основних центрів багатополярного світу. У вересні 2006 р. міністром оборони США Д. Рамсфельдом введено в дію ***концепцію «стратегічних комунікацій»***

---

[288] Громыко Ю. Консциентальное оружие и консциентальные войны [Електронний ресурс]. – Режим доступу: hvylya.org/ interview/society2/taynoe-oruzhie-rossii-chto-takoe-voeni-za-identichnost. html

[289] Громыко Ю. Оружие, поражающее сознание, – что это такое? // Кому будет принадлежать консциентальное оружие в XXI веке? – М., 1997. – С. 7–8.

[290] Макаров В. Война в сфере смыслов [Електронний ресурс] // Реферативный журнал социокультурного и политического анализа (Тема выпуска: Постмодерн). – 2011. – Вып. 1 (Июнь 2011 г.). – 75 с. – Режим доступу: URL: http://sovschola.ru/content/rzhskpa-vyp-1-postmodern

(Strategic Communications) (СК), яка доповнювала попередню концепцію інформаційної війни – концепцію «інформаційних операцій непрямої дії».

Інформаційна війна у формі «стратегічних комунікацій» – це комплекс заходів цілеспрямованого впливу на військово-політичне керівництво, суспільно-політичні рухи та сили, міжнародні організації (т.зв. – цільова аудиторія, ЦА) урядові організації за допомогою інформаційних кампаній, економічної та гуманітарної допомоги для створення ідеального іміджу США з метою переконання або примусу ЦА до прийняття рішень та здійснення дій, які забезпечують національні інтереси США.

Принципами реалізації основних положень концепції є:

- професійне централізоване керівництво – наявність єдиної системи управління силами та засобами «стратегічних комунікацій» на основі чіткого і всебічного усвідомлення цілей, особливостей та завдань;
- цілеспрямованість – підпорядкування цілей та завдань задуму військової операції;
- координованість – стратегічне визначення конкретних дій усіх складових цивільної та військової інформаційно-комунікаційних структур у проведенні операції;
- оперативність – здатність сил і засобів інформаційної війни до високої активності та швидкого реагування на події, правильного вибору ЦА, часу та місця здійснення акцій із використанням заданого обсягу й спрямованості інформації у встановлені терміни;
- безперервність – постійний систематичний вплив на ЦА;
- достовірність – декларативне проголошення «правдивості» інформації в інтересах завоювання довіри ЦА;
- переконливість – комплексне застосування усіх форм і методів переконання та навіювання;
- ефективність – використання комплексу традиційних методик впливу із максимальним охопленням ЦА, оперативне ситуаційне коригування дій[291].

Ця концепція реалізовується через об'єднання, координацію та максимальну уніфікацію інформаційних ресурсів країн-учасників блоку в інтересах НАТО. Метою раціонального використання інформаційних ресурсів є організація ефективного управління громадською думкою для підміни чи трансформації ціннісних

[291] Олевский В. Концепция «стратегической пропаганды НАТО // Зарубежное военное обозрение. – 2014. – № 10. – С. 26.

орієнтирів великих мас населення. На думку аналітиків альянсу, цього ефекту можна досягти через здійснення адресного впливу на окремі категорії населення від яких залежить прийняття важливих воєнно-політичних рішень. При цьому основні зусилля зосереджено на конкретних, елементах системи, переміна яких призведе до переформатування цілої системи в потрібний стан. Об'єктом «стратегічних комунікацій» є єдиний інформаційний простір НАТО, як складова частина глобального інформаційного простору. Інформаційне середовище розглядається як комплекс інформації, окремих суб'єктів, організацій та систем, які отримують, обробляють та передають інформацію через віртуальний та фізичний простір. Концепція «стратегічних комунікацій» розглядається воєнно-політичним керівництвом блоку у взаємодії із мережево-центричним принципом ведення війн та інформаційно-мережевою війною з метою досягнення домінування в інформаційному просторі та створення необхідної бази для поширення певних соціально-політичних поглядів в середовищі еліти, серед населення та особового складу ЗС супротивника з використанням усієї могутності інформаційно-комунікаційної інфраструктури блоку НАТО[292].

Поняття «*мережі стратегічних комунікацій*» структурно розділялося на інформаційні та фізичні домени. До інформаційних доменів зараховано радіо, наземне, кабельне, супутникове телебачення, пресу, Інтернет, потокове відео, мобільні телефони, громадські організації та чутки. До фізичних доменів – військові навчання, демонстрація сили, візити, конференції, семінари, наукові та військові обміни, асоціації випускників, торгівля та гуманітарна допомога.

Основні принципи «стратегічних комунікацій» визначені у березні 2008 р. на конференції комітету начальників штабів у військовому коледжі м. Норфолк. Це принципи кваліфікованого керівництва, достовірності, доступності, діалогу, масштабності, координації, цілеспрямованості, оперативності та безперервності. З метою практичної реалізації принципів «стратегічних комунікацій» у МО США проводиться моніторинг соціальних мереж (глобальних і локальних), ЗМІ, моделювання динаміки розвитку різних систем і створення єдиного середовища «стратегічних комунікацій» як в міністерстві, так і на міжвідомчому рівні. Процес СК реалізовується за такими етапами:

- уточнення військово-політичних цілей;

[292] Там само. – С. 9–16.

- визначення ЦА;
- визначення потрібного ефекту поведінки об'єкту впливу;
- проведення аналізу аудиторії;
- визначення ідеологічних установок;
- формулювання основних цілей для публічних звітів і запланованих акцій;
- координація інформаційного впливу при проведенні організованих акцій та політичних дій;
- синхронізація дій носіїв інформації у часових рамках;
- планування першочергових заходів і заходів протидії;
- оцінка результатів і корекція планів[293].

Система блоку НАТО з організації протидії інформаційно-психологічному та інформаційно-технічному впливу ґрунтується на практичній реалізації концепції «стратегічних комунікацій». З метою реалізації ефективного інформаційного впливу на цільову аудиторію супротивника та захисту власної інформаційно-комунікаційної системи в рамках ЄІП НАТО суттєво збільшилась кількість функціональних обов'язків воєнно-політичного керівництва НАТО[294].

Геополітичний підхід можна визначити як сукупність принципів, методів, поглядів і дій глобальних інституціолізованих структур у глобальному інформаційному просторі з метою впливу та формування уніфікованої системи світогляду у соціально-економічній, духовній, культурній сферах життя суспільства через інтенсифікацію поширення потрібного інформаційного продукту у глобальній мережі комунікаційних каналів. У межах геополітичного підходу слід визначити інформаційно-мережеву та мережеву концепцію воєн.

На рубежі XX–XXI ст. у західному суспільстві були розроблені численні технології прихованого руйнівного впливу, що мають комплексний характер, які з часом оформилися в новий тип воєн – «мережево-інформаційні» («мережеві»), які можна визначити як загрози, а потім і руйнування, базових основ нації і держави в основних сферах її існування. Кінцевою метою війни є захоплення більшої частини стратегічно важливих ресурсів країни-жертви агресором. При цьому «передача» цих ресурсів здійснюється елітою цієї країни добровільно, оскільки сприймається не як захоплення, а як прогрес. Це породжує складність у розпізнаванні технологій і методів

[293]Колесов П. Ведение Соединенными Штатами информационных войн. Концепция „стратегических коммуникаций" // Зарубежное военное обозрение. – 2010. – № 6. – С. 9–14.
[294] Олевский В. Концепция «стратегической пропаганды НАТО // Зарубежное военное обозрение. – 2014. – № 9. – С. 9–16.

мережево-інформаційної війни та призводить до відсутності своєчасної й адекватної реакції на дії агресора[295].

Особливістю мережевої війни при геополітичному підході є стирання відмінностей між ідеологією та технологіями, перетворення їх у єдиний комплекс інформаційно-мережевого, інформаційно-психологічного впливу на свідомість світової спільноти. «Інформаційні війни в сучасних умовах ведуться не державами, а численними некомерційними, суспільними організаціями – фондами, центрами, інститутами, лігами тощо, що формуються державою-агресором, яка веде війну. Створюється ціла мережа організацій, що впливають на суспільну свідомість й непомітно скеровують її у потрібному напрямі»[296].

Головною ціллю мережевої війни, на думку В. Коровіна, є захоплення території та встановлення контролю над нею без використання класичних видів зброї, в ідеалі – без військового вторгнення. Це технологія перемоги є дієвою, коли ворог не в змозі скористатися своїм озброєнням для відбиття агресії, у тому числі й ядерною зброєю. Головний зміст мережевої війни – це використання соціальних мереж, не лише Інтернет-спільнот, а й реального суспільства – соціальних ком'юніті індивідів, груп, рухів, організацій, як середовища конструювання передумов для створення нової системи соціальних сенсів. Мотивацією ведення мережевої війни є есхатологічні ідеї про еталонні моделі світопорядку на основі ідеалізованих уявлень. Результатом мережевої війни є зміна правлячих режимів, «кольорові революції», контроль над простором, розміщення військових баз і контингентів та перекодування свідомості мас[297]. Таким чином, на нашу думку, поняття ***мережевої війни*** можна визначити як форму геополітичної протидії між глобальними інституціями за допомогою використання механізму залучення великої кількості індивідів у комплекс мереж соціально-політичного, духовно-інтелектуального, торгівельно-економічного, сектантсько-терористичного характеру з метою уніфікації світоглядних основ мережевого суспільства епохи постмодерну в інтересах домінуючої групи глобальних інституцій.

---

[295] Шумка А.В. Інформаційно-мережева війна – нова форма міждержавного протиборства початку XXI ст. // Військово-науковий вісник. – 2013. – Вип. 19. – С. 244.

[296] Сенченко М. Четверта світова. Інформаційно-психологічна війна [Електронний ресурс]. – К., 2014. – 384 с. – Режим доступу: https://lib.rus.ec/b/241595/read

[297] Коровин В. Третья мировая сетевая война [Електронний ресурс]. – Питер; Санкт-Петербург; 2014. – Режим доступу: http://www.litres.ru/pages/biblio_book/?art=8481662

Мережа є основою, необхідною інфраструктурою, головною передумовою існування мережевого суспільства. При цьому підході поняття **«мережі»** визначається як інтегрована *система* інформаційних комунікацій ЗМІ, ЗМК та інтеграційний *процес* перетворення технічних засобів передачі інформації та мережевих структур (*засоби зв'язку, мас-медіа, транснаціональні корпорації, релігійні організації, неурядові організації, політичні партії, спецслужби різних держав, мережі закусочних, молодіжних клубів, «розкрутки» брендів (мемів*)) у спільну, надзвичайно гнучку та мультифункціональну структуру для ведення підривної діяльності в усіх сферах життя суспільства та політичній системі держави-конкурента з метою руйнування її системи національної безпеки. В рамках цих системи і процесу взаємодіють елементи, які раніше не мали досвіду співіснування та комунікації, а насильство може реалізовуватись неусвідомлено, навіть об'єктами агресії, набувати ознак системно-мережевого характеру[298].

Український дослідник О. Курбан вважає, що поява інтернет-технологій web 2.0 сприяла формуванню нового напряму інформаційних конфліктів – ***мережевої війни***, як інформаційно-комунікаційного протистояння в форматі офлайн та онлайн мережевих структур. Типовими офлайн-мережевими структурами вважаються організації або тимчасові/ситуативні об'єднання індивідів на основі спільної діяльності або загальних інтересів. До онлайн-мережевих структур належать інтернет-ресурси формату WEB 2.0 – віртуальні соціальні мережі (ВКонтакте, Facebook та ін.)[299].

Львівські дослідники А. Шумка та П. Черник характер мережево-інформаційної війни визначають як форму протиборства яка «ведеться … не прямими воєнними діями, а методом спостереження за ситуацією в країні противника, переміщення підконтрольних об'єктів (фізичних осіб) на відповідні позиції в механізмі його державного управління. Моделювання та програмування необхідних процесів та результатів у державі противника здійснюється через засоби інформаційного інструментарію. Мережево-інформаційна війна – багатофункціональне поняття, в яке входить також створення загрози

[298]Дугин А.Г. Сетевые войны. Доклад на заседании Изборского клуба 08.07.2013 [Електронний ресурс]. – Режим доступу: http:// dynacon.ru/content/articles/2318/

[299] Курбан А.В. Современные информационные войны в социальных онлайн-сетях // Information Society. 2016. Issue 23 (January-June). – С. 88.

продовольчої, екологічної, політичної, релігійної, інформаційної та інших видів безпеки для противника невоєнним шляхом»[300].

Український дослідник А.С. Дорошкевич визначає цей тип війни складником гібридної війни. Він вважає, що інформаційно-мережева війна побудована за принципами рекламної кампанії. Її завдання – продати ідею гібридного агресора. Спрямованість інформаційних атак відбувається на свідомість супротивника[301].

Мережево-інформаційні війни призначені для ведення в умовах неможливості використання ядерної зброї та необхідності економії використання технічних засобів індустріальних війн. Простором для інформаційно-мережевої війни є уся територія планети.

Глобальні політичні та економічні інституції, політичні еліти держав розуміють, що контроль за якістю інформації й цілеспрямоване управління її потоками здійснює значний вплив на суспільно-політичні процеси. Тому головним завданням суб'єктів мережево-інформаційних війн є перенесення центру протиборства з матеріально-військової сфери в інформаційно-духовну. Для цього здійснюється прихована кардинальна переорієнтація ментального коду населення тих країн, які є об'єктом інформаційно-мережевої війни, а потім знищення традиційних духовних і культурних цінностей народу. При цьому здійснюється свого роду психологічна анестезія для того, щоб інформаційно-мережеве вторгнення сприймалось суспільством-жертвою як добровільне бажання слідувати шляхом загальнолюдського прогресу у відповідності із «загальнолюдськими цінностями» демократії. У масовій свідомості народу це створює хибні фантомні уявлення про безкорисливу допомогу супротивника…для трансформації архаїчного, відсталого в розвитку суспільства з боку іншого, більш високорозвиненого, яке простягає йому руку «допомоги»[302].

Сутність концепції інформаційно-мережевого впливу полягає в інтеграції зусиль у чотирьох напрямах: фізичному, інформаційному, інтелектуальному та соціальному. Це досягається формуванням механізмів управління поведінки великих мас людей, котрі забезпечують перемогу несиловим шляхом – не за рахунок знищення

[300] Там само. – С. 254.
[301] Дорошкевич А.С. Гібридна війна в інформаційному суспільстві // Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». – 2015. – № 2 (25). – С. 24.
[302] Коровин В. Главная военная тайна США. Сетевые войны. – М., 2009. – 86 с.

збройних сил супротивника, а через деструктивний вплив на його морально-психологічний стан[303].

На думку Д. Джошуа, особливістю мережево-інформаційних війн є остаточний характер її результатів, незворотні процеси трансформації свідомості, зміна ментального коду нації внаслідок насильницького інформаційного переформатування веде до втрати духовних цінностей та базових принципів народу і заміні їх морально-психологічними установками і міфотворчістю агресора[304]. Наслідком цього є формування пристосовницької, «колоніальної» ідеології.

На початку XXI ст. чинники несилових форм ведення боротьби, які виконували раніше переважно допоміжну функцію, набули пріоритетного значення у спектрі комплексу технологій інформаційно-психологічного впливу, що застосовуються в сучасних конфліктах,управління якими змістилось в глобальний інформаційний простір, де сформувалися численні соціально-комунікативні мережі, що є практично неконтрольованими. Це дає можливість сторонам інформаційного протиборства проводити тотальний моніторинг суспільних настроїв, здійснювати на них вплив і маніпулювати ними у реальному часі.

Аналізуючи особливості усіх концепцій інформаційних війн сучасності слід визначити те, що є загальним для усіх підходів і концепцій. Це їх ***трансгуманітарний характер.*** Кінцевою метою усіх видів інформаційних воєн є переформатування ментального коду людини, суспільства, нації, позбавлення її традиційних світоглядних констант, деформація етичних і культурних основ, нівелювання національної ідентичності з метою насадження колоніальної, пристосовницької ідеології.

Концепція мережево-центричної війни є новою воєнно-світоглядною філософією, яка ґрунтується на пріоритеті інформаційно-когнітивної сфери ведення бойових дій над сферою фізичних способів ведення війни. Розвиток теорії гібридної війни, як комплексу традиційних і нетрадиційних форм і методів збройної та не збройної боротьби, без сумніву, має перспективний напрямок розвитку, що вже реалізується на практиці у вигляді інформаційно-центричної війни та активною теоретичною розробкою положень інформаційної війни майбутнього – знаннє-центричної війни.

---

[303] Шумка А.В., Черник П.П. Інформаційно-мережева війна – нова форма міждержавного протиборства початку XXI ст. // Військово-науковий вісник. – 2013. – Вип. 19. – С. 245.

[304] Джошуа Д. Перша мережева війна / переклад Дмитра Губенка // Новинар. – 12–18 січня 2008. – № 1.

Світова військово-політична практика свідчить про високу ефективність використання форм гібридних загроз в досягненні тактичних і стратегічних цілей і завдань. Преемптивна війна є формою комбінованого використання силових і несилових дій, яка в комплексі вирішує завдання забезпечення диктату одного із світових центрів сили через захоплення влади і ресурсів та створення «нової людини» і архетипу нації.

Концепція консцієнтальної війни визначає сутність інформаційної війни, як війни за свідомість у самій свідомості з метою досягнення визначених змін у самоідентифікації індивіда та суспільства Розвиток концепції «стратегічних комунікацій» є продовженням стратегії непрямих дій, яка зосереджує основні зусилля на трансформації другорядних елементів, зміни яких призводять до необхідних системних трансформацій.

Мережево-інформаційна війна – якісно новий рівень міждержавного глобального протиборства та воєнного мистецтва. Це нове багатофункціональне поняття у воєнній науці, яке містить теорії створення загроз продовольчій, екологічній, політичній, релігійній безпеці держави для супротивника шляхом цілеспрямованого інформаційного впливу. Мережева війна – форма глобального протистояння у геополітичному просторі з використанням комплексу мережевих технологій (не тільки Інтернету, а також технологій властивих нетократії) в усіх сферах життя суспільства.

Боротьба держав в інформаційному просторі ведеться декілька тисячоліть за зони політичного і економічного впливу, джерела ресурсів, ринки збуту і території як на міжнародній арені, так і всередині кожної держави, в першу чергу за владу, власність та політичний вплив, за можливість маніпулювати настроями та поведінкою великих мас людей. І вищою формою цього протиборства є інформаційна війна, яка на сучасному етапі динамічно трансформується у якісно нові форми ефективного застосування комплексу психологічних знань, інноваційних технологій та ідеологічних трансформацій.

3.2 Перспективи системи забезпечення кібербезпеки в Україні. Аспекти проблеми.

Динамічний розвиток інформаційних технологій, проникаюча здатність Інтернету в сукупності з політикою тотальної інформатизації нівелюють кордони між суверенними державами. Загострення геополітичних протиріч між традиційними та новітніми

центрами сили створило проблему розбалансування світової системи безпеки, що призвело до низки збройних конфліктів в Європі, у т.ч. і на українських теренах. Все це в сукупності із зростанням масштабів інформаційного протистояння, кіберзлочинності, кібертероризму і, відповідно, гонки інформаційних, у тому числі кібернетичних, озброєнь, стає новим чинником, що впливає на міжнародну безпеку та геополітичну стабільність. Тому, актуальною проблемою стає побудова стійкої та надійної системи захисту національних інтересів України у глобальному інформаційному просторі, особливо в умовах гібридного протистояння з РФ.

Як зазначають науковці: «Жодна стратегія знання не буде повною без …захисту від атак супротивника. Меч знань – двогострий. Він може знищити супротивника раніше, ніж той зможе захищатися, але, може й відрізати руку, котра цей меч тримає»[305].

Аналіз реального стану забезпечення кібернетичної безпеки в Україні, на жаль, не дає підстав навіть для стриманого оптимізму. Розбалансування політичних інститутів, економічна криза, соціальна диференціація суспільства призвели до майже катастрофічного стану боротьби із загрозами у сфері активного протистояння в кіберпросторі. Вітчизняні реалії забезпечення національної безпеки у кіберпросторі свідчать про існування низки важливих питань, подолання яких є, на нашу думку, одним із першочергових завдань воєнної політики України. Передовсім це: термінологічна невизначеність, відсутність належної координації діяльності відповідних відомств, залежність України від програмних та технічних продуктів іноземного виробництва, складнощі із кадровим забезпеченням належних структурних підрозділів. У таких умовах особливого значення набуває пошук нових можливостей забезпечення безпеки держави з огляду на формування нового поля протиборства – кіберпростору.

Тому, на нашу думку, слід окреслити ***комплекс проблем***, які потребують негайного вирішення.

1. **Відсутність ефективної системи забезпечення інформаційної та кібербезпеки України**. У системі забезпечення кібербезпеки держави задіяна низка військових та правоохоронних органів. Це Міністерство оборони України (та його спеціальні підрозділи – зокрема, Головне управління розвідки), Служба безпеки України, Державна служба спеціального зв'язку та захисту

[305] Тоффлер, Э. Тоффлер Х. Война и антивойна. Что такое война и как с ней бороться. Как выжить на рассвете XXI века. – М., 2005. – С. 221.

інформації, Міністерство внутрішніх справ України, Служба зовнішньої розвідки. Але, забезпечення діяльності цих відомств не завжди відповідає вимогам часу. У системі Міністерства оборони України існують спеціальні підрозділи на які покладено задачі із забезпечення кібербезпеки військових інформаційних ресурсів та мереж, але, вони за станом технічного та кадрового забезпечення не завжди в змозі виконувати їх на належному рівні.

2. **Серйозні проблеми кадрового забезпечення відомств фахівцями у сфері інформаційної безпеки**. Незважаючи на те, що низка вищих навчальних закладів (військових, цивільних та відомчих) здійснюють підготовку фахівців за різноманітними спеціальностями, що можуть бути зараховані до сфери інформаційної безпеки, рівень їх підготовки не відповідає потребам сучасного часу. Водночас, слід зазначити, що проблема залучення висококласних фахівців (молодих спеціалістів) у структури, що задіяні в забезпеченні безпеки кіберпростору держави, пов'язана не лише із якістю підготовки, але й браком матеріальних та нематеріальних стимулів для таких фахівців працювати на державній (військовій) службі. Окрім того, відсутні поліпрофільні науково-дослідні інститути, що здійснювали б комплексні дослідження з інформаційної безпеки (не лише проблеми обмеження доступу до інформації чи забезпечення технологічної безпеки, але й соціально-гуманітарної компоненти, і, особливо – комплексного поєднання цих компонентів).

Загальнодержавного масштабу набуває проблема масової еміграції підготовлених висококласних фахівців IT-технологій за кордон.

3. **Тотальна залежність від закордонного програмного забезпечення та відсутність розробок та обов'язкового впровадження програмного забезпечення вітчизняного виробництва в органах влади з метою забезпечення кібернетичної безпеки в України**. Незважаючи на зусилля спеціальних відомств, на думку фахівців, Україна все ще залишається незахищеною (особливо її телекомунікаційна складова), частково та через надмірне впровадження західних програмних продуктів (зокрема фірми Microsoft) і використання матеріально-технічної бази іноземного виробництва. Актуальною залишається проблема створення національної операційної системи, відновлення вітчизняних потужностей із виробництва матеріально-технічної телекомунікаційної бази (особливо для потреб закритих відомчих

інформаційних систем), стимулювання з боку держави створення національного продукту антивірусу.

4. **Відсутність аналізу реального стану спроможності забезпечити захист від кіберзагроз критично важливих об'єктів національної інфраструктури**, зокрема атомних електростанцій, гідроелектростанцій, трубопроводів тощо, шляхом проведення аудиту інформаційної безпеки і запровадження відповідних вимог, обов'язкових для підприємств усіх форм власності.

5. Неузгодженість національної системи захисту державних інформаційних ресурсів з вимогами і стандартами Європейського Союзу, що ускладнює процедуру рівноправного залучення України до систем забезпечення національної безпеки у європейському просторі та загальносвітовому масштабі.

6. Наявність консервативних тенденцій при введенні у науковий обіг нового комплексу категорійного апарату в галузь воєнних наук.

Визначене коло проблем формує для держави та громадянського інформаційного суспільства України низку відповідних ***уроків.***

Урок перший – воєнно-політичний. На сучасному етапі в інформаційному полі України триває безперервна війна за посилення впливу, контролю та управління ресурсами на даній території. Фактично, можна зауважити, що Україна стала своєрідним полігоном для відпрацювання сучасних концепцій інформаційних воєн для держав конкурентів в умовах потенційних і реальних агресій.

У середовищі експертів усталеною є думка, що першою перемогою в інформаційній війні над незалежною Україною було поширення в суспільстві стереотипу про неможливість утримання та обслуговування нашою державою ядерної зброї. Як наслідок – Україна добровільно відмовилася від ядерного статусу, тим самим зменшуючи свій вплив на міжнародній арені. Наступні найбільш відомі інформаційні війни, що торкались безпосередньо інтересів України, – так званий «кольчужний скандал» за часів Л.Д. Кучми, «касетний скандал», українo-російські газові війни, російсько-грузинська війна 2008 р. та звинувачення України у продажу зброї одній із сторін. Потрібно зауважити, що Україна зайняла оборонну позицію та впродовж майже 30-ти років незалежності не спромоглася працювати на випередження чи, хоча б, зайняти активну позицію[306].

[306] Малик І.Р. Інформаційні війни в Україні: історія, сучасний стан та перспективи [Електронний ресурс]. – Режим доступу: Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

Суттєві поразки в інформаційній війні у ході російсько-української преемптивної війни 2014 р. тільки підтверджують попередні тенденції дезорганізаційного системного хаосу, неготовності інформаційно-комунікаційної інфраструктури до дієвого протистояння ідеологічно-інформаційній системі Російської Федерації.

Урок другий – військово-стратегічний. Характер преемптивної війни між РФ та Україною ще раз засвідчив високу бойову ефективність СКбО та комплексного застосування інформаційної зброї, що дає можливість досягати стратегічних і тактичних перемог у війні без вторгнення масованих сухопутних угрупувань.

Низька ефективність самостійної інформаційної політики України, нехтування передовими воєнно-науковими розробками в галузі кібернетичної безпеки, ігнорування передового досвіду провідних військових країн світу в створенні власних сил кіберзахисту призвели до проблемного стану інформаційної безпеки держави та її збройних сил в умовах безпрецедентної інформаційної війни проти України.

Як позитивний приклад вирішення цієї проблеми слід зазначити створення у липні 2016 р. Національного координаційного центру кібербезпеки, який є робочим органом Ради національної безпеки і оборони України. Центр має забезпечити координацію діяльності суб'єктів національної безпеки і оборони України під час реалізації Стратегії кібербезпеки України, підвищити ефективність системи державного управління у формування та реалізації державної політики у сфері кібербезпеки.

Об'єктивно, в силу низки чинників (насамперед економічних) Україна не в змозі створити власні кібервійська. Але, реалії сьогодення вже вносять корективи в процес створення прообразу майбутньої системи кіберзахисту держави. Так, наприклад, команді реагування на кіберзагрози в Україні CERT-UA присвоєно офіційний статус у складі Держспецзв'язку. Ця норма закріплена у «Законі про захист інформації», оновлена редакція якого опублікована на сайті Верховної Ради 17 травня 2014 р. Раніше кіберкоманда працювала на державній службі на громадських засадах[307].

Окрім державних структур, функції своєрідних «волонтерів» кібервійськ виконує хакерська спільнота. Так, київський інтернет-

[307] Watcher. Україна створила кібервійська [Електронний ресурс]. – Режим доступу: http://watcher.com.ua/2014/05/22/ukrayina-stvoryla-kiber-viyska/

користувач і програміст Є. Докукін оголосив про створення «Українських Кібервійськ». Про це він написав у соціальній мережі Facebook, відзначивши, що разом з однодумцями має намір протистояти інформаційній війні, яку веде Росія проти України. «Це кібербатальон для проведення оборонних і наступальних операцій в Інтернеті, для протидії сепаратистам і терористам і протидії інформаційній війні проти України», – написав Є. Докукін. Він підкреслив, що «Українські Кібервійська» щодня проводять акції проти сепаратистів і терористів[308].

Урок третій – інформаційно-організаційний. Стратегічним завданням держави в Україні повинна стати кардинальна трансформація іміджу Збройних Сил і об'єктивно необхідний шлях мілітаризації суспільної свідомості.

Надмірний наголос на мирному багатовекторному курсі України призвів до тотальної демілітаризації суспільної свідомості українського народу. Ігнорування проблем армії, перетворення її у «сплячий» політичний інститут держави від якого ні шкоди, ні користі, призвело до радикального падіння престижу військової служби та вкорінення стереотипу про те, що Україна – мирна держава з неагресивною оборонною військовою політикою, призвело до думки про непотрібність армії в умовах «всезагального мирного демократичного співіснування». Це відображено у результатах соціологічних досліджень інституту ім. Горшеніна у 2010 р. ¾ населення України вважають професію військового непрестижною[309]. Складні процеси т.зв. руйнівного «реформування ЗС Украйни» тільки посилили цю негативну тенденцію. Трагічні події при проведенні бойових стрільб ракетних військ у Броварах, зенітних ракетних військ на м. Опук, загибель цивільного населення на святковому шоу в Скнилові наочно продемонстрували недостатній рівень професійної підготовки військових та стану озброєння. Негативно вплинули на престиж військової служби й низка корупційних скандалів, що пов'язані з посадовими особами з МОУ та ГШ ЗСУ. Імідж армії твориться на основі синтезу знань та уявлень, на основі таких складових: офіційна інформація про Збройні сили з офіційних джерел, власний досвід та чутки у суспільстві. Саме останні два компоненти найбільше впливають на сприйняття армії народом та

[308] Корреспондент.net. Хакери створюють „Українські кібервійська" для протидії інформаційній війні [Електронний ресурс]. – 12 червня 2014. – Режим доступу: http://ua.korrespondent.net/ukraine/politics/3377310-khakery-stvoruiuit-ukrainski-kiberviiska-dlia-protydii-informatsiinii-viini

[309] Офіційний сайт інституту ім. Горшеніна. – Режим доступу: institute. – gorshenin.ua/researches/29_Sostoeanie_ukrainskoy_armii.html.

визначають ступінь довіри до них. Втрата довіри до армії – прямий шлях до втрати держави. Тому, питання іміджу військової організації, насамперед армії, як його ключового компоненту є питанням існування та розвитку держави та суспільства.

Слід зазначити, що комплексна цілеспрямована політика підвищення авторитету воєнної організації держави дозволяє зробити попередні висновки про суттєві позитивні зрушення в формуванні шанобливого ставлення народу до захисників Вітчизни. Але зменшення інтенсивності бойових дій на Сході України, наявність об'єктивно існуючих проблем з деформацією психіки комбатантів містить загрози огульної дискредитації військовослужбовців.

Урок четвертий – воєнно-науковий. В обіг категорійного апарату сучасної воєнної науки слід ввести нові фундаментальні поняття, які відповідають провідним сучасним тенденціям розвитку воєнного мистецтва. Це насамперед категорії, які розкривають сутність бойових операцій у кіберпросторі.

Не знижуючи значення досвіду використання підрозділів і частин Сухопутних військ, слід зазначити, що характер сучасних бойових дій носить переважно гібридний характер, що визначає провідну роль невоєнних асиметричних дій застосування маніпулятивних технологій інформаційно-психологічного впливу та новітніх методів інформаційно-технічних наступальних операцій.

Урок п'ятий – військово-прикладний. Морально-психологічне забезпечення (МПЗ) як вид забезпечення підготовки та ведення бойових дій на сучасному етапі не відображає сутнісних змін у військової науці та практиці ведення сучасних інформаційних війн.

Складові МПЗ органічно входять в систему видів забезпечення бойових дій, та їх зміст потребує удосконалення, відповідно до сучасних реалій. Але ця проблема впродовж двох десятків років знаходилися на периферії інтересів органів військового управління. Що призвело до суттєвих концептуальних розбіжностей у трактуванні змісту МПЗ в наказах МОУ, директивах НГШ ЗСУ та Бойових Статутах (особливо на початку 2000-х рр.). Можна зауважити, що складові МПЗ знаходяться на рівні теоретичної розробки початку 90-х рр. минулого століття і не враховують ні особливості розвитку новітніх концепцій сучасних інформаційних війн, ні розширення інформаційно-технічних можливостей засобів масової та індивідуальної комунікації, їх визначного впливу на особовий склад.

Додамо також і відверто хаотичний характер «реформування» структур МПЗ ЗСУ. Впродовж майже 30-і років цей кластер військового управління пережив не менш 7-і системних організаційно-штатних змін, які в більшості випадків вели до дезорганізації виховного процесу. Механістичне перенесення стандартів НАТО на організаційно-штатну структуру органів МПЗ без врахування особливостей становлення та розвитку ЗСУ впряму веде до зруйнування основ побудови і функціонування важливого складнику забезпечення бойових дій – морально-психологічного забезпечення.

Урок шостий – військово-освітній. Єдина система підготовки фахівців з кібербезпеки держави та її збройних сил як комплексу інформаційно-пропагандистської та інформаційно-технічної протидії фактично відсутня.

На цей час в багатьох ВНЗ держави проводиться набір на навчання за вузько визначеними спеціальностями у галузі ІТ-технологій, технічних фахівців, програмування та ін., але орієнтовані випускники цих вузів на роботу у комерційних структурах, закордонних компаніях або у приватному бізнесі. Питання підготовки воєнних фахівців з ефективного інформаційно-пропагандистського впливу та захисту інформаційно-комунікативного простору, як всередині держави, так і у глобальному середовищі, знаходяться у зародковому стані.

Урок сьомий – національно-державний. Відновлення державного пріоритету у формуванні моделі нації, формування національної ідентичності – найважливіше завдання влади на сучасному етапі, яка тісно пов'язана із завданням збереження та зміцнення єдності країни.

Надскладний спектр геополітичних викликів для Української держави вимагає комплексного аналізу причин критичного розшарування суспільства у соціальній, національній, духовній сферах та розробки ефективних механізмів подолання цих кризових явищ. Ретельний, виважений аналіз даної проблеми дозволяє виробити шляхи національної єдності та згоди, які дадуть можливість пройти шлях до створення єдиного народу, національної ідентичності та громадянського суспільства.

Слід визнати, що на фоні падіння морально-етичних норм суспільства, впливів масової культури, привнесеної ззовні, й головне, ще не сформованої національної ідеї, яка здатна згуртувати націю та мобілізувати усі сили на відсіч агресору, «духовна терапія» потрібна

не менш, ніж військова техніка. Внутрішнє визнання народом справедливого характеру війни дозволяє під час безнадійної ситуації переломити хід бойових дій та одержати перемогу над сильнішим супротивником.

На основі визначеного комплексу проблем і сформульованих уроків, доречно сформулювати низку ***практичних рекомендацій*** для реалізації конструктивної державної політики в питаннях ефективності організації кіберзахисту та інформаційної безпеки.

Військово-організаційна. На нашу думку, оптимальною моделлю для організації кіберзахисту держави могла б слугувати система інформаційної безпеки, яка діє в Ізраїлі. Відсутність СКбО в Армії Оборони Ізраїлю (ЦАХАЛ) не зменшує ефективності скоординованих дій множини установ і відомств з боротьби в глобальному інформаційному просторі. Також, на нашу думку, слід внести відповідні зміни у систему взаємодії між структурами виховної роботи та структурними підрозділами зв'язку та РЕБ у захисті військ від інформаційного впливу супротивника. Власне, ця складова МПЗ діяльності військ знаходиться на перетині інформаційно-психологічного та інформаційно-технічного впливу інформаційної війни. На нашу думку, слід визначити систему оперативного підпорядкування Головному управлінню морально-психологічного забезпечення ЗСУ (при збереженні цього підрозділу у ГШ ЗСУ) відповідних структурних підрозділів Головного управління зв'язку ГШ ЗСУ, Головного управління РЕБ ГШ ЗСУ в плані координації та зосередження зусиль у цьому напрямку за досвідом НВАК.

Військово-інформаційна. Першим кроком з посилення рівня інформаційної безпеки у військовій сфері повинно бути процесу акцентуації мілітаризації свідомості людини й суспільства, боротьба із абстрактним гуманізмом, стереотипним пацифізмом і пропаганда громадянського обов'язку захисту недоторканості та територіальної цілісності країни.

Військово-ідеологічна. Проголошення Конституцією України вищою цінністю поняття людського життя у його екзистенціально-філософському значенні, безумовно відповідає світовим гуманістично-ліберальним стандартам (Розділ 1, Стаття 3. Людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю), але в умовах гібридного конфлікту з РФ та боротьби з проявами сепаратизму викликає тенденції «розщеплення» свідомості військової людини, яка

за призначенням повинна знищувати ворога, а ні абстрактну людину, як носія «вищої цінності».

У преамбулі Конституції Французької Республіки 1958 р. зазначено: «Французький народ урочисто проголошує свою прихильність правам людини та національного суверенітету». Згідно статті 2 «Про суверенітет»: «Девіз республіки – Свобода, Рівність, Братство. ЇЇ принцип – правління народу, народом, для народу»[310]. Ці ціннісні константи конкретизують основоположні пріоритети військово-патріотичного виховання громадян.

Одночасно, враховуючи важкий досвід домінування «единого правильного учения», слід вкрай обережно трактувати ідеологічні течії та доктрини як виключно патріотичні. Необхідно зосередитися на впровадженні у суспільно-політичну практику принципів плюралізму поглядів і свободи слова.

Воєнно-наукова. **С**учасний інформаційний простір фактично стає театром глобального інформаційного протиборства, де кожна сторона конфлікту прагне отримати перевагу у вирішенні воєнно-політичних і соціально-політичних завдань, а в разі потреби – знищити конкурента чи ворога. Природне, що тектонічні зміни епохи постмодерну спровокували концептуальні трансформації в стратегії, оперативному мистецтві та тактиці.

Ще у 1996 р. експерт Пентагону Р. Банкер запропанував розділити театр військових дій на традиційний простір та кіберпростір[311]. Експерт також запропонував доктрину «кіберманевру», яка є доповненням традиційних військових концепцій, спрямованих на нейтралізацію збройних сил противника. Відтепер ключовими об'єктами ураження в війнах стають інформаційна інфраструктура та психіка останнього[312].

На нашу думку, у зв’язку з сутнісними й категоріальними новаціями сучасного соціокультурного поля, в обіг категорій воєнного мистецтва доцільно внести поняття ***театр глобального інформаційного протиборства.*** Це глобальний інформаційний простір, який використовують суб’єкти інформаційного протиборства для проведення широкомасштабної інформаційної війни з метою досягнення інформаційного домінування, посилення військового,

---

[310] Сайт Французские конституции [Електронний ресурс]. – Режим доступу: http://www.labex.ru/page/konst_france.html

[311] Цит. по: Жовтенко Т., Яблонський В. Інформаційний вимір сучасних військових конфліктів (Іракська кампанія 2003 року) // Стратегічні приорітети. – №4 (9). – 2008. – С. 173. – Режим доступу: http://old.niss.gov.ua/book/StrPryor/9/ 23.pdf

[312] Рудницька У.І. Інформаційні війни як засіб геополітичного протистояння // Гуманітарний журнал. – 2015. – 1-2. зима-весна. – С. 136.

політичного, економічного та духовного потенціалу з одночасним послабленням або знищенням потенціалу противника чи конкурента. Головною особливістю театру глобальної інформаційної війни є його тотально-всеохоплюючий характер на тлі оперативного реагування на зміну воєнно-політичної обстановки. На відміну від класичного театру війни він впливає на суб'єктів інформаційного протиборства нейтральних і невоюючих держав й охоплює зони, які міжнародним правом визначені як такі, що не підлягають нападу та знищенню (санітарні зони, райони АЕС, дамб, ГЕС, зони Суецького й Панамського каналів, архіпелаг Шпіцберген, Аландські острови, Антарктика).

На театрі глобального інформаційного протиборства вирішуються завдання стратегічного характеру, а саме:

- формування позитивного (або трансформація негативного) іміджу власної держави та дискредитація країни-конкурента;
- тотальна дезінформація світової спільноти з метою формування потрібної картини сприйняття становища в інтересах власної держави;
- створення необхідних «опорних точок» ведення та посилення інформаційно-пропагандистських заходів за допомогою умовно «незалежних» джерел інформації з метою маскування власних інформаційних ресурсів.

Силами та засобами виступають ЗМІ, ЗМК світового рівня, глобальні мережеві ресурси, міжнародні організації.

У межах театру глобальної інформаційної війни, на нашу думку, формується ***інформаційний театр воєнних дій*** – частина глобального інформаційного простору, де проводяться сплановані за місцем, часом і метою заходи розгортання угруповань для ведення інформаційного протиборства оперативно-стратегічного масштабу, координація зосередження їх зусиль за напрямами та районами й організація їх взаємодії в загальній системі інформаційної інфраструктури держави.

Особливостями інформаційного театру воєнних дій є:

- використання комп'ютерних комунікацій;
- глобальний масштаб;
- надшвидкісна мінливість.

У рамках інформаційного театру воєнних дій вирішуються такі завдання:

- формування потрібного інформаційного контексту;

- швидке поширення потрібного інформаційного продукту в межах інформаційного театру;

- оперативність і створення величезного об'єму комбінованої інформації (дезінформації та достовірних даних) з метою унеможливлення швидкого реагування адекватними та ефективними заходами протидії.

Інформаційний театр воєнних дій, на нашу думку, складається з таких *основних компонентів*:

1. ***Оперативно-стратегічний операційний напрямок зосередження основних зусиль інформаційного протиборства*** – частина інформаційного театру воєнних дій між державами з визначеними важливими елементами системи державного та військового управління, стратегічними об'єктами інформаційно-комунікаційної інфраструктури, складом сил і засобів інформаційно-психологічних операцій противника, на які спрямовані інформаційні операції оперативно-стратегічного рівня.

2. ***Тактичний район інформаційного протиборства*** – сегмент периферійного інформаційного простору для проведення дезінформуючих акцій з метою створення сприятливої суспільної думки місцевого населення в інтересах тактичних дій дестабілізаційного характеру та виведення з ладу тактичної ланки системи інформаційно-комунікаційної інфраструктури супротивника проти яких здійснюються інформаційні операції.

До сил і засобів інформаційного театру воєнних дій належать:

1. Електронні ЗМІ і ЗМК, друкована продукція.
2. Фахівці прес-служб ЗС, оперативних командувань і тимчасових формувань для проведення антитерористичних акцій.
3. Організована інфраструктура інформаційного протиборства.
4. Резервна інфраструктура для поновлення та організації маневру силами та засобами.

На нашу думку, з метою підвищення ефективності превентивних заходів інформаційно-психологічної протидії, слід ввести у воєнно-науковий дискурс поняття ***«зона виявлення імовірних загроз» інформаційно-психологічного впливу противника.*** Це частина географічного та кіберпростору, де зосереджено посилене угруповання сил і засобів інформаційно-психологічного впливу противника, яке характеризується підвищеною активністю ведення наступальних інформаційних операцій.

Параметри цієї зони, на наш погляд, визначаються:

1. Зосередженням сил і засобів інформаційної війни противника та інформаційно-психологічної протидії власної інформаційно-комунікаційної інфраструктури.

2. Рубежами дій, які обумовлені:

- рівнем спецпідготовки фахівців інформаційної війни та інформаційно-психологічної протидії;
- тактико-технічними характеристиками інформаційно-технічної інфраструктури противника;
- ступенем ефективності системи інформаційно-психологічного захисту військової інформаційно-комунікаційної інфраструктури та морально-психологічного стану військ;
- наявністю слабких місць противника у проведенні інформаційно-психологічних дій.

3. Районами дій, які характеризуються:

- особливостями розвитку інформаційної та морально-психологічної обстановки;
- виявленням найбільш уразливих сегментів власної інформаційно-комунікаційної інфраструктури;
- ступенем активності та спрямованості інформаційних потоків та операцій на можливі об’єкти і канали потенційного негативного інформаційно-психологічного впливу на війська (сили);
- можливого рівня деморалізації та психогенних втрат особового складу від інформаційно-психологічного впливу противника та оцінка ступеня уразливості своїх військ (сил).

Також доцільно було б розглянути введення в практику заходів інформаційно-психологічної протидії поняття ***«зона імовірного інформаційно-психологічного ураження особового складу»*** – як частини географічного та кіберпростору, в межах якого відбувається прогнозоване зниження морально-психологічного стану військ (сил) із високим ступенем ймовірності.

Комплексом причин, який сприятиме появі, функціонуванню та розширенню розмірів цієї зони, є:

- недоліки бойового, матеріально-технічного, тилового забезпечення підготовки та ведення бойових дій;
- наявність неосвічених (або скомпрометованих) військових керівників;
- несприятливі події в державі;
- непопулярні та незрозумілі для особового складу дії влади;
- низький рівень підготовки особового складу;

- недоліки національної інформаційної політики та інформування особового складу;
- факти порушення військової дисципліни, законності, міжнародного гуманітарного права;
- загострення національних, релігійних, соціальних суперечностей;
- незадовільна роз'яснювальна робота з місцевим населенням;
- потужний вплив інформаційно-пропагандистської інфраструктури противника.

Параметри цієї зони визначаються:

1. Рубіжними просторовими характеристиками домінуючого впливу структурних компонентів власної інформаційно-комунікаційної інфраструктури, а також ЗМІ та ЗМК противника.
2. Рівнем концентрації підготовлених високопрофесійних фахівців з інформаційно-психологічної протидії та їх розподілом по уразливих ділянках ведення бойових дій та в підрозділах з низьким рівнем морально-психологічного стану.
3. Кількісно-якісними показниками ефективності інфраструктури інформаційно-психологічної протидії (прес-центри, ЗМІ військової преси, радіомовлення та телебачення та ін.) та її здатністю протистояти ворожому інформаційно-психологічному впливу[313].

Таким чином, *стратегія інформаційного протиборства*, на нашу думку, містить такі основні складові:

1. Визначення глобального інформаційного простору як театру глобального інформаційного протиборства та прогнозування множини комбінованих варіантів його використання.
2. Скерування заходів інформаційного протиборства на соціальну активність населення та особового складу ЗС країни-ворога, через перехід від маніпулювання суспільною свідомістю на демонстрацію акцій громадянської непокори в режимі реального часу.
3. Визначення слабких елементів у системі інформаційної безпеки противника для найбільш ефективного проведення операцій інформаційної війни.
4. Удосконалення власної інформаційно-комунікативної інфраструктури та посилення заходів її безпеки.
5. Визначення головних операційних напрямків і тактичних районів інформаційного протиборства, характеру інформаційного

[313] Інформаційна війна і національна безпека: монографія / П.П. Ткачук, Р.В. Гула, О.І. Сивак та ін. – Львів, 2015. – С. 175–177.

впливу залежно від особливостей цих компонентів інформаційного театру воєнних дій.

6. Визначення резервів поновлення та зміцнення сил і засобів інформаційного протиборства з метою здійснення маневру для нарощування інформаційного впливу й удосконалення системи захисту власних інформаційних ресурсів.

7. Побудова ефективної системи резидентів та суб'єктів дезінформації противника.

8. Визначення об'єктів інформаційної блокади противника (в комплексі з економічною, технологічною, соціальною) для створення умов локальної (а в ідеалі тотальної) нейтралізації здатності його воєнно-політичного керівництва до прийняття адекватних рішень.

Військово-правова. На нашу думку, необхідно внести в законодавчу базу України зміни, що стосуються внесення в правове поле держави понять, що безпосередньо пов'язані із сучасними загрозами національній безпеці держави у глобальному середовищі в епоху інформаційного суспільства. В «Положення про Міністерство Оборони України» та «Положення про Генеральний Штаб Збройних Сил України», на нашу думку, доцільно внести зміни з конкретизацією функцій.

Міністерство Оборони:

- планування і реалізація заходів протидії та нейтралізації кіберзагроз національним інтересам України у воєнній сфері та захист державної інформаційно-комунікаційної інфраструктури;

- участь у підготовці та забезпеченні кібербезпеки об´єктів критичної інформаційно-комунікаційної інфраструктури держави до функціонування в особливий період та в умовах воєнного стану;

- забезпечення розвитку і безпеки інформаційно-комунікаційної інфраструктури та ресурсів, впровадження новітніх інформаційних технологій у сфері оборони та національної безпеки;

- проведення організаційно-технічних та інших заходів із запобігання загроз несанкціонованого кібернетичного впливу на ІТ інфраструктуру МОУ та ГШ Збройних Сил України;

- пошук і добування розвідувальної інформації про інформаційні системи й мережі, технології та засоби кібервпливу, а також кібернетичні операції потенціальних протиборчих сторін;

- аналіз і відстеження кібернападів на ІТ інфраструктуру МОУ і ГШ Збройних Сил України та формування баз даних;

- виявлення ознак кіберзагроз, їх класифікації, оцінка форм проявів і напрямків дії, потенційних об’єктів кібератак та прогнозування можливих наслідків.

- здійснення заходів з організації взаємодії державних установ, інших силових структур, спецслужб, правоохоронних та судових органів в процесах обміну інформацією, а також проведення спільних заходів з кібер-захисту власних ІТ інфраструктур та протидії кіберзлочинам тощо.

Генштаб буде зобов´язаний організувати, координувати роботу зі створення і захисту від кібернетичних загроз єдиної автоматизованої системи управління ЗСУ.

Військово-практична. Доцільно застосовувати в практиці проведення командно-штабних навчань (КШН) відпрацювання оперативними відділами (управліннями) операцій з протидії кіберзагрозам на рівні оперативно-тактичних з’єднань, об’єднань, видів ЗС України та здатності штабних структур до координації, узгодженості дій структурних підрозділів органів військового управління з захисту військ від несанкціонованого проникнення супротивника у мережі інформаційно-комунікаційної інфраструктури військ.

Військово-освітня. На нашу думку, слід ввести в навчальний процес військових навчальних заходів для усіх спеціальностей навчальну дисципліну «Інформаційні війни сучасності». Для спеціальностей фахівців морально-психологічного забезпечення у видових військових навчальних закладах передбачити введення спецкурсу «Інформаційно-психологічна та інформаційно-технічна протидія» («Протидія кіберзагрозам в інформаційному просторі»). Видами занять дисципліни повинні бути лекції, семінари та практичні заняття, проводити які будуть фахівці з інформаційно-психологічної та інформаційно-технічної протидії при організації взаємодії кафедр гуманітарного та технічного циклу.

Національно-консолідуюча. Необхідною умовою протистояння та протидії проявам консцієнтальної війни у сучасному інформаційному суспільстві в умовах глобалізації світу є відмова від етнічного регіонального ізоляціонізму і кристалізація національної ідеї та ідентичності на принципах мультикультуралізму. Критерієм визначення самоідентичності народу України може бути система необхідних теоретичних положень та практичних дій, що будуть втримувати баланс між інтернаціональним і національним, громадянським та етнічним, як умову збереження миру та злагоди в

країні. З таких позицій у сучасному цивілізованому суспільстві ведеться боротьба з тотальною корупцією, з проявами радикального націоналізму, сепаратизму, тероризму та ксенофобії.

У умовах інформаційної революції, швидкого становлення та розвитку відносин в інформаційному суспільстві виявляється неефективність системи захисту, обробки й раціонального використання накопиченого в державі інформаційного ресурсу на тлі застарілих, колізійних, недосконалих законодавчих норм.

Негативні явища у кіберсфері України зумовлюють необхідність охоплення її регулятивними та охоронними функціями права, а також акцентують на потребі вирішення проблем у сфері кібербезпеки, як однієї з найважливіших складових національної безпеки держави. Формування системи захисту кіберпростору на національному рівні триває досить повільно та безсистемно, виникає низка проблем, які обумовлені інноваційним характером проблематики та об'єктивними умовами технічної відсталості країни. Важливою проблемою є також і термінологічна невизначеність категорійного апарату, розбалансованість та неготовність чинної правової бази протистояти новим загрозам в умовах інтенсифікації інформаційного протиборства.

Сучасні реалії в Україні потребують негайного прийняття низки рішень в галузі захисту власної інформаційно-комунікаційної інфраструктури від безпрецедентних кіберзагроз в умовах комплексного застосування проти неї сучасних інформаційно-психологічних технологій, форм і методів новітніх розробок концепцій інформаційних воєн.

Розвиток інформаційно-комунікаційної сфери кардинально змінив функціональне призначення інформаційної складової у веденні бойових дій, перетворив її із засобу забезпечення в дієвий інструмент ведення війни. У класичних військових доктринах відбулася перманентна інформаційна революція, значення та масштаби якої ще потребують наукового осмислення та ретельного аналізу її застосування у збройних конфліктах сучасності.

Досвід минулого та уроки сьогодення свідчать про те, що потенційними можливостями з організації і проведення інформаційно-психологічних операцій володіють повною мірою лише системи органів влади і державного управління. Тому, усвідомлення військово-політичним керівництвом держави потреби формування ефективної сучасної структури для ведення інформаційних воєн (як в агресивних цілях, так і з метою захисту),

впровадження спеціальних нормативно-правових актів із забезпечення їх діяльності а також створення Сил кібероперацій є формуванням нового типу наступальної та оборонної зброї, що може бути використане на усіх стадіях військового конфлікту.

Загрози кібербезпеці виникають на національному рівні. Але, створення ефективної системи кібербезпеки може бути здійснено лише у взаємодії узгоджених дій на міжнародному, світовому рівні, де особливу роль має вага міжнародного права і міжнародні структури.

У умовах сьогодення діяльність України у сфері боротьби з внутрішніми та зовнішніми кіберзагрозами є недосконалою. Незважаючи на те, що питаннями забезпечення безпеки національного інформаційного простору, здійсненням заходів з кіберзахисту інфраструктури та протидії внутрішнім і зовнішнім кібернетичним загрозам, у тому чи іншому аспекті займаються як на державному, так і на військовому рівнях, існує низка проблем, які потребують оперативного вирішення. Проблемні чинники удосконалення системи координації зусиль, достатнього фінансового забезпечення, підготовки фахівців належного рівня, впровадження дієвої системи управління інформаційними операціями та кіберзахистом військ впливають на оперативність прийняття рішень та динамічність процесів з організації сучасної системи кібернетичного захисту держави й армії. Але, одночасно, слід визнати й позитивні тенденції, а саме поява правового регулювання та впровадження сучасних інформаційно-комунікаційних новацій в практику удосконалення інформаційної політики в системі національної безпеки держави.

РОЗДІЛ 4
КІБЕРВІЙСЬКА – СТРУКТУРА ТА ФУНКЦІОНАЛЬНЕ ПРИЗНАЧЕННЯ (ЗА ДОСВІДОМ ПРОВІДНИХ ДЕРЖАВ СВІТУ)

...Військові називають кіберпростір «п'ятим театром» бойових дій і вважають досягнення переваги над цьому театрі необхідним для виконання місії, точно так же, як і на чотирьох інших: суші, морі, повітряному та космічному просторі.

Ш. Харріс

Розвиток інформаційно-комунікаційних технологій в глобальному інформаційному просторі об'єктивно обумовили необхідність створення системи комплексного застосування сил і засобів кібернетичних операцій у військової сфері. Кіберпростір, як «глобальна сфера», домен глобального інформаційного простору є взаємопов'язаною сукупністю інформаційних структур і технологій, що разом з сухопутним, повітряно-космічним і морським простором стає реальним театром воєнних дій, загрози якого дорівнюють загрозам від ЗМУ[314].

Кіберпростір поступово увійшов до всіх сфер сучасного суспільного життя. Однак його визначення, на сьогодні, не має єдиної уніфікованої форми. Якщо розглядати кіберпростір як словосполучення «кібернетичний простір», то кіберпростір – це простір (територія), який створений та працює на основі принципів, методів кібернетики (науки про загальні закони одержання, зберігання, передачі та обробки інформації)[315].

Відповідно до міжнародного стандарту, кіберпростір – це середовище існування, що виникло в результаті взаємодії людей, програмного забезпечення та послуг в Інтернеті за допомогою технологічних пристроїв і мереж, що під'єднані до них, якого не існує в будь-якій фізичній формі[316].

---

[314] Давыдов Д. Информационные операции как средство достижения целей военно-политического руководства США // Зарубежное военное обозрение. – 2013. – № 10. – С. 5.

[315] Манжай О.В. Використання кіберпростору в оперативно-розшуковій діяльності // Право і Безпека. – 2009. – №4. – С. 215–219.

[316] Присяжнюк М.М., Цифра Є.І. Особливості забезпечення кібербезпеки // Реєстрація, зберігання і обробка даних. – 2017. – Т.2. – С. 62. – Режим доступу: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/131678/06-Prysiazhniuk.pdf?sequence=1

У нормативній базі США зазначено, що кіберпростір – це сфера, яка характеризується можливістю використання електронних і електромагнітних засобів для запам'ятовування, модифікування та обміну даними в мережевих системах і пов'язану з ними фізичну інфраструктуру.

За офіційними документами Євросоюзу, кіберпрострір – це віртуальний простір, у якому циркулюють електронні дані світових персональних комп'ютерів.

Для Великобританії кіберпростір – це всі форми мережевої цифрової активності, що включають у себе контент і дії, здійснювані через цифрові мережі.

У Німеччині вважають, що кіберпростір – це вся інформаційна інфраструктура, яка доступна через Інтернет поза будь-якими територіальними кордонами.

У Україні на сьогодні відсутнє стандартизоване поняття кіберпростору. Варто навести найбільш повні визначення вітчизняних фахівців щодо цього поняття.

Так С. Гнатюк, провівши багатокритеріальний аналіз, запропонував таке узагальнене визначення: кіберпростір – це віртуальний простір, що отриманий у результаті взаємодії користувачів, програмного та апаратного забезпечення, мережевих технологій (у т.ч. Інтернет) для підтримки та управління процесами перетворення інформації (електронних інформаційних ресурсів) з метою забезпечення інформаційних потреб суспільства[317].

В. Бурячок, В. Толубко, В. Хорошко та інші автори підручника «Інформаційна та кібербезпека: соціотехнічний аспект» наводять ще одне визначення кіберпростору як віртуального комунікаційного середовища, що утворений системою зв'язків між користувачами та об'єктами інформаційної інфраструктури, такими як електронний інформаційний ресурс, системи та мережі всіх форм власності, керовані автоматизованими системами управління, що використовуються не лише для перетворення та передачі інформації, яка в них циркулює, з метою забезпечення інформаційних потреб суспільства, а й для впливу на аналогічні об'єкти протиборчої сторони[318].

Про важливість захисту національної військової інформаційної інфраструктури свідчать такі статистичні дані: інформаційно-

[317] Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи // Безпека інформації. –2013. – Т. 19. – № 2. – С. 118–129. – Режим доступу: ИКЬ: ЬіІр://пЬиу.доу.иа/ШКЛ/Ье2іп_2013_19_2_8

[318] Бурячок В.Л., Толубко Б. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. / За заг. ред. д-ра техн. наук, професора Б. Толубка. – Київ, 2015. – 288 с.

комунікативна система МО США складається з 15 000 комп'ютерних мереж і більш ніж 7 млн комп'ютерів; на інформаційні ресурси Пентагону (в тому числі і внутрішню мережу SPIRNET) здійснюється 360 млн кібератак на рік, а на Глобальну інформаційну мережу (Global Information Grid) МО США – близько 3 млн кібератак на добу. Військові фахівці вважають, що у сучасності загроза початку «комп'ютерних воєн» («кібервійни») стає реальністю і вимагає постійного уважного ставлення до неї. За оцінками фахівців, у такій війні переможеною може виявитися навіть та держава, яка володіє військовим потенціалом, що перевершує могутність супротивника[319].

Поступово світове співтовариство починає усвідомлювати, що кіберпростір перетворюється у поле боротьби, яке потребує розробки відповідної стратегії національної та міжнародної безпеки. Американський фахівець з питань кібербезпеки К. Гірс, наголошує, що «стратеги повинні усвідомлювати, що частина кожного політичного чи військового конфлікту буде реалізовуватись в Інтернеті»[320]. Віце-президент американського Інституту вивчення тероризму та політичного насильства, в минулому – аналітик Міністерства оборони США, П. Пробст зауважив, що у міжнародному середовищі в добу інформаційного суспільства «Розвиваючись, держави все більшою мірою стають залежними від високих технологій. Комплексні національні системи є потенційно небезпечними, тому, що нанесення ударів по життєво важливих вузлах, може призвести до незворотних руйнівних наслідків. Така атака може бути здійснена через комп'ютери… або з використанням вибухівки, або шляхом виведення з ладу кабелів, що спричинить ланцюг аварій із колапсом усіх контрольних систем трубопроводу чи аеропорту»[321]. Співробітник вашингтонського Центру міжнародних і стратегічних досліджень У. Лакер вважає, що «...втручання комп'ютерних хакерів може зробити всю державу не здатною до нормального функціонування. Звідси зростання тривоги з приводу можливостей інформаційного тероризму та кібервійни... достатньо 20 кваліфікованих хакерів і одного мільярду доларів, щоб знищити Америку»[322].

---

[319] В информационной войне превосходство в военной мощи не гарантирует от поражения [Електронний ресурс]. – Режим доступу: http:// www. arms-expo.ru/049051124053053051052.html

[320] Geers K. Cyber spaceand the chang in gnature of warfare [Електронний ресурс]. – Режим доступу: http://www.scmagazineus.com/Cyberspace-and-the-changing-nature-of-arfare/article/115929/

[321] Компьютерный абордаж военного спутника // Эхо планеты. – 1999. – № 10. – С. 10.

[322] Laqueur W. Postmodern Terrorism / W. Laqueur // Foreign Affairs. – 1996. – № 75. – P. 35.

Визнання необхідності забезпечення безпеки держави у сфері кіберпростору від загрози несанкціонованого кібервторгнення, обумовили появу дискусій про визнання на міжнародному рівні кібератаки «актом війни». 30 січня 2010 р. сенатор США від республіканської партії С. Колінз зазначила, що США розглядають питання щодо ставлення до кібератак як до оголошення війни, а 12 травня 2010 р. помічник заступника міністра оборони США з політичних питань Дж. Мілер заявив, що США готові завдати воєнного удару у відповідь на кібератаки в комп'ютерних мережах. Таким чином, реальність і масштабність інформаційних загроз національній безпеці держав у сучасному глобальному інформаційно-комунікаційному середовищі зумовили створення спеціалізованих підрозділів у правоохоронних органах і збройних силах країн, так званих кібервійськ. На нашу думку, **кібервійська (Сили кібероперацій – СкбО)** – це спеціальні військові формування в складі збройних сил, які за своїм функціональним призначення забезпечують комплексний захист інформаційно-комунікаційної інфраструктури національної безпеки держави від несанкціонованого втручання з боку державних, недержавних і транснаціональних кіберугрупувань, доступ до комп'ютерних мереж ймовірного супротивника та використання їх у власних інтересах через застосування новітніх ІТ-технологій силами професійних комунікаторів та фахівців з ведення інформаційної війни.

У структурі ЗС країн створюються спеціальні підрозділи кібератак і кіберзахисту. Згідно з офіційними заявами, такі підрозділи створено в США (U.S. Cyber Command), Великобританії (Cyber Security Operations Centre при уряді Великобританії), Німеччині (Internet Crime Unit та Federal Office for Information Security), Австралії (The Cybersecurity operations centre), Індії та інших державах. На цей час, за даними розвідки США, створенням кібервійськ займаються приблизно у 30 країнах світу.

Засобами кібервійськ (т.зв. ***кіберзброєю)***, на нашу думку, є: електронні технології та засоби поширення електромагнітних випромінювань інформаційно-комунікаційної інфраструктури, інші матеріальні інфраструктури, які пов'язані із соціотехнічним простором і здатні створювати, модифікувати, зберігати й передавати інформацію (управляти її потоками), а також впливати на стан фізичних інфраструктур супротивника.

Скоординовані дії в інформаційній війні, масштабне застосування інформаційно-комунікаційних технологій в

кіберпросторі вперше було здійснено у ході підготовки та проведення військової операції «Союзницька сила» проти СРЮ 24.05. – 10.06.1999 р. Уперше в практиці НАТО, за 6 місяців до операції був створений спеціальний комітет, який координував дії союзників в інформаційному просторі в умовах проведення військової операції. Під час цієї операції вперше була організована всебічна інформаційна підтримка операції НАТО в Інтернеті. У мережі було розміщено близько 300 тис. сайтів, які тією чи іншою мірою стосувалися проблеми Косово та військової операції альянсу в Югославії. Більшість сайтів були створені американськими фахівцями з комп'ютерних технологій, та значно посилили ефективність пропагандистської компанії. Також були визначені об'єкти потенційної інформаційної загрози – національні ЗМІ, система управління та зв'язку, що стали пріоритетними цілями для повітряно-вогневого придушення.

Одночасно, у сфері інформаційно-технічного протиборства загострилася боротьба за інформацію в цифрових системах. Хакери неодноразово робили вдалі спроби проникнення через мережу Інтернет в локальні обчислювальні мережі штабу Об'єднаннях ЗС НАТО. Масові запити серверів цих мереж в окремі періоди часу паралізували роботу електронної пошти, що можна вважати першою ефективною акцією із застосуванням інформаційної зброї[323]. Дії югославських хакерів спровокували появу в теорії та практиці інформаційного протиборства поняття «кібератака».

У 2006 р. в іракському інформаційному сегменті було зафіксовано системне протиборство в кіберпросторі між опозицією та владою цієї ісламської республіки. Боротьбу за контроль над електронними ЗМІ та соціальними мережами американські фахівці охарактеризували як першу в світі кібервійну, яку вели між собою високопрофесійні фахівці. Першим системним протиборством в кіберпросторі в ході бойових дій слід вважати проведення інформаційно-психологічних операцій у грудні 2008 р. між Армією Оборони Ізраїлю та рухом ХАМАС. Ізраїльтяни активно використовували спеціальні інтернет-портали для пропаганди могутності ізраїльської високоточної зброї, блокування радіо-телесигналів у Секторі Газа, та вогневе знищення телекомунікацій арабів. ХАМАС, за допомогою хакерських спільнот Марокко і Саудівської Аравії, вже у січні 2009 р. зламали систему безпеки 10

[323] Морозов Ю.В. Балканы сегодня и завтра: военно-политические аспекты миротворчества – М., – 2001. – С. 247–249.

тис. ізраїльських сайтів, які містили інформацію про події на Близькому Сході. Основною метою кібератак було фальсифікування контенту електронних сторінок і переадресація трафіку низки ізраїльських інформаційних служб на неіснуючі електронні адреси. Улітку 2009 р. хакери Азербайджану та Туреччини здійснили серію кібератак на вірменський сегмент Інтернету внаслідок чого була блокована робота урядових установ Республіки Вірменії[324]. На початку липня 2009 р. хвиля кібератак, імовірно з території КНДР, тимчасово придушила роботу веб-сайтів окремих державних установ Південної Кореї та США. Сталося це в період здійснення КНДР послідовної серії пусків балістичних ракет, посилення загальної дипломатичної напруженості, пов'язаної з її ядерною програмою і загрози введення санкцій США й ООН.

За класифікацією українського дослідника В. Конах, система інформаційної безпеки **Сполучених Штатів Америки** з моменту свого виникнення і дотепер зазнала значного організаційного розвитку, в якому можна виокремити такі етапи:

– виникнення (І Світова війна – 1947 рр.) – інформаційна безпека зводиться до забезпечення безпеки зв'язку та криптографічного захисту інформації;

– становлення (1947–1982 рр.) – характеризується глобальним розвитком розвідувальної мережі США, зокрема систем радіо- і радіоелектронної розвідки з використанням супутникових систем, та створенням систем захисту інформаційних ресурсів;

– розвиток (1983–2001 рр.) – започатковується процес усвідомлення загроз національній безпеці США в інформаційній сфері та формування урядової політики в сфері забезпечення інформаційної безпеки, поширення знань про безпеку інформації у суспільстві, відбувається розподіл зон відповідальності в інформаційному просторі між американськими спецслужбами;

– реінсталяція (2001 р. – дотепер) – особливістю цього етапу є формування нової парадигми національної безпеки, що ґрунтується на визнанні урядом повної залежності інфраструктури США від інформаційних систем і мереж та їхньої уразливості, надання захисту інформаційній безпеці набули пріоритетного значення у системі національної безпеки сучасних держав.

У сфері забезпечення інформаційної безпеки в США було розроблено кілька моделей, одна з яких передбачала створення

[324] Мединн А. Особенности применения киберсредств в межгосударственных военных и внутренних конфликтах // Зарубежное военное обозрение. – 2013. – № 3. – С. 11.

значної переваги США у знешкодженні систем захисту держави-супротивника засобами інформаційного впливу, координації дій із союзними державами з використанням інформаційної зброї для ідентифікації ймовірних джерел і множини типів потенційних загроз. Інша модель передбачала наявність у світі кількох держав-інфолідерів та рецесивного протиборства між ними, а в перспективі – забезпечення домінування США у сфері міжнародної інформаційної безпеки з можливостями значного впливу на глобальну інфосферу та верховного права участі у вирішенні проблем глобального світового порядку. Нині в США на практиці впроваджено модель, яка передбачає створення абсолютної системи захисту США, як світової держави-інфолідера, проти будь-якого виду наступальної інформаційної зброї, що обумовлює об'єктивні переваги в потенційній інформаційній війні, змушує інші держави шукати альянсу у військово-інформаційних діях з нею[325]. Тому, 17 травня 2011 р. Президент США Б. Обама підписав «Міжнародну стратегію розвитку кіберпростору», яка обґрунтувала правові основи створення єдиної системи державного забезпечення інформаційної безпеки під військовим командуванням. Цей документ визначив пріоритетні напрямки державної політики з протидії інформаційним загрозам.

Військова стратегія кіберкомандування у «Міжнародній стратегії розвитку кіберпростору» визначена як комплексна функція, що складається з:

- підготовки, координації, інтеграції, синхронізації дій по проведенню операцій та захисту інформаційних мереж МО США;
- проведення військових інформаційних операцій глобального масштабу з метою забезпечення дій ЗС США в усіх сферах;
- забезпечення свободи дій ЗС США та їх союзників в кіберпросторі;
- завдання удару та поразки інформаційним засобам супротивника.

У вересні 2018 р. президент США Д. Трамп ухвалив новий концептуальний документ – «National Cyber Strategy – Національна киберстратегия» (далі «Стратегія»). У ньому розкрити погляди американської адміністрації на виклики і погрози у цифровій сфері, принципи забезпечення інформаційної безпеки і організації протидії противнику в комп'ютерних мережах, основи всебічного захисту

[325] Конах В. Забезпечення інформаційної безпеки держави як складової системи національної безпеки (приклад США): автореф. дис. … на здобуття канд.. політ. наук : спец. 21.01.01 „Основи національної безпеки держави”. – К., 2005. – С. 6, 11.

інтересів країни, а також порядок вирішення загальнонаціональних і відомчих завдань в кіберпросторі. У «Стратегії» наголошується, що масштаби деструктивної мережевої діяльності останніми роками різко зросли. Кіберпростір перетворився в середовище стратегічного міждержавного суперництва, де основні загрози виходять від Росії та Китаю, які володіють «киберпотенціалом», який можна порівняти з американським. Отже, ті сили і засоби, що раніше застосовувалися до їх нейтралізації та захисту національних інформаційних систем, фактично визнаються малоефективними.

«Національна кіберстратегія» розроблена з врахуванням положень «Стратегії національної безпеки» 2017 р. і, на думку президента США Д. Трампа, є «першим за 15 років документом, де чітко сформульовані ключові напрями діяльності американських міністерств і відомств відносно мережевого середовища». Основними завданнями «Стратегії» визначено захист держави за рахунок забезпечення безпеки інформаційних мереж, систем і даних; підвищення безпеки і розвитку цифрової економіки, а також стимулювання американських інновацій; збереження міру за допомогою нарощування можливостей США по забороні суб'єктів, які використовують кіберзасоби в деструктивних цілях, і у разі потреби здійснення на них тиску (спільно з союзниками і партнерами); підвищення міжнародного впливу Вашингтона для просування основоположних принципів відкритого, сумісного, надійного і безпечного Інтернету[326].

Реалізація проголошених принципів військової стратегії у кіберпросторі відбувалася в процесі кардинального реформування організаційно-штатної системи ЗС США, оптимізації її функціонального призначення для вирішення завдань ведення кібервійни в сучасних умовах[327].

Створення сучасних органів управління бойовими діями у кіберпросторі та сил кібероперацій (СКбО) було розпочато у період організаційно-штатної реорганізації ***об'єднаного стратегічного командування (ОСК)*** **США**. У 2003 р. на ОСК були покладені завдання централізованого планування та ведення об'єднаннях

[326] Баталов А. Национальная киберстратегия США (2019) // Зарубежное военное обозрение. – 2019. – № 2. – С. 3–11.

[327] Шариков П.А. США хотят стать планетарным модератором. Американская глобальная стратегия развития киберпространства в полицентричном мире [Електронний ресурс] // Независимое военное обозрение. – 01.07.2011. – Режим доступу: http://pentagonus.ru/ publ/ amerikanskaja_globalnaja_strategija_razvitija_kiberprostranstva_v_policentrichnom_mire/19-1-0-1765

інформаційних операцій у ході яких ОСК повинне було вирішити наступні основні завдання:

- захист військових комп'ютерних мереж і систем від несанкціонованого доступу;
- забезпечення доступу до комп'ютерних мереж вірогідного супротивника та використання їх у власних інтересах;
- ведення РЕБ;
- проведення психологічних операцій військового характеру;
- розробка та здійснення заходів з реалізації планів військово-політичного керівництва США.

Для практичної реалізації визначеного комплексу завдань в структурі штабу ОСК було створено у 2003 р. ***управління інформаційних операцій***, а вже у 2004 р. воно було реформовано у ***функціональне командування інформаційних операцій (ФКІО)*** з розширенням кола завдань. До них входять:

- планування та проведення самостійних і спільних з федеральними органами США глобальних інформаційних операцій, які за своїми просторовими характеристиками виходять за межі повноважень одного зонального об'єднаного командування;
- координація планування ІО зональних об'єднаних командувань ЗС США у зонах відповідальності;
- розробка форм і способів протидії загрозам, які виникають, для систематичного та надійного функціонування інформаційних мереж Пентагону, у т.ч. за рахунок цілеспрямованого виводу із ладу комп'ютерних мереж вірогідного супротивника;
- розробка рекомендацій та організація психологічних операцій для дезінформації вірогідного супротивника;
- координація планування і проведення спеціальних операцій з застосуванням засобів РЕБ для вирішення завдань глобальних ІО.

Керівництво функціональним командуванням інформаційних операцій здійснює директор управління національної безпеки (УНБ) США.

Виконання цих завдань передбачало високий рівень координації зусиль на міжвідомчому рівні. З цією метою ОСК були оперативно підпорядковані *об'єднані центри (ОЦ) забезпечення захисту інформаційних мереж МО та сумісних інформаційних операцій ВПС*, які у рамках організаційно-штатної структури входили в ***оперативний центр забезпечення захисту інформаційних мереж (ОЦЗЗІМ).***

Функції ОЦЗЗІМ передбачали виконання наступних завдань:

- захист усієї інформаційної інфраструктури МО США від несанкціонованого доступу;

- організацію заходів із забезпечення доступу до аналогічних мереж супротивника при проведенні бойових операцій ЗС США;

- координацію ІО в інтересах забезпечення бойових дій ЗС у зонах конфліктів за допомогою груп планування ОЦЗЗІМ з метою забезпечення діяльності командувань з'єднань та об'єднаних оперативних формувань (ООФ) ЗС США.

Наступним етапом удосконалення організаційно-штатної структури та оптимізації функціонального призначення ОСК стало створення нових формувань, які у повному обсязі відповідали постійному зростанню ролі інформаційного протиборства у глобальному масштабі та були б здатні ефективно нарощувати свої можливості з вирішення завдань забезпечення інформаційної переваги ЗС США.

У період з січня 2005 р. по січень 2007 р. в структурі ОСК на базі ФКІО та ОЦЗЗІМ були створені ***командування бойових дій в інформаційних мережах (КБДІМ)*** та ***командування спільних інформаційних операцій (КСІО)***, а ОЦЗІМ був включений у склад ОСК.

Нова організаційна-штатна структура конкретизувала обсяг функцій нових підрозділів. Діяльність КБДІМ була спрямована на виконання таких завдань:

- систематичний моніторинг сфери використання інформаційних мереж Пентагону;

- своєчасне виявлення загроз та попередження про них інформаційним мережам МО;

- координація планування, розробки та проведення самостійних спільних з іншими функціональними командуваннями ОСК операцій в інформаційних мережах, які здійснюються в інтересах ОСК а також інших об'єднаних командувань ЗС США;

- розробка рекомендацій щодо складу сил і засобів інформаційних операцій (ІО);

- оперативне керівництво силами та засобами ведення операцій в інформаційних мережах.

Основними завданнями КСІО було визначено:

- координація між підрозділами та службами МО, федеральними агентствами і відомчими установами в інтересах проведення ІО єдиних сил;

- планування та проведення командуванням єдиних сил наступальних й оборонних інформаційних операцій;

- забезпечення бойових командувань інформацією, яка необхідна для організації планування операцій та даними про об'єкти інформаційно-комунікаційної інфраструктури супротивника;

- організація заходів з розвідувального забезпечення інформаційних операцій єдиних сил;

- участь у розробці стратегії, тактики та визначенню найбільш ефективних форм і методів проведення ІО;

- проведення аналітично-дослідної роботи з питань визначення ефективності ІО;

- збір, накопичення, узагальнення досвіду проведення ІО та розробка пропозицій щодо підвищення ефективності проведення ІО.

У новій структурі ОЦЗІМ були визначені такі стратегічні завдання:

- моніторинг, підтримання боєздатного стану та забезпечення захисту глобальної інформаційної мережі МО США;

- визначення необхідних сил і засобів ІО та координація їх розгортання;

- організацію взаємодії з об'єднаними командуваннями, федеральними міністерствами та відомствами США в інтересах вирішення завдань забезпечення безпеки інформаційних мереж МО.

Відповідно до рішення МО США від грудня 2008 р. ведення бойових операцій у кіберпросторі визначена як окрема функція ОСК, яка передбачала:

- планування і здійснення заходів, які спрямовані на виявлення та нейтралізацію загроз в кіберпросторі;

- координацію діяльності в кіберпросторі з іншими об'єднаними командуваннями (ОК) і відповідними федеральними міністерствами й агенціями;

- представлення інтересів МО США в федеральних органах, комерційних структурах, міжнародних організаціях з питань діяльності в кіберпросторі;

- розробку рекомендацій щодо складу сил і засобів основних компонентів ЗС США, які приймають участь в бойових діях у кіберпросторі;

- інтеграцію з ОК усіх заходів, які здійснюються в рамках міжнародної співпраці в галузі кібербезпеки;

- координацію розгортання сил і засобів в інтересах забезпечення дій в кіберпросторі та підготовка невідкладних рекомендацій МО США;
- розробку пропозицій з підвищення оперативних можливостей на ТВД у взаємодії з командуванням зональними ОК;
- ведення бойових дій в кіберпросторі.

У липні 2009 р. вищенаведений комплекс завдань ведення бойових дій в кіберпросторі був покладений на ***командування бойових дій у кіберпросторі (КБДКП)***, сформоване на основі КБДІМ і ОЦЗЗІМ. КБДКП стало основним органом управління бойовими діями в кіберпросторі в ЗС США.

Основними завданнями КБДКП є:

- забезпечення захисту інформаційних мереж МО США і національних розвідувальних структур;
- координація взаємодії профільних структур МО у сфері кібербезпеки;
- представлення інтересів МО на національному рівні з питань кібербезпеки;
- надання допомоги та участь у загальнонаціональних заходах, які проводяться під керівництвом федеральних національних структур з питань забезпечення кібербезпеки;
- оперативне управління силами і засобами ЗС для ведення бойових дій у кіберпросторі;
- координація планування, розробка та ведення розвідувальних, оборонних і наступальних операцій в кіберпросторі[328].

Система координації та організації діяльності ОСК містить отримання необхідної розвідувальної інформації від Управління національної безпеки (УНБ) і технічної підтримки від управління інформаційних систем (УІС) МО США. КБДКП через ***центр спільних операцій у кіберпросторі*** здійснює координацію та управління оперативно підпорядкованими військовими формуваннями і профільними структурами а також взаємодію з спеціалізованими федеральними відомствами.

У оперативному підпорядкуванні КБДКП ОСК є такі структурні компоненти видів ЗС США:

- командування бойових дій у кіберпросторі СВ ЗС США (2-а Польова армія);

[328] Тулин С. Органы управления ВС США боевыми действиями в кибернетическом пространстве // Зарубежное военное обозрение. – 2012. – № 2. – С. 3–10.

- командування бойових дій у кіберпросторі ВМС ЗС США (10-й оперативний флот);
- 24-а повітряна армія (бойових дій у кіберпросторі) ВПС;
- командування бойових дій у кіберпросторі морської піхоти;
- командування бойових дій у кіберпросторі берегової охорони.

Командування бойових дій у кіберпросторі СВ ЗС США є функціональним командуванням СВ ЗС США. Адміністративно воно підпорядковане штабу армії США, оперативно – ОСК ЗС США і є його сухопутною компонентою.

Основними завданнями Командування бойових дій у кіберпросторі СВ ЗС США є:

- захист комп'ютерних мереж і автоматизованих систем управління СВ глобальної інформаційно-управляючої мережі від несанкціонованого доступу;
- організація та проведення кібероперацій в інтересах СВ і ЗС США;
- забезпечення безпеки інформації в засобах обчислювальної техніки СВ;
- проведення досліджень у сфері ведення бойових дій в кіберпросторі, модернізація кіберзасобів, підготовка персоналу;
- реалізація проектів удосконалення функціонування комп'ютерних мереж і систем СВ.

Командування бойових дій у кіберпросторі ВМС ЗС США (10-й оперативний флот (ОФ)) є у складі основних командувань ВМС. Адміністративно підпорядковане начальнику штабу флоту США через його заступника з розвідки та інформаційної переваги. Оперативно підпорядковане КБДКП ОСК ЗС США та є його морською компонентою.

Основні функції командування:

- управління силами радіоелектронної розвідки і РЕБ ВМС США;
- організація зв'язку та забезпечення безпеки комунікаційних мереж;
- криптографічне забезпечення діяльності ВМС.

24-а повітряна армія (ПА) (бойових дій у кіберпросторі) ВПС є командно-штабною структурою, яка адміністративно підпорядкована космічному командуванню ВПС США, оперативно – КБДКП ОСК ЗС США та є його повітряно-космічною компонентою. Основними завданнями 24-ої ПА є:

- організація та проведення кібероперацій в інтересах ВПС і ЗС США;

- захист комп'ютерних мереж і глобальних систем зв'язку ВПС від несанкціонованого доступу;
- забезпечення безпеки інформації та цілісності комп'ютерних мереж ЗС США;
- підготовка спеціалістів для дій у кіберпросторі;
- підготовка пропозицій з переозброєння ВПС США новітніми апаратно-програмними засобами;
- розробка та реалізація проектів з удосконалення функціонування комп'ютерних мереж ВПС США.

Командування бойових дій у кіберпросторі морської піхоти є функціональним елементом системи організації бойових дій виду ЗС США та адміністративно підпорядкована коменданту морської піхоти США. Оперативне підпорядкування здійснюється керівництвом КБДКП ОСК ЗС США. Основними завданнями командування бойових дій у кіберпросторі морської піхоти є:

- ведення бойових дій у кіберпросторі під оперативним керівництвом КБДКП ОСК в інтересах вирішення завдань оперативних формувань морської піхоти (МП);
- забезпечення захисту та надійного функціонування єдиної комп'ютерної мережі МП;
- інтеграція можливостей глобальної інформаційної мережі національних ЗС в інтересах вирішення завдань оперативних формувань МП;
- криптографічне забезпечення діяльності МП.

Командування бойових дій у кіберпросторі берегової охорони знаходиться на стадії формування. Визначено такі основні функціональні завдання, які будуть покладені на структуру:

- захист комп'ютерних мереж та АСУ від несанкціонованого доступу;
- проведення ІО різного масштабу;
- забезпечення безпеки інформації;
- реалізація проектів удосконалення функціонування комп'ютерних систем і мереж.

Слід зазначити, що з 2017 р. система управління бойовими діями в кіберпросторі зазнала принципових змін – Президентом США Д. Трампом було прийнято рішення про виведення Кіберкомандування із підпорядкування ОСК[329]. Отже, Кіберкомандування поставлено на один ієрархічний рівень з 6-ма регіональними та 3-ма

[329] Statement by President Donald J. Trump on the Elevation of Cyber Command https://www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/

функціональними (Стратегічним, Транспортним, Спецоперацій) командуваннями. Процес оформлення самостійного функціонального командування тривав з 10.08.2017 р. по 04.03.2018 р. Питання найскорішого введення командування у боєздатний стан було вирішення шляхом координації його функцій з Агенцією національної безпеки. У травні 2018 р. головою Кіберкомандування був призначений генерал П. Накасоне.

Перспективною моделлю формування нової системи управління, за планами МО США є створення зональних центрів із забезпечення дій в кіберпросторі в штабах об'єднаних командувань ЗС США. Це дозволить удосконалити взаємодію з центром спільних операцій, уникнути появи зайвих ланок управління і збільшити швидкість проходження потоків усіх видів інформації в кіберпросторі в межах відповідальності зональних командувань.

Загальними рисами СКбО ЗС США є:

- координація та уніфікація завдань в інтересах держави та збройних сил;
- конкретизація цілей для кожного виду збройних сил, обумовлених специфікою його бойового призначення;
- систематизований порядок адміністративного та оперативного підпорядкування та взаємодії;
- наявність потужних оперативних об'єднань в складі видових СКбО ЗС США.

Слід зазначити, що організаційно-штатна структура СКбО постійно динамічно оновлюється і модернізується та оперативно реагує на зміни у характері бойових дій в кіберпросторі. Так, у 2013 р. МО США додатково створило 30 спеціальних груп для захисту інформаційних систем федерального уряду, національної інфраструктури та ЗС США від кібернападу. Основним завданням цих груп є створення системи активного кіберзахисту, розвідка планів і задуму супротивника та миттєва адекватна реакція на них. 13 груп працюють безпосередньо для захисту кіберпростору США та дислокуються за кордонами країни, у місцях безпосередньої кіберзагрози. 17 груп задіяні безпосередньо для захисту інформаційних систем і баз даних Пентагону[330].

Кібервійська ЗС США є ефективним інструментом захисту як власного кіберпростору, так і потужною силою для здійснення кібератак у глобальному інформаційно-комунікаційному просторі. За даними газети «Вашингтон Пост» від 31.08.2013 р., у 2011 р. було

[330] Защита киберпространства США // Зарубежное военное обозрение. – 2013. – № 5. – С. 105.

проведено 231 комп'ютерну атаку, дій три чверті яких були спрямовані на інформаційно-комунікаційні системи Росії, Ірану, КНР і КНДР. Основною метою кібератак було зараження вірусами комп'ютерних систем ядерних програм[331]. 27 червня 2013 р. голова Комітету начальників штабів ЗС США адмірал М. Демпсі зазначив, що упродовж 2011–2013 рр. інтенсивність кібератак на інформаційно-комунікаційну структуру США збільшилась у 17 разів.

З метою мінімізації кіберзагроз до 2017 р. планується використати на кібербезпеку 23 млрд дол. і збільшити штат відповідних структурних підрозділів до 4 тис. осіб[332]. На 01.01.2017 р. за даними кампанії Zecurion щорічні затрати США на кібербезпеку складають $7 млрд на рік, а чисельність кібербійців налічує 9 тис. осіб[333].

Процес формування в ЗС США СКбО обумовлений потребою створення необхідного підрозділу, який здатен виконувати завдання у такій специфічній сфері збройної боротьби, як кіберпростір.

Одним із напрямків діяльності в інтересах зростання цього потенціалу є активне залучення СКбО до заходів оперативної та бойової підготовки ЗС США, активне використання нових форм, методів і способів бойового застосування в різних видах військових дій ЗС, у тому числі – в інформаційних та повітряно-космічних операціях.

Головні зусилля в заходах оперативної та бойової підготовки із залученням СКбО спрямовані на:

- практичне відпрацювання методик і варіантів переводу СКбО з мирного на воєнний стан;
- організацію дій в умовах воєнного часу з урахуванням особливостей підпорядкування СКбО;
- моделювання різних станів військово-стратегічної обстановки;
- вибір варіантів застосування СКбО в усіх фазах військового конфлікту;
- моделювання кібероперацій для вивчення способів та специфіки впливу на інформацію, об'єкти мережевої інфраструктури та органи управління супротивника;
- оцінку ефектів і наслідків для супротивника та власних ЗС;

---

[331] Американские кибератаки // Зарубежное военное обозрение. – 2013. – № 9. – С. 104.

[332] Председатель КНШ ВС США о защите военных компьютерных сетей // Зарубежное военное обозрение. – 2013. – № 8. – С. 105.

[333] Лещев В. Названы самые боеспособные страны в киберпространстве [Електронний ресурс] / LIFE.RU. 10 января 2017. – Режим доступу: https://life.ru/t/%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B8/957102/nazvany_samyie_boiesposobnyie_strany_v_kibierprostranstvie

- перевірку реалізації способів боротьби у кіберпросторі в умовах автоматизації управління ЗС та активної протидії супротивника;

- оцінку бойових можливостей кібероперацій та перспектив їх інтеграції з можливостями наземного, морського, повітряно-космічного компонента для досягнення ефекту синергії при проведенні усього спектру військових операцій[334].

З 2012 р. Міністерство оборони Сполучених Штатів Америки приступило до підготовки фахівців з «Програми навчання офіцерів ВС США веденню розвідки в кіберпросторі» (Army Intelligence Development Program – Cyber). Завдання щодо забезпечення навчального процесу за цим напрямом покладені на 780-у бригаду військової розвідки США (Форт-Мід, штат Меріленд).

Практичне навчання офіцерів орієнтується на формування розуміння ролі і місця кіберрозвідки в діяльності ЗС США, інших державних структур, а також в ході організації міжвідомчої взаємодії. При цьому основна увага приділяється викладанню універсальної для всіх відомств базової моделі розвідувально-інформаційного забезпечення операцій, що включає чотири послідовних блоки: 1) вивчення операційного простору; 2) аналіз впливу зовнішніх чинників на операцію; 3) визначення можливих загроз цілям операції; 4) оцінка ефективності результатів проведення операції[335].

Визначним завданням для ЗС США є створення та забезпечення функціонування єдиного інформаційно-комунікаційного простору (ЄІКП) на основі концепції «Ведення бойових дій в єдиному інформаційно-комунікаційного просторі». На стратегічному рівні завдання формування ЄІКП вирішується у межах ідеї створення Глобальної інформаційної мережі (ГІМ) МО США (Global Information Grid). Вона ґрунтується на трьох концепціях – мережевих операції, мережевого управління та управління спектром і розподілу даних[336].

Комплексний аналіз умов, засобів і методів перспективного розвитку форм бойових дій майбутнього відображений у доповіді Об'єднаного командування єдиних сил 2010 р., де до прогнозованих загроз ЗС США у стратегії до 2030 р. зараховано можливість

[334] Мелин А. Система подготовки Вооружённых сил США с участием сил кибероперацій // Зарубежное военное обозрение. – 2012. – № 5. – С. 20–24.
[335] Филенков А. Обучение офицеров ВС США ведению разведки в киберпространстве // Зарубежное военное обозрение. – 2019. – № 1. – С. 24–26.
[336] Московитов Н. Перспективы создания Глобальной информационной сети МО США // Зарубежное военное обозрение. – 2013. – № 7. – С. 8.

перетворення Космосу та кіберпростору на новий театр для військового протиборства[337].

Таким чином, ЗС США активно готуються до ведення широкомасштабних новітніх кібервійн у глобальному інформаційному просторі майбутнього. У ЗС США створена ефективна структура сил кібероперацій. Система оперативного й адміністративного управління СКбО постійно удосконалюється, про що свідчить як практика дій усіх видів ЗС США, так і концептуальні розробки командування армії США.

Одночасно, США намагаються посилити кібербезпеку (а точніше, організувати оборону в кіберпросторі) через підтримання співпраці та співробітництва з міжнародними інститутами забезпечення колективної безпеки. Результатом активної діяльності розвинених світових держав стало прийняття Комітетом міністрів Ради Європи у листопаді 2001 р. Конвенції Ради Європи про кіберзлочинність. Конвенцію підписали 46 країн, ратифікували – 30 (Україна – у 2006 р.), у тому числі неєвропейські країни – США, Канада, Японія, Мексика, ПАР, Філіппіни, Чилі, Коста-Ріка, Домініканська Республіка та ін. Ані Росія, ані Китай досі не згодні приєднуватися до Конвенції.

Великобританія (потенціал якої в сфері кіберзахисту вважається одним з найпотужніших) продовжує активно розбудовувати та модернізовувати власні сили безпеки у кіберпросторі. У 2010 р. розпочав інтенсивно діяти новостворений Оперативний центр з кібербезпеки (у штаті 20 співробітників) виконуючи функцію координації множини вже існуючих центрів із кібербезпеки багатьох відомств й створення поля для співпраці між урядом і цивільним суспільством (приватним сектором) із забезпечення інформаційної безпеки у глобальному кіберпросторі. Окрім того, у Великобританії ефективно працює Командування урядових комунікацій (Government Communications Headquarters), що забезпечує як захист критично важливої урядової інформації, так і отримання розвідувальних даних за допомогою новітніх комунікативних засобів.

У 2013 р. розпочався процес формування кіберсил Великобританії. У відповідності до «Стратегії Кібербезпеки З'єднаного Королівства» була створена Міжвидова кібергрупа (Joint Forces Cyber Group), яка займається плануванням та координацією кібероперацій. У структуру цього формування входять

[337] Николаев Н. Взгляды военно-политического руководства США на ведение вооруженной борьбы в современных условиях // Зарубежное военное обозрение. – 2014. – № 3. – С. 3–4.

кіберпідрозділи Центру урядового зв'язку, що виконує функції радіоелектронної, мережевої розвідки та шифрування, кіберрезервісти, інформаційна служба.

Додатково у 2016 р. Великобританія створила Національний центр кібербезпеки в складі Центру урядового зв'язку. Тобто, Великобританія комплексно використає можливості Центру не лише для кіберзахисту цивільної, але й військової інформаційно-технічної інфраструктури.

На початку 2016 р. в Збройних силах **ФРН** була розпочата активна фаза створення нового роду військ – кібервійськ. Літом 2016 р. Міністерством оборони ФРН була розроблена концепція кібербезпеки на основі якої був сформований міжвидовий компонент Kommando Cyber-und Informationsraum CIR (сили кібероперацій та інформаційного забезпечення (СКІЗ) (м. Бонн, 260 осіб персоналу, штатна категорія командувача (інспектора) – генерал-лейтенант).

Головною метою проведених оргштатних заходів є організація та координація компонентів централізованого управління для вирішення наступних завдань:

- збір, обробка, аналіз відомостей про вірогідного супротивника;
- організація кібератак проти органів державного та військового управління, об'єктів критичної інфраструктури держав-супротивників;
- картографічне забезпечення збройних сил;
- проведення інформаційних операцій з метою пропаганди своїх успіхів і дезінформації супротивника;
- радіоелектронна боротьба;
- захист інформаційних ресурсів бундесверу;
- забезпечення надійного, стійкого та прихованого функціонування систем управління, у тому числі й систем зв'язку.

У 2016 р. в структурі центрального апарату міністерства оборони створено головне управління кібероперацій та інформаційного забезпечення (130 осіб, штатна категорія начальника – генерал-лейтенант). Військово-адміністративний орган призначений для вирішення завдань правового унормування дій бундесверу в кіберпросторі, прийняття рішення на застосування підлеглих сил і засобів, розробки концепцій і стандартизації проектів, які пов'язані з інформаційними технологіями і геоінформаційними системами, здійснення надзору за підприємствами, які реалізують проекти у цієї галузі в інтересах військового відомства.

Склад підрозділів налічує приблизно 15 тис. військовослужбовців і цивільних працівників бундесверу, які спеціалізуються на інформаційній безпеці. З метою підготовки фахівців з проведення кібероперацій та захисту інформації в університеті бундесверу (м. Мюнхен) у 2018 р. створена профільна кафедра яка забезпечує навчання до 70 слухачів на рік. Повноцінне функціонування нового роду військ заплановане на 2021 р.[338].

Особливостями організаційно-штатної побудови кібервійськ ФРН є функціонування як окремого роду військ і розширений функціонал: крім проведення кібероперацій покладені завдання захисту інформації, кібербезпеки, радіоелектронної безпеки, картографії та зв'язку.

Пріоритетні напрями **Франції** в організації кібербезпеки були окреслені в «Білих Книгах» 2008, 2013 рр. Згідно визначеної стратегії, у грудні 2016 р. було проголошено про створення кіберкомандування Франції. Орієнтовні терміни визначені 2019 р.

Організаційно-штатна структура кіберкомандування включає чотири відділи: відділ захисту комп'ютерних мереж, центр аналізу оборонної тактики, відділ наступальних операцій та резервний підрозділ. Питання координації зусиль покладені на штаб Об'єднаного командування комп'ютерного управління під керівництвом віце-адмірала А. Костил'є. Структурно кібервійська підпорядковані безпосередньо начальнику штабу армій. На 2019 р. чисельність фахівців, що будуть займатися питаннями кіберзахисту варіюється від 2600 до 4600. Фінансові витрати за п'ять років на створення нової інфраструктури складуть 2,1 млрд євро.

Основне завдання нового роду військ полягатиме у відбитті ймовірних загроз з боку держав, які мають кібервійська.

Також кіберкомандування має на меті здійснювати збір інформації про ідентифікацію слабких місць інформаційних мереж і виявленням недружніх дій у кіберпросторі. На новий рід військ покладені завдання забезпечення захисту від інформаційної агресії та проведення наступальних інформаційних операцій[339].

Особливістю побудови французької моделі є створення вузькоспеціалізованої структури вищого стратегічного рівня.

5 лютого 2019 р. оголошено початок створення власних кібервійськ у ЗС **Польщі.** Впродовж цього року у Війську

[338] Круглов Д. Силы кибероперацій и информационного обеспечения бундесвера (2017) // Зарубежное военное обозрение. – 2017. – №7. – С. 23–25.

[339] Во Франции в 2017 году появятся кибервойска [Електронний ресурс] // Коммерсант. 13/12/16 21:38. – Режим доступу: https://novostipmr.com/ru/news/16-12-13/vo-francii-v-2017-godu-poyavyatsya-kibervoyska

Польському будуть створені перші підрозділи боротьби з кіберзагрозами та захистом віртуального національного кіберпростору. За задумом голови Міноборони Польщі нова структура діятиме як інтегративний складник між існуючим Центром криптології та інспекторами інформатики. Планується завершити формування кібервійськ упродовж 2020 р. Підготовка кадрів для нового роду військ здійснюватиметься у Військової технічної академії. З цією метою при академії планується відкрити спеціальний ліцей інформатики[340].

Активну позицію з протидії кіберзагрозам обстоює і провідна міжнародна безпекова організація – НАТО (Cooperative Cyber Defence Centre of Excellence). Інтенсифікація процесів створення кібервійськ країнами **НАТО** логічно висуває на перший план питання координації зусиль в межах цього військово-політичного блоку.

У червні 2010 р. група експертів під керівництвом М. Олбрайт запропонувала трактувати масштабні кібератаки як такі, що підпадають під п'яту статтю Північноатлантичного договору та вважаються атаками на всіх членів Альянсу[341]. Тому за даними агентства Reuters «новий військовий командний центр НАТО з протидії комп'ютерним хакерам повинен бути повністю укомплектований до 2023 р.». До роботи у центрі планується залучити 70 експертів, які будуть представляти інформацію військовій розвідці про хакерів злочинних груп ворожих держав.

У липні 2016 р. на саміті НАТО в Варшаві кіберпростір був визнаний сферою операцій, аналогічно традиційних сфер взаємодії. У лютому 2017 р. був прийнятий оновлений План кібероборони з визначенням орієнтирів освоєння кіберпростору як нової сфери операцій. 8 листопада 2017 р. на засіданні НАТО на рівні міністрів оборони було ухвалено рішення про створення Центра кібероперацій[342].

Посилена увага до забезпечення кібербезпеки та створення засобів ведення кібервійни, ставить перед урядами держав завдання перегляду внутрішньої політики в кіберсфері та концепцій воєнної політики. Такі тенденції обумовлені появою випадків використання розвідувальними службами та спеціалізованими військовими підрозділами держави можливостей і технічних потужностей

[340] Польша создает кибервойска [Електонний ресурс] // REGNUM. 5 февраля 2019, 20:43. – Режим доступу: https://regnum.ru/news/polit/2566806.html

[341] Дубов Д.В. Кібербезпека: світові тенденції та виклики для України. – К., 2011. – С. 4.

[342] Карасев П. Кибервойска Европы и НАТО // «Expert Online». – 2019.20.02. – Режим доступу: http://expert.ru/2018/03/13/kibervojska-evropyi-i-nato/

транснаціональних кримінальних груп, що спеціалізуються у сфері кіберзлочинності. Це спричинює зміни у політиці провідних держав світу стосовно застосування нормативно-правових механізмів обмеження та цензури, як однієї із форм реалізації внутрішньої інформаційної політики. Отже, НАТО офіційно визнала кіберпростір у якості нового рубежу, який потрібно захищати на одному рівні із сухопутним, повітряним і морським[343].

Загальносвітові тенденції створення національних формувань кіберзахисту притаманні й державам Азіатсько-Тихоокеанському регіону.

У Народно-Визвольній армії **Китаю** (НВАК), за оцінками окремих фахівців, створені кращі у світі моделі чи системи кібервійськ. Але, найвищий рівень закритості інформаційного простору держави та високий гриф таємності інформації, не дають можливості детально проаналізувати організаційно-штатну структуру та її функціональне призначення. Разом з тим, 31 грудня 2015 р. КНР проголосила про створення нового роду військ захисту інформаційного простору. Впродовж 2016 р. йшло формування кібервійськ НВАК. Характерною особливістю застосування кібервійськ є взаємодія з військами РЕБ. Це дозволить контролювати одночасно віртуальний і електромагнітний простір на полі бою.

За фрагментами доступної інформації за ведення інформаційної війни і забезпечення інформаційно-психологічного захисту військ відповідає Головне Політичне управління НВАК. Координацію зусиль з організації інформаційного протиборства у комп'ютерних мережах здійснює управління РЕБ ГШ НВАК. Йому підпорядковані центри, які вивчають можливості доступу до комп'ютерних мереж супротивника та захисту власної мережевої інфраструктури, частини РЕБ та зв'язку центрального та окружного підпорядкування, що взаємодіють з частинами психологічних операцій. З 2006 р. при управлінні зв'язку ГШ НВАК діє структурний підрозділ з підготовки та ведення інформаційної війни. До нього входять:

- Ханкоуський навчальний центр – відпрацювання форм та методів інформаційної війни;
- лабораторія ведення інформаційної війни – дослідження в галузі розвідки, РЕБ, протиборства в комп'ютерних мережах, психологічних воєн і деструктивного інформаційного впливу;

[343] Киберкомандование НАТО полностью закончит формироваться в 2023 году [Електронний ресурс] // УКРИНФОРМ 16.10.2018. – Режим доступу: https://www.ukrinform.ru/rubric-technology/2559824-nato-sformiruet-sobstvennye-kibervojska-v-2023-godu.html

-лабораторія забезпечення безпеки інформації – дослідження особливостей застосування спеціальних і технічних засобів.

Фундаментальні дослідження у галузі інформаційної війни проводить Академія військових наук НВАК.

Китайські військові експерти зараховують до організаційно-штатна структури кібервійськ підрозділи комп'ютерної розвідки і контррозвідки, електронно-вірусних атак, антивірусного захисту та захисту від інших видів впливу на електронно-обчислювальну техніку[344].

На основі фрагментарної інформації можна визначити такі характерні риси організації діяльності кібервійськ НВАК:

1. Зосередження уваги на наступальному превентивному призначенні ІО. Головним елементом кіберстратегії Китай обрав доктрину «асиметричного стримування» при нанесенні «прихованого удару».

2. Високий рівень професійної підготовки персоналу. За даними експертів загальна чисельність китайської кіберармії приблизно 6 тис. хакерів. Близько 20 тис. ІТ-фахівців працюють на китайські спецслужби. Вони потенційно здатні забезпечити захист вітчизняних життєво важливих об'єктів і нанести превентивний удар по супротивнику. За даними ФБР, КНР на сьогоднішній день має армію з 180 000 хакерів, які щоденно атакують кібермережі США, лише у 2009 р. було здійснено близько 90 тис. атак на комп'ютери Міністерства оборони США. З 180 тис. хакерів 30 тис. є військовими, а 150 тис. – комп'ютерні цивільні експерти (працівники приватних компаній, що залучаються до виконання військових чи розвідувальних завдань в кіберпросторі), місією яких є отримання доступу до військових і комерційних секретів США та спричинення безладу в діяльності урядових і фінансових служб[345].

3. Концентрація кібератак несанкціонованого входу в інформаційні системи США з метою отримання необхідної політичної, військової та економічної інформації. У 2003 р. була здійснена серія кібератак, яка отримала назву «титановий дощ». Були зламані ресурси корпорації «Локхід Мартін», національної лабораторії ядерного дослідного центру «Сандія», ракетно-космічного центру та комп'ютерні мережі НАСА. Унаслідок організованої кібератаки була викрадена секретна технічна

[344] Кировец А. Органы пропаганды и информационной войны КНР // Зарубежное военное обозрение. – 2013. – № 9. – С. 28–33.

[345] China's Secret Cyberterrorism [Електронний ресурс]. – Режим доступу: http://www.thedailybeast.com/blogs-andstories/2010-01-13/chinas-secret-cyber-terrorism/full

документація винищувача-бомбардувальника 5-го покоління F-35 (приблизна вартість проекту – $300 млрд). У 2007 р. китайські хакери здійснили вдалі кібератаки на електронну пошту міністра оборони США, комунікаційні мережі Пентагону Державного департаменту США, міністерства фінансів, енергетики та торгівлі. Унаслідок чого стався масштабний витік інформації[346] Постановка задач для кібервійськ НВАК була конкретизована в «Основах бойової підготовки та оцінок», які почали діяти з 2009 р., вони передбачають:

- навчання та підготовку НВАК до проведення міжвидових військових операцій;
- формування у особового складу знань, навичок та вмінь, необхідних для ведення бойових дій в умовах мережевих центричних війн із застосуванням високотехнологічних інформаційних й засобів інформаційної протидії;
- виведення із ладу інфраструктури управління супротивника з одночасним захистом власних інформаційно-управляючих систем[347].

Практична реалізація завдань відбувається під час проведення спеціальних кібернетичних навчань, а саме:

- удосконалення бойового застосування спеціальних підрозділів, армійської авіації, сил РЕП в умовах війни із застосуванням інформаційних технологій;
- відпрацювання сценарію «безконтактного нападу» – комплексного застосування кібервійни, радіоелектронної війни та дій розвідки;
- взаємодії різнорідних сил, ВВНЗ при загрозі масштабної кібервійни[348]. За даними видання The Daily Beast, ФБР підготувало секретний звіт, у якому відображено рівень розвитку кібервійськ КНР та наголошено на загрозах цього підрозділу для США. Звіт називає КНР «найбільшою цілісною загрозою США у сфері кібертероризму та силою, що вже зараз може володіти потенціалом, потрібним для знищення життєво важливої інфраструктуру, отримання доступу до секретних банківських, комерційних, військових та оборонних баз даних»[349].

За думкою західних експертів кібервійська **Корейської Народної Демократичної республіки (КНДР)** за своїм потенціалом та

[346] Дергачев В. Силовые возможности Китая [Електронний ресурс] // Независимое военное обозрение. – 29.11.2013. – Режим доступу: http://prpk.info/articles/armija-i-oruzhie/silovye-vozmozhnosti-kitaja

[347] Шлындов А. Минобороны в поиске интеллектуалов [Електронний ресурс] // Независимое военное обозрение. – 29.06.2012. – Режим доступу: http://nvo.ng.ru/forces/2012-06-29/ 11_minoborony. html

[348] Киберучения НОАК // Зарубежное военное обозрение. – 2013. – № 6. – С. 86–87.

[349] China's Secret Cyberterrorism [Електронний ресурс]. – Режим доступу: http://www.thedailybeast.com/blogs-andstories/2010-01-13/chinas-secret-cyber-terrorism/full

чисельністю (6–7 тис.) можуть бути порівняні з кібервійськами ЗС США. Аналітики поділяють кібервйська Північної Кореї на чотири групи: Stardust Chollima спеціалізується на комерційних атаках; діяльність Silent Chollima спрямована на нейтралізацію ЗМІ та державних установ, насамперед північнокорейських; Labyrinth Chollima протидіє операціям спецслужб; Ricochet Chollima займається несанкціонованим збором персональних даних.

Характерною особливістю організації атак і захисту кібервійськами КНДР є унікальність внутрішньополітичної ситуації в країні. Так самоізоляція Північної Кореї зводить нанівець усі спроби побудови ефективної стратегії протидії кібератакам Пхеньяна. Одночасно обмеження доступу КНДР до світовій мережі не впливає на організацію роботи північнокорейських хакерів, які розсіяні по всьому Південно-Східному регіону та можуть здійснювати атаки з будь-якого місця, де є доступ до Інтернету[350].

У 2014 р. відбулося урочисте представлення першого в історії **Японії** кібер-військового підрозділу, що був створений Міністерством оборони держави для боротьби з кібератаками на мережі міністерства та частини Сил самооборони країни. У складі підрозділу – 90 фахівців високого рівня кваліфікації. Він підпорядкований безпосередньо міністерству оборони. Підрозділ працюватиме цілодобово, постійно перебуватиме у стані підвищеної бойової готовності, щоб миттєво реагувати на загрози національній безпеці Японії. Серед основних обов'язків ІТ-військ будуть виявлення і блокування загроз від іноземних держав, на військові й промислові цифрові мережі, а також захист від хакерських атак комунальної та соціальної інфраструктур держави[351].

Існують особливості організації діяльності силових структур з питань кіберзахисту в країнах Близького Сходу.

У Армії Оборони **Ізраїлю** (ЦАХАЛ) діють спеціальні підрозділи для ведення інформаційної війни в кіберпросторі[352].

В Ізраїлі досвід здійснення вдалих інформаційних операцій під час ізраїльсько-арабських збройних конфліктів, дав можливість створити досить потужну систему інформаційно-пропагандистської роботи, функціонування якої забезпечують такі структури:

---

[350] Смирнов В. Лучшие кибервойска в мире сейчас у КНДР (возможно) [Електронний ресурс] / CHANNEL4IT. 16 июля, 2018. – Режим доступу: http://channel4it.com/publications/Luchshie-kibervoyska-v-mire-seychas-u-KNDR-vozmozhno-31131.html#

[351] СєйТВ. Японія створила кібервійська [Електронний ресурс]. – Режим доступу: http://say.tv/day_block2/topic/14273

[352] Гула Р.В., Вітринська О.В. Кібер-Цахал проти кібер-джихаду // Історичні студії суспільного прогресу. – 2018. – Вип. 6. – С. 46–53.

- відділ пропаганди при Міністерстві закордонних справ;
- відділ пропаганди при управлінні міжнародних відносин збройних сил країни;
- інформаційно-аналітичний відділ та відділ соціально-психологічних досліджень Головного штабу збройних сил Ізраїлю;
- управління військових рабинів збройних сил Ізраїлю;
- бюро пропаганди, яке координує дії єврейської діаспори;
- місцеві та закордонні засоби масової інформації;
- Інтернет ресурси[353].

Ця система інформаційно-пропагандистської роботи дозволяє державним структурам Ізраїлю досить успішно вирішити цілий комплекс завдань, а саме:

- сформувати негативний імідж руху ХАМАС як агресора та показати Ізраїль, як країну, яка вимушена давати адекватну відповідь агресору під час боротьби з тероризмом;
- досягнути суттєвого ослаблення ХАМАСу з боку країн-лідерів регіону та своїх ключових союзників;
- попередити і мінімізувати прогнозовану негативну реакцію в світі на наслідки можливих контртерористичних операцій ЦАХАЛу з неминучими жертвами серед мирного населення та зруйнуванням інфраструктури об'єктів ведення бойових дій.

У останнє десятиріччя досягнення цих результатів все частіше відбувається у площині комп'ютерних мереж. Наприклад, під час операції «Литий свинець» (ізраїльська військова операція в Секторі Газа (27.12. 2008 – 18.01.2009) метою якої ставилося знищення військової інфраструктури правлячого в Газі ісламського радикального руху ХАМАС) інтернет-ресурси ХАМАСу вивели з ладу низку ізраїльських фірм, які пов'язані із високими технологіями, телекомунікаціями, електронної комерцією, а також ЗМІ та медичні заклади. На деякий час були навіть заблоковані сайти міністерства оборони і зовнішніх справ.

У відповідь хакери Ізраїлю заблокували майже 50 сайтів руху «Хезболла», міністерства сільського господарства Ірану, торговельних компаній Йорданії та Лівану, які були пов'язані з діяльністю ХАМАСу. Відносно пропалестинських російсько-, англо-, арабомовних сайтів була спланована вдала кібератака ізраїльських хакерів.

[353] Певцов В. Информационное противостояние организации ХАМАС и Израиля в новом тысячелетии // Зарубежное военное обозрение. – 2013. – № 6. – С. 30.

Реальність і масштабність інформаційних загроз національній безпеці держав у сучасному глобальному інформаційно-комунікаційному середовищі зумовили створення спеціалізованих підрозділів у правоохоронних органах і збройних силах країн, так званих кібервійськ[354].

У 2012 р. були вперше відкрити курси з кіберзахисту для офіцерів ЦАХАЛу. Інтенсифікований навчальний процес включав 13-годинний навчальний день і два заліки щодня. З метою відпрацювання навичок фахівці створили для курсантів ізольовану комп'ютерну мережу. Вже на початок 2013 р. Армія Оборони Ізраїлю подвоїла кількість офіцерів у структурах, які на той час займалися питаннями кіберзахисту[355].

За інформацією з відкритих джерел у ЦАХАЛі з 2013 р. було проголошено про початок процесу створення спеціальних підрозділів кібератак і кіберзахисту. Ізраїльський веб-сайт «Курсорінфо» від 16 липня 2013 р. інформував своїх читачів, що начальник генерального штабу Армії Оборони Ізраїлю генерал-лейтенант Г. Айзенткот наказав сформувати новий вид військ, який буде займатися веденням кібервійни і відбиттям кібератак противника. Паралельно голові військової розвідки Х. Халеві було наказано визначити напрями дій кібервійськ в оборонній і в наступальній сфері. Новий рід військ планувалося сформувати поетапно впродовж двох років[356].

Організаційне будівництво нових структур кіберзахисту було розпочато після заяви прем'єр-міністра Ізраїлю Б. Нетаніягу в червні 2013 р. про створення Національної цільової кібернетичної групи для захисту життєво важливих об'єктів інфраструктури Ізраїлю[357]. Вже у серпні 2013 р. армія взяла на службу близько 300 молодих комп'ютерних фахівців, причому багато хто з них не закінчив коледж або не мав повної шкільної освіти, але в той же час вони були визнаними фахівцями у сфері комп'ютерних технологій. Новобранці проходили службу в підрозділі військової розвідки 8200, а також в Управлінні командування, контролю, зв'язку, комп'ютерів і розвідки С4І. Власне на базі цих двох підрозділів було розпочато процес створення кібервійськ ЦАХАЛу. Ключовим завданням кібервійськ

[354] Інформаційна війна і національна безпека: монографія / П.П. Ткачук, Р.В. Гула, О.І. Сивак та ін. – Львів, 2015. – С. 219.

[355] ЦАХАЛ усиливает киберзащиту [Електронний ресурс] // jewish.ru. 13.01. 2013. – Режим доступу: https://jewish.ru/ru/news/articles/158611/. – Назва з екрану

[356] Начальник генштаба ЦАХАЛа приказал начать формирование кибервойск [Електронний ресурс] // Cursorinfo. – Режим доступу: https://cursorinfo.co.il/. – Назва з екрану.

[357] Йак И. Израиль успешно противостоит врагу в киберпространстве [Електронний ресурс] // 7 канал, 10.06.2013. – Режим доступу: https://www.7kanal.co.il/News/News.aspx/160803. – Назва з екрану.

стало підвищення рівня оборони Ізраїлю та координація розробки нового програмного забезпечення між армією й ізраїльськими компаніями сектора високих технологій[358].

Але вже на початку 2017 р. начальник генерального штабу Армії Оборони Ізраїлю генерал-лейтенант Г. Айзенкот прийняв рішення не створювати новий вид військ, який буде відповідати за кібербезпеку. На цей час відповідальність за управління та координації дій кіберзахисту збройних сил Ізраїлю покладена на Управління зв'язку та кіберзахисту Генерального штабу ЦАХАЛу, а за атакуючі дії на кіберфронті відповідає розвідувальне управління (АМАН)[359].

Тому побудова системи кіберзахисту Армії Оборони Ізраїлю відбувається на основі створення структурних підрозділів видів військ і включення елементів кіберзахисту армії до єдиної державної інформаційно-технічної інфраструктури.

У грудні 2017 р. був сформований окремий напрям кіберзахисту в складі Сухопутних військ. Новий підрозділ входив до організаційно-штатної структури відділу зв'язку штабу Сухопутних військ. Завданнями напряму кіберзахисту визначено забезпечення захисту всіх видів озброєння та військової техніки Сухопутних військ, що мають комп'ютерні системи, від взлому або захоплення контролю. Напрям кіберзахисту складається з 4 секторів, які відповідають за розробку засобів захисту, впровадження їх у бойову техніку та розробку планів розвитку. Кадрове забезпечення здійснене за допомогою фахівців Головного управління зв'язку Головного Штабу, в тому числі управління захисних систем, різних комп'ютерних підрозділів[360] та бази підготовки – школи комп'ютерних професій «БИС ля-Макциот ха-Махшев». Основною формою бойового навчання структур кіберзахисту ЦАХАЛу є навчання та тренування відбиття можливих інформійно-технічних атак зі сторони ворога[361].

За планами ізраїльського політичного керівництва структури кіберзахисту Армії Оборони Ізраїлю тісно взаємодіють із компонентами єдиної державної системи боротьби з кібертероризмом. 15 лютого 2015 р. на щотижневому засіданні уряду

---

[358] ЦАХАЛ формирует новые кибер-войска [Електронний ресурс] // Mignews. – Режим доступу: http://mignews.com/news/130112_104545_00238.html. – Назва з екрану.

[359] Начгенштаба ЦАХАЛа отказался от идеи создания войск кибербезопасности [Електронний ресурс] // NEWSRU.CO.IL. – Режим доступу: http://m.newsru.co.il/israel/02jan2017/cyber303.html. – Назва з екрану.

[360] Направление Киберзащиты СВ АОИ [Електронний ресурс] // CYCLOWIKI.ORG. – Режим доступу: http://cyclowiki.org/wiki/%D0%9D%D. – Назва з екрану.

[361] "ל"צה של התמרון את שיבשה לא סייבר תקיפת שום" [Електронний ресурс] // ISRAEL DEFENCE. – № 8, 2018. – Режим доступу: http://www.israeldefense.co.il/he/content. – Назва з екрану.

Ізраїлю було затверджено рішення про створення нового державного органу Управління по боротьбі з кібернетичної загрозою. Планувалося, що управління буде займається комплексним захистом від кібератак, у тому числі відпрацюванням загроз і атак в реальному часі. При управлінні також мав працювати національний центр підтримки CERT (Cyber Event Readiness Team) для боротьби з кіберзагрозами з метою забезпечення захисту різних організацій і галузей[362]. Завдання Управління – координувати відображення атак у кібернетичному просторі, які, за словами прем'єр-міністра Біньяміна Нетаніягу, «здатні паралізувати цілі країни». Формування державної інституції з істотно ширшими оперативними повноваженнями і завданнями значно підвищило статус органу координаційного центру протидії кібертероризму країн-супротивників[363]. Створення його структури відбувається поетапно, протягом трьох років. Нове керівництво працює спільно з нині чинним національним штабом з кібербезпеки. Управління та штаб утворюють єдину систему національної кіберзахисту при міністерстві глави уряду.

Окрім побудови організаційно-штатної структури ізраїльська влада приділяє велику увагу розвитку інформаційно-технічної інфраструктури для захисту національних інтересів. 15 серпня 2018 р. уряд Ізраїлю оголосив про початок трьохрічної програми розвитку технологій інформаційної безпеки, намагаючись зробити країну лідером у цьому напрямку. Інвестиції в проект складуть 90 млн. шекелів (близько $ 24 млн за курсом на момент анонса)[364].

Отже, Армії Оборони Ізраїлю вдалося побудувати ефективну та збалансовану систему кіберзахисту на основі систематизованої концепції ізраїльського політичного керівництва. Відмовившись від затратного шляху формування окремого виду військ, підрозділи кіберзахисту ЦАХАЛу органічно вбудовані до загальнодержавної структури інформаційно-психологічного та інформаційно-технічного захисту, що дозволяє успішно виконувати завдання протидії інформаційного впливу супротивника в умовах перманентного загострення воєнно-політичної обстановки в регіоні.

---

[362] 2015: Национальное управление по киберзащите создадут в Израиле [Електронний ресурс] // TADVISER. – Режим доступу: http://www.tadviser.ru/index.php/Статья:Киберпреступность_и_киберконфликты_:_Израиль#2015:_ . – Назва з екрану.

[363] Правительство утвердило создание новых "кибервойск" [Електронний ресурс] // NEWS.RAMBLE. – Режим доступу: http://news.rambler.ru/27363679/. – Назва з екрану.

[364] Запуск трехлетней программы развития технологий кибербезопасности [Електронний ресурс] // TADVISER. – Режим доступу: http://www.tadviser.ru/index.php/Статья:Киберпреступность_и_киберконфликты_:_Израиль#. – Назва з екрану.

У **Ірані** заявляють, що група хакерів, які працюють на воєнізовану групу гвардії Басідж мають на меті підвищення «цифрової готовності» країни, щоб Іран отримав перевагу в цифровому світі. Генерал Алі Фазлі, керівник гвардії Басідж, заявив, що хакерські групи складаються переважно з викладачів та студентів іранських інститутів та університетів. Іранське напівофіційне новинне агентство Mehr повідомляє, що кіберпідрозділ буде використовувати ті ж методики нападу, що раніше були використані проти самого Ірану. У той же час, влада відмовляється від надання будь-яких конкретних даних про новий підрозділ. Раніше влада Ірану не заперечувала наявність воєнізованих кіберпідрозділів, але заявляла, що їхня робота призначена тільки для оборони під час так званих «м'яких воєн»[365].

На теренах колишнього СРСР найбільш ефективні структури проведення кібероперацій створені в Естонії та Російської Федерації.

У «Глобальному індексі кібербезпеки – 2017» **Естонія** займала лідируючу позицію в Європі та п’яте місце в світі. Тому цілком закономірно, що з 2008 р. в Таллінні розміщений Об’єднаний центр кібероборони НАТО.

2 серпня 2018 р. в Таллінні відбулась урочиста церемонія, під час якої офіційно приступило до роботи командування кібервійськ Сил Оборони Естонії на чолі з командувачем А. Хайрком. Орієнтовна чисельність персоналу командування складає 300 осіб. Повноцінне функціонування командування планується забезпечити з 2023 р.[366].

Досить активно процеси зі створення кібервійськ відбуваються в **Росії (РФ).** Начальник ГШ ЗС РФ генерал армії В. Гєрасимов і російська військова наука визнають об’єктивну тенденцію переважного використання методів прихованого інформаційного протиборства перед силовим рішенням бойових завдань[367]. Разом з тим, інформація про створення кібервійськ є вкрай суперечливою. У лютому 2014 р. представник МО РФ генерал-майор Ю. Кузнецов заявив про перспективу з 2017 р. створення «загонів спеціалістів з кібербезпеки»[368], незважаючи на те, що МО РФ вважає створення військ для боротьби з кіберзагрозами вкрай фінансово затратним.

---

[365] Центр інформаційної безпеки. Іран офіційно визнав: у нього є кібервійська. – 15.03.2011. – Режим доступу: http://www.bezpeka. com/ua/ news/ 2011/03/15/iran-has-cyberforces.html

[366] Глава Кибервойск Эстонии: Чтобы защититься, надо уметь атаковать // eadaily, 19.08.2018. – Режим доступу: https://eadaily.com/ru/news/2018/08/19/glava-kibervoysk-estonii-chtoby-zashchititsya-nado-umet-atakovat

[367] Герасимов В. Ценность науки в предвидении [Електронний ресурс] // Военно-промышленный курьер. – 2013, 27 февраля. – № 8. – Режим доступу: http/ vpk-news.ru/articles/14632

[368] Сулейменов С. Неуловимые кибервойска [Електронний ресурс]. – 12.05.2014. – Режим доступу: http://tjournal.ru/paper/cyber-warfare

Одночасно, те ж відомство 20.04.2014 р. повідомило про створення у МО РФ органів військового управління, які відповідальні за інформаційні та телекомунікаційні технології, інноваційні дослідження та робототехніку. А саме:

- Головного управління розвитку інформаційних та телекомунікаційних технологій МО РФ (березень 2014 р). Його основним завданням є здійснення єдиної військово-технічної політики в сфері розвитку інформаційних, обчислювальних і телекомунікаційних технологій.
- Головного науково-дослідного випробувального центру робототехніки (червень 2013 р., лютий 2014 р. – наданий статус федерального бюджетного закладу). Основне завдання центру – проведення прикладних наукових досліджень і випробувань в галузі розробки та створення робототехнічних комплексів військового призначення та здійснення функцій головної науково-дослідної організації МО РФ з робототехніки.
- Головного управління науково-дослідної діяльності технологічного супроводження передових технологій (інноваційних досліджень) МО РФ виконує функції організації інноваційної діяльності, здійснення перспективних досліджень і розробок, супроводження передових програм і наукових проектів.

Усі ці управління об’єднані в Систему перспективних військових досліджень і розробок (СПВДР) разом з Науково-дослідним центром «Бюро оборонних рішень» в м. Москва та Відділом інноваційних розробок в м. Санкт-Петербург. Планується створення регіональних центрів в мм. Єкатеринбург Новосибірськ, Владивосток.

Інформація про створені функціональні підрозділи є досить фрагментарною та неофіційною, практично не містить даних про конкретні плани діяльності цих управлінь, що, очевидно, залежить від високого рівня секретності.

Цікавою є й активізація діяльності структурного компоненту МО РФ – Центру спеціальних розробок (ЦСР). Інформація на офіційному сайті МО РФ про центр відсутня, цілі та завдання не оголошуються, про включення в систему СПВДР – не відомо. Але, впродовж 2013–2014 рр. ЦСР виклав на порталах працевлаштування та сайтах окремих ВНЗ повідомлення про відкриті вакансії для фахівців з електроніки, телекомунікації, інформаційної безпеки, аналітики парчей та вразливості експлойтів (програм для проведення комп’ютерних атак), цифрової обробки сигналів, методів захисту інформації, її кодування та декодування, системного програмуванню

ІБ-модулів під Windows и Linux, а також мобільних ОС Android і iOS, розробки програмного забезпечення для смарт-карт і систем їх безпеки, аналітиків програмного забезпечення для мікропроцесорів. Інформація про те, реалізацію яких проектів будуть забезпечувати ці спеціалісти в галузі інформаційно-комунікаційних технологій відсутня[369]. Одночасно, забезпечення фахівцями цих вакансій є досить проблематичним, внаслідок об'єктивної технічної відсталості РФ в галузі інформаційно-комунікаційних технологій, недостатнього рівня заробітної платні в ЗС РФ, відсутності продуманої системи управління ІТ-персоналом[370].

Одночасно з 2013 р. почалася серйозна підготовка кадрів за рахунок створіння «наукових рот» та рекрутування ІТ-спеціалістів на службу в структурних підрозділах МО РФ. Наприклад, Новосибирський державний технічний університет проводив набір в наукову роту ЦНДІ МО РФ в Сергієвому Посаді для «застосування суперкомп'ютерних технологій. У вересні 2015 р. МО РФ відкрило кадетську школу ІТ-технологій, а у грудні того ж року був здійснений перший випуск фахівців спецназу інформаційної безпеки наукових рот із Військової академії зв'язку.

10 січня 2017 р. газета «Коммерсант» опублікувала дослідження міжнародної кампанії Zecurion Analytics, згідно якого РФ входить у п'ятірку держав з чисельності та фінансування кібервійськ. Але у тому ж січні 2017 р. голова комітету Ради Федерації з оборони та безпеки В. Озєров заявив, що кібервійськ в структурі ЗС РФ немає. Нарешті у лютому 2017 р. факт створення кібервійськ в ЗС РФ визнав й міністр оборони С. Шойгу. У виступі на засіданні Державної Думи РФ він наголосив на тому, що «створені війська інформаційних операцій є набагато ефективніше й сильніше»[371].

У цілому, аналіз відкритих джерел інформації дає можливість зробити висновок, про те, що в ЗС РФ створена низка структур, які за відповідних умов створення якісної системи взаємодії та координації зможуть ефективно виконувати функції СКбО.

Багато держав світу зараз активно розробляють і застосовують комплекс заходів для захисту свого суспільства від «інформаційної інтервенції», яка умовно здійснюється високорозвиненими державами у галузі використання ІТ-технологій. Сучасні держави

[369] Министерство обороны РФ набирает бойцов в кибервойска [Електронний ресурс]. – 20.04.2014. – Режим доступу: http://ru-an.info

[370] Шлындов А. Минобороны в поиске интеллектуалов [Електронний ресурс] // Независимое военное обозрение. – 29.06.2012. – Режим доступу: http://nvo.ng.ru/forces/2012-06-29/ 11_minoborony. html

[371] В России 22 февраля 2017 года Сергей Шойгу объявил о создании войск информационных операцій [Електронний ресурс] // Интерфакс. – Режим доступу: https://www.interfax.ru/russia/551054

розглядають перевагу в інформаційній сфері як найважливіший чинник забезпечення національної безпеки та реалізації національної стратегії. Про це свідчить об’єктивно зумовлена активність зі створення спеціалізованих підрозділів у структурах збройних сил і спеціальних служб, а також розробка та впровадження концептуальних документів, що регламентують процеси підготовки та ведення інформаційних операцій у сучасному глобалізованому інформаційному просторі.

Таким чином, активно впроваджуються в практику армійського життя елементи сил кібероперацій з різним ступенем організаційно-штатної структури, функціональних завдань та бойового призначення. На сьогодні світові держави-лідери перебувають на стадії трансформації власних військових потенціалів з огляду на потенційні можливості мережі Інтернет. Активно формуються спецпідрозділи з ведення розвідки, здійснення операцій з блокування інформаційних ресурсів супротивника в мережі Інтернет, захисту власних мереж та критично важливих ресурсів. Такі підрозділи створено в США, Великобританії, Німеччині, Австралії, Індії, Північній та Південній Кореї, Естонії – загалом, більш ніж у 20 країнах. Таким чином, кіберпростір реально стає новітнім глобальним театром бойових дій.

Інформаційна війна, як агресивне протиборство сторін в інформаційній сфері, негативно позначається на стані політичних комунікацій суспільства в цілому. Застосування таких кампаній політичними акторами пов'язане зі збільшенням ризиків конфліктогенного характеру, результатом чого є швидка зміна статусів і позицій у відносинах влади. Висока інтенсивність акцій інформаційної війни провокує системну нездатність до управління та свідомого регулювання суспільно-політичних процесів, а також становить загрозу воюючим сторонам. Досягнення цілей таким методом посилює політичну конфронтацію, соціальні ризики, національні конфлікти та одночасно знижує можливість поширення толерантності, консенсусної культури, підриває стабільність у суспільстві.

У сучасному світі, в умовах загострення суспільно-політичних, релігійно-конфесійних та національно-державницьких протиріч, геополітичні центри розподілу сил впливу не змогли досягти консенсусу у фундаментальних питаннях щодо боротьби зі зростаючою загрозою інформаційних воєн, інформаційного протиборства в епоху кібератак, які можуть становити загрозу світовій системі безпеки.

ВИСНОВКИ

Упродовж усієї історії людство умовно перебуває у двох абсолютно полярних станах – війни та миру, які обумовлюють його циклічний розвиток. Сподівання інтелектуалів, надії та прогнози гуманістів, на те, що завдяки прогресу у соціально-духовній сфері, рівню цивілізованості та зростанню інтелектуального потенціалу сучасні суспільства уникатимуть конфліктних, руйнівних форм взаємовідносин, особливо воєн, на жаль, не справдилися. Навпаки, в останнє століття виявляється тенденція до зростання кількості збройних конфліктів та їх масштабів, числа держав та коаліцій, що у них залучаються, степені жорстокості, а також жертв і втрат. Конфлікти та війни XX ст. продемонстрували мегамасштаби людської войовничості та еволюцію війни, як особливого суспільно-політичного явища. Новий етап цивілізаційного розвитку людства у XXI ст. принципово змінив основні форми і методи військового протистояння, трансформував відверте збройне насильство у комбінований варіант застосування інформаційно-психологічних технологій. Експансія інформації у XXI ст. виявляється в усіх сферах життєдіяльності сучасних світових розвинених держав та суспільств, завдяки використанню майже безмежних можливостей інформаційно-комунікаційних інфраструктур як транснаціонального так і локального масштабу.

У другій половині XX ст. прогресивний розвиток технологій у сфері доступу громадян до інформації, обумовив поширення масової освіти і розквіт ЗМІ та ЗМК. Виникнення сучасних потужних інформаційних і комунікаційних технологій стало причиною глобальної інформаційної революції та зламом традиційних форм, методів та інструментів створення, зберігання, поширення а також трансформації інформаційного продукту. Масштаби, реальні та потенційні наслідки цього культурно-цивілізаційного стрибка суттєво перевершують значення промислової революції XIX ст. і науково-технічної революції XX ст. Під впливом процесів інформатизації, розширення можливостей комунікації, що відбуваються в суспільстві, зазнають зміни всі сфери життєдіяльності. Визначну роль в перетворенні соціально-політичного простору у нову геополітичну інформаційну реальність відіграли поява на інформаційному ринку електронних ЗМІ та ЗМК, виникнення та бурхливий розвиток діалогових способів комунікації, різке збільшення швидкості передачі повідомлень, формування «електронних спільнот», як нової форми соціуму та ін.

Людство перебуває на стадії кардинальних цивілізаційних змін та формування глобального інформаційного суспільства, революційною ознакою якого стає використання інформації у практично-утилітарних цілях, як засобу для досягнення бажаної мети, особливо у конфліктах локального та глобального характеру. Інформаційний простір поряд з класичними театрами воєнних дій стає сферою ведення протиборства, середовищем протистояння, де інструментом здійснення насильства є інформація, а боротьба ведеться за вплив і маніпуляцію індивідуальною та суспільною свідомістю.

Відповідно до цих змін трансформуються і наукові концепції інформаційних воєн минулого і сучасності. У війнах минулого поєднувались компоненти того, що зараз ми визначаємо концепціями гібридної, мережево-центричної, преемптивної, консцієнтальної а також, частково, й інших сучасних концепцій війн. Ситуаційно обумовлене використання регулярної армії та партизанських формувань, сучасного озброєння та саморобної зброї, застосування класичних схем організації бою та іррегулярної тактики, комбатантів і некомбатантів, ідеологічне, дипломатичне забезпечення військових компаній та фінансово-торгові блокади були характерними практично для усіх війн людства до XXI ст. Принциповою основою для ведення сучасних воєн, яка кардинально диференціює їх від війн минулого, стало пріоритетне значення інформаційного чинника, масштабне застосування інформаційних технологій у військовій справі. Основним концептом сучасних теоретичних розробок воєнної науки стала відсутність межі між власне військовою та мирною формами протиборства держав і перенесення протистояння у сферу впливу на людську свідомість та психіку.

Головний об’єкт сучасних воєн – людина, її внутрішній світ, світогляд, стан психіки, що передбачає особливу увагу до інформаційного чинника при оцінці морально-психологічного стану військ для виконання бойових завдань за призначенням. Історичний розвиток психологічно-маніпулятивних технологій епохи інформаційної війни можна аналізувати крізь призму зовнішнього та внутрішнього чинників. Тотальний інформаційний вплив держав-ворогів, конкурентів, супротивників істотно впливає на громадську думку та морально-психологічний стан як військ, так і населення, провокуючи появу найнебезпечнішого різновиду сучасних воєн – інформаційної громадянської війни. Руйнуються традиційні ідентифікаційні патерни нації, нівелюються ознаки, що синтезували окремі образи «Я» у органічний комплексний «МИ-образ» єдиного народу чи громадян, спекуляція на негативних історично утворених

стереотипних конструктах диференціює суспільство, породжуючи панічні настрої, атмосферу ксенофобії та нетерпимості, становить загрозу національній ідеї та єдності нації загалом, особливо у переломні кризові моменти. Середовище для пошуку «Ворога» зміщується з зовнішньої сфери у антагоністичні суперечки суспільства всередині держави. Поняття «Свій» «Чужий» втрачають визначеність, і тоді статусу «Ворога» набуває кожна людина, що має відмінні преференції та погляди від визнаних «єдино правильними і вірними», виникає криза плюралізму та загроза демократичним принципам функціонування суспільства, а також демократичним формам правління у державі. Активна «більшість», намагаючись уникнути реальних чи псевдозагроз, втрачає реальність, постійно перебуваючи у стані інформаційного стресу, прагне захиститись усіма як законними, так і антигуманними способами, підриваючи стабільність у соціальній, економічній, політичній та духовно-культурній сферах життєдіяльності суспільства і держави загалом. Маніпуляції психо-інформаційним здоров'ям націй за умов відсутності стабільності в державі, застосування нею дієвих механізмів уникнення таких загроз, інформаційної системи запобігання та протидії їм, потужного апарату пропаганди, виваженої і адекватної інформаційної політики, майже завжди є впливовим елементом війни на сучасному етапі розвитку інформаційно-комунікаційних технологій в епоху глобального інформаційного суспільства. Потужні інформаційні атаки на тлі збройного протистояння з ворогом в умовах кризи можуть спровокувати системний інформаційний хаос, що розділить суспільство на кілька ідейних таборів. Замість життєво необхідного єднання, соціум диференціюється, в глобальних мережах транслюються і популяризуються негативна інформація, що ще більше провокує ескалацію конфліктів всередині держави. На нашу думку, саме атаки, що активно і цілеспрямовано здійснюються в Інтернеті, в соціальних мережах, є частиною інформаційної війни ворога, і становлять не меншу загрозу, аніж бойові дії. Будь-яка нація в умовах інформаційної війни, на сучасному етапі розвитку геополітичних відносин, перебуває в стані перманентних конфліктів масової свідомості, що сприяє домінуванню конфронтаційних форм вирішення конфліктів у суспільстві. Криза толерантності та гуманізму, ескалація ненависті – чинники, які супроводжують бойові дії, також загрожують консолідації суспільства та обумовлюють нагальну потребу пошуку оптимальних механізмів для реалізації інформаційної політики держави в умовах як військового, так і інформаційного протиборства. Інтенсифікація інформаційних атак та

агресія загрожують державам втратою контролю не лише в інформаційному та духовно-культурному просторах, а й спрямовані на прийняття не виважених політичних рішень керівництвом держави, колапсу економіки, формування негативного образу влади, що не здатна управляти державою, для провокації акцій громадської непокори, паніки, актів вандалізму та громадянської війни. Тому, у кризові моменти функціонування суспільства та держави, особливої уваги потребує інформаційна сфера, яка є інтегруючою основою життєдіяльності суспільства, а побудова системи національної інформаційної безпеки визнається однією з концептуальних засад його подальшого розвитку. За таких умов особливого значення набуває формування виваженої дієвої державної інформаційної політики, на основі системних наукових досліджень інформаційної сфери, провідне місце серед яких займає інформаційна безпека.

Результати науково-технічного прогресу в галузі інформаційно-комунікаційних технологій, розвиток засобів масової комунікації створили майже необмежені можливості для організації агресивного інформаційного впливу на населення інших держав із метою нав'язування принципів устрою та життя суспільства, деформації національних духовних цінностей, зниження та розбалансування економічного й військового потенціалу держав, через вплив на індивідуальну, групову і масову свідомість за допомогою застосування комплексу інформаційно-психологічного та інформаційно-технічного інструментарію. Аналіз інформаційного протиборства останнього десятиліття засвідчує, що інформаційна зброя,враховуючи її асиметричний характер, надає безпрецедентні можливості – як окремим терористичним групам, так і державам – розв'язувати повномасштабні інформаційні війни практично на рівні із провідними, розвиненими світовими державами та міжнародними інституціями.

Активне використання маніпулятивних і дезінформаційних технологій в ході інформаційного протиборства є об'єктивною реальністю. На нашу думку, істинним є твердження Уїнстона Черчіля, який оцінюючи важливість інформаційної компоненти під час бойових дій, зазначав, що «у військовий час правда є наскільки цінною, що оберігати її повинні вартові брехні», наголошуючи на необхідності використання усіх механізмів та інструментів інформаційної стратегії національної безпеки держави для захисту власного інформаційного простору. Досвід провідних держав світу з питань формування спеціальних підрозділів і родів військ з кіберзахисту, створення ефективних механізмів і підготовку сил та засобів організації інформаційної протидії може бути корисним для

України в умовах безпрецедентної ескалації рівня «гібридних загроз» з боку Російської Федерації.

Основним завданням інформаційної війни у системі національної безпеки є захист власного інформаційного простору та збереження національного духу народу та армії від інформаційного впливу ворога. Ментальність нації містить раціональні та ірраціональні патерни, які формують індивідуальну та колективну свідомість, через комплексну дію чинників, де основним, на нашу думку, є вплив повсякденного життя, досвіду, зовнішнього середовища, державних інститутів а також, особливо, інформації. В умовах воєн органічний зв'язок ідеології та психології в системі інформаційно-пропагандистського забезпечення набуває особливого значення, тому, що він комплексно обумовлює та визначає морально-психологічний стан армії, її стійкість в умовах надзвичайної емоційної та фізичної напруги.

У сучасній геополітичній ситуації, для України життєво необхідним є усвідомлення урядом держави і суспільством надзвичайної важливості вивчення сутності та специфіки інформаційних воєн і створення дієвої системи національної безпеки, визнання історичної необхідності захисту територіальної цілісності та недоторканості власного географічного та інформаційного простору. Інформаційні війни стали аксіомою у сучасних міжнародних відносинах і дозволяють дуже ефективно, із залученням малих фінансових та людських ресурсів досягати цілей в усіх сферах суспільно-політичного життя. Ці війни ведуть із активним використанням інформаційної зброї, а ступінь захищеності інформаційного простору держави визначається рівнем забезпечення її інформаційної безпеки.

Отже, інформаційна революція відкриває невичерпні можливості для впливу на народи та владу, маніпулювання свідомістю та поведінкою людей на необмеженому просторі. Беручи до уваги процес глобалізації інформаційно-комунікаційних мереж, що відбувається в світі, можна висунути припущення, що саме інформаційні види агресії матимуть пріоритетне значення у майбутньому. Тому, наукові розвідки та дослідження цього сучасного суспільно-політичного явища дадуть можливість в майбутньому уникнути руйнівних негативних наслідків воєн для усього людства.

ЛІТЕРАТУРА

1. Адрианова Н.С. Интернет-коммуникация – реальность или симулякр? [Електронний ресурс] / Н.С. Адрианова. – Режим доступу: http:// www. nbuv. gov.ua/portal/natural/vdpu/Movozn/2010_16/article/1.pdf. – С. 17–18.
2. Акайомова А. Теоретична ідентифікація терміна „інформаційна політика” (на прикладі Російської Федерації) [Електронний ресурс] / Анжеліка Акайомова // Віче. – 2011. – № 4. – Режим доступу: http:// www.viche.info/ journal/2420/
3. Алещенко В. Проблеми захисту від негативного інформаційно-психологічного впливу противника / В.І. Алещенко, В.Г. Сербін // Математичні машини і системи. – 2010. – № 1. – С. 77–86.
4. Американские кибератаки // Зарубежное военное обозрение. – 2013. – № 9. – С. 104.
5. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти [Електронний ресурс] ; за заг. ред. д-ра юрид. наук, проф. О.М. Бандурки: монографія. / І.В. Арістова. – Харків: вид-во Ун-ту внутр. справ, 2000. – 368 с. – Режим доступу: http://www.coolreferat.com=11
6. Арістова І.В. Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади [Електронний ресурс] : автореф. дис. … на здобуття наук. ступеня д-ра юрид. наук : спец. 12.00.07 „Теорія управління; адміністративне право і процес; фінансове право” / І.В. Арістова. – Харків, 2002. – Режим доступу: dysertaciya.org.ua
7. Афанасьев Д. Роль Інтернет-мережевих спільнот у становленні інформаційного суспільства в Україні [Електронний ресурс] / Д. Афанасьев // Віче. – № 2. – 2010. – Режим доступу: http://www.viche.info/journal/1827/
8. Бабаєва Н.Р. Глобалізація сучасного світу / Н.Р. Бабаєва // Гілея. – 2012. – № 59. – С. 362–366.
9. Багиров Р.З. Политическая коммуникация в обеспечении военной безопасности Российской Федерации: автореф. дис. … на соискание науч. степени канд. полит. наук : спец. 23.00.02 „Политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии” / Р.З. Багиров. – М., 2009. – 21 с.
10. Балахонцев Н. Влияние концепции „сетецентрическая война” на эффективность разведывательного обеспечения вооруженных сил

США / Н. Балахонцев, А. Кондратьев // Зарубежное военное обозрение. – 2011. – № 2. – С. 14–18.
11. Балуевский Ю. Глобализация и военное дело [Електронний ресурс] / Ю. Балуевский, М. Хамзатов // Независимое военное обозрение. – 08.08.2014. – Режим доступу: http://nvo.ng.ru/concepts/2014-08-08/1_globalisation.html
12. Баранівський В.Ф. Основні напрямки застосування психологічних знань під час виконання бойових завдань в умовах збройних конфліктів [Електронний ресурс] / В.Ф. Баранівський, А.Я. Боднар, Л.Ф. Терещенко. – Режим доступу: http://www.ekmair.ukma.kiev.ua/bitstream/123456789/1055/1/Bodnar_Osnovni_napriamky.pdf
13. Бард А., Зодерквист Я. Netократия. Новая правящая элита и жизнь после капитализма / А. Бард, Я. Зодерквист; перевод со шведского. – СПб.: Стокгольмская школа экономики в Санкт-Петербурге, 2004. – 252 с.
14. Баталов А. Национальная киберстратегия США (2019) // Зарубежное военное обозрение. – 2019. – № 2. – С. 3–11.
15. Башкиров Н. Взгляды военного и политического руководства США на защиту инфраструктуры от киберугроз / Н.Башкиров // Зарубежное военное обозрение. – 2018. – №12. – С. 13–17.
16. Бек У. Что такое глобализация? Ошибки глобализма – ответы на глобализацию / У. Бек. – М.: Прогресс-Традиция, 2001. – 304 с.
17. Белл Д. Грядущее постиндустриальное общество: Опыт социального прогнозирования / Д. Белл ; перевод с англ. – Изд. 2-е, испр. и доп. – М.: Academia, 2004. – 788 с.
18. Бердяев Н.А. Человек и машина (Проблема социологии и метафизики техники) / Н.А. Бердяев // Вопросы философии. – 1989. – № 2. – С. 147–162.
19. Біленчук П.Д. Інформаційна діяльність в правознавстві: монографія. / П.Д. Біленчук, О.В. Кравчук, В.Б. Міщенко, Ю.О. Пілюков. – К.: Наука і життя, 2007. – 244 с.
20. Блажиевская Г.А. Труд как социально-культурная ценность: дисс. … канд. филос. наук : 24.00.01 / Г.А. Блажиевская. – Казань, 2007. – 173 с.
21. Блохин Л.Ф. Традиционные экосоциальные системы как основа устойчивого развития в тропиках (на примере Западной Африки) / Леонид Федорович Блохин // Человек: образ и сущность (гуманитарные аспекты). Биосфера, ноосфера и экология. Ежегодник ИНИОН РАН. – М., 1999. – С. 44–66.

22. Бойовий Статут Сухопутних військ Збройних Сил України. – К.: Командування Сухопутних військ, 2010. – 216 с.
23. Бояндин К. Инфосфера как разумная среда обитания [Електронний ресурс]. – Режим доступу: http://boyandin.name/blog/590/infosfera-kak-razumnaya- sreda-obitaniya
24. Буренок В.М. Курс – на сетецентрическую систему вооружения [Електронний ресурс] / В.М. Буренок, А.Ю. Кравченко, С.С. Смирнов. // ВКО. – 2009. – № 5. – Режим доступу: www. vko.ru/koncepcii/kurs-na-setectntrscyeskuyu-sistemu-vooruzhenia# d-comments
25. Буряк В. Актуальные проблемы философии. Методологические основания экономического знания, постиндустриальное общество, глобализация / В. Буряк. – Симферополь: Атика, 2006. – 182 с.
26. Буряк В.В. Глобальное гражданское общество и сетевые революции / В.В. Буряк. – Симферополь: Диайпи, 2011. – 152 с.27.Бурячок В.Л., Толубко Б. Інформаційна та кібербезпека: соціотехнічний аспект: підручник; за заг. ред. д-ра техн. наук, професора Б. Толубка. / В.Л. Бурячок, Б.Толубко. – Київ: ДУТ, 2015. – 288 с.
27. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз): монографія / В.М. Бутузов. – К.: КИТ, 2010. – 408 с.
28. Валлерстайн І. Глобалізація або вік змін? Довгостроковий погляд на шлях розвитку світової системи / І. Валлерстайн // Глобалізація. Регіоналізація. Регіон. політика. – Луганськ: Альма матер – Знання, 2002. – С. 49–67.
29. Вахула Б.Я. Соціальні Інтернет-мережі з позицій інтегративної парадигми / Б.Я. Вахула // Роль суспільних наук у забезпеченні стабільності розвитку глобальних світових процесів у XXI ст.: мат. міжнар. наук.-практ. конф. – К., 2013. – С. 58–60.
30. Вебер М. В 26 Избранные произведения: Пер. с нем. / М. Вебер; сост., общ. ред. и послесл. Ю.Н. Давыдова; предисл П.П. Гайденко. – М.: Прогресс, 1990. – 808 с.
31. Вершинин М.С. Политическая коммуникация в информационном обществе / М.С. Вершинин. – СПб.: Изд-во Михайлова В.А., 2001. –
253 с.
32. Виговська О.С. Державна інформаційна політика: концептуальні засади формування та розвитку / Ольга Виговська // Гілея. – 2014. – № 82. – С. 371–3 73.

33. В информационной войне превосходство в военной мощи не гарантирует от поражения [Електронний ресурс]. – Режим доступу: http:// www. arms-expo.ru/049051124053053051052.html
34. В России 22 февраля 2017 года Сергей Шойгу объявил о создании войск информационных операцій [Електронний ресурс] // Интерфакс. – Режим доступу: https://www.interfax.ru/russia/551054
35. Властивості інформації. Інформаційні процеси [Електронний ресурс]. – Режим доступу: http://informatyka179.blox.ua/2009/12/Vlastivosti–inofrmatsiyi–Informatsijni–protsesi.html
36. Во Франции в 2017 году появятся кибервойска [Електронний ресурс] // Коммерсант. 13/12/16 21:38. – Режим доступу: https://novostipmr.com/ru/news/16-12-13/vo-francii-v-2017-godu-poyavyatsya-kibervoyska
37. Война и мир в терминах и определениях [Електронний ресурс] ; под общ. ред. Д. Рогозина. – М.: Издательский дом ПоРог, 2004. – Режим доступу: www. royallib.ru/book/rogozin_dmitriy.html
38. Войтасик Л. Использование психологии в системе пропаганды / Леслав Войтасик // Реклама: внушение и манипуляция. Медиа-ориентированный поход. – М.: Издат. дом «БАХРАХ-М», 2001. – 292 с.
39. Войтенко В.П. Феномен людини: Дванадцять дзеркал / В.П. Войтенко; Медикодослідницьке товариство „Гіппократ”. – К., 1999. – 58 с.
40. Волокин А.В. Электронная коммерция: учебное пособие для служащих государственных организаций и коммерческих фирм / А.В. Волокин, А.П. Маношкин, А.В. Солдатенков. – М.: НТЦ „Фиорд-Инфо”, 2002. – 272 с.
41. Воронкова В.Г. Філософія глобалізації: соціоантропологічні, соціоекономічні та соціокультурні виміри: монографія / В.Г. Воронкова. – Запоріжжя: вид-во ЗДІА, 2010. – 272 с.
42. Габермас Ю. Структурні перетворення у сфері відкритості: дослідження категорії громадянське суспільство / Ю. Габермас. – Львів: Літопис, 2000. – 318 с.
43. Гаман Т.В. Проблемні питання нормативно-правового забезпечення інформаційної діяльності органів державного управління (регіональний аспект) / Т.В. Гаман // Університетські наукові записки. – 2005. – № 1-2 (13-14). – С. 272–276.
44. Гарбуз Л. Неужели Европа еще представляет, что есть возможность отстранения от драматических событий в Украине?

[Електронний ресурс] / Людмила Гарбуз // День. – 06.05.2014. – Режим доступу: http:// m.day.kiev.ua/ ru/article/mirovye-diskussii/gibridnaya-voyna-putina
45. Герасимов В. Ценность науки в предвидении [Електронний ресурс] / Валерий Герасимов // Военно-промышленный курьер. – 2013, 27 февраля. – № 8. – Режим доступу: http/ vpk-news.ru/articles/14632
46. Гирич В.Л. Глобальное информационное пространство и проблема доступа к мировым информационным ресурсам [Електронний ресурс] / В.Л. Гирич, В.Н. Чуприна. – Режим доступу: www.rsl.ru/upload/mba2007_05
47. Гибридная война и доктрина Герасимова [Електронний ресурс] // ИнВоенInfo. – 2018, 22 июня. – Режим доступу: https://invoen.ru/analitika/doktrina-gerasimova/
48. Гібридна війна: як це працює [електронний ресурс]. – Режим доступу: www.csr.org. ua/index.php/uk/aktsenti-dnya/318-gibridna-vijna-yak-tse-ratsyue. (дата звернення 20.02.2015) – Назва з екрану.
49. Глава Кибервойск Эстонии: Чтобы защититься, надо уметь атаковать // eadaily, 19.08.2018. – Режим доступу: https://eadaily.com/ru/news/2018/08/19/glava-kibervoysk-estonii-chtoby-zashchititsya-nado-umet-atakovat
50. Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С.Гнатюк // Безпека інформації. − 2013. − Т. 19. − № 2. − С. 118−129. - Режим доступу: ИКЬ: ЬіІр://пЬиу.доу.иа/ШКЛ/Ье2іп_2013_19_2_8.
51. Говорухина К.А. Глобальное информационное общество и новые аспекты изучения пропаганды в контексте информационной безопасности / К.А. Говорухина // Человек. Общество. Управление. – 2012. – № 1. – С. 26–31.
52. Горбенко А. СМИ в сфере информационного противоборства / А. Горбенко // Власть. – 2008. – № 11. – С. 23–26.
53. Горбенко І.Д. Інформаційна війна – сутність, методи та засоби ведення / І.Д. Горбенко, В.І. Долгов, Т.О. Гріненко // Ювілейна науково-технічна конференція „Правове, нормативне та метрологічне забезпечення захисту інформації в Україні”. – К., 1998. – С. 11–15.
54. Горовий В. Національні інформаційні ресурси в контексті посилення глобальних інформаційних впливів / Валерій Горовий // Наукові праці Національної бібліотеки України імені В.І. Вернадського. Вип. 36 [НАН України, Нац. б-ка України ім. В.І. Вернадського, Асоц. б-к України]. – К., 2013. – 420 с.

55. Горовий В.М. Питання забезпечення національного інформаційного суверенітету / В.М. Горовий, О.Д. Довгань // Інформаційна безпека людини, суспільства, держави. – 2012. – № 1 (8). – С. 6–10.
56. Гриняев С.Н. Концепции ведения информационной войны в некоторых странах мира / С.Н. Гриняев // Зарубежное военное обозрение. – 2002. – № 2. – С. 25–28.
57. Гриценко В.С. Труд в постиндустриальном обществе: автореф. дисс. … канд. филос. наук : 09.00.11 / В.С. Гриценко; [место защиты: ФГБОУ ВПО „Пермский государственный национальный исследовательский университет”]. – Пермь, 2012. – 22 с.
58. Громыко Ю. Консциентальное оружие и консциентальные войны [Електронний ресурс] / Юрий Громыко. – Режим доступу: hvylya.org/ interview/society2/taynoe-oruzhie-rossii-chto-takoe-voeni-za-identichnost. Html
59. Громыко Ю. Оружие, поражающее сознание, – что это такое? / Ю. Громыко // Кому будет принадлежать консциентальное оружие в XXI веке? – М.: Россия XXI, 1997. – С. 7−8.
60. Гула Р.В. Патриотизм и национализм. Опыт историософского анализа / Р.В. Гула. – Д.: Герда, 2014. – 196 с.
61. Гула Р.В. «Русский мир» – концепція імперського фантому в геополітичній реальності / Р.В. Гула // Науковий семінар „Інформаційна агресія Російської Федерації проти України”: тези доповідей, 25 жовтня 2018 року. – Х.: ХНУПС ім. І. Кожедуба, 2018. – С. 31–33.
62. Гула Р.В. Кібер-Цахал проти кібер-джихаду / Р.В. Гула, О.В. Вітринська // Історичні студії суспільного прогресу. – 2018. – Вип. 6. – С. 46–53.
63. Гула Р.В. Концепт гібридної війни Ф. Хоффмана як модель форми асиметричного протистояння в епоху постмодерну / Р.В. Гула, І.Г. Передерій // Тези 71-ої наукової конференції професорів, викладачів, наукових працівників. Аспіратнів та студентів університету. Том 2. (Полтава, 22 квітня – 17 травня 2019 р.). – Полтава: ПолтНТУ, 2019. – С. 252–254
64. Гула Р.В. Концепція „керованого хаосу” – форма гібридної війни у поглядах воєнно-політичного керівництва РФ / Р.В. Гула, О.П. Зеленько // XV Міжнародна конференція „Новітні технології – для захисту повітряного простору” 10 – 11 квітня 2019 року. Тези доповідей. – Х.: ХНУПС ім. І. Кожедуба, 2019. – С. 588–589.

65. Гула Р.В. Глобальне інформаційне суспільство: транснаціонально-громадянський науковий підхід / Р.В. Гула // Соціально-правові виміри правової держави: еволюційна парадигма: зб.тез Всеукр. наук.-практ. конф. (м. Дніпро, 28 березня 2019 р.). – Дніпро: ДДУВС, 2019. – С. 121–124.
66. Гула Р.В. Доктрина Герасимова – теорія „організованого хаосу" в філософській парадигмі постмодерну / Р.В. Гула // Збірник наукових праць XI Міжнародної науково-практичної конференції „Проблеми й перспективи розвитку академічної та університетської науки", 20–21 грудня 2018 року – Полтава: ПолтНТУ, 2018. – С. 91–93.
67. Гула Р.В. Еволюція концепцій інформаційних воєн в реаліях сучасності / Р.В. Гула // Документно-інформаційні комунікації в умовах глобалізації: матеріали III Всеукраїн. наук.-практ. конф., м. Полтава, 22 листопада 2018 р. – Полтава, ПНТУ, 2018. – С. 281–283.
68. Гулай В.В. Комунікативні механізми та масштаби пропагандистського впливу радянських партизан та підпільників на населення Львівщини в роки нацистської окупації / В.В. Гулай // Військово-науковий вісник. – 2014. – Вип. 21. – С. 104–119.
69. Гуріна Н. Інформаційне протиборство – один з головних напрямків політики сучасних міжнародних відносин [Електронний ресурс] / Н. Гуріна. – Режим доступу: ukrlife.org/main/cxid/gurina.doc; http: // www.dtic.mil/ doctrine/ jel/new_pabs/jp 3_13.pdf
70. Давыдов Д. Информационные операции как средство достижения целей военно-политического руководства США / Д. Давыдов // Зарубежное военное обозрение. – 2013. – № 10. – С. 3–10.
71. Даник Ю.Г. Кібернетичний простір та забезпечення кібернетичної безпеки держави / Ю.Г. Даник // Тези доповідей IV міжнародного науково-технічного симпозіуму „Нові технології в телекомунікаціях" (8–21 січня 2011 р.). – К.: ДУІКТ. – С. 56–58.
72. Даніл'ян В.О. Інформаційне суспільство: базові концепції аналізу / В.О. Даніл'ян // Наукові записки Харківського університету Повітряних Сил. Соціальна філософія, психологія. – Х.: ХУПС, 2005. – Вип. 2. – С. 131–138.
73. Дергачев В. Силовые возможности Китая [Електронний ресурс] / В. Дергачев // Независимое военное обозрение. – 29.11.2013. – Режим доступу: http://prpk.info/articles/armija-i-oruzhie/silovye-vozmozhnosti-kitaja

74. Джошуа Д. Перша мережева війна / Д. Джошуа ; переклад Дмитра Губенка // Новинар. – 12–18 січня 2008. – № 1.
75. Дзьобань О.П. Інформаційне суспільство: морально-етичний дискурс / О.П.Дзьобань, О.Г. Данильян // Інформація і право. – К., 2014. – № 1 (10). – С. 16–25.
76. Дзьобань О.П. Інформаційне суспільство як новий спосіб соціальної взаємодії / О.П.Дзьобань, С.Б. Жданенко // Правова інформатика. – № 1 (41). – 2014. – С. 3–11.
77. Дзьобань О.П. Комунікаційна природа інформаційного простору / О.П.Дзьобань, Ю.В. Мелякова // Інформація і право. – 2012. – № 2 (5). – С. 81–88.
78. Дзьобань О.П. Діалектика глобалізації віртуальної реальності й суспільного розвитку / О.П. Дзьобань // Гілея: науковий вісник. Збірник наукових праць. 2012. – Випуск 63 (№ 8). – С. 254–260.
79. Дзьобань О.П. Вплив глобалізаційних процесів на державний суверенітет України / О.П.Дзьобань, В.Г. Пилипчук // Вісник Національної юридичної академії України імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія / Редкол.: А.П.Гетьман та ін. – Х.: Право, 2010. – Вип. 3. – С. 96–103.
80. Дзьобань О.П. Проблема агресії і насильства: світоглядно-інформаційний вимір / О.П.Дзьобань, В.Г. Пилипчук // Освіта регіону. – 2012. – № 2. – С. 171–177.
81. Дзьобань О.П. Теоретичні та державно-правові аспекти протидії інформаційному тероризму в умовах глобалізації / О.П.Дзьобань, В.Г. Пилипчук // Стратегічні пріоритети. – 2011. – № 4 (21). – С. 12–17.
82. Дзьобань О. Інформаційна безпека: нові виміри загроз, пов’язаних з активізацією міжнародної діяльності в інформаційно-комунікаційній сфері / О.П.Дзьобань, О. Соснін // Вісник Львівського університету. Серія: міжнародні відносини. – 2015. – Випуск 37. – Частина 3. – С. 35–43.
83. Довгань О.Д. Кібертероризм як загроза інформаційному суверенітету держави / О.Д. Довгань, В.Г. Хлань // Інформаційна безпека людини, суспільства, держави. – 2011. – № 3 (7). – С. 49–53.
84. Додонов О.Г. Захист інформації в інформаційно-аналітичних системах державних органів управління / О.Г. Додонов, О.С. Горбачик, М.Г. Кузнєцова // Реєстрація, зберігання і обробка даних. – 2000. – Т. 2. – № 2. – С. 66–72.

85. Доповідь про стан інформатизації та розвиток інформаційного суспільства в Україні за 2013 рік [Електронний ресурс]. – Режим доступу: http://dknii.gov.ua/?q=node/1469
86. Дорошкевич А.С. Гібридна війна в інформаційному суспільстві /А.С. Дорошкевич // Вісник Національного університету „Юридична академія України імені Ярослава Мудрого". – 2015. – № 2 (25). – С. 21–28.
87. Дракер П. Посткапиталистическое общество / П. Дракер // Новая постиндустриальная волна на Западе: антология; под ред. В.Л. Иноземцева. – М.: Academia, 1999. – С. 67–100.
88. Дубас О.П. Інформаційний розвиток сучасної України у світовому контексті: монографія / О.П. Дубас. – К.: Генеза, 2004. – 208 с.
89. Дубов Д.В. Зрушення сфер геополітичного протиборства: від географічної експансії – до конструювання інформаційно-кібернетичних просторів / Д.В.Дубов // Стратегічні пріоритети. − 2014. − № 1. − С. 106−115.
90. Дубов Д.В. Кібербезпека: світові тенденції та виклики для України / Д.В. Дубов, М.А. Ожеван. – К.: НІСД, 2011. – 30 с.
91. Дугин А.Г. Сетевые войны. Доклад на заседании Изборского клуба 08.07.2013 [Електронний ресурс] / А.Г. Дугин. – Режим доступу: http:// dynacon.ru/content/articles/2318/
92. Думанський Д. Інформаційно-психологічна боротьба як системний виклик сучасності [Електронний ресурс] / Дмитро Думанський. – Режим доступу: http://moloda-naciya.smoloskyp.org.ua/?p=210
93. Дятлов С.А. Принципы информационного общества [Електронний ресурс] / С.А. Дятлов. – Режим доступу: http: // emag.iis.ru/arc/ infosoc/ emag.nsf/BPA
94. Экс-глава военной разведки ес о влиянии гибридных угроз на оценку ситуации в мире // Зарубежное военное обозрение. – 2018. – № 12. – С. 92.
95. Єжель М. Управління за новітніми зразками / Михайло Єжель // Оборонний вісник. – 2012. – № 1. – С. 4–5.
96. Жаров М. Хроники информационной войны / М. Жаров, Т. Шевяков. – М.: Европа, 2009. – 48 с.
97. Закон України „Про основи національної безпеки України" // Урядовий кур'єр. – 2003. – 30 липня.
98. Запуск трехлетней программы развития технологий кибербезопасности [Електронний ресурс] // TADVISER. – Режим

доступу: http://www.tadviser.ru/index.php/Статья:Киберпреступность_и_киберконфликты_:_Израиль#. – Назва з екрану.
99. Защита киберпространства США // Зарубежное военное обозрение. – 2013. – № 5. – С. 105.
100. Звіт про НДР „Комунікатор-Р” (заключний). – К.: НУОУ, 2012. – 83 с.
101. Зеленін В.В. По той бік правди: нейролінгвістичне програмування як зброя інформаційно-пропагандиської війни [Текст] / В.В. Зеленін. – Вінниця: Віндрук, 2014. – 384 с.
102. Землянова Л.М. Сетевое общество, информационализм и виртуальная культура / Л.М. Землянова // Вестник Московского университета. Сер. 10. Журналистика. – 1999. – № 2. – С. 58–69.
103. Зернецька О.В. Глобальний розвиток систем масової комунікації і міжнародні відносини / О.В. Зернецька. – К.: Освіта, 1999. – 351 с.
104. Зуев С.Э. Измерения информационного пространства (политики, технологии, возможности) / С.Э. Зуев // Музей будущего: информационный менеджмент. – М.: Прогресс-Традиция, 2001. – С. 230–250.
105. Иванов А.К. Глобальное информационное пространство и его место в современном международном праве / А.К. Иванов // Ползуновский вестник. Барнаул: АлтГТУ – 2005. – № 1. – С. 219–227.
106. Иванов Д.В. Виртуализация общества / Д.В. Иванов. – СПб.: Петербургское Востоковедение. – 2000. – 96 с.
107. Измерение информационного общества, 2012, МСЭ [Електронний ресурс] – Режим доступу: http://www.itu.int/ITU-D/ict/publications/ idi/material/ 2012/MIS2012-ExecSum-R.pdf
108. Ильин И.В. Глобалистика в контексте политических процессов : дисс. ... д-ра. полит. наук : 23.00.04 / Ильин Илья Вячеславович; [место защиты: Моск. гос. ун-т им. М.В. Ломоносова]. – Москва, 2011. – 428 с.
109. Інформаційна безпека сучасного суспільства: навчальний посібник; за заг. ред. А.І. Міночкіна. – К.: ВІТІ НТУУ „КПІ”, 2006. – 188 с.
110. Інформаційна війна і національна безпека: монографія / П.П. Ткачук, Р.В. Гула, О.І. Сивак та ін. – Львів: АСВ, 2015. – 265 с.
111. Інформаційне суспільство в світі та Україні: проблеми становлення та закономірності розвитку: колективна монографія / за ред. д. філософ. н., проф. В.Г.Воронкової. – Запоріжжя: Вид-во ЗДІА, 2017. – 292 с.

112. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / В.П. Горбулін, О.Г. Додонов, Д.В. Ланде. – К.: Інтертехнологія, 2009. – 164 с.
113. Інформаційно-психологічна безпека особистості [Електронний ресурс]. – Режим доступу: https://sites.google.com/site/infobezosob/informacijno-psihologicna-bezpeka-osobistosti/ob-ektom-informacijno-psihologicnogo-zahistu-sobistosti/informacijna-zbroa---ce
114. Информационная политика: учебник ; под общ. ред. В.Д. Попова. – М.: Изд-во РАГС, 2003. – 463 с.
115. Информационная цивилизация – XXI век. [Електронний ресурс] / Нелетальное оружие уже убивает. – Режим доступу: http // info21.ru/second.php?id=53
116. Информационная эра [Електронний ресурс]; перевод Владимира Казеннова. – Режим доступу: http://www.lib.ru/SECURITY/kvn/corner.txt_with-big-pictures.html
117. Информационное общество: Сборник. – М.: ООО Изд-во АСТ, 2004. – 507 с.
118. Информационное противоборство на современном этапе: анализ и тенденции [Електронний ресурс]. – Режим доступу: http://www.molych.ru/ politika/ informatsionnoe-protivoborstvo-na-sovremennom-etape-analiz-i-tendentsii.html
119. Історія інформаційно-психологічного протиборства: підруч. / [Я.М. Жарков, Л.Ф. Компанцева, В.В. Остроухов, В.М. Петрик, М.М. Присяжнюк, Є.Д. Скулиш]; за заг. ред. д.ю.н., проф., засл. юриста України Є.Д. Скулиша. – К.: Наук.-вид. відділ НА СБ України, 2012. – 212 с.
120. Йак И. Израиль успешно противостоит врагу в киберпространстве [Електронний ресурс] // 7 канал, 10.06.2013. – Режим доступу: https://www.7kanal.co.il/News/News.aspx/160803. – Назва з екрану.
121. Карасев П. Кибервойска Европы и НАТО / П. Карасев // «Expert Online». – 2019.20.02. – Режим доступу: http://expert.ru/2018/03/13/kibervojska-evropyi-i-nato/
122. Кастельс М. Галактика Интернет: Размышления об Интернете, бизнесе и обществе / М. Кастельс. – М.: У-Фактория, 2004. – 328 с.
123. Кастельс М. Информационная эпоха: экономика, общество и культура / М. Кастельс; пер. с англ.; под. науч. ред. О.И. Шкартана. – М.: ГУ ВШЭ, 2000. – 608 с.

124. Кастельс М. Становление общества сетевых структур / М. Кастельс // Новая постиндустриальная волна на Западе: антология; под ред. В.Л. Иноземцева. – М.: Academia, 1999. – С. 494–495.
125. Киберкомандование НАТО полностью закончит формироваться в 2023 году [Електронний ресурс] // УКРИНФОРМ 16.10.2018. – Режим доступу: https://www.ukrinform.ru/rubric-technology/2559824-nato-sformiruet-sobstvennye-kibervojska-v-2023-godu.html
126. Киберучения НОАК // Зарубежное военное обозрение. – 2013. – № 6. – С. 86–87.
127. Кісілевич-Чорнойван О.М. Міжнародне інформаційне право / О.М. Кісілевич-Чорнойван. – К.: Персонал, 2011. – 160 с.
128. Кировец А. Органы пропаганды и информационной войны КНР / А. Кировец // Зарубежное военное обозрение. – 2013. – № 9. – С. 28–33.
129. Клаузевиц К. О войне: в 2-х т. – Т. 2 / К. Клаузевиц. – М.: АСТ, Terra Fantastica, 2002. – 558 с.
130. Климчук О.О. Кібервійна у сучасних умовах / О.О. Климчук, Р.М. Кравченко // Інформаційна безпека. Людина. Суспільство. Держава. – 2011. – № 1(5). – С. 78–84.
131. Козловец Н.А. Национальная идентичность в контексте модернизационных процессов / Н.А. Козловец // Гілея. – 2013. – № 65. – С. 255–262.
132. Козуб О.О. Кіберпростір як середовище породження і самореалізації принципу космополітизму / О.О. Козуб // Гуманітарний вісник ЗДІА. – 2010. – № 43. – С. 176–179.
133. Козье Д. Электронная коммерция / Д. Козье. – М.: Русская редакция, 1999. – 288 с.
134. Колесов П. Ведение Соединенными Штатами информационных войн. Концепция „стратегических коммуникаций” / П. Колесов // Зарубежное военное обозрение. – 2010. – № 6. – С. 9–14.
135. Комлева Н.А. Преэмптивная война как технология ресурсного передела мира [Електронний ресурс] / Наталья Комлева. – Режим доступу: komleva@yandex.ru
136. Компьютерный абордаж военного спутника // Эхо планеты. – 1999. – № 10. – С. 10–16.
137. Конах В. Забезпечення інформаційної безпеки держави як складової системи національної безпеки (приклад США): автореф. дис. … на здобуття канд.. політ. наук : спец. 21.01.01 „Основи національної безпеки держави” / В.К. Конах. – К., 2005. – 13 с.

138. Кондратьев А. Будущее сетецентрических войн [Електронний ресурс] / А. Кондратьев // Независимое военное обозрение. – 07.09.2012. – Режим доступу: http://nvo.ng.ru/concepts/2012-09-07/1_web_war.html
139. Кондратьев А. Исследование „сетецентрических" концепций в вооруженных силах ведущих зарубежных стран / А. Кондратьев // Зарубежное военное обозрение. – 2010. – № 12. – С. 3–9.
140. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: навчальний посібник / Б.А. Кормич. – К.: Кондор, 2008. – 384 с.
141. Коровин В. Главная военная тайна США. Сетевые войны / В. Коровин. – М.: Яуза: Эксмо, 2009. – 86 с.
142. Коровин В. Третья мировая сетевая война [Електронний ресурс] / В. Коровин. – Питер: Санкт-Петербург, 2014. – Режим доступу: http://www.litres.ru/pages/biblio_book/?art=8481662
143. Корреспондент.net. Хакери створюють „Українські кібервійська" для протидії інформаційній війні [Електронний ресурс]. – 12 червня 2014. – Режим доступу: http://ua.korrespondent.net/ukraine/politics/3377310-khakery-stvoruiuit-ukrainski-kiberviiska-dlia-protydii-informatsiinii-viini
144. Костина А.В. Тенденции развития культуры информационного общества: анализ современных информационных и постиндустриальных концепций [Електронний ресурс] / А.В. Костина // Информационный гуманитарный портал „Знание. Понимание. Умение". – № 4. – 2009. – Культурология. – Режим доступу: http://www.zpu-journal.ru/e-zpu/2009/4/Kostina_Information_Society
145. Коттер Брайн П. Русский мир / П. Коттер Брайн // Concordiam. Журнал по проблемам безопасности и обороны в Европе. – 2016. – Специальный выпуск: „Противодействие российской пропаганде". – С. 31–35.
146. Кочнев И.П. Концепция преэмптивной войны и пограничная безопасность государства / И.П. Кочнев // XII всероссийское совещание по проблемам управления ВСПУ-2014, Москва 16–19 июня 2014 г. – С. 6214–6219.
147. Кравець Є.Я. Інформаційна безпека держави / Є.Я. Кравець // Юридична енциклопедія: В 6 т. [редкол.: Ю.С. Шемшученко (голова) та ін.]. – К.: Укр. енцикл., 1998. – 1999. – Т. 2. – 744 с.
148. Кравченко В.Ю. Теорія «Гібридної війни»: український вимір / В.Ю. Кравченко // Вісник Дніпропетровського університету. – 2015. – № 2. – С. 139–148.

149. Кривошееєва О.І. Громадсько-політичні рухи в глобальному інформаційному просторі / О.І. Кривошееєва // Гілея. – 2013. – № 68. – С. 883–888.
150. Круглов Д. Силы кибероперацій и информационного обеспечения бундесвера (2017) / Д. Круглов // Зарубежное военное обозрение. – 2017. – №7. – С. 23–25.
151. Крупнов Ю. Преэмптивная война [Електронний ресурс] / Юрий Крупнов. – Режим доступу: httm: www. kroupnov. ru /5/30 1shtml
152. Кузьмин И. Future Combat System – революция или эволюция? [Електронний ресурс]. / И. Кузьмин. – Режим доступу: http://www. 3dnewsru/ editorial/ future_combat_system
153. Кучма Л. Аксіологічний вимір політичного маніпулювання [Електронний ресурс] / Л. Кучма. – Режим доступу: http // www. ena.lp.edu.ua: 8080/bitstream/ ntb/7862/7862/1/21/pdfn2
154. Курбан А.В. Современные информационные войны в социальных онлайн-сетях / А.В. Курбан // Information Society. 2016. Issue 23 (January-June). – С. 83–90.
155. Лещев В. Названы самые боеспособные страны в киберпространстве [Електронний ресурс] / LIFE.RU. 10 января 2017. – Режим доступу: https://life.ru/t/%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B8/957102/nazvany_samyie_boiesposobnyie_strany_v_kibierprostranstvie
156. Ливенко В.І. Інформаційне протиборство у політичній сфері: до уточнення базових термінологічних конструкцій / В.І. Ливенко // Нова парадигма. – 2012. – Вип. 108. – С. 136–144.
157. Лібікі М. Що таке інформаційна війна? http:// viysko.com.ua/texnologiji-voyen/martin-libiki-shhotake-informacijna-vijna/
158. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції / В.А. Ліпкан, Ю.Є. Максименко, В.М. Желіховський: навч. посібник. – К.: КНТ, 2006. – 280 с.
159. Літнарович Р.М. Сучасні технології інформаційної безпеки. Частина 1: навчальний посібник / Р.М. Літнарович. – Рівне: МЕГУ, 2011. – 97 с.
160. Лопатин В.Н. Информационная безопасность России: Человек. Общество. Государство / В.Н. Лопатин. – Спб: Фонд «Университет», 2000. – 428 с.

161. Лугуценко Т.В. Людина в структурі комунікативної реальності як суб'єкт віртуального простору / Т.В. Лугуценко // Гілея. – 2014. – № 81. – С. 179–183.
162. Лук'яненко О. Геополітичне інформаційне протиборство: сутність і варіанти захисту / О.Лук'яненко // Університетська кафедра. − 2016. − № 5. − С. 173–184.
163. Любарський С.В. Місце та роль мережевої розвідки в моделях інформаційного протиборства / С.В. Любарський // Збірник наукових праць ВІТІ НТУУ „КПІ". – 2013. – № 1. – С. 31–39.
164. Магда Є. В. Виклики гібридної війни: інформаційний вимір / Є. В. Магда // Наукові записки Інституту законодавства Верховної Ради України. – 2014. – №5. – С. 138–142.
165. Макаренко А. Введение в сетецентрические информационно-управляющие системы [Електронний ресурс] / А. Макаренко. – 2010. – Режим доступу: http://www.rdcn.ru/estimation/2010/03042010.shtml
166. Макаренко Є.А. Міжнародні інформаційні відносини: монографія / Є.А. Макаренко. – К.: Наша культура і наука, 2002. – 452 с.
167. Макаров В. Война в сфере смыслов [Електронний ресурс] / Владимир Макаров // Реферативный журнал социокультурного и политического анализа (Тема выпуска: Постмодерн). – 2011. – Вып. 1 (Июнь 2011 г.). – 75 с. – Режим доступу: URL: http://sovschola.ru/content/rzhskpa-vyp-1-postmodern
168. Макеев А.В. Политология: учеб. пособие для вузов / А.В. Макеев. – М.: Юнити. – ДАНА, 2000. – 334 с.
169. Маклюэн Г.М. Галактика Гуттенберга. Сотворение человека печатной культуры [Електронний ресурс]; перевод с англ. и прим. А. Юдина. – М., 2003 // Центр гуманитарных технологий. – Режим доступу: URL: http:// gtmarket.ru/ laboratory/basis/3568
170. Маклюэн Г.М. Понимание Медиа: Внешние расширения человека / Пер. с англ. В. Николаева; Закл. ст. М. Вавилова. – М.; Жуковский: «КАНОН-пресс-Ц», «Кучково поле», 2003. – 464 с.
171. Малик І.Р. Інформаційні війни в Україні: історія, сучасний стан та перспективи [Електронний ресурс] / І.Р. Малик. – Режим доступу: Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua
172. Малик Я. Інформаційна війна і Україна / Я. Малик // „Демократичне врядування" Науковий вісник. – 2015. – Вип. 15. – Режим доступу: http://nbuv.gov.ua/UJRN/DeVr_2015_15_3

173. Манжай О.В. Використання кіберпростору в оперативно-розшуковій діяльності / О.В.Манжай // Право і Безпека. – 2009. – № 4. – С. 215–219.
174. Манойло А.В. Государственная информационная политика в условиях информационно-психологической войны / А.В. Манойло, А.И. Петренко, Д.П. Фролов. – М.: Горячая линия Телеком, 2009. – 541 с.
175. Манойло А.В. Государственная информационная политика в особых условиях [Електронний ресурс] / А.В. Манойло. – Режим доступу: http://razom.znaimo.com.ua/docs/45/index-18501.html
176. Манойло А.В. Управление психологической войной [Електронний ресурс] / А.В. Манойло. – Режим доступу: http ://andreymanoylo. vov. ru/ uprpsiv.html
177. Маринин С. Подходы военных экспертов в США к разработке понятийного апарата в сфере борьбы в киберпространстве / С. Маринин // Зарубежное военное обозрение. – 2011. – № 10. – С. 24–30.
178. Маруховський О.О. Політичні аспекти зарубіжних концепцій інформаційного суспільства : дис. … на здобуття наук. ступеня канд. політ. наук : спец. 23.00.01 „Теорія та історія політичної науки” / Маруховський Олег Олександрович; НАН України, Інститут політичних і етнонаціональних досліджень ім. І.Ф. Кураса. – К, 2008. – 239 с.
179. Махлуп Ф. Производство и распространение знаний в США / Ф. Махлуп. – М.: Прогресс, 1966. – 462 с.
180. Медвідь Ф. Інформаційна безпека України: виклики й загрози [Електронний ресурс] / Ф. Медвідь. – Режим доступу: http://nato.pu.if.ua/ journal/ 2009-2/2009-2-28.pdf
181. Мелин А. Особенности применения киберсредств в межгосударственных военных и внутренних конфликтах / А. Мелин, С. Маринин // Зарубежное военное обозрение. – 2013. – № 3. – С. 11–16.
182. Мелин А. Система подготовки Вооружённых сил США с участием сил кибероперацій / А. Мелин, С. Маринин // Зарубежное военное обозрение. – 2012. – № 5. – С. 20–24.
183. Меморандум про взаєморозуміння між Генеральним Директоратом з питань Інформаційного суспільства Європейської Комісії та Державним комітетом зв'язку та інформатизації України щодо розвитку Інформаційного суспільства [Електронний ресурс]. – Режим доступу: http:// zakon2.rada. gov.ua/ laws/show/994_447

184. Мешкова Т.А. Социально-политические аспекты глобальной информатизации / Т.А. Мешкова // Полис. – 2002. – № 6. – С. 24 – 33.
185. Микешина Л.А. Эпистемология ценностей / Л.А. Микешина. – М.: РОССПЭН, 2007. – 439 с.
186. Министерство обороны РФ набирает бойцов в кибервойска [Електронний ресурс]. – 20.04.2014. – Режим доступу: http://ru-an.info
187. Мироненко Г.В. Інтернет-психологія: напрями досліджень і перспективи розвитку / Г.В. Мироненко, Н.В. Климчук // Ученые записки Таврического національного университета им. В.И. Вернадского. Серия „Филология. Социальная коммуникация”. – 2008. – Том 21 (60). – № 1. – С. 333–337.
188. Моисеев Н.Н. Информационное общество как этап новейшей истории / Н.Н. Моисеев // Свободная мысль. – 1996. – № 1. – С. 81–83.
189. Морально-психологічне забезпечення у Збройних Силах України: підручник: у 2 ч. Ч. 1 / [В.М. Вилко, В.М. Грицюк, В.Г. Дикун та ін.] ; за заг. ред. В.В. Стасюка. – К.: НУОУ, 2012. – 464 с.
190. Морозов А.М. От физической к психологической войне. Эволюция форм войны в процессе развития цивилизации [Електронний ресурс] / А.М. Морозов. – Режим доступу: http://psyfactor.org/biowar.htm
191. Морозов Ю.В. Балканы сегодня и завтра: военно-политические аспекты миротворчества / Ю.В. Морозов, В.Ю. Глушков, А.С. Шаравин. – М.: ЦВСИ ГШ ВС РФ, 2001. – 376 с.
192. Московитов Н. Перспективы создания Глобальной информационной сети МО США / Н. Москвитов, Г. Рыбаков // Зарубежное военное обозрение. – 2013. – № 7. – С. 8–19.
193. Набруско В. Чи стане Україна господарем у власному інформаційному просторі? / В. Набруско // Дзеркало тижня. – 2008. – № 34 (713). – 13 вересня.
194. Най Дж. „Мягкая” сила и американо-европейские отношениях [Електронний ресурс] / Дж. Най // Свободная мысль. – XXI. – 2004. – № 10. – Режим доступу: http://www.postindustrial.net
195. Начальник генштаба ЦАХАЛа приказал начать формирование кибервойск [Електронний ресурс] // Cursorinfo. – Режим доступу: https://cursorinfo.co.il/. – Назва з екрану.
196. Начгенштаба ЦАХАЛа отказался от идеи создания войск кибербезопасности [Електронний ресурс] // NEWSRU.CO.IL. – Режим доступу: http://m.newsru.co.il/israel/02jan2017/cyber303.html. – Назва з екрану.

197. Национальное управление по киберзащите создадут в Израиле [Електронний ресурс] // TADVISER. – Режим доступу: http://www.tadviser.ru/index.php/Статья:Киберпреступность_и_киберконфликты_:_Израиль#2015:_ . – Назва з екрану.
198. Національна безпека у філософсько-правовому дискурсі: монографія / О.Г.Данильян, О.П.Дзьобань, Є.М.Білоусов, Ю.Ю.Калиновський, І.В.Яковюк. – Харків: б/в, 2019. – 244 с.
199. Нижник Н.Р. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): Навчальний посібник / За заг. ред. П.В. Мельника, Н.Р. Нижник. – Ірпінь: Академія ДПС України, 2000. – 304 с.
200. Николаев Н. Взгляды военно-политического руководства США на ведение вооруженной борьбы в современных условиях / Н. Николаев // Зарубежное военное обозрение. – 2014. – № 3. – С. 3–7.
201. Новая военная доктрина РФ: подготовка к масштабной войне // Українська правда. – 9 марта 2019. – Режим доступу: https://www.pravda.com.ua/rus/news/2019/03/9/7208764/
202. Новая философская энциклопедия: в 4 т. / Ин-т философии РАН, Нац. общ-науч. фонд. – Т. II. – М.: Мысль, 2010. – 634 с.
203. Окинавская хартия глобального информационного общества [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/998_163
204. Олевский В. Концепция „стратегической пропаганды НАТО” / В. Олевский // Зарубежное военное обозрение. – 2014. – № 9. – С. 9–16.
205. Олевский В. Концепция „стратегической пропаганды НАТО” / В. Олевский // Зарубежное военное обозрение. – 2014. – № 10. – С. 19–28.
206. Олегин А. Силы кибероперацій сухопутных войск США. Взгляды американского командования на их применение / А. Олегин, М. Алтуфьев // Зарубежное военное обозрение. – 2014. – № 1. – С. 41–46.
207. Олкотт М.Б. Второй шанс Центральной Азии / М.Б. Олкотт. – М.: Моск. Центр Карнеги; Вашингтон: Фонд Карнеги за Междунар. мир, 2005. – 487 с.
208. Основи демократії: підруч. для студ. вищ. навч. закл. ; ред. Антоніна Колодій. – 3-тє вид., оновлене і доп. – Л.: Астролябія, 2009. – 832 с.
209. Основні поняття маніпулятивного впливу [Електронний ресурс]. – Режим доступу: http://psychlib.com.ua/osnovni-ponyattya-manipulyativnogo-vplivu.htm

210. Отюцкий Г.П. Информационная антропология: предмет и проблематика / Г.П. Отюцкий // Гілея. – 2013. – № 70. – С. 473–477.
211. Офіційний сайт інституту ім. Горшеніна. – Режим доступу: institute. – gorshenin.ua/researches/29_Sostoeanie_ukrainskoy_armii.html
212. Павліченко О.О. Сутнісні характеристики сучасної інформаційної війни // Науковий семінар Харківського національного університету Повітряних Сил імені Івана Кожедуба „Інформаційна агресія Російської Федерації проти України": тези доповідей, 25 жовтня 2018 року. – Х.: ХНУПС ім. І. Кожедуба. – С. 42–46.
213. Панарин И.Н. Информационная война и мир / И.Н. Панарин, П.Г. Панарина. – М.: ОЛМА-ПРЕСС, 2003. – 204 с.
214. Панін В.Г. Різновиди та тенденції розвитку інформаційної зброї / В.Г. Панін, О.Л. Борзяк, Лалетін С.П. // Вісник Київського національного університету імені Т. Шевченка. – 2012. – Вип. 28. – С. 4–6.
215. Патьял Р. Принципы войны: необходимость переосмысления / Раджпут Патьял // Геополитика. Информационно-аналитическое издание. Тема выпуска: Война. – Вып. XXI. – М.: МГУ им. М. Ломоносова. – 162 с.
216. Певцов В. Информационное противостояние организации ХАМАС и Израиля в новом тысячелетии / В. Певцов // Зарубежное военное обозрение. – 2013. – № 6. – С. 28–33.
217. Пилипчук В.Г., Дзьобань О.П. Інформаційне суспільство: філософсько-правовий вимір: Монографія / В.Г. Пилипчук , О.П. Дзьобань. – Ужгород, 2014. – 282 с.
218. Писаренко О.Л. Розвиток сучасного суспільства в умовах інформаційної нестабільності / О.Л. Писаренко // Розвиток сучасного суспільства в умовах глобальної нестабільності: мат. міжнар. наук.-практ. конф. – Одеса, 2013. – С. 46.
219. Погорєлова І. Медіакратія [Електронний ресурс] / І. Погорєлова. – Режим доступу: http://www.day.kiev.ua/uk/article/podrobici/mediakratiya
220. Політологічний енциклопедичний словник [Упор. В.П. Горбатенко; за ред. Ю.С. Шемшученка та ін.]. – 2-ге вид., доп. і перероб. – К.: Ґенеза, 2004. – 736 с.
221. Польских Л. О применении глобальной компъютерной сети Интернет в интересах информационного противоборства / Л. Польских // Зарубежное военное обозрение. – 2005. – № 7. – С. 20–23.

222. Польша создает кибервойска [Електонний ресурс] // REGNUM. 5 февраля 2019, 20:43. – Режим доступу: https://regnum.ru/news/polit/2566806.html
223. Попов В.Д. Государственная информационная политика: состояние и проблемы формирования. Массовые информационные процессы в современной России: очерки; отв. ред. А.В. Шевченко. – М.: РАГС, 2004. – 306 с.
224. Попов И. Сетецентрическая война. Готова ли к ней Россия? // Красная звезда. – 13.09.2012 [Електронний ресурс]. / И. Попов– Режим доступу: http://www. redstar. ru/index.php/news-menu/ino-military-menu/usarmy/item/4659-setetsentricheskaya-voyna
225. Попов И.М. Сетецентрическая война Пентагона // Независимое военное обозрение [Електронний ресурс] / И.М. Попов. – 2004. – № 9 (369). – Режим доступу: http://nvong.ru/concepts/2004-03-12/1_pentagonhtml
226. Попов М.О. До забезпечення воєнної безпеки в умовах загрози інформаційної війни / М.О. Попов, А.Г. Лук'янець // Наука і оборона: наук.-теорет. та наук.-практ. журнал. – 1999. – № 2. – С. 37–43.
227. Почепцов Г. Інформаційна політика: навч. посіб. / Г. Почепцов, С. Чукут. – К.: вид-во УАДУ, 2002. – Ч. 1. – 88 с.
228. Почепцов Г.Г. Информационные войны / Г.Г. Почепцов. – М.: Рефл-бук, К.: Ваклер, 2000. – 576 с.
229. Почепцов Г.Г. Пропаганда и контрпропаганда/ Г.Г. Почепцов – М.: Центр, 2004. – 256 с.
230. Почепцов Г. Революция. com. Основы протестной инженерии [Електронний ресурс] / Георгий Почепцов. – Москва: Европа, 2005. – Режим доступу: http://www.litres.ru/pages/biblio_book/?art=3006095
231. Правительство утвердило создание новых „кибервойск” [Електронний ресурс] // NEWS.RAMBLE. – Режим доступу: http://news.rambler.ru/27363679/. – Назва з екрану.
232. Прайс М. Телевидение, телекоммуникации и переходный период: право, общество и национальная идентичность / М. Прайс. – М.: Изд-во Моск. ун-та, 2000. – 336 с.
233. Председатель КНШ ВС США о защите военных компъютерных сетей // Зарубежное военное обозрение. – 2013. – № 8. – С. 105.
234. Присяжнюк М. Аналіз засобів ведення інформаційної боротьби з використанням інформаційних технологій, форм і способів їх застосування [Електронний ресурс] / М. Присяжнюк, Я. Жарков. – Режим доступу: http://

defpol.org.ua/site/index.php/uk/component/content/article/51-kolonkaavtora/56-10082009
235. Присяжнюк М.М., Цифра Є.І. Особливості забезпечення кібербезпеки / М.М.Присяжнюк, Є.І.Цифра // Реєстрація, зберігання і обробка даних. – 2017. – Т.2. – С. 61–68 – Режим доступу: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/131678/06-Prysiazhniuk.pdf?sequence=1
236. Присяжнюк М.М. Прийоми маніпулювання свідомістю людей через засоби масової інформації [Електронний ресурс] / М.М. Присяжнюк. – Режим доступу: http//www.nbuv.gov.ua /portal/natural/sitsbo/01-18/01-18.pdf
237. Проблема захисту національних інтересів України у сфері державної безпеки в умовах геополітичних трансформацій XXI століття: Монографія / О.П. Дзьобань, В.Я. Настюк, В.В. Бєлєвцева. – Харків: Право, 2013. – 296 с.
238. Прохоров Е.П. Введение в теорию журналистики: учебник для студентов вузов / Е.П. Прохоров. – 7-е изд., испр. и доп. – М.: Аспект Пресс, 2009. – 368 с.
239. Радіо Свобода. Путін веде в Україні гібридну війну – генерал Каппен [Електронний ресурс]. – Режим доступу: ww.radiosvoboda.org/ content/ article/ 25363591.html
240. Расторгуев С.П. Информационная война / С.П. Расторгуев. – М.: Радио и связь, 1998. – 416 с.
241. Рекомендації парламентських слухань на тему: „Законодавче забезпечення розвитку інформаційного суспільства в Україні” [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/1565-vii
242. Ремизов М. Неоколониальная революция: осмысление вызова / М. Ремизов // Стратегический журнал. – 2005. – № 1. – С. 83–88.
243. Рогов П.Д. Проблеми та шляхи організації захисту особового складу військ (сил) від негативного інформаційно-психологічного впливу / П.Д. Рогов, М.А. Малахов, Л.В. Бухало, Ю.В. Турченко // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: вид-во ВІКНУ, 2013. –
С. 91–98.
244. Романенко Ю.М. Мифология конфликта, или Конфронтация образов / Ю.М. Романенко // Конфликтология. – Спб. – 2004. – № 2. – С. 15–20.

245. Сайт Французские конституции [Електронний ресурс]. – Режим доступу: http://www.labex.ru/page/konst_france.html
246. Рудницька У.І. Інформаційні війни як засіб геополітичного протистояння / У.І. Рудницька // Гуманітарний журнал. – 2015. – №1-2. зима-весна. – С. 134–139.
247. Северинчик О.П. Маніпулятивний аспект діяльності ЗМІ / О.П. Северинчик // Філософія і соціологія в контексті сучасної культури: Збірник наукових праць – Дніпропетровськ: ДНУ, 2008. – С. 326–329.
248. СєйТВ. Японія створила кібервійська [Електронний ресурс]. – Режим доступу: http://say.tv/day_block2/topic/14273
249. Семен Н.Ф. Російські інтернет-ресурси як чинник інформаційної війни проти України (на прикладі сайтів «Правда.ру» та «Российский диалог») / автореф. … здобуття наукового ступеня кандидата наук із соціальних комунікацій. – спец. 27.00.01 – теорія та історія соціальних комунікацій. / Н.Ф. Семен. – Дніпро, 2018. – 23 с.
250. Сенченко М. Четверта світова. Інформаційно-психологічна війна [Електронний ресурс] / Микола Сенченко. – К.: ФОП Стебляк М.І., 2014. – 384 с. – Режим доступу: https://lib.rus.ec/b/241595/read
251. Серов А. О роли дезинформации в современных конфликтах и войнах / А. Серов // Зарубежное военное обозрение. – 2011. – № 7. – С. 15–21.
252. Скаленко А.К. Глобальные резервы роста / А.К. Скаленко. – К.: Информационно-издательский центр „Интеллект”, 2002. – 428 с.
253. Скуленко М.І. Логічні засади пропаганди: монографія / М.І. Скуленко. – Запоріжжя: Вид-во КПУ, 2010. – 312 с.
254. Слипченко В. Природа войны: вчера, сегодня, завтра / В. Слипченко. – М.: Третий Рим, 2004. – 196 с.
255. СМИ и политика: учебное пособие ; под ред. Л.Л. Реснянской. – М.: Аспект Пресс, 2007. – 256 с.
256. Стадніченко О.І. Інформаційна безпека України: стан і перспективи розвитку / О.І. Стадніченко // Вісник Маріупольського державного університету серія: Історія. Політологія. – 2011. – № 2. – С. 101–106.
257. Старіш О.Г. Інформаційна політика держави в контексті глобалізації [Електронний ресурс]: дис. … д-ра наук : спец. 23.00.03 – 2008 / О.Г. Старіш. – Режим доступу: http://www.lib.ua-ru.net/diss/cont/349643.html

258. Стратегія інтеграції України до Європейського Союзу [Електронний ресурс]. – Режим доступу: http:// zakon4.rada.gov.ua/ laws/ show/ 615/98
259. Стратегія розвитку інформаційного суспільства в Україні [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/386-2013-%D1%80
260. Стрельбицька Л.М. Забезпечення багатоманітності поглядів і єдності нації в умовах сучасної інформаційної війни / Л.М. Стрельбицька, М.П. Стрельбицький // Інформаційна безпека людини, суспільства, держави. – 2011. – № 3 (7). – С. 78–81.
261. Сулейменов С. Неуловимые кибервойска [Електронний ресурс] / С. Сулейманов. –12.05.2014. – Режим доступу: http://tjournal.ru/paper/cyber-warfare
262. Сун-Цзы. Трактаты о военном искусстве / Сун-Цзы, У-Цзы. – М.: АСТ, 2002. – 558 с.
263. Супрунов Ю.М. Нормативно-правове забезпечення розгортання систем кібернетичної оборони провідних країн світу / Ю.М. Супрунов // Інформаційна безпека людини, суспільства, держави. – 2011. – № 1 (5). – С. 85–89.
264. Сусська О. Право людини на інформацію як базова ознака комунікативних стосунків в інформаційному суспільстві / Ольга Сусська // Комунікація. – 2012. – № 2. – С. 30–41.
265. Сучасне суспільство: філософсько-правове дослідження актуальних проблем: монографія / О.Г. Данильян, О.П. Дзьобань, С.Б. Жданенко та ін.; за ред. О.Г. Данильяна. – 2-ге видан., перероб. і допов. – Харків: Право, 2017. – 416 с.
266. Тавокин Е.П. Системные основы государственной информационной политики. Массовые информационные процессы в современной России: очерки; отв. ред. А.В. Шевченко. – М.: РАГС, 2002. – С. 31–42.
267. Телелим В. Планування сил для виконання бойових завдань у «гібридній війні» / В. Телелим, Д. Музиченко, Ю. Пунда // Наука і оборона. – 2014. – № 3. – С. 30–35.
268. Тишков В. Отрицание России [Електронний ресурс] / В. Тишков // Отечественные записки. – 2005. – № 1. – С. 240–252. – Режим доступу: http:// www.strana-oz.ru/?numid=22&article=1021
269. Ткаченко В.М. Патріотизм // Енциклопедія освіти / Василь Михайлович Ткаченко. – К.: Юрінком Інтер, 2008. – 1040 с.

270. Ткачова Ю. Ціннісно-комунікативні характеристики науки в умовах інформаційного суспільства / Ю. Ткачова // Гілея. – 2014. – № 86. – С. 215–218.
271. Толубко В.Б. Підготовка і ведення інформаційної боротьби в Збройних Силах: навч. посіб. / В.Б. Толубко, Я.М. Жарков, І.В. Замаруєва, А.О. Рось та ін. За ред. В.Б. Толубка. – К.: НАОУ, 2004. – 280 с.
272. Тоффлер Э. Война и антивойна. Что такое война и как с ней бороться. Как выжить на рассвете XXI века / Э. Тоффлер, Х. Тоффлер. – М.: Аст: Транзиткнига, 2005. – 412 с.
273. Тоффлер Э. Метаморфозы власти / Э. Тоффлер ; пер. с англ. – М.: АСТ, 2003. – 669 с.
274. Тофлер Е. Третя Хвиля / Елвін Тофлер ; пер. з англ. Андрія Євса. – К.: Всесвіт, 2000. – 475 с.
275. Тоффлер Э. Третья волна / Э. Тоффлер. – М.: АСТ, 1999. – 784 с.
276. Тоффлер Э. Шок будущего / Э. Тоффлер. – М.: АСТ, 2002. – 557 с.
277. Требін М. Феномен «гібридної» війни / М. Требін // Гілея. – 2014. – Випуск 87(8). – С. 366–371.
278. Требін М.П. Феномен інформаційної війни в світі, що глобалізується // Вісник Національного університету „Юридична академія імені Ярослава Мудрого”. – 2014. – № 2(16). – С. 188–198.
279. Тулин С. Органы управления ВС США боевыми действиями в кибернетическом пространстве / Сергей Тулин // Зарубежное военное обозрение. – 2012. – № 2. – С. 3–10.
280. Украина заняла 87 место в мире по уровню развития електронного правительства [Електронний ресурс]. – Режим доступу: http:// www.unian.net/ science/933604-ukraina-zanyala-87-e-mesto-v-mire-po-urovnyu-razvitiya-elektronnogo- pravitelstva.html
281. Українські підручники он-лайн. Психофізична зброя [Електронний ресурс]. – Режим доступу: http:// pidruchniki. ws/ 1334020336973/ politologiya/ psihotronna_psihofizichna_zbroya
282. Философский словарь от А до Я [Електронний ресурс]. – Режим доступу: http://yandex.ua/yandsearch?p=2&text=родинаclid=48648&lr=144&tld=ua
283. Филенков А. Обучение офицеров ВС США ведению разведки в киберпространстве / А. Филенков // Зарубежное военное обозрение. – 2019. – № 1. – С. 24–26.
284. Фісун А.О. Ґенеза поняття „інформаційна війна” / А.О. Фісун // Гілея. – 2011. – № 49. – С. 534–538.

285. Фурашев В.М. Інформаційні операції крізь призму системи моніторингу та інтеграції Інтернет-ресурсів / В.М. Фурашев, Д.В. Ланде // Правова інформатика. – 2009. – № 2(22). – С. 49–57.
286. Халипов В.Ф. Власть. Основы кратологии / В.Ф. Халипов. – М.: Луч, 1995. – 304 с.
287. Хантингтон С. Столкновение цивилизаций / С. Хантингтон; под общ. ред. К. Королева; пер. с англ. Т. Велимееева, Ю. Новикова. – М.: АСТ, 2003. – 603 с.
288. Хелд Д., Гольдблатт Д., Макгрю Э., Перратон Дж. Глобальные трансформации политика, экономика, культура / Д. Хелд [и др.]. – М.: Праксис, 2004. – 576 с.
289. Хоффман Ф. Гибридные угрозы: переосмысление изменяющегося характера современных конфликтов / Фрэнк Г. Хоффман // Геополитика. Информационно-аналитическое издание. Тема выпуска: Война. – Вып. XXI. – М.: МГУ им. М. Ломоносова. – 162 с.
290. ЦАХАЛ усиливает киберзащиту [Електронний ресурс] // jewish.ru. 13.01. 2013. – Режим доступу: https://jewish.ru/ru/news/articles/158611/. – Назва з екрану
291. ЦАХАЛ формирует новые кибер-войска [Електронний ресурс] // Mignews. – Режим доступу: http://mignews.com/news/130112_104545_00238.html. – Назва з екрану.
292. Центр інформаційної безпеки. Іран офіційно визнав: у нього є кібервійська. – 15.03.2011. – Режим доступу: http://www.bezpeka. com/ua/ news/ 2011/03/15/iran-has-cyberforces.html
293. Чернов А.А. Становление глобального информационного общества: проблемы и перспективы : монографія / А.А. Чернов. – М.: «Дашков и К°», 2003. – 232 с.
294. Чирва Р. Інформаційна війна – зброя, страшніша за ядерну [Текст] / Раїса Чирва // Профспілкові вісті. – 2014. – № 13. – С. 8–9.
295. Шариков П.А. США хотят стать планетарным модератором. Американская глобальная стратегия развития киберпространства в полицентричном мире [Електронний ресурс] / П.А. Шариков // Независимое военное обозрение. – 01.07.2011. – Режим доступу: http://pentagonus.ru/ publ/ amerikanskaja_globalnaja_strategija_razvitija_kiberprostranstva_v_policentrichnom_mire/19-1-0-1765
296. Шарп Дж. Від диктатури до демократії: концептуальні засади здобуття свободи / Пер. з англ. Ін-т ім. Альберта Ейнштейна. — Львів : Сполом, 2004. – 83 с.

297. Шевченко М.М. Методологічні засади аналізу міждержавного протиборства / М.М. Шевченко // Нова парадигма / гол. ред. В.П. Бех. – К. : Вид-во НПУ ім. М. Драгоманова, 2007. – Вип. 68. – С. 125–133.
298. Шлындов А. Минобороны в поиске интеллектуалов [Електронний ресурс] / А. Шлындов, Н. Требин // Независимое военное обозрение. – 29.06.2012. – Режим доступу: http://nvo.ng.ru/forces/2012-06-29/ 11_minoborony. html
299. Шпига П.С. Основні технології та закономірності інформаційної війни [Текст] / П.С. Шпига, Р.М. Рудник // Проблеми міжнародних відносин . – 2014. – Вип. 8. – С. 326–339.
300. Шумка А.В. Інформаційно-мережева війна – нова форма міждержавного протиборства початку XXI ст. / А.В. Шумка, П.П. Черник // Військово-науковий вісник. – 2013. – Вип. 19. – С. 243–255.
301. Яковец Ю.В. Глобализация и взаимодействие цивилизаций / Ю.В. Яковец. – М.: Экономика, 2001. – 346 с.
302. Яковлева Н.І. Пропаганда як складова політичної комунікації: автореф. дис. … канд. політ. наук : спец. 23.00.02 „Політичні інститути та процеси” / Н.І. Яковлева. – К., 2010. – 18 с.
303. Adams J. The Next World War. Computers Are the Weapons and the Front Line Is Everywhere / Adams James. – NewYork, 1998. – 368 p.
304. Alberts David S. Defensive Information Warfare. National Defense University Press, 1996 [Електронний ресурс]. – Режим доступу: http:// www. dodccrp.org/ files/Alberts_Defensive.pdf
305. Alberts D.S., Garstka J.J., Stein F.P. Network Centric Warfare: Developing and Leveraging Information Superiority / D.S. Alberts, J.J. Garstka, F.P.Stein // CCRP Publ., 2nd Edition (Revised). Aug 1999, Second Print Feb. – 2000. – P. 284 [Електронний ресурс]. – Режим доступу: http://www.dodccrp.org/files/Alberts_NCW.pdf
306. Anheier H. etal. Introducing Global Civil Society // Ed. by Helmut Anheier, Marlies Glasius and Mary Kaldor; Global Civil Society 2001; Centre for Civil Societyand Centre for the Study of Global Governance; London School of Economics and Political Science. Oxford University Press, 2001. – P. 3–22.
307. Arquilla J. Cyber war is Coming! Comparative Strategy 2 (April-June 1993) / Arquilla John., Ronfeldt David. [Електронний ресурс]. – Режим доступу: http:// www.rand.org/ pubs/reprints/RP223.html
308. Bar-Ilan J. Information hub blogs / J. Bar-Ilan // Journal of Information Science. – 2005. – Vol. 7. – No. 4. – P. 297–307.

309. Bond, Margaret. Hybrid War: A New Paradigm for Stability Operations in Failing States, Carlisle arracks, PA: U.S. Army War College, March 30, 2007.
310. Braman S. Defining information policy. Journal of Information Policy, 1(1), 1–5, 2011 [Електронний ресурс]. – Режим доступу: http:// jip.vmhost. psu.edu/ ojs/index.php/jip/article/viewFile/19/14
311. Bryant W.D. Cyberspacesuperiority. A conceptual model / W.D. Bryant // Air & Space Power Journal. – 2013. – November – December.
312. Brzezinski Zb. Between Two Ages. America's Role in the Technetronic Era / Zb. Brzezinski. – N.Y.: Viking Press, 1970. – 334 p.
313. Butler S.C. Refocusing cyberwarfare thought / S.C. Butler // Air & Space Power Journal. – 2013. – January – Februaty.
314. Castells M. Informationalism, Networks, and the Network Society: a Theoretical Blueprinting, The network society: a Cross–Cultural Perspective [Електронний ресурс]. – Northampton, MA: Edward Elgar, 2004. – Режим доступу: http://annenberg.usc.edu/Faculty/Communication/~/media/Faculty/ Facpdfs/ Informationalism%20pdf.ashx
315. Castells M. The New Public Sphere: Global Civil Society, Communication Networks, and Global Governance / M. Castells // The ANNALS of the American Academy of Political and Social Science. – 2008. – Vol. 616. – No. 1. – P. 78–93.
316. Cebrovski A. Network Centric Warfare and information Superiority. / A. Cebrovski. – RUSI. Whitehall. London. – 2000
317. China's Secret Cyberterrorism [Електронний ресурс]. – Режим доступу: http://www.thedailybeast.com/blogs-andstories/2010-01-13/chinas-secret-cyber-terrorism/full
318. Coale John C. Fighting Cybercrime / John C. Coale // Military Review. – March-April. – 1998. – P. 77–82.
319. Dahl R. The Concept of Power [Електронний ресурс] / R. Dahl // Behavioral Science. – 1957. – No 2. – P. 201–215. – Режим доступу: http:// openpdf.com/ebook/robert-dahl-pdf.html
320. Daniel Bell. The Coming of Post' Industrial Society: A Venture in Social Forecasting. Harmonds worth: Penguin, Peregrine, 1973 [Електронний ресурс]. – Режим доступу: http://www.worldcat.org/title/coming-of-post-industrial-society-a-venture-in-social-forecasting/oclc/16377221
321. DoDD 8000.01. Management of the Department of Defense Information Enterprise, dated February 10. – 2009. – P. 11. [Електронний

ресурс]. – Режим доступу: http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf
322. Easton D., Dennis J. Children in the Political System / D. Easton, J. Dennis. – N.Y., 1969, Handbook of Political Socialization. Theory and Research. – N.Y., 1977.
323. Galeotti, Mark. The ‘Gerasimov doctrine’ and Russian Non-Linear War. In Moscow’s shadows. 6 July 2014, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimovdoctrine-and-russian-non-linear-war/
324. Garstka J. Network Centric Warfare: An Overview of Emerging Theory / J. Garstka. – PHALANX. – December. – 2000. – № 4. - P. 28 – 33.
325. Geers K. Cyber spaceand the chang in gnature of warfare [Електронний ресурс]. – Режим доступу: http://www.scmagazineus.com/Cyberspace-and-the-changing-nature-of-arfare/article/115929/
326. Gertz B. Russia, China, Iran Waging Political Warfare, Report Says [Electronic resource] / Bill Gertz // The Washington Free Beacon. – Access mode: http://freebeacon.com/national-security/ russia-china-iran-waging-unconventional-warfare-report-says/. (Accessed 20 Febrary 2015).
327. Giddens A. The thirdway: the renewal of social democracy [Електронний ресурс] / Anthony Giddens. – Cambridge: PolityPress, 1998. – 166 p. – Режим доступу: http://www.lib.miamioh.edu/multifacet/record/mu3ugb2687994
328. Goban-Klas T. Media i komunikowanie masove. Teorie i analizyprasy, radia, telewizji i Internetu / T. Goban-Klas. – Warszawa–Krakow: Wydawnictwo naukowe PWN, 1999. – 336 s.
329. Hoffman F. Further Thoughts on Hybrid Threats [Electronic resource] / F. Hoffman // Small Wars Journal. – Access mode: www.smallwarsjournal.com/blog/2009/03/further-thoughts-onhybrid-thr/. (Accessed 20 Febrary 2015).
330. Hoffman F. G. Hybrid vs. compound war / F. G. Hoffman // Armed Forces Journal, Oct. 2009.
331. Hula R. Information Wars Concepts in Present Social and Communication Technologies Realities / R. Hula, I. Perederii, O. Vitrynska // International journal of Engineering and Technology, 7 (4/8) (2018). P. 741 – 744.
332. Hutchins S.G., Kleinman D.L., Hocevar S.P., Kemple W.G. and Porter G.R. Enablers of Self-synchronization for Network-Centric Operations: Designof a Complex Command and Control Experiment //Proceedings of the 6 the international command and control research and

technology symposium, CCRP, Annapolis, MD, USA, 2001 [Електронний ресурс]. – Режим доступу: www.dtic.mil/cgi-bin/ GetTRDoc?AD
333. Information Operations Roadmap – Do DUS. – 30 October 2003. – 78 p. [Електронний ресурс]. – Режим доступу: http://www.information-retrieval. info/ docs/info_ops_roadmap.pdf
334. Internet World States [Електронний ресурс]. – Режим доступу: http:// www.internetworldstats.com/stats4.htm#europe
335. Kuperwasser, Yosef. Lessons from Israel's Intelligence Reforms. The Saban Center for Middle East Policy at the Brookings Institute, 2007. – ANALYSIS PAPER. − № 14. − P. 7−9.
336. Laqueur W. Postmodern Terrorism / W. Laqueur // Foreign Affairs. – 1996. – № 75. – P. 35–44.
337. Lewis J.A. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies, December 2002. – P. 9.
338. Libicki M. What is Information Warfare? [Електронний ресурс]. – Режим доступу: http:// www.iwar. org.uk/iwar/resources/ndu/infowar/a003cont.html
339. McCuen J. Hybrid Wars / John McCuen // Military rewiew. – 2008. – March-April. – P. 108.
340. McDermott R. Does Russia Have a Gerasimov Doctrine? // Parameters : журнал. – 2016. – Spring (т. 46, № 1). – P. 97–105.
341. McKew Molly K. The Gerasimov Doctrine [Електронний ресурс] / Molly K. McKew // Politico Magazine, September/October 2017. – Режим доступу: https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538
342. Monaghan A. The «War» in Rusian's «Hybrid Warfare» // Parameters. – 2015–2016. – Winter (т. 45, № 4). – С. 65–74.
343. Narr S.J. Expanding Tolstoy and Shrinking Dostoyevsky // Military Review. – 2017. – September-October (т. 97, № 5). – P. 39.
344. Newson, Robert A. Counter-Unconventional Warfare Is the Way of the Future. How Can We Get There? In Janine Davidson Blogspot: Defense in Depth. October 23, 2014. http://blogs.cfr.org/davidson/2014/10/23/counterunconventional-warfare-is-the-way-of-the-future-how-can-we-get-there/
345. Norris P., Curtice J., Sanders D., Scammel M., Semetko H. On Message. Communikating the campaign. – London, 1999. – P. 9.

346. Oxford English Dictionary, second edition, edited by John Simpson and Edmund Weiner, Clarendon Press, 1989, twenty volumes, hardcover [Електронний ресурс]. – Режим доступу: http://www.oed.com/
347. Radin A. Hybrid Warfare in the Baltics. Threats and Potential Responses. – RAND Corporation, 2017. – (Project Air Force). – 48 p.
348. Robertson R. Globalization: Social Theory and Global Culture / Roland Robertson. – London: Sage Publications Ltd, 1992. – 224 p.
349. Shannon C.E. A Mathematical Theory of Communication [Електронний ресурс]. – Режим доступу: http://cm.bell-labs.com/cm/ms/what/ shannonday/ shannon1948.pdf
350. Statement by President Donald J. Trump on the Elevation of Cyber Command https://www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/
351. Summer A., Dunran Gr. E-COMMERCE. Маркетинг: Пятая волна. – М.: Русская редакция, 1999. – 187 с.
352. Szafranski R. A Theory of Information Warfare. Preparing For 2020 [Електронний ресурс]. – Режим доступу: http:// www.airpower. maxwell.af. mil/ airchronicles/apj/apj95/spr95_files/szfran.htm
353. The Networked Readiness Index 2013. – World Economic Forum [Електронний ресурс]. – Режим доступу: http:// www3.weforum.org/ docs/GITR/ 2013/ GITR_OverallRankings_2013.pdf
354. Van Audenhove L. Transnational Civil Society in the Networked Society: A study on the relation between ICTs and the rise of a transnational civil society / L. Van Audenhove, B. Cammaerts, V. Frissen, L. Engels., A. Ponsioen // Study in the framework of TERRA 2000, EU Project under IST 2000 for Instituteof Infonomics. – P. 17–23.
355. Van Creveld M. The Transformation of War: The Most Radical Reinterpretation of Armed Conflict Since Clausewitz. – Free Press, 1991. – 272 p.
356. Warkentin C. International Institutions, the State, and Global Civil Society in the Age of the World Wide Web /Craig Warkentin, Karen Mingst // Global Governance. – 2000. – Apr-Jun. – Vol. 6. – Issue 2. – P. 237–255.
357. Watcher. Україна створила кібервійська [Електронний ресурс]. – Режим доступу: http://watcher.com.ua/2014/05/22/ukrayina-stvoryla-kiber-viyska/
358. Wilkie R. Hybrid Warfare. Something Old, Not Something New / Robert Wilkie // Air & Space Power Journal. – 2009. – Vol. 23, № 4. – P. 13−17.

359. Williamson, Murray, and Peter Mansoor. Hybrid warfare: fighting complex opponents from the ancient world to the present. Cambridge University Press, 2012. – P. 3
360. Yoshihara T. Chinese Information Warfare: A Phantom Menace or Emerging Threat? – Strategic Studies Institute, U.S. Army War College. – 43 p.
361. "ל"צה של התמרון את שיבשה לא סייבר תקיפת שום" [Електронний ресурс] // ISRAEL DEFENCE. – № 8, 2018. – Режим доступу: http://www.israeldefense.co.il/he/content. – Назва з екрану.

СЛОВНИК

Агітація (лат. *agitatio* – приведення в рух, спонукання) – найважливіший засіб впливу на свідомість і настрій широких мас, з метою спонукати їх до політичної чи іншої активності, ідеологічна зброя боротьби наступального агресивного характеру.

Агресія (лат. *aggressio*– напад) – несумісне зі Статутом ООН пряме чи опосередковане застосування сили однією державою (чи групою держав) проти іншої, яке має на меті захоплення території, скасування або обмеження державної незалежності, насильницьке підкорення її населення.

Агресія інформаційна – масоване комплексне застосування сил і засобів інформаційно-комунікаційної інфраструктури однією державою (чи групою держав) проти іншої, метою якої є дестабілізація та зруйнування системи воєнно-політичного управління, розбалансування структурних компонентів національної економіки та перекодування ключових основ суспільної свідомості.

Акаунт – запис, що містить набір відомостей, які користувач передає будь-якій комп'ютерній системі.

Акти зовнішньої інформаційної агресії – легальні та/або протиправні інформаційні акції, реалізація яких негативно впливає на безпеку інформаційного простору держави та руйнує його.

Акція інформаційного впливу – одноразова акція інформаційно-психологічного та інформаційно-технічного впливу, яка передбачає спланований вплив на свідомість і поведінку людей шляхом поширення упередженої,неповної чи недостовірної інформації та (або) інформаційно-технічну інфраструктуру об’єкта (об’єктів).

Армія (від лат. *armare* – озброювати) – орган держави, призначений для здійснення її політики засобами збройного насильства. Державна військова організація, яка здатна вести збройну боротьбу на всіх рівнях – тактичному, оперативному, стратегічному.

Асиметрична війна – вид війни, який характеризується істотною різницею у військовій силі або можливостях використання стратегій і тактик сторонами-учасниками; конфлікт, в якому ресурси двох сторін суттєво різняться, і під час боротьби суперники намагаються використовувати характерні недоліки один одного.

Базовий протокол TCP/IP (Transmission Control Protocol Internet Protocol) – сукупність протоколів – систем стандартів і правил зв'язку та передавання інформації у глобальній мережі.

Блог – веб-сайт або персональний сайт, який містить короткі записи тимчасової важливості та значущості, має публічний характер

і передбачає широке обговорення у формі публічної полеміки в коментарях до блогозаписів або на власних блогах у середовищі мережевого спілкування.

Блогосфера – сегмент глобального інформаційного простору, який утворюється і функціонує яккомплекс взаємодіючих суб'єктів віртуального середовища та джерел інформації, щоформуютьсистему інформаційно-комунікаційних зв'язків, яка здатна до синергетичного оновлення, трансформації, розповсюдження та кореляції інформаційних ресурсів для маніпуляції суспільною свідомістю.

Боєздатність – визначений стан здатності військ (авіації, сил флоту) вести бойові дії, виконувати бойові завдання.

Бойова готовність – стан військ (сил), який дозволяє їм у встановлені строки почати бойові дії, у ході яких успішно виконувати бойові завдання.

Бойовий потенціал – узагальнена характеристика бойових можливостей (вогневих, ударних та маневрених) військового формування (об'єднання, з'єднання, частини або підрозділу) або зразка військової техніки та озброєння в певному виді бойових дій (наступі, обороні тощо), який розраховується математично та позначається числом.

Бойові дії в кіберпросторі – організовані акти відповідних частин і з'єднань. які скоординовані та взаємопов'язані за цілями, завданням, місцем та часом здійснюються одночасно і послідовно, а також маневру сил, що здійснюється за єдиним задумом і планом стратегічних, оперативно-стратегічних, оперативних і оперативно-тактичних завдань в кіберпросторі, які проводяться з метою досягнення перемоги у цій сфері та забезпечення інформаційної переваги над супротивником, дезорганізації та виводу з ладу його систем державного, військового та цивільного управління, а також порушення функціонування або знищення об'єктів критичної інфраструктури.

Бот – скорочена форма від «робот». Це акаунти неіснуючих персон, програми зі створення фейковий акаунтів, або боти-одноденки, боти-лідери суспільної думки. За допомогою ботів поширюється та чи інша інформація з метою цілеспрямованого впливу на цільову аудиторію. Крім того функції ботів можуть виконувати і реальні популярні особистості.

Ботоферма – віртуальний майданчик, який призначений для розповсюдження інформації ботами.

Введення супротивника в оману – цілеспрямований інформаційно-психологічний вплив на командно-штабні структури супротивника, на систему збору, обробки, зберігання і трансляції інформації через поширення хибних чи спотворених відомостей.

Війна – збройна боротьба між державами (їх коаліціями) або соціальними, етнічними та іншими спільнотами.

Військова могутність – сукупність матеріальних і духовних сил і засобів суспільства, які можуть бути використані державою для досягнення мети війни або вирішення інших військово-політичних завдань.

Віртуальна коаліція – суб'єкти геополітичної конкуренції у вигляді віртуальних союзів в складі медіа-холдингів, масштаби діяльності яких мають глобальний характер.

Віртуальна соціальна спільнота – соціальна система, сукупність різних соціальних систем та їх окремих елементів, сегментів інформаційного простору, джерел інтелектуальних і матеріальних ресурсів, які існують безвідносно до реального часу-простору та об'єднаних у рамках досягнення єдиної мети єдиною ідеологією, яка є головним системоутворюючим чинником.

Віртуальний простір – суб'єктивно-ідеалістичне відображення в свідомості індивіда абстрактних уявлень про часо-простір, утворене високорозвиненою формою комп'ютерного моделювання з імітацією штучно згенерованих образів явищ, фактів та об'єктів уявної реальності.

Воєнна доктрина (від лат. *doctrina* – вчення) – основний документ певних політичних сил та утворених ними інститутів влади, в якому викладені основні принципи та зміст їхньої військової політики. Держава у воєнній доктрині формулює свої воєнно-політичні цілі та міжнародні пріоритети в галузі національної безпеки.

Воєнна організація держави – сукупність військових, політичних, економічних, наукових та інших органів, установ, інститутів держави, які об'єднані спільною військовою діяльністю.

Воєнна політика України – діяльність суб'єктів забезпечення національної безпеки держави щодо запобігання воєнним конфліктам, організації та здійснення військового будівництва і підготовки Збройних Сил України, до збройного захисту національних інтересів.

Воєнні дії – організоване застосування військ, сил і засобів для виконання поставлених військових завдань на суші, на морі, в повітрі,

в космосі, – в стратегічному і оперативному масштабах; ведуться у формі кампаній, операцій, битв, ударів, боїв, систематичних бойових дій.

Генеральний штаб збройних сил України – головний військовий орган з планування оборони держави, управління застосуванням Збройних Сил України, координації та контролю за виконанням завдань у сфері оборони органами виконавчої влади, органами місцевого самоврядування, військовими формуваннями, утвореннями відповідно до законівУкраїни та правоохоронними органами у межах, визначених законами України і нормативно-правовими актами ПрезидентаУкраїни, Верховної Ради та Кабінету Міністрів України. Генеральний штаб Збройних Сил України в особливий період є робочим органом Ставки Верховного Головнокомандувача.

Гібридна війна – це форма збройного конфлікту, яка передбачає використання традиційних засобів збройної боротьби, змішаних форм тактичного застосування військових формувань в умовах неоголошеного військового (надзвичайного) стану на обмеженій території, ведення бойових дій на тлі інтенсифікації інформаційної війни у глобальному інформаційному просторі, економічної війни в системі світової економічно-торгової інтеграції, дипломатичної війни, як засобу тиску на супротивника через глобальні міжнародні інституції сторонами конфлікту і «державами-спонсорами», або коаліціями держав, які мають геополітичні інтереси в регіоні конфлікту.

Гіпертекст – метод надання інформації у вигляді тексту, окремі фрагменти якого з'єднані за допомогою посилань, що дають змогу легко переходити від одного матеріалу до іншого.

Глобальні мережі (WideArea Network, WAN) – це телекомунікаційні структури, що об'єднують локальні комп'ютерні мережі, які мають загальний протокол зв'язку, методи підключення і протоколи обміну даними. Кожна з глобальних мереж (INTERNET, BITNET, DECNET і ін.) організовувалася для певних цілей, а надалі розширювалася завдяки підключенню локальних мереж, що використовують її послуги і ресурси.

Глобалізація – синтезована категорія, яка розкриває процес, механізм й тенденцію функціонування світового розвитку, як цілісної, взаємопов’язаної та взаємообумовленої інтегративної світосистеми, характеризується транснаціональними та транскордонними особливостями, що виявляються

черезінтенсифікацію процесів культурної, політичної, економічної та військової інтеграції та уніфікації, інноваційну діяльність та необмеженість комунікативних потенцій в епоху техногенної цивілізації.

Глобальний інформаційний простір – продукт інтелектуальної діяльності інформаційного суспільства, яке намагається завдяки модернізуючим інформаційним технологіям максимально задовольнити свої потреби у спілкуванні, а також в інформаційних продуктах та послугах у межах політичної, економічної та інших видах діяльності. Це надскладна просторово-часова структура в межах якої відбуваються взаємопов'язані інформаційно-комунікаційні процеси вироблення, кодування, трансформації, передачі, декодування й зберігання інформації.

Громадянська війна – організована збройна боротьба всередині країни між різними групами населення (націями, класами, соціальними групами, партіями) з участю держави.

Дезінформація – хибна інформація, яка свідомо надається супротивнику для більш ефективного ведення бойових дій власними збройними силами, перевірки можливих каналів і джерел витоків інформації, процес маніпулювання інформацією з метою введення супротивника в оману шляхом надання неповної або повної, але застарілої інформації, або спекулятивного використання її частини у спотвореному вигляді.

Демократичний політичний режим – певний спосіб функціонування державно-владної сфери, заснований на участі громадян у процесі прийняття рішення через пряме народовладдя і делегування свого владного суверенітету представницьким органам, при якому гарантуються права і свободи особистості та меншин, забезпечується право громадян на контроль за діяльністю владних структур, реалізуються принципи представництва інтересів всіх суспільних груп.

Деморалізація (від лат. *de...* – припинення і *moralis* – моральний) – деструктивний психологічний вплив на сферу моралі; порушення ієрархії в аксіології; розлад дисципліни у поведінці; втрата здатності до дій, праці, активності.

Держава – публічна влада, що поширює свою дію на певну територію і виступає від імені її населення при вирішенні загальносуспільних проблем; система політичних інститутів, які організують суспільне життя на визначеній території; центральне поняття в політиці.

Державна безпека – стан захищеності державної влади, суверенітету, територіальної цілісності, обороноздатності, спокою людей (народу), громадської злагоди, довкілля, національної і релігійної рівності. Буває: внутрішня – передбачає систему законів, спрямованих на охорону державних інтересів у гуманітарній, інформаційній, політичній та економічній сферах та проведення ефективної внутрішньої політики держави, яка забезпечує цю систему заходів; зовнішня – діяльність державних органів щодо забезпечення суверенітету, територіальної недоторканності та обороноздатності держави, забезпечує мирне життя, вирішення проблем у гуманітарній, інформаційній, політичній та економічній сферах.

Державна влада – це форма політичної влади, яка виражає волю економічно і політично пануючої спільноти в соціально неоднорідному суспільстві, спирається на спеціальний апарат примусу, володіє монопольним правом на видання законів і розпоряджень, обов'язкових для всього населення.

Державна політика – свідома цілеспрямована діяльність владних структур та органів державного управління різних рівнів, спрямована на регулювання суспільних відносин з метою забезпечення їх стабільності шляхом розробки і реалізації політичних курсів і програм соціального, економічного, культурного розвитку.

Диверсифікація громадської думки – розпорошення уваги панівної еліти держави на різні штучно акцентовані проблеми й відволікання цим від вирішення нагальних завдань суспільно-політичного та економічного розвитку для ефективного функціонування суспільства й держави.

Дискредитація – цілеспрямовані, зумисні дії позбавлення довіри до об'єкта впливу, підрив авторитету, приниження гідності для втрати кредиту довіри у суспільстві.

Документ – сукупність інформації, що може бути збережена та передана від одного носія до інших, скомпонована для динамічного використання у конкретному випадку з метою повідомлення, ознайомлення, попередження.

«Доктрина Герасимова» – система поглядів політичного керівництва РФ на сутність і перспективи розвитку міждержавного конфлікту для досягнення потрібних геополітичних, стратегічних результатів; воєнно-політична теорія, яка систематизує основи воєнної науки з урахуванням положень філософської парадигми постмодерну; керівний теоретичний воєнно-політичний принцип,

вихідним началом якого є поєднання в єдину систему нетрадиційних (нелінійних) військових дій із політичними, економічними, інформаційними, гуманітарними та іншими невійськовими заходами.

Друкована пропаганда **–** форма психологічного впливу на свідомість супротивника через поширення інформації у друкованому вигляді (листівок, інструкцій, плакатів, газет, бюлетенів, брошур тощо), що розповсюджуються агентурним, артилерійським або авіаційно-повітряним методом.

Експансія (від лат. *expansio* – поширення) – активне проникнення у будь-яку сферу, поширення економічного, інформаційного, політичного і духовного панування.

Екстремізм (від лат. extremus – крайній) – прихильність в ідеології і політиці до крайніх поглядів і засобів у досягненні певних цілей. Екстремізм виступає проти існуючих громад, структур та інституцій, намагаючись підірвати їх стабільність, розхитати та ліквідувати їх заради своїх цілей.

Електронна війна – створення системи тотального контролю за інформаційними ресурсами ворога, його системами управління та зв’язку і способи їх знищення.

Електронна пошта (E-mail) – електронне повідомлення, що пересилається з одного комп'ютера на інший. Електронною поштою можна також пересилати будь-яку інформацію: відео- та аудіо-файли, фотографії, електронні таблиці в певному форматі, графічні файли, програми тощо.

Еліта політична (від франц. *elite* – кращий, добірний) – меншість суспільства, що становить достатньо самостійну, вищу, відносно привілейовану групу, наділену видатними психологічними, соціальними й політичними якостями, яка бере безпосередню участь у затвердженні та здійсненні рішень, пов’язаних із використанням державної влади або здійсненням впливу на неї.

Етнос – особливий вид спільності людей, яка утворилася внаслідок природного розвитку людей на основі специфічних стереотипів свідомості й поведінки, формується і розвивається об'єктивним історичним шляхом (не залежить від волі окремих людей), здатна до стійкого багатовікового існування за рахунок самовідтворення.

Етноцентризм **–** сукупність концепцій, поглядів, установок, згідно яких власний етнос (раса, народ, нація, народність) є центром філософських роздумів і об’єктом глорифікації та сакралізації.

Європейська інтеграція (від лат. *integratio* – поповнення, відновлення) – процес поступової уніфікації та зрощування національних економік європейських держав з метою подолання суперечностей між інтернаціоналізацією господарського життя та обмеженими можливостями внутрішніх ринків.

Забезпечувальна інформаційна зброя – це комплекс засобів комп'ютерної розвідки та засобів подолання систем захисту, який застосовують у атаках проти інформаційних систем супротивника.

Загрози політичній безпеці України – реальні впливи, які ускладнюють або роблять неможливим захист національних інтересів і створюють небезпеку для суверенітету нації, незалежності, соборності і прогресивного розвитку держави як рівноправного суб'єкта міжнародних відносин.

Закон – нормативно-правовий акт, що приймається з ключових питань суспільного, державного життя і має вищу юридичну силу.

Закон інформаційної політики– характерна для інформаційної сфери форма необхідних, суттєвих, істотних, стійких та загальних об'єктивних зв'язків й відносин, яка розкриває ефективність її взаємодії з елементами політичної системи держави в реалізації цілей держави в інформаційному просторі.

Закон інформаційної війни – необхідний, суттєвий, істотний, стійкий та загальний об'єктивний зв'язок, який розкриває співвідношення структури та функціонування елементів інформаційної війни у відповідних траєкторіях їх змін і розвитку в інформаційному просторі.

Засоби ведення інформаційного протиборства – національні й транснаціональні ЗМІ, а також будь-які інші інформаційні мережі, здатні впливати як на світогляд, політичні погляди, правосвідомість, менталітет, духовні ідеали та ціннісні установки окремої людини, так і на суспільство в цілому.

Захист військ (сил) від інформаційно-психологічного впливу противника – комплекс погоджених за цілями, місцем та часом заходів, що проводяться у мирний і воєнний часи органами державного та військового управління усіх рівнів, командуючими (командирами) штабами, органами виховної та соціально-психологічної роботи з метою запобігання, зриву, нейтралізації і усунення наслідків негативного інформаційно-психологічного впливу противника на особовий склад військ і населення країни.

Знаннє-центрична війна – принцип ведення бойових дій, який на основі комплексу інформації використовує інноваційні методики

прогнозування розвитку військово-політичної обстановки та характеру ведення бойових дій за допомогою «штучного інтелекту» та новітніх технологій отримання знань.

Зовнішня політика – загальний курс держави в міжнародних справах, який регулює взаємовідносини з іншими державами та інституціями у відповідності до потреб, принципів і цілей її внутрішньої політики.

Зомбування – сучасна практика управління суспільною думкою чи свідомістю індивіда, через потужний вплив на нейролінгвістичну систему людини, повторення психо-емоційних подразників, образів (кров, смерть) та негативної інформації, що провокують інстинктивні жах та паніку, для беззаперечного підкорення свідомості з метою маніпулювання діями об'єкта.

Зона виявлення імовірних загроз інформаційно-психологічного впливу супротивника – частина географічного та кіберпростору, де зосереджено посилене угрупування сил і засобів інформаційно-психологічного впливу супротивника, яке характеризується підвищеною активністю ведення наступальних інформаційних операцій.

Зона імовірного інформаційно-психологічного ураження особового складу – частина географічного та кіберпростору в межах якого відбувається прогнозоване зниження морально-психологічного стану військ (сил) з високим степенем ймовірності.

Ідеологія – система концептуально оформлених уявлень та ідей, яка виражає інтереси, світогляд та ідеали різних суб'єктів політики – класів, націй, суспільства, політичних партій, громадських рухів – виступає формою санкціонування або існуючих в суспільстві панування та влади, або радикального їх перетворення.

Ідеологія політична (від грец. *idea* – поняття і *logos* – учення) – система концептуально оформлених уявлень, ідей і поглядів на політичне життя, яка відображає інтереси, світогляд, ідеали, настрої людей, класів, націй, суспільства, політичних партій, громад, рухів та інших суб'єктів політики.

Інтернаціоналізм – принцип концентрації загального та індивідуального в різних аспектах життя народу з врахуванням істотної «національної» компоненти на основі чого формується інтегроване нове явище класової, національної та духовної єдності суспільства, націй та етносів.

Інтернет – глобальна децентралізована мережа, всесвітня сукупність технічних засобів, стандартів та домовленостей, яка дає

змогу підтримувати зв'язок між різними комп'ютерними мережами у світі.

Інтернет-середовище – особливий агент, що формує автономну реальність і впливає на специфіку взаємодії індивідів у новому соціальному просторі. Одна зі сфер розділу суспільства на реальне і віртуальне.

Інформатизація – складний соціальний процес формування оптимальних умов для вироблення, розвитку, трансформації, використання, споживання та задоволення інформаційних потреб людства.

Інформаційна безпека – стан захищеності інформаційного простору, його формування і розвиток в інтересах громадян, організацій і держави в цілому, захист від неправомірного зовнішнього і внутрішнього втручання; стан інформаційної інфраструктури, в якому інформацію використовують в мирних цілях лише за призначенням, і вона нездатна негативно впливати на інформаційну чи інші системи як самої держави, так і інших країн.

Інформаційна блокада – тотальне придушення офіціальним альтернативних, неконтрольованих джерел інформації.

Інформаційна війна – маніпулятивна, агресивна несанкціонована діяльність в інформаційному просторі. Форма ведення інформаційного протиборства між різними суб'єктами (державами, неурядовими, економічними або іншими структурами), що передбачає здійснення комплексу заходів із завдання шкоди інформаційній сфері конфронтуючої сторони й захисту власної інформаційної безпеки.

Інформаційна війна – суспільно-політичне явище, яке у політичному аспекті є продовженням домінуючих ідеологічних засад державної політики, що здійснюється за допомогою комплексу засобів інформаційно-технологічної індустрії, механізмів інформаційно-психологічного впливу на суспільство всередині держави чи населення країн-конкурентів в умовах політичного (воєнно-політичного, економічного) конфлікту з метою формування у соціальному аспекті єдності суспільства, визначення його ідентичності та інформаційного захисту світоглядних цінностей, а також – деморалізації та фрагментації населення та силової компоненти держав-супротивників в межах глобального інформаційного простору.

Інформаційна війна у формі «стратегічних комунікацій» – комплекс заходів цілеспрямованого впливу на військово-політичне

керівництво, суспільно-політичні рухи та сили, міжнародні організації (т.зв. – цільова аудиторія, ЦА) урядові організації за допомогою інформаційних кампаній, економічної та гуманітарної допомоги для створення ідеального іміджу США з метою переконання або примусу ЦА до прийняття рішень та здійснення дій, які забезпечують національні інтереси США.

Інформаційна експансія – форма реалізації цілей інформаційного протиборства шляхом активного досягнення організованого комплексного системного домінування в інформаційній сфері супротивника (конкурента).

Інформаційна зброя – сукупність організаційних та організаційно-технічних впливів на інформаційні системи, комплекси автоматизованого та автоматичного керування, системи та мережі зв'язку, тощо, здійснених з використанням систем та засобів знищення, спотворення, розкриття, крадіжки чи створення хибної інформації, подолання систем захисту, обмеження або розширення доступу до інформації та ресурсів законних користувачів, протидії та дезорганізації роботи технічних засобів, комп'ютерних систем і управління ресурсами інформаційних систем.

Інформаційна оборона – вид інформаційного захисту, комплекс взаємопов'язаних і узгоджених за метою, завданням, місцем і часом адміністративно-розпорядчих, організаційно-штатних, координаційно-плануючих і техніко-регламентуючих заходів, які спрямовані на підтримання духовного потенціалу суспільства, морально-психологічного стану військ, збереження інформаційно-технічної інфраструктури національної безпеки, ефективної нейтралізації інформаційних атак та операцій супротивника, нанесення максимальної шкоди морально-психологічному стану його суспільству, збройним силам і технічним засобам інформаційної агресії та створення необхідних умов для проведення власної наступальної інформаційної операції.

Інформаційна перевага – ступінь панування, що дає змогу певним силам збирати, управляти, використовувати та захищати інформацію без ефективної протидії з боку супротивника.

Інформаційна розвідка – комплекс заходів з отримання і обробки даних про існуючого або ймовірного супротивника, його військові ресурси, бойові можливості і уразливості, а також про потенційний театр військових дій

Інформаційна система – організаційно упорядкована сукупність спеціалістів, інформаційних ресурсів, інформаційних технологій, яка реалізує інформаційні процеси.

Інформаційна сфера – сукупність суб'єктів інформаційної взаємодії та впливу, яка забезпечує можливість створення, обміну, обробки, зберігання та поширення інформації.

Інформаційне домінування – комплексне використання можливостей сучасних інформаційно-комунікативних технологій з накопичення обсягів інформації, що при відповідних методах її обробки дають змогу прогнозувати комплекс можливих сценаріїв розвитку соціальних і політичних явищ із метою визначення найбільш імовірного з них і сформувати інформаційне поле такої концентрації, яка б перевищувала інформаційний рівень структури, що має вплив на ці сценарії

Інформаційне поле – комплекс зосередженої у заданому об'ємі в просторово-часових характеристиках інформації, яка існує безвідносно до об'єкта відображення та суб'єкта сприйняття.

Інформаційне протиборство – форма боротьби, сукупність спеціальних (політичних, економічних, дипломатичних, технологічних, військових та інших) методів, способів і засобів вигідного впливу на інформаційну сферу об'єкта зацікавленості та захисту власної інформаційної сфери в інтересах досягнення поставлених цілей.

Інформаційне протиборство в безконтактних війнах – нова стратегічна форма боротьби сторін в глобальному інформаційному просторі, де використовується комплекс спеціальних технічних і психологічних способів і засобів досягнення геополітичних цілей; сукупність спеціальних (політичних, економічних, дипломатичних, технологічних, військових та інших) методів, способів і засобів вигідного впливу на інформаційну сферу об'єкта, зацікавленості та захисту власної інформаційної сфери в інтересах досягнення поставлених цілей.

Інформаційний вплив – організоване цілеспрямоване застосування спеціальних інформаційних засобів і технологій для внесення деструктивних змін у свідомість та психіку особистості, соціальних груп чи населення (корекція поведінки), в інформаційно-технічну інфраструктуру об'єкта впливу та (чи) фізичний стан людини.

Інформаційний захист – комплексна система спланованих і скоординованих за метою, часом і завданням заходів органів

державного та військового управління, які спрямовані на нейтралізацію та ліквідацію наслідків негативного інформаційно-психологічного впливу на особистість, суспільство та руйнівних наслідків інформаційно-технічного впливу на інформаційно-комунікаційну інфраструктуру національної безпеки держави.

Інформаційний колапс – стану мережевого інформаційного простору, який загрожує його стабільній роботі та функціонуванню, внаслідок різкого зниження перепускної здатності каналів зв'язку та неможливості передачі збільшених об'ємів трафіку.

Інформаційний наратив – суб'єктивно-ідеалістичний структурований опис об'єктивної дійсності за допомогою заданого обсягу інформації у жорстко окреслених рамках інтерпретацій.

Інформаційний потік – сукупність інформації, яка переміщується у інформаційному просторі по каналах комунікації.

Інформаційний ресурс – сукупність текстових документів, баз даних, нерухомих й рухомих зображень, звукових і графічних матеріалів.

Інформаційний спротив – організовані та скоординовані зусилля органів державного управління, державної інформаційно-комунікаційної інфраструктури та частини громадянського суспільства, які спрямовані на активну протидію розпочатій проти держави інформаційній війні та захист національних інтересів в інформаційному просторі.

Інформаційний суверенітет – інтегральна категорія, яка розкриває механізм використання державою сукупності прав на захист національних інтересів, степінь ефективності системи органів державного управління у використанні інформаційної інфраструктури при виконанні своїх функціональних обов'язків з метою доведення до громадян обґрунтованої інформації внутріполітичного та зовнішньополітичного змісту; об'єктивного відображення усіх сфер життя суспільства; налагодження взаємодії та взаємозв'язку структур громадянського суспільства для реалізації основних конституційних положень щодо прав забезпечення суверенітету держави та можливості реалізації комплексу заходів стосовно забезпечення національної безпеки України в інформаційній сфері.

Інформаційний театр воєнних дій – частина глобального інформаційного простору, де проводяться сплановані за місцем, часом і метою заходи розгортання угрупувань для ведення інформаційного протиборства оперативно-стратегічного масштабу,

координація зосередження їх зусиль за напрямками та районами й організація їх взаємодії в загальній системі інформаційної інфраструктури держави.

Інформаційний тероризм – особливий різновид психологічного терору, синтезована форма інформаційно-психологічного насильницького впливу на суспільну свідомість та злочинного використання інформаційно-комунікативних систем, мереж і їх компонентів, фізичного або технологічного порушення роботи критичних телекомунікаційних вузлів для здійснення терористичних дій та інших акцій, що прирівнюються до них.

Інформаційний тиск – потужне цільове спрямування інформаційних ресурсів на об'єкт впливу з метою досягнення системних змін його ціннісно-інформаційних констант.

Інформаційні операції – комплексний термін, який об'єднує поняття електронної війни, комп'ютерних мережевих операцій (радіоелектронної боротьби), психологічних операцій, воєнної дезінформації з метою здійснення впливу, процеси управління інформаційними потоками та контролю за ними, руйнування діяльності інформаційної системи, пошкодження чи захоплення засобів підтримки прийняття рішень командним складом супротивника, а також заходи, які спрямовані на підвищення захищеності від відповідної діяльності супротивника.

Інформаційно-комунікаційна інфраструктура – сукупність територіально розподілених державних і недержавних інформаційних систем, засобів зв'язку, мереж і каналів передачі даних, засобів комунікації в управлінні інформаційними потоками.

Інформаційно-психологічна безпека особи – стан захищеності психіки людини від негативного впливу, який здійснюється шляхом упровадження деструктивної інформації у її свідомість чи підсвідомість, що приводить до неадекватного сприйняття дійсності.

Інформаційно-психологічна безпека суспільства та держави – стан захищеності (інтелектуальної, соціально-політичної, морально-етичної), за якого досягається стабільне функціонування та гармонійний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційно-психологічних впливів.

Інформаційно-психологічна операція – комплекс узгоджених заходів, які проводять органи державного та воєнного керівництва для цілеспрямованого інформаційно-психологічного впливу на міжнародні інституції, світове співтовариство, органи управління,

інформаційні джерела, системи зв'язку та інформаційного забезпечення об'єкта у відповідь на аналогічні дії супротивника.

Інформаційно-психологічне протиборство – процес цілеспрямованого виробництва та розповсюдження комплексу спеціальної інформації, яка безпосередньо впливає (позитивно чи негативно) на масову та індивідуальну свідомість, розвиток інформаційно-психологічної сфери суспільства, психіку і поведінку політичної еліти та населення країни з метою трансформації соціальних процесів у напрямку необхідному для сторони, що впливає.

Інформаційно-психологічна протидія (для вирішення військових завдань) – складова інформаційно-психологічної боротьби, спрямована на власну аудиторію, яка одночасно є мішенню для пропаганди (психологічних операцій) противника (опозиції), з метою нейтралізації або зведення до мінімуму ефекту від негативного інформаційно-психологічного впливу

Інформаційно-психологічна протидія (на державному рівні) – планова організаційна діяльність органів державної влади та суспільства, яка спрямована на формування дієвої політики інформаційного суверенітету, захисту національного інформаційного простору, здатності створення ефективних механізмів формування суспільної думки та можливості протистояти інформаційно-психологічному впливу супротивника. Вона містить комплекс заходів, які спрямовані на захист певної системи світоглядних орієнтирів, настанов, стереотипів (патріотичних констант), на яких ґрунтується здатність народу до відсічі агресору.

Інформаційно-психологічний вплив – комплекс заходів цілеспрямованого виробництва та поширення спеціальної інформації в середовищі політичної еліти та суспільства, формування певних соціальних ідей, уявлень, переконань, нав'язування цілей, які не входять до числа їх інтересів і безпосередньо впливають на системні зміни у світоглядних орієнтирах суспільства, його свідомість, психіку і поведінку.

Інформаційно-психологічні операції – форма ведення психологічної боротьби що передбачає використання складної сукупності різних видів, способів і прийомів інформаційних впливів, які починають проводиться в мирний час, активізуються в загрозливий період і повною мірою розгортаються у ході бойових дій.

Інформаційно-технічна протидія – комплексна діяльність органів державного та військового управління, яка спрямована на

забезпечення ефективності безпеки функціонування інформаційно-технічної інфраструктури з метою реалізації необхідних системних змін у функціонуванні технічних засобів інформаційної війни супротивника та надійного захисту власної інфраструктури інформаційно-технічної протидії.

Інформаційно-технічний вплив – система заходів інструментального впливу на інформаційно-технічну інфраструктуру об'єкта з метою забезпечення реалізації необхідних негативних змін у її функціонуванні, а також вплив на фізичний стан людини.

Інформаційно-технічне протиборство – вид соціотехнічної протидії інформаційно-аналітичних комунікативних систем інформаційно-технічної інфраструктури через організацію цілеспрямованого процесу виробництва і поширення спеціального інформаційного продукту, за допомогою якого можна проникати в об'єкти інформаційно-технічної сфери суспільства і порушувати їх роботу.

Інформаційно-центрична війна – принцип ведення бойових дій з метою досягнення інформаційної переваги над супротивником на основі комплексу високотехнологічних інформаційних систем збору, обробки, моделювання, візуалізації даних та підтримки прийняття рішень в режимі реального часу.

Інформаціоналізм *(«інформаційний капіталізм»)* – технологічна парадигма, заснована на збільшенні людського потенціалу при обробці інформації і зв'язку, що стало можливим завдяки революції в галузі мікроелектроніки, програмного забезпечення та генної інженерії.

Інформація – універсальна комплексна категорія, що може бути визначена як субстанціональна основа об'єктивної реальності у вигляді матеріальних й ідеальних зв'язків, що утворюють систему взаємодії елементарних елементів структури, забезпечують процес її отримання, декодування, трансформацію і споживання.

Інформація (в системі національної безпеки) – документовані або публічно оголошені повідомлення, відомості про події та явища у світі, суспільстві, державі, які людина сприймає безпосередньо або за допомогою спеціальних пристроїв, зокрема через мережі мовлення та зв'язку, пресу. Відповідно до чинного законодавства, інформація буває відкритою та з обмеженим доступом (конфіденційна і таємна)

Кібератака – цілеспрямована та спланована інформаційно-технічна акція, яка характеризується невпинністю, стрімкістю, рішучістю дій проникнення і активного впливу на систему

державного та військового управління, інформаційно-комунікаційні мережі й ресурси системи національної безпеки супротивника з метою їх дезорганізації та знищення.

Кібербуллінг – некоректна поведінка, приниження та переслідування у мережі Інтернет повідомленнями, що містять образи, агресію, залякування; хуліганство; соціальне бойкотування за допомогою різних Інтернет-сервісів.

Кібервійна – форма розвитку, поширення та бойового застосування інформаційних технологій в воєнній сфері, складова частина інформаційних воєн, що здійснюються із використанням всесвітньої мережі.

Кібервійська (Сили кібероперацій – СкбО) – спеціальні військові формування в складі збройних сил, які за своїм функціональним призначення забезпечують комплексний захист інформаційно-комунікаційної інфраструктури національної безпеки держави від несанкціонованого втручання з боку державних, недержавних і транснаціональних кіберугрупувань,доступ до комп'ютерних мереж ймовірного супротивника та використання їх у власних інтересах через застосування новітніх ІТ-технологій силами професійних комунікаторів та фахівців з ведення інформаційної війни.

Кіберзахист – захист інформації, комп'ютерних мереж, реагування на несанкціоновану активність.

Кіберзброя – електронні технології та засоби поширення електромагнітних випромінювань інформаційно-комунікаційної інфраструктури, інші матеріальні інфраструктури, які пов'язані із соціотехнічним простором і здатні створювати, модифікувати, зберігати й передавати інформацію (управляти її потоками), а також впливати на стан фізичних інфраструктур супротивника.

Кібероборона – комплекс спланованих і скоординованих дій органів державного та військового управління для впровадження ефективних заходів конвергенції усіх компонентів інформаційно-комунікаційної інфраструктури національної безпеки держави з метою забезпечення надійного захисту цілісності та цінності інформації й інформаційних систем і гарантування підтримання належних умов її обігу.

Кіберпростір – середовище, в якому електронний та електромагнітний спектр використовується для зберігання, модифікації та обміну даними через мережеві системи та відповідні фізичні інфраструктури. У сфері військового протиборства –

комплексне середовище для застосування сил і засобів інформаційної та збройної боротьби.

Клієнт – це комп'ютер чи програма, що використовує ресурси серверу Internet. Як правило, на комп'ютері користувача Internet одночасно працюють кілька програм-клієнтів (наприклад, це програми для роботи з електронною поштою, програма-браузер для перегляду гіпертекстових Web-документів тощо). Більшість користувачів Internet працюють на звичайних персональних комп'ютерах. Кількість доступних їм послуг Internet залежить від типу сполучення з мережею.

Командна війна – визначення стратегії й тактики нейтралізації органів управління супротивника з метою порушення систем управління військами, знищення його комунікаційних мереж на стратегічному, оперативному та тактичному рівнях у формі комплексу інформаційних операцій.

Компрометація – будь-який випадок (втрата, розголошення, крадіжка, несанкціоноване копіювання тощо) з ключовими документами (ключовими даними) та засобами КЗІ, який призвів (може призвести) до розголошення (витоку) інформації про них, а також інформації, яка обробляється та передається.

Комп'ютерна війна – застосування комп'ютерних технологій та Інтернету однією державою, або за її безпосередньої підтримки, проти іншої держави, спрямоване проте її безпеки і оборони, яке є настільки інтенсивним і серйозним, що становить реальну загрозу безпеці та суверенітету цієї іншої держави *(амер.)*.

Комп'ютерна мережа – система зв'язку між двома чи більше комп'ютерами. У ширшому розумінні комп'ютерна мережа – це система зв'язку через кабельне чи бездротове середовище, самі комп'ютери різного функціонального призначення і мережеве обладнання.

Комунікація – соціальний процес, пов'язаний із спілкуванням, обміном думками, відомостями, ідеями тощо за допомогою комплексу технологічного інструментарію з метою вироблення нових системних культурних сенсів і парадигм в умовах конкретних просторово-часових характеристик.

Конституція (від лат. *constitution* – побудова, організація) – основний закон держави, який закріплює її суспільний та державний устрій, права, свободи та обов'язки громадян, організацію державної влади і місцевого самоврядування, територіальний устрій тощо.

Консцієнтальна війна – війна психологічна за формою, цивілізаційна за змістом та інформаційна за засобами, у якій об’єктом впливу є знищення або деструкція інтелектуального ресурсу нації та руйнування універсальних установок населення.

Контрпропаганда – створення модифікованого інформаційного потоку, проведення інформаційних і психологічних операцій зі зниження ефективності інформаційно-психологічних заходів супротивника з метою послаблення, а в ідеалі – повної ліквідації ефекту від пропаганди ворога.

Конфронтація – протиборство, протиставлення інтересів, принципів тощо.

Космополітизм (від грец. kosmopolites – громадянин світу) – ідея та ідеологія «світового громадянства»; принцип ставлення до нації та країни, який базується на розумінні визначних інтересів (загальнолюдських інтересів) та відповідальності за долю людства.

Криза легітимності влади (від грец. *krisis* – завершення, злам) – заперечення правочинності влади і владних відносин у суспільстві, відмова виконувати розпорядження владних структур, безвладдя.

Криза політична – тимчасове призупинення чи припинення функціонування окремих елементів або інститутів політичної системи, значне поглиблення й загострення наявних.

Криптографічний захист інформації – вид захисту інформації, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

Культурна політика держави – сукупність цілей, завдань, практичних заходів, спрямованих на створення реальних умов, стимулів і конкретних механізмів реалізації культурних інтересів громадян країни; це – система політичних рішень у сфері науки, освіти, літератури і мистецтва, діяльності культурно-освітніх і релігійних установ, засобів масової комунікації, організації довкілля тощо.

Локальна війна (лат. *localis* – місцевий) – обмежений територіальний воєнний конфлікт, пов'язаний з релігійними, територіальними суперечками, міжплемінними протиріччями між двома і більш державами, обмежений за політичними цілями, в якому військові дії вестимуться, як правило, у межах протиборчих держав і стосуються переважно інтересів лише цих держав.

Людська гідність – самоцінність та суспільна значимість людини як біосоціодуховної істоти, яка визначається існуючими суспільними відносинами, не залежить від конкретної людини і має бути рівною для всіх людей.

Маніпуляція (від лат. *manipula* – складовий підрозділ, звичайно – 1/36 частина римського легіону) – довільне, необмежене управління поведінкою людей, їх свідомістю, емоціями з метою отримання запланованого результату у політиці (на полі бою).

Маніпулювання – спосіб управління (панування) через емоційно-духовний вплив, програмування поведінки, спрямований на психічні структури людини, здійснюється приховано й ставить своєю задачею зміну думок, переконань та мети людей у потрібному напрямку.

Мас-медіа – засоби одночасної передачі інформації групі людей, тобто масової інформації. Преса (газети, журнали, книги), радіо, телебачення, Інтернет, кінематограф, звукозаписи та відеозаписи, відеотекст, телетекст, рекламні щити та панелі, домашні відеоцентри, що поєднують телевізійні, телефонні, комп'ютерні та інші лінії зв'язку. Усім цим засобам притаманні спільні якості – масова аудиторія, доступність, корпоративний зміст виробництва і поширення інформації.

Масова політична свідомість – виражає зміст і рівень потреб широкого загалу, усієї маси населення та його уявлення про способи задоволення цих потреб через політичну діяльність; відображає рівень знань народу про суспільно-політичну реальність, які частково вироблені різними ідеологіями та закріплені в політичній культурі, а частково здобуті ціною власного досвіду та досвіду діяльності соціальних груп і масових рухів.

Медіакомпетентність – вміння ефективно використовувати сучасні медіатехнології, вести пошук необхідної інформації, раціонально та розумно споживати, аналізувати чи створювати медіа-продукти.

Медіа-культура – сукупність інформаційно-комунікаційних засобів, що функціонують у суспільстві, знакових систем, елементів культури комунікації, пошуку, збирання, виробництва і передачі інформації, а також культури її сприйняття окремими громадянами, соціальними групами та соціумом в цілому.

Мережева війна – форма геополітичної протидії між глобальними інституціями за допомогою використання механізму залучення великої кількості індивідів у комплекс мереж соціально-політичного, духовно-інтелектуального, торгівельно-економічного,

сектантсько-терористичного характеру з метою уніфікації світоглядних основ мережевого суспільства епохи постмодерну в інтересах домінуючої групи глобальних інституцій.

Мережевий захист – комплекс інформаційно-технічних заходів, які передбачають відслідковування та аналіз мережевих кібератак на комп'ютерні об'єкти інформаційно-комунікаційної інфраструктури та захист їх від шкідливого впливу.

Мережево-інформаційна війна – форма геополітичного інформаційного протиборства держав (або коаліцій держав) у створенні загрози продовольчій, екологічній, політичній, релігійній, інформаційній та іншим видам безпеки супротивника невоєнним шляхом, підрив, а потім і руйнування ідентифікаційних патернів нації та основ держави.

Мережевий соціум – група людей, взаємодія яких відбувається переважно в глобальних комп'ютерних мережах.

Мережево-центрична війна – принцип бойового застосування комплексу взаємопов'язаних і взаємодіючих підсистем, які використовують для створеннянової ефективноїмоделі управління процесами збору, обробки та використання усіх видів інформації в кіберпросторі з метою досягнення цілей і завдань військової компанії у формі збройного, а в ідеалі, –незбройного конфлікту.

Міжнародна безпека – стан міжнародних відносин, який включає порушення миру та створення реальної загрози розвитку людства, за якого народи можуть суверенно, без втручання і тиску ззовні, визначати шляхи і форми свого суспільно-політичного розвитку; діяльність держав та міжнародних інститутів щодо підтримання такого стану, універсальна система механізмів, заходів і гарантій якого виключає застосування сили в міжнародних стосунках.

Міжнародна політика – система економічних, правових, дипломатичних, ідеологічних, військових, культурних та ін. зв'язків і відносин між народами, державами і групами держав, організаціями, що діють на світовій арені; комплекс двосторонніх та багатосторонніх політичних, економічних, дипломатичних, військових, культурних, науково-технічних відносин між державами.

Міжнародне право – сукупність юридичних норм, що регулюють відносини між державами та іншими суб'єктами міжнародного спілкування.

Мілітаризація (від лат. *militaris* – воєнний) – 1) підпорядкування економічного, політичного і громадського життя держави головним чином для підготовки загарбницьких воєн, придушення опозиційних

до існуючого режиму рухів; 2) перенесення форм і методів військової організації на сферу цивільних відносин; 3) створення воєнної економіки в мирний час; 4) виховання населення у військовому дусі.

Міністерство оборони України – центральний орган виконавчої влади і військового управління, у підпорядкуванні якого перебувають Збройні сили України, що забезпечує реалізацію державної політики у сфері оборони.

Моральний дух – духовна готовність і здатність військовослужбовців долати випробування війни (бойових дій), труднощі військової служби, досягати перемоги над ворогом.

Морально-психологічне забезпечення – система заходів, спрямованих на формування й підтримання високого морального духу армії, морально-психологічного стану й дисципліни особового складу, військового правопорядку, згуртування військових колективів і протидію інформаційно-психологічному впливу противника для забезпечення виконання службово-виховних завдань в умовах мирного і воєнного часу.

Морально-психологічний потенціал – сукупність духовних можливостей особового складу, його свідомості, професійної підготовленості, які можуть стати фактором перемоги під час бою.

Морально-психологічний стан – активна частина морально-психологічного потенціалу, наявні духовні сили військовослужбовців, ступінь їх мобілізованості на виконання конкретної бойової задачі, морально-психологічний чинник досягнення перемоги.

Морально-психологічний стан особового складу – цілісна, інтегральна сукупність політичних, духовних цінностей і позицій, потреб і інтересів, почуттів, які переважають і домінують в свідомості військовослужбовців у даний час чи протягом його певного проміжку.

Надзвичайний стан – передбачений конституцією або конституційними законами правовий режим діяльності органів державної влади та місцевого самоврядування, підприємств, установ і організацій, котрий тимчасово допускає обмеження в здійсненні окремих прав і свобод людини і громадянина та прав юридичних осіб, а також покладає на них додаткові обов’язки.

Наступальна інформаційна війна – спланована та цілеспрямована діяльність органів державного та військового управління, соціальних інститутів суспільства, яка передбачає рішучі

дії проникнення та активного впливу на інформаційні мережі та ресурси супротивника з метою їх дезорганізації та повного знищення.

Націоналізм – принцип мобілізації суспільства на основі абсолютизації національних цінностей в умовах реальної чи умовної зовнішньої загрози (воєнної, економічної, політичної, культурної, інформаційної та ін.).

Національна безпека – стан захищеності державного суверенітету, конституційного ладу, територіальної цілісності, економічного, науково-технічного і оборонного потенціалу України, законних інтересів держави та прав громадян від розвідувально-підривної діяльності іноземних спеціальних служб, посягань з боку окремих організацій, груп та осіб.

Національна ідея – аполітичний проект майбутнього нації, імператив її свідомості й чину, смисложиттєвий чинник національного розвитку; певний комплекс вірувань, національного світобачення і розуміння, своєрідний духовно-інтелектуальний потенціал нації, людини – державотворця і співгромадянина; система ціннісних орієнтирів, що полягає в урахуванні інтересів усіх верств суспільства, усіх народів; форма державного самоусвідомлення народу, показник того, як народ розуміє себе, своє місце і роль у світі.

Національна свідомість – сукупність соціальних, економічних, політичних, моральних, етичних, філософських, релігійних поглядів, норм поведінки, звичаїв і традицій, ціннісних орієнтацій та ідеалів, які відображають особливості життєдіяльності націй і народностей.

Національний інтерес – історично змінна система основних внутрішніх і зовнішніх інтересів нації, які реалізуються без компромісу.

Недержавна інформаційна політика – діяльність соціальних груп в ЗМІ та ЗМК, що може забезпечувати інтереси держави, одночасно вступати у протиріччя з громадянським суспільством, організовувати діалог з державою чи виступати проти її інститутів, або працювати на інтереси окремих груп інтересу, партій та особистостей.

Нейтралітет (від лат. *neuter* – ні той, ні інший) – спосіб міждержавного політичного розвитку, при якому правовий статус держави та її зовнішньополітична мета встановлюються відповідно до відносин, що встановлюються між суб’єктами, які мають близькі інтереси, наближені цілі, однак їх розділяють власні інтереси, зобов’язання перед прибічниками.

Об'єкт інформаційного протиборства – складові форм буття, сфер суспільства стосовно яких можливо використовувати механізмита інструменти інформаційного протиборства з метою перекодування, трансформації та модифікації їх якісних характеристик як елементів інформаційної сфери.

Об'єкт інформаційної політики держави – сукупність інформації, державне управління інформаційною сферою, станом суспільної свідомості, системою ЗМК, ЗМІ, інформаційні процеси, які відображають та захищають права особистості, інтереси суспільства та політику держави.

Оборонна інформаційна війна – сплановані цілеспрямовані дії органів державного та військового управління, соціальних інститутів суспільства з метою досягнення повного інформаційного контролю над супротивником з одночасним захистом своїх інформаційних комунікацій й ресурсів, що здійснюються як всередині держави, так і у міжнародному середовищі.

Обороноздатність держави – здатність держави до захисту у разі збройної агресії або збройного конфлікту. Вона складається з матеріальних і духовних елементів та є сукупністю воєнного, економічного, соціального та морально-політичного потенціалу у сфері оборони та належних умов для його реалізації.

Он-лайн спільнота – спільнота суб'єктів діяльності, яка ґрунтується на масовому переносі людьми, групами, організаціями інформаційної активності та взаємодій інтермереж в режим он-лайн.

Оперативне маскування – комплекс інформаційних та організаційно-технічних заходів з дезорієнтації розвідувальних органів супротивника для забезпечення максимальної секретності чи прихованих дій власних сил (військ).

Оперативність інформаційно-психологічного впливу – здатність сил і засобів інформаційної війни до високої активності та швидкого реагування на події, правильного вибору аудиторії, часу та місця здійснення акцій із використанням заданого обсягу і спрямованості інформації у встановлені терміни.

Оперативно-стратегічний операційний напрямок зосередження основних зусиль інформаційного протиборства – частина інформаційного театру воєнних дій між державами з визначеними важливими елементами системи державного та військового управління, стратегічними об'єктами інформаційно-комунікаційної інфраструктури, складом сил та засобів

інформаційно-психологічних операцій супротивника на які спрямовані інформаційні операції оперативно-стратегічного рівня.

Опозиція (від лат. *oppositio* – протиставлення) – протидія, опір певній політиці, політичній дії; організація, партія, група, особа, які виступають проти панівної думки, уряду, системи влади, конституції, політичної системи в цілому; будь-яка політично організована група, що протистоїть урядові, критикує його і прагне здобути владу, легальна (узаконена) та активно діюча опозиція – одна з головних ознак демократичного ладу.

Організаційні заходи захисту інформації – комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту шляхом регламентації діяльності персоналу і порядку функціонування засобів (систем) забезпечення інформаційної діяльності та засобів (систем) забезпечення ТЗІ.

Організація інформаційного протиборства – комплекс взаємопов'язаних і взаємообумовлених заходів, які спрямовані на досягнення найбільш повної та ефективної реалізації його цілей та завдань.

Основне завдання інформаційної війни (між державами) – здійснення безпосереднього негативного впливу на могутність держави-конкурента чи супротивникачерез послаблення її реальних і потенційних можливостей із забезпечення власної безпеки, створення перешкоддля активної внутрішньо та зовнішньополітичної діяльності; руйнування іміджу, послаблення владної еліти, загроза стабільності соціально-політичного режиму, конституційному устрою чи територіальній цілісності держави.

Паблік рілейшнз – наука і мистецтво організації та здійснення зв'язків суб'єктами управління економічною, соціальною, політичною і духовно-культурною діяльністю з громадськістю, досягнення взаєморозуміння та суспільного консенсусу за допомогою обміну інформацією на основі цілеспрямованого формування громадської думки та управління нею.

Паніка (дав.-гр. *πανικός* – підсвідомий жах) – психічний стан людей, несвідомий, нестримний страх, спровокований дійсною чи уявною небезпекою, що охоплює людину чи багатьох людей, неконтрольоване прагнення уникнути небезпечної ситуації.

Патріотизм – суспільний моральний принцип діяльного ставлення до свого народу, що віддзеркалює національну гордість і любов до вітчизни, громадянську відповідальність за її долю, а також емоційне підпорядкування особистістю свого життя спільним

національним інтересам і виявляється у готовності служити Батьківщині й захищати її від ворогів.

Плюралізм (від лат. *pluralis* – множинний) – принцип суспільно-політичного й соціального розвитку, що випливає з існування декількох незалежних начал політичних знань і розуміння буття; система влади, заснована на взаємодії та протилежності дій політичних партій і громадсько-політичних організацій.

Політика (від грец. *politike* – мистецтво управляти державою, державні та суспільні справи) – одна з найважливіших сфер діяльності суспільства, суспільних груп та індивідів, спрямована на усвідомлення, захист та реалізацію своїх інтересів через використання інститутів влади; діяльність осіб, макро- і мікрогруп та інститутів для отримання, реалізації влади; система відносин у суспільстві для урегулювання нормованої ієрархії підпорядкування.

Політична боротьба – форма політичних відносин між суб'єктами політики, спрямованих на досягнення міцних позицій у системі владарювання, впливу на владу шляхом реалізації своєї політичної волі.

Політична влада – здатність і можливість здійснювати визначальний вплив на політичну діяльність і політичну поведінку людей та їхніх об'єднань з допомогою будь-яких засобів – волі, авторитету, права, насильства; центральні, організаційні й регулятивно-контрольнізасадиполітики.

Політична діяльність – специфічна форма активного ставлення людей до свого соціального середовища, яка має на меті цілеспрямоване його регулювання та перетворення за допомогою фактора влади.

Політична ідеологія (від грец *idea* – поняття і *logos* – думка, розум, учення) – система ідей та поглядів на політичне життя, яка відображає світогляд, інтереси, ідеали суб'єктів політики (індивідів, націй, класів, політичних партій, політичних еліт та лідерів, громадських рухів і т.д.).

Політична культура – частина загальної культури, яка формується і виявляється в процесі політичного життя; історично і соціально зумовлений продукт політичної життєдіяльності людей, їх політичної творчості, який відбиває процес опанування суспільством, націями, класами, іншими соціальними спільнотами та індивідами політичних відносин, а також розвиток їх сутності і діяльнісних здібностей як суб'єктів політичного життя; сукупність стійких

соціально-психологічних знань, уявлень, орієнтацій, позицій, цінностей і зразків поведінки у сфері взаємовідносин влади та народу.

Політична пропаганда – діяльність, що передбачає системне поширення,поглиблене роз'яснення соціально-політичних, економічних, правових поглядів, ідей, теорій та забезпечує формування у суспільстві певних настроїв, закріплення усвідомості громадян тих чи інших цінностей, орієнтацій,уявлень з метою максимального розширення кола прибічників відповідної ціннісної системи.

Політична свідомість – опосередковане відображення політичного життя суспільства, суттю якого є проблеми влади, формування, розвиток і задоволення інтересів та потреб політичних суб'єктів; сукупність поглядів, оцінок, установок, які, відображаючи політико-владні відносини, набувають відносної самостійності.

Політична система суспільства (від грец. *systema* – складене з частин) – сукупність державних і недержавних соціально–політичних інститутів, які здійснюють владу, управління справами суспільства, регулювання політичних процесів, взаємовідносини між соціальними групами, націями, державами та забезпечують політичну стабільність і прогресивний розвиток.

Політичне маніпулювання – система засобів ідеологічного та духовно-психологічного впливу на масову свідомість з метою нав'язування певних ідей, цінностей та цілеспрямований вплив на громадську думку та політичну поведінку задля спрямування їх у заданому напрямку.

Популізм (від лат. *populus* – народ) – схильність політиків домагатися визнання їхньої громадської діяльності, популярності, вдаючись до простих, прийнятних для населення аргументів та пропозицій, уникаючи непопулярних, але необхідних заходів щодо вирішення суспільних проблем.

Правова держава – організація політичної влади, яка обмежена в своїх діях правом, підпорядкована волі суверенного народу, зобов'язана охороняти індивідуальну свободу та не втручатися у сферу громадянського суспільства.

Превентивна війна (від англ. *prevent* – запобігати) – початок військових дій, мета яких, нанесення удару на випередження для перешкоджання очікуваної агресії з боку вірогідного супротивника.

Преемптивна війна – комплексна форма збройного конфлікту, компонентами якої є цілеспрямована інформаційна війна, мережево-центричний принцип ведення бойових дій, «гібридний» характер

застосування регулярних і нерегулярних формувань з метою досягнення політичних цілей і трансгуманітарна перебудова в формах консцієнтальної війни індивідуальної та суспільної свідомості, перекодування національних ментальних рис (національної ідентичності) переможеного народу.

Президент держави – (від лат. *praesidens* – той, що сидить попереду) – виборний глава держави в більшості країн з республіканською формою правління; –вища посадова особа, яка обирається громадянами чи парламентом, або спеціальною виборчою колегією на цей пост (посаду) на визначений термін.

Принципи організації інформаційного протиборства – найзагальніші імперативи, основоположні начала, які формуються в інтересах практики та використовуються в залежності від ситуації.

Провайдер (Internet service provider, ISP) – установа, яка надає комерційні послуги з підключення до комп'ютерної мережі.

Пропаганда (лат. *propaganda* – підлягає розповсюдженню) – поширення політичних, філософських, наукових, художніх та ін. поглядів та ідей з метою впливу на громадську думку на користь певного суб'єкта для активізації масової практичної діяльності.

Психіка (від грец. *psyche* – душа; *psychickos* – душевний) – системна якість високоорганізованої матерії; активне відображення об'єктивної дійсності в ідеальних образах, на основі яких регулюється життєдіяльність організму.

Психологічна боротьба – комплекс спеціальних заходів інформаційної війни спрямованих на підрив морально-бойового духу особового складу військ противника (або місцевого населення) для успішного здійснення військової операції чи виконання бойових завдань та перемоги.

Психологічна війна – цілеспрямоване застосування прямих і опосередкованих психологічних та інших (дипломатичних, пропагандистських, економічних) впливів на думки, настрої, психіку ворога (конкурента) з метою створення необхідних ідеологічних і соціальних установок свідомості, формування стереотипів його поведінки та прийняття рішень, необхідних для деморалізації супротивника.

Психологічна операція – складова частина інформаційної операції, акт інформаційної війни, що реалізовується через сплановані та скоординовані дії з поширення серед цільової аудиторії інформації для маніпулювання свідомістю, управління емоціями,

конструювання системи уявлень про сприйняття подій, явищ та фактів.

Психологічна реабілітація – система заходів, спрямованих на відновлення, корекцію психологічних функцій, якостей, властивостей особи, створення сприятливих умов для розвитку та утвердження особистості.

Психологічні операції – планова пропагандистська і психологічна діяльність, що проводиться в мирний або воєнний час, спрямована на іноземні ворожі, дружні або нейтральні аудиторії з метою впливу на їхсвідомість та поведінку в потрібному напрямку для досягнення як політичних, так і військових національних цілей держави.

Психотронна (психофізична) зброя – сукупність інтелектуальних і технологічних можливостей та знань психотроніки, її засобів, методів, приладів, конструкцій, генераторів, які застосовуються у дистанційних психотропних атаках на людину з метою корекції та програмування її поведінки чи фізіологічних функцій.

Психотропні речовини (від грец. *tropos*– поворот, напрямок) – хімічні сполуки і природні продукти, здатні викликати стан залежності та спричиняти депресивний або стимулюючий вплив на центральну нервову систему, спричиняють порушення сприйняття, емоцій, мислення, чи поведінки і становлять небезпеку для здоров’я.

Радіоелектронна боротьба – комплексне застосування засобів передачі електромагнітної енергії для виявлення та придушення засобів управління супротивника і захисту своїх військ від радіоелектронного впливу.

Розвідувальна війна – несанкціоноване отримання та обробка даних про віддалену інформаційну систему, її ресурси, засоби захисту, пристрої та програмне забезпечення для отримання стратегічно важливих відомостей про потенціал супротивника.

Сайт – певне місце в мережі, яке доступне з будь-якої точки світового простору, адреса розташування інформаційного ресурсу в Internet, сукупність Web-сторінок, об'єднаних за змістом.

Свідомість – вищий рівень психічного відображення і саморегуляції, властивий тільки людині, як мислячій активній суспільно-історичній істоті, яка емпірично продукує множину чуттєвих і розумових образів, що існують у «внутрішньому досвіді» людини та обумовлюють її практичну діяльність.

Світовий політичний процес – сукупна діяльність народів, держав та інших інститутів, соціальних спільностей та їхніх організацій і рухів, які переслідують певні політичні цілі в міжнародному житті.

Свобода – можливість прояву суб'єктом своєї волі; незалежність, відсутність будь-яких незручностей або обмежень для влади або для членів суспільства.

Сепаратизм (від франц. *separatisme*, лат. *separatus* – окремий) – рух за територіальне відокремлення тієї чи іншої частини держави з метою створення нового державного утворення або надання певній частині держави автономії за національними, релігійними чи мовними ознаками.

Сервери – комп'ютери, що забезпечують роботу та надають послуги іншим комп'ютерам та програмам у складі мережі.

Сили та засоби інформаційного протиборства – комплекс організованих структур і матеріальних ресурсів, інформаційно-комунікаційних систем, органів управління і забезпечення, які застосовують для ведення інформаційної війни.

Синергетика (від грецьк. *συν* – «спільно» і *εργος* – «діючий») – міждисциплінарний напрямок наукових досліджень, завданням якого є вивчення природних явищ і процесів на основі принципів самоорганізації систем (що складаються з підсистем).

Система міжнародних відносин – сукупність економічних, політичних, ідеологічних, правових, дипломатичних, гуманітарних зв’язків і взаємостосунків між народами, державами і об’єднаннями держав, між основними силами та організаціями, що діють на світовій арені.

Соціальні мережі – структури, що ґрунтуються на людських зв’язках або взаємних інтересах у різних сферах буття людини та суспільства; може розглядатися як Інтернет-платформа, за допомогою якої люди можуть комунікувати та об’єднуватися за специфічними інтересами.

Соціальна система – співтовариство активних суб’єктів, що прагнуть забезпечити собі найкращі умови виживання при обмеженні наявних ресурсів.

Соціальна структура суспільства – сукупність усіх соціальних груп і спільнот даного суспільства, що в певний спосіб взаємодіють між собою.

Соціальна сфера – складова суспільного життя, сутність якої становлять соціальні стосунки і зв'язки, в яких перебувають люди, задовольняючи свої матеріальні і духовні інтереси й потреби.

Спеціальна інформаційна операція (СІО) – сплановані дії, спрямовані наворожу, дружню або нейтральну аудиторію з метою спонукання до прийняття управлінських рішень або (та) вчинення дій, вигідних для суб'єкта інформаційного впливу.

Спеціальна пропаганда (спецпропаганда) – комплекс технологій військово-психологічної інженерії під час війни або локального конфлікту у формі ефективного застосування маніпуляцій суспільною свідомістю (переконання та навіювання) з метою деморалізації мирного населення і військ супротивника та досягнення політичних (військових, економічних) перемог.

Способи інформаційного протиборства – спланована та цілеспрямована система дій державної інформаційно-комунікативної інфраструктури, якавизначає послідовність та порядок типових прийомів застосування сил та засобів для ведення інформаційного протиборства при досягненні воєнно-політичних і стратегічних завдань.

Стан війни – відносини держав з моменту оголошення війни між ними або фактичного початку військових дій до їх закінчення.

Суб'єкт політики – особистість, організація чи суспільна група, яка здатна створити політику, тобто постійно і відносно самостійно брати участь у політичному житті відповідно до своїх інтересів, впливати на становище та поведінку інших, викликати своїми діями важливі зміни в політичних відносинах.

Суб'єкти інформаційного протиборства – це соціально-політичні формування, які мають інтереси в інформаційному просторі, спеціальні структури для ведення інформаційного протиборства, що розробляють ефективні зразки інформаційної зброї, контролюють національні сегменти інформаційного простру та діють в правовому полі державних нормативних положень, які дозволяють брати участь в інформаційному протиборстві.

Суверенітет (франц. *souverainite* – верховна влада) – незалежне від будь-яких сил, обставин і осіб верховенство; незалежність держави в зовнішніх і внутрішніх справах.

Суспільний інтерес – спонукальні сили діяльності груп, мас людей, опираючись на які суспільство може вдаватися до необхідних управлінських впливів на цю діяльність.

Суспільство – організована соціальна самодостатня система, заснована на взаємовідносинах людей в процесі реалізації особистих потреб, об'єднаних характерними відносинами на певному етапі історичного розвитку.

Тактика в політиці– сукупність певних прийомів і форм політичної діяльності, спрямованих на досягнення того чи іншого результату у політичній діяльності.

Тактичний район інформаційного протиборства – сегмент периферійного інформаційного простору для проведення дезінформуючих акцій з метою створення сприятливої суспільної думки місцевого населення в інтересах тактичних дій дестабілізаційного характеру та виведення із ладу тактичної ланки системи інформаційно-комунікаційної інфраструктури супротивникапроти яких здійснюються інформаційні операції.

Театр воєнних дій – певний регіон, частина континенту з водами навколишнього океану, внутрішніми морями, повітряним простором або акваторія одного океану, що охоплює ближні острови, моря, в межах яких розгортаються і можуть розгортатися воєнні дії, стратегічні угруповання військових сил супротивника.

Театр глобального інформаційного протиборства – глобальний інформаційний простір, який використовують суб’єкти інформаційного протиборства для проведення широкомасштабної інформаційної війни з метою досягнення інформаційного домінування, посилення військового, політичного, економічного та духовного потенціалу з одночасним послабленням або знищенням потенціалу супротивника чи конкурента.

Телеконференції – це послуга Internet, за допомогою якої абонент може залишити своє відкрите повідомлення у мережі.

Терор (від лат. *terror*– жах, страх) – політика залякування, придушення супротивників насильницькими методами. Використовується як засіб досягнення мети.

Тероризм – ведення політичної боротьби із застосуванням (або погрозою застосування) насильства, методів залякування, фізичної розправи, політичних убивств, придушення конкурентів, провокацій.

Терористичний політичний акт – особлива форма цілеспрямованого, жорстокого політичного насильства (або загрози його застосування), організованого з метою змінити внутрішню чи зовнішню політику держави або з іншими політичними цілями.

Технічний захист інформації (ТЗІ) – діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації.

Технічний захист секретної інформації – вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та унеможливлення блокування інформації.

Толерантність (від лат. *tolerantis* – терплячий) – терпиме ставлення до інших, чужих думок, вірувань, політичних поглядів та позицій. Є неодмінною умовою демократичного, правового, стабільного суспільно-політичного устрою.

Тролі – реальні люди, які створюють фейковий акаунт, щоб провокувати інших користувачів на дискусії, суперечки.

Троллінг – порушення етики мережевого спілкування з метою штучного створення конфліктної ситуації.

Указ – постанова глави держави, верховного органу влади, що має силу закону.

Унітарна держава (від лат. *unitar* – єдність) – форма державного устрою, яка ґрунтується на зверхності суверенітету єдиної держави над адміністративно-територіальними або національно-територіальними одиницями (областями, департаментами, префектурами, провінціями тощо), на які вона поділена і які не мають статусу державного утворення.

Уряд (англ. *government* – керування, правління) – вищий орган у системі виконавчої влади держави, підпорядкований парламенту і главі держави, який здійснює державне управління суспільними справами, впроваджує в життя рішення законодавчої влади та забезпечує дотримання встановлених у державі законів, наділених для цього політичною виконавчою владою.

Участь політична – форма активної поведінки громадян у сфері політики; дії пересічних громадян, які намагаються впливати на прийняття владою політичних рішень або на вибір політичних лідерів.

Фальсифікація (від лат. *falsificatio*) – умисне викривлення або ж неправильне тлумачення тих чи інших явищ, подій, фактів; вчинене з корисливих мотивів, підроблення чогось.

Федеративна держава (від лат. *federatio* – союз, об’єднання) – форма децентралізованого державного устрою, при якій ознаки державного утворення притаманні як державі в цілому, так і її складовим частинам (штатам, провінціям, кантонам, землям,

республікам тощо), що вважаються суб'єктами федерації, а вищі органи як держави в цілому, так і суб'єктів федерації мають широку сферу власної виключної компетенції.

Фейк – (букв. – підробка) поширення неправдивої інформації в мережі Інтерент.

Фейкові новини – повністю або частково вигадана інформація про суспільні події, явища, певних осіб, яка подається у ЗМІ під виглядом справжніх журналістських матеріалів.

Форма державного правління – характеристика держави, що визначаться структурою, шляхом формування і правовим статусом вищих державних органів влади. Існує дві основні форми державного правління: монархія та республіка.

Форма державного устрою – адміністративно-територіальна організація держави, якою визначається система відносин держави як цілого та її складовими частинами – адміністративно-територіальними чи національно-територіальними одиницями.

Хакерство – діяльність, що пов'язана з протиправними діями в цифрових мережах та Інтернеті, що спрямовані на здійснення доступу до ресурсів та даних, які становлять приватну, комерційну чи державну таємницю з метою одержання захищеної інформації чи економічної вигоди.

Хакер (від англ. *chaker* – зламувач) – спеціаліст з комп'ютерних технологій, що володіє інтелектуальним потенціалом та знаннями, які дають йому можливість одержати несанкціонований доступ до комп'ютерних мереж з метою їх незаконного використання.

Хайп (англ. hype) – агресивна та нав'язлива реклама, метою якої є формування споживацької психології клієнта.

Хости – комп'ютери або машини, об'єднані каналами зв'язку в Internet, серед яких можна виділити дуже потужні мейнфрейми, менш потужні мінікомпютери і персональні комп'ютери.

Цензура – спеціальний спосіб обмеження свободи слова, друку та інформації; особливо поширений у тоталітарних державах і режимах. Основою Ц., яку здійснюють державні органи, є жорстка система правил і заборон, через які уніфікується інформація.

Цивілізація (від лат. *civilis* – цивільний, громадянський) – форма суспільного життя людей, якій притаманне відтворення власної матеріальної та соціально-політичної структури відносин на основі пріоритету духовних норм, цінностей.

Цивілізація політична – складається з поліетнічного населення, яке живе на окремій території і утворює державу, може існувати деякий час у переддержавному стані, але як сурогат політичної нації.

Цивільний контроль над збройними силами – комплекс здійснюваних у відповідності з Конституцією і законами України правових, організаційних, інформаційних заходів для забезпечення неухильного дотримання законності й відкритості діяльності збройних сил держави, сприяння їх ефективній діяльності і виконанню покладених на них функцій, зміцненню державної та військової дисципліни.

Цільова аудитоорія – це сегмент соціуму на який спрямована діяльність інформаційні кампанії з метою переконання або примусу ЦА до прийняття рішень і дій, які забезпечують національні інтереси держав-конкурентів, держав-ворогів.

Час політичний – певний відрізок часу, період, впродовж якого здійснюються політичні події, що визначають усе політичне життя.

Чат (від англійського chat) – служби Інтернету, що дозволяють проводити текстові дискусії в режимі реального часу. Від традиційної форми розмови їх відрізняє те, що вони ведуться в текстовому вигляді – шляхом набору тексту на клавіатурі. Найпопулярнішим відкритим стандартом, що лежить в основі чатів, є IRC (Internet Relay Chat).

Шовінізм (від франц. *chauvinisme*) – надмірний патріотизм з покладаннями надії на військову силу; ультранаціоналізм з елементами авторитаризму.

Явище політичне – невід'ємний елемент політичної діяльності, що відображає певні процеси у політичних системах.

Ядерна зброя – зброя масового ураження вибухової дії, в якій застосовується внутрішньоядерна енергія, яка виділяється під час ланцюгових реакцій поділу важких ядер деяких ізотопів урану та плутонію або у термоядерних реакціях синтезу легких ядер – ізотопів водню (дейтерій та тритій).

Ядерна політика – діяльність політичних суб'єктів у сфері мирного чи потенційного воєнного використання атомної енергії.

FTP – служба прямого доступу, що вимагає повноцінного підключення до Інтернету.

HTML (Hyper Text Markup Language) – мова розмітки гіпертекстових документів. За її правилами форматуються Web-сторінки та розповсюджуються дані WWW-системи.

On-line – робота в режимі реального часу.

Off-line – робота користувача на комп'ютері до початку сеансу зв'язку з іншим комп'ютером в мережі.

Skype – безкоштовне програмне забезпечення, що забезпечує текстовий, голосовий зв'язок і відео зв'язок через Інтернет між комп'ютерами (IP- телефонія), використовує технології пірінгових мереж, а також платні послуги для дзвінків на мобільні і стаціонарні телефони.

URL (Universal Resource Locator) – уніфікований покажчик ресурсу, адреса інформаційного ресурсу в Internet, де вказаний протокол, за правилами якого передаються дані, ім'я серверу, на якому зберігається файл, а також може бути вказаний шлях до каталогу файлу та безпосередньо ім'я.

Web-браузери (browsers) – програми перегляду WWW-сторінок та інших ресурсів. Сучасні браузери мають широкі мультимедійні можливості. Найвідомішими з них є Netscape Navigator Microsoft Internet Explorer.

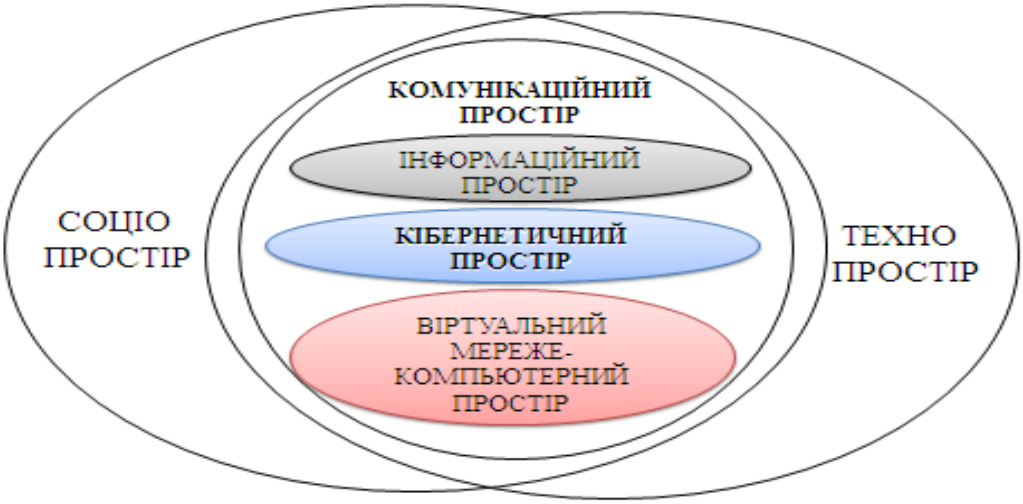
Web-сторінка – HTML-файл, який може містити тексти, зображення, програми на мові Java та інші Web-елементи.

WWW (World Wide Web) – світова інформаційна павутина.

ДОДАТКИ

Додаток 1

СТРУКТУРА КОМУНІКАЦІЙНОГО ПРОСТОРУ



12

Додаток 2

СТРУКТУРА КІБЕРНЕТИЧНОГО ПРОСТОРУ

11

Додаток 3

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ РІЗНИХ ВИДІВ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОЇ ЗБРОЇ

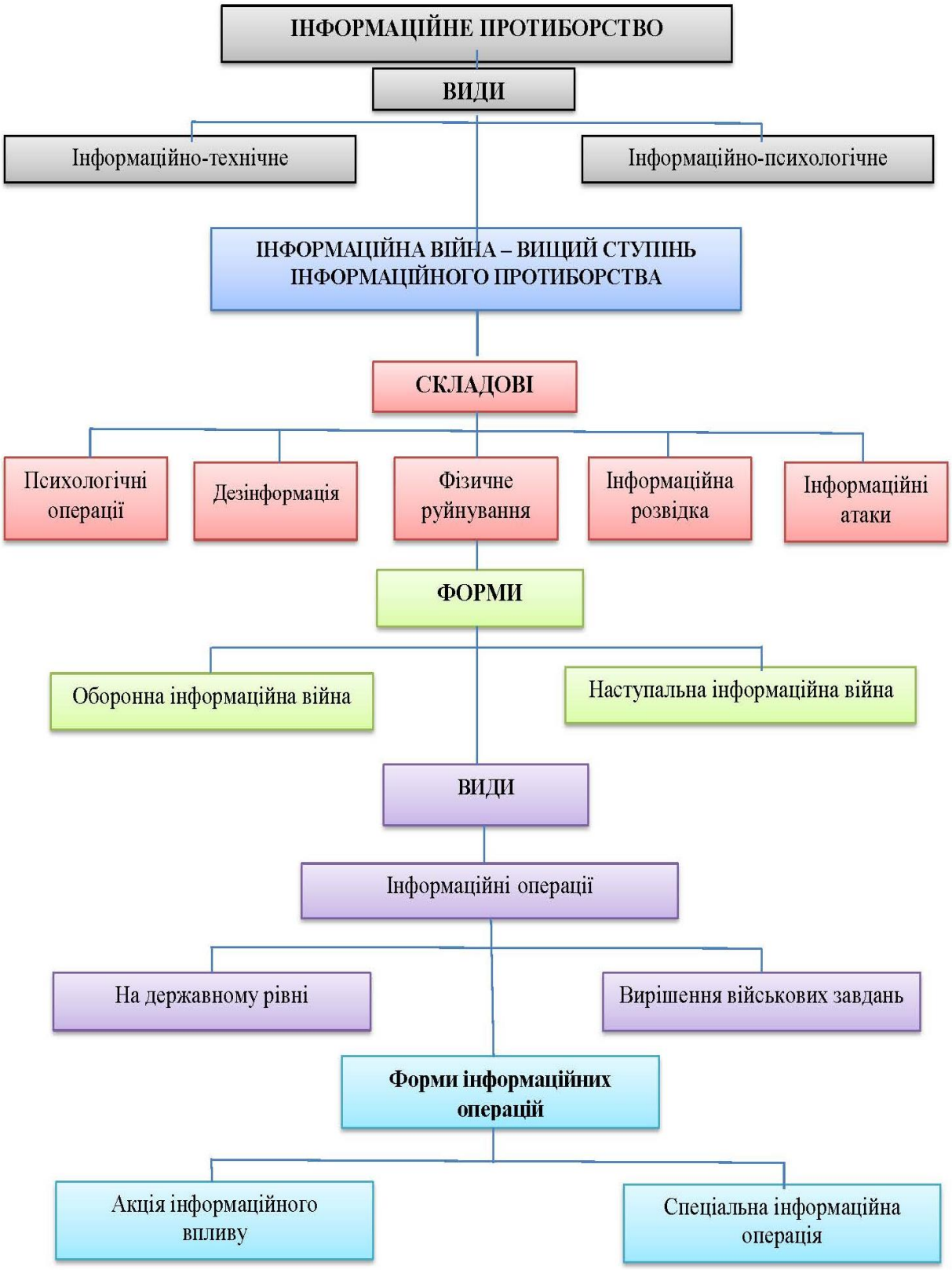
№ з/п	Вид ІПЗ	Види інформації	Мета	Результат
1.	Концептуально-методологічна	Світоглядна, методологічна	Формування картини світу людини, її ціннісної свідомості та методологічної культури; Визначення напрямів розвитку та стратегії захисту базових цінностей суспільства	Світоглядний хаос, некритичність мислення і диктат забобонів, комплекс меншовартості народу або ж, навіть, психологія раба; громадянський інфантилізм; вкрай низький рівень релігійної та етичної культури; деспотизм лінійного, моноказуального мислення; концептуальна залежність та гіпостазування еліти; вкрай низький рівень або навіть відсутність стратегічної культури
2.	Хронологічна (історична)	Інформація хронологічного порядку фактів та явищ, їх взаємозв'язку	Формування історичної свідомості народу, його самоідентифікації на тлі розвитку національної ідеології	Інформаційна «моральна ліквідація» національних героїв та видатних людей, знищення історичної пам'яті, історичних традицій народу і зведення їх до категорії неісторичних
3.	Фактологічна	Інформація прикладного характеру: релігія, ідеологія, політичні міфи, виборчі технології і маніпуляції свідомістю засобами масової інформації	Конструктивне застосування спрямоване на консолідацію нації, деструктивне – на розкол і руйнування історичних основ духовної цілісності народу, його дезорієнтацію та дезорганізацію	Використання просторово-часової парадигми формування ідеополя нації. Масова втрата віри, світоглядний хаос та безлад у соціальній сфері
4.	Лінгвістична	Мова	Контроль над засобами комунікації та передачі інформації	Втрата значущості мовного чинника у формуванні моделей освіти та культури

Додаток 4

УПРАВЛІННЯ ПРОЦЕСАМИ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА В ЗАЛЕЖНОСТІ ВІД РІВНЯ ТЕХНОЛОГІЧНОГО РОЗВИТКУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ ІНФРАСТРУКТУРИ

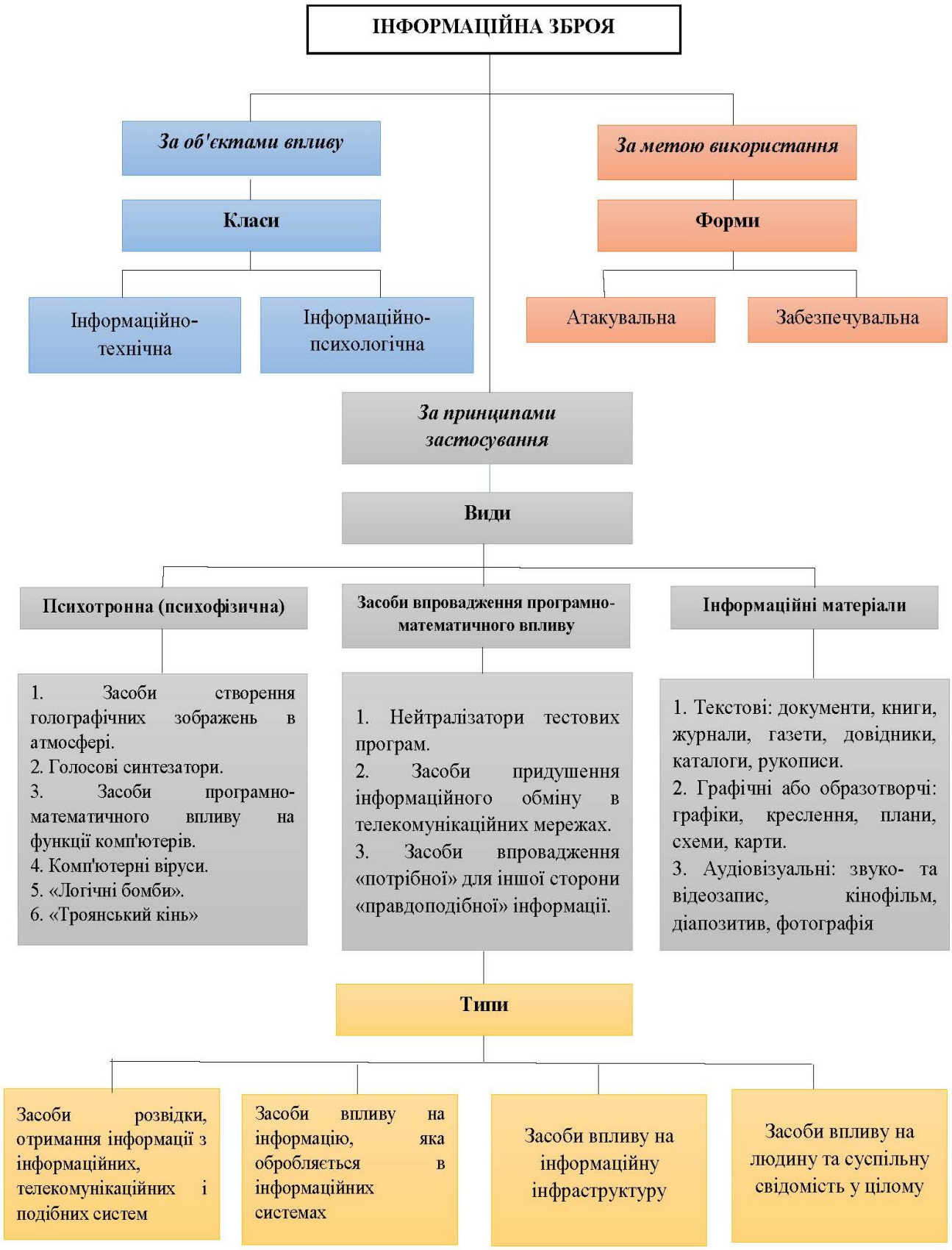
Рівень	Засоби	Сили	Цілі	Форма управління
IV	Телебачення, радіомовлення, друкована продукція	Політики, військові та цивільні журналісти, працівники телебачення, кіно, театру, творчі особистості	Обґрунтування летального сценарію для противника, фізична смерть, санкції внутрішніх репресій для власного населення, обґрунтування застосування ЗЗМУ, ліквідація соціальних груп, недопущення формування громадянського суспільства та його інститутів	Військова бюрократія, централізація учасників інформаційного протиборства, жорстка ієрархія, сувора підпорядкованість, інститут єдино начальства
V	Комп'ютери, Інтернет, соціальні мережі, МК, інформаційні ресурси, засоби мобільного зв'язку, ЗМК, ЗМІ	Політики, соціальні активісти, мережеві активісти, блогери, кібер-командування	Обґрунтування летального сценарію для противника, застосування ВТЗ, фізична смерть, соціальне самогубство, комплекс санкцій, блокування застосування ЗЗМУ, тероризм, екстремізм, ліквідація лідерів соціальних груп, позбавлення впливу соціальних груп, монополізація влади, боротьба з громадянським суспільством і його інститутами	Маніпуляції, децентралізація учасників інформаційного протиборства, демократія процедур прийняття та контролю рішень, самостійність і автономність дій
VI	Віртуальне середовище, віртуальні реальності та гіперреальності, інформаційні гіпертекстові концентратори, інформаційні та програмні продукти, соціометри, мережі впливу	Мобільний натовп, експертні спільноти, солдати й офіцери інформаційного протиборства	Нелетальні ротації в еліті противника, соціальна смерть опонентів, демобілізація людського фактору та соціального ресурсу, поява людського сміття (зайвих людей), імітація громадянського суспільства та його інститутів	Антиманіпуляції, мережеві структури, динамічні ієрархії, відсутність старшинства, дискурсивні процеси
VII (перспективний)	Гіперманіпулятори, антиманіпулятори	*У стадії розробки*	Прискорення соціальних процесів і ротацій та переформатування еліт, відродження громадянського суспільства	Перехід до найміцнішого виду енергії – енергії людських мас

ІНФОРМАЦІЙНЕ ПРОТИБОРСТВО ТА ІНФОРМАЦІЙНА ВІЙНА



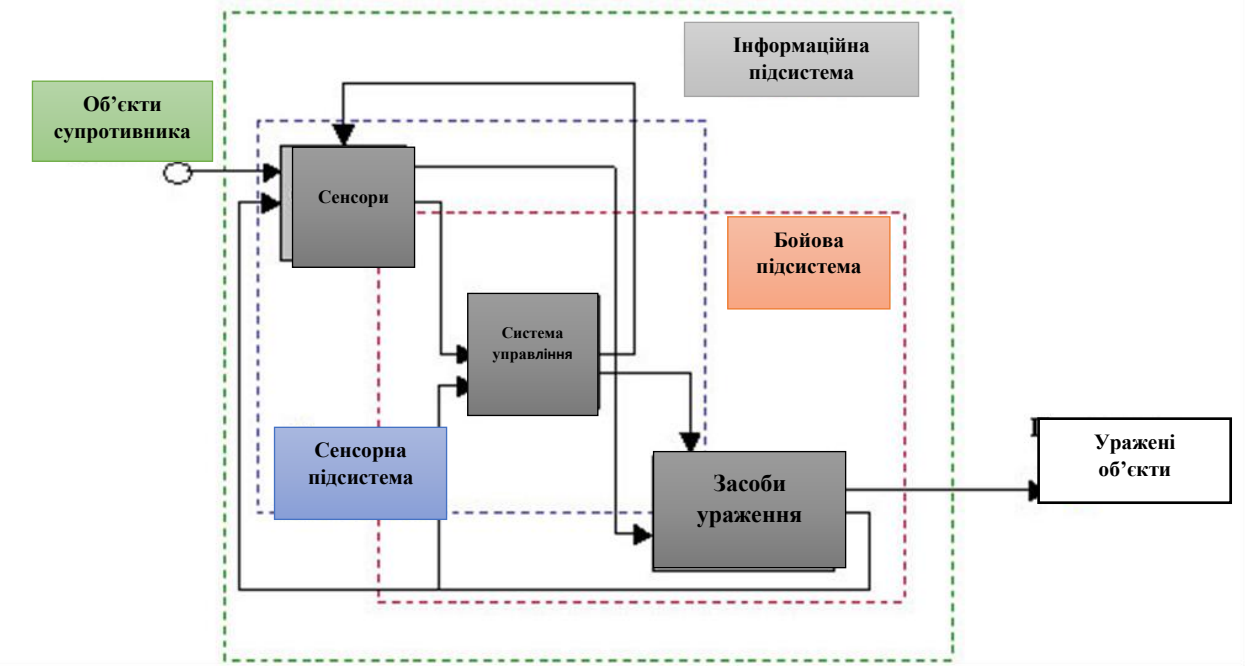
Додаток 6

ІНФОРМАЦІЙНА ЗБРОЯ



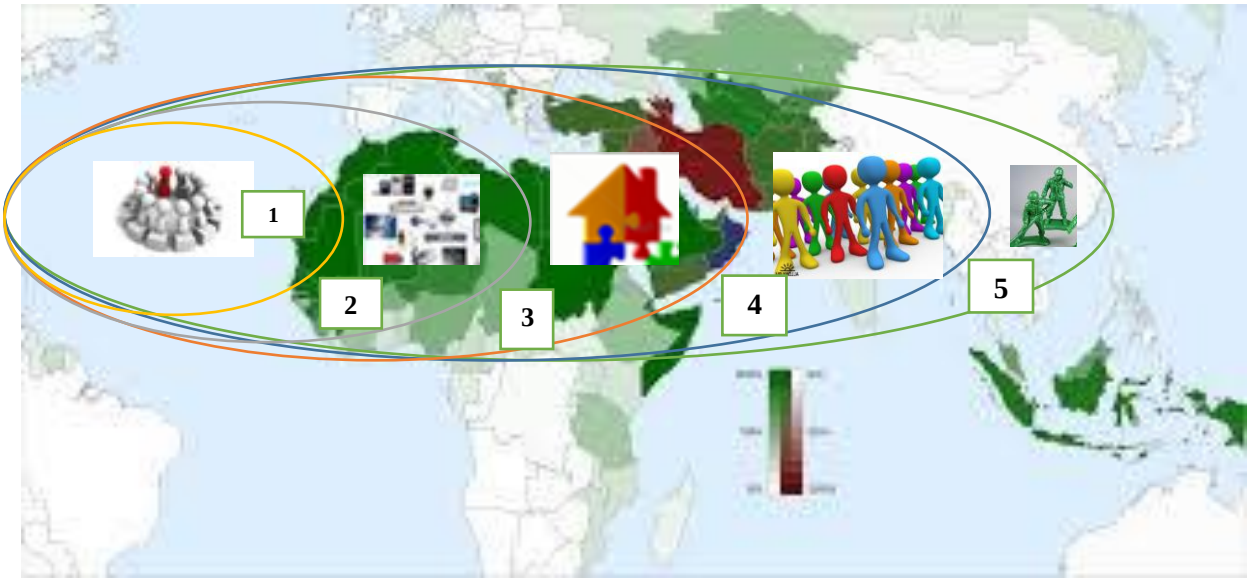
Додаток 7

МОДЕЛЬ ПРИНЦИПУ «МЕРЕЖЕЦЕНТРИЧНОЇ ВІЙНИ»



Додаток 8

«П'ЯТЬ КІЛЕЦЬ» ПОЛКОВНИКА УОРДЕНА



1. Військово-політичне керівництво
2. Система життєзабезпечення
3. Об'єкти інфраструктури
4. Населення
5. Збройні сили

Додаток 9

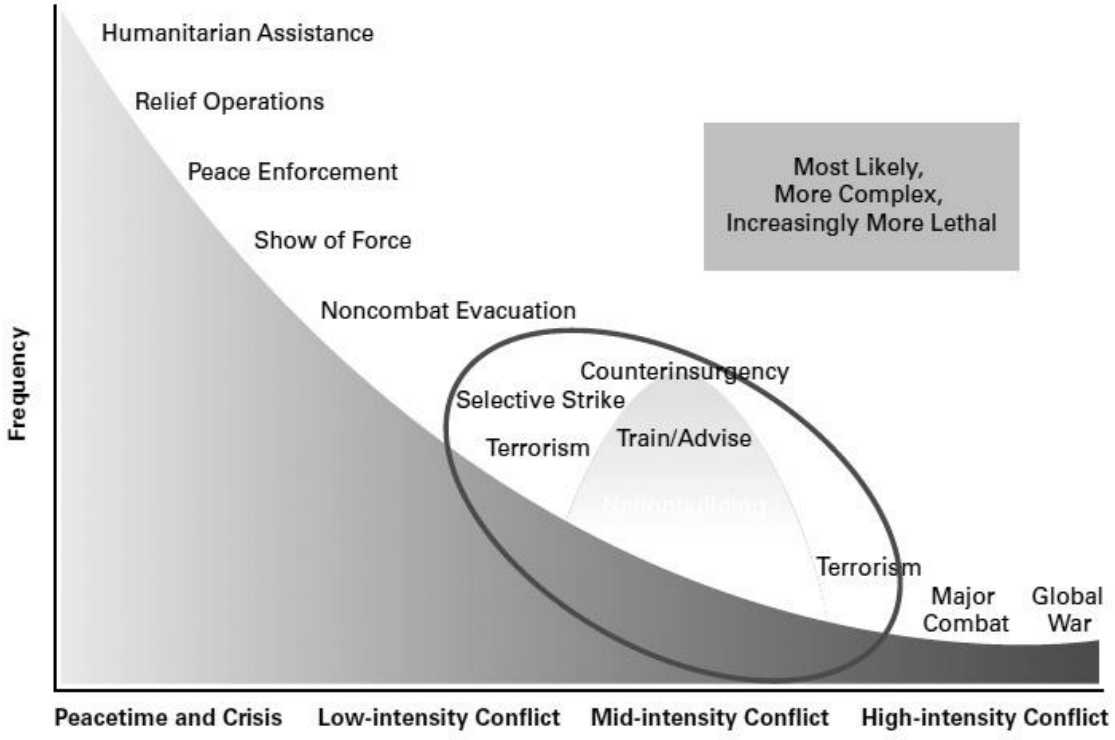
ЕВОЛЮЦІЙНИЙ РОЗВИТОК СУЧАСНИХ КОНЦЕПЦІЙ ВЕДЕННЯ БОЙОВИХ ДІЙ

№ з/п	Концепції	Мета	Технології
1	Мережецентрична війна	Створення нової ефективної моделі управління процесами збору, обробки та використання усіх видів інформації в кіберпросторі	1. Технології управління військами та зброєю. 2. Мережеві технології. 3. Технології систем і засобів зв'язку
2	Інформаційно-центрична війна	Досягнення інформаційної переваги над противником	1. Інформаційні технології. 2. Технології підтримки прийняття рішень. 3. Технології моделювання та імітації
3.	Знаннєцентрична війна	Передача знань, прогнозування розвитку військово-політичної обстановки та характеру ведення бойових дій	1. Методи прогнозування бойової обстановки. 2. Технології штучного інтелекту. 3. Новітні технології отримання знань

Додаток 10

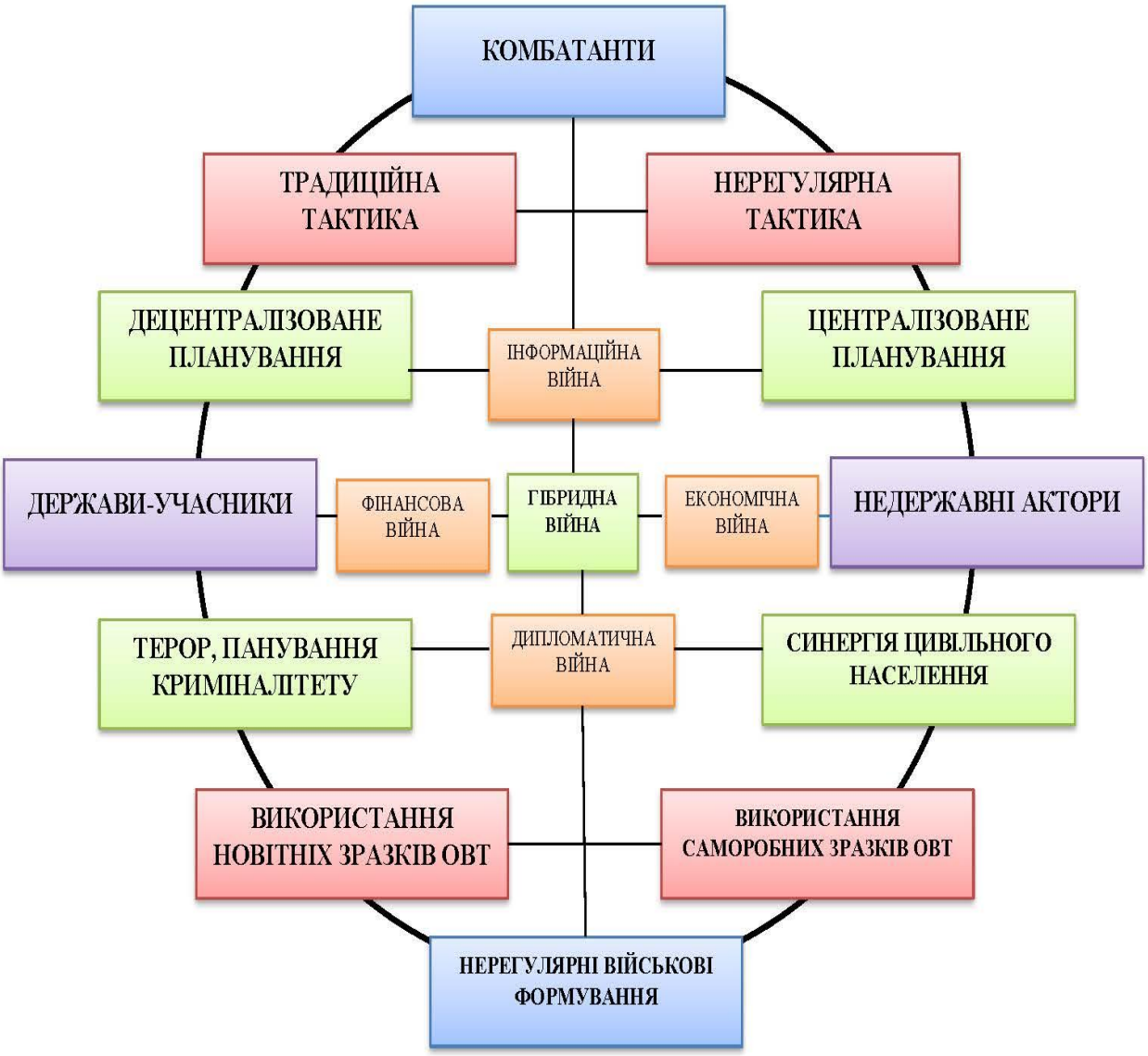
ГІБРИДНІ ЗАГРОЗИ ЗА Ф. ХОФМАНОМ

Figure 2. Implied Change in Spectrum of Conflict



Додаток 11

ГІБРИДНА ВІЙНА



Додаток 12

КОНЦЕПЦІЯ ПРЕЕМПТИВНОЇ ВІЙНИ

№ з/п	Етапи	Цілі	Способи	Інструменти
1	Підготовчий	Вибір жертви агресії	Створення іміджу «парії», «терористичної» держави, «фашистського» («нацистського») режиму	Масований інформаційний вплив за допомогою ЗМІ та ЗМК
2	1-й	Створення в соціумі держави-об'єкта опозиційного прошарку	Мирні «демократичні» протестні акції	Провокування загострення національних, релігійних і соціальних протиріч у країні світовими ЗМІ та ЗМК
3	2-й	Ескалація збройного насильства, напруженості та безладу в країні. Створення тимчасового (опозиційного) уряду	Мирні демонстрації набувають форму збройного зіткнення опозиції з владою. Відбувається захоплення складів зі зброєю, нейтралізація військових і правоохоронних формувань, провокування міжнаціональних зіткнень та передислокація НЗФ через державний кордон	Захоплення національного сегмента ЗМІ та ЗМК (або на обмеженій території), встановлення цензурних обмежень на користь «влади народу»
4	3-й	Максимальна активізація НЗФ	Інтенсифікація бойових зіткнень з регулярними військами, знищення місцевих мешканців, які нелояльно ставляться до «повстанців», криміналізація та маргіналізація суспільного життя	Масштабна інформаційна кампанія держави-агресора з метою формування світової суспільної думки необхідності зміни «недемократичного» режиму
5	Заключний	Зміна законного уряду на «демократичний» («легітимний», «антифашистський», «народної довіри»)	Пряма збройна агресія або введення «миротворчого» контингенту *(при недосягненні мети заключного етапу)*	Використання авторитету міжнародних організацій, світових політичних, духовних лідерів

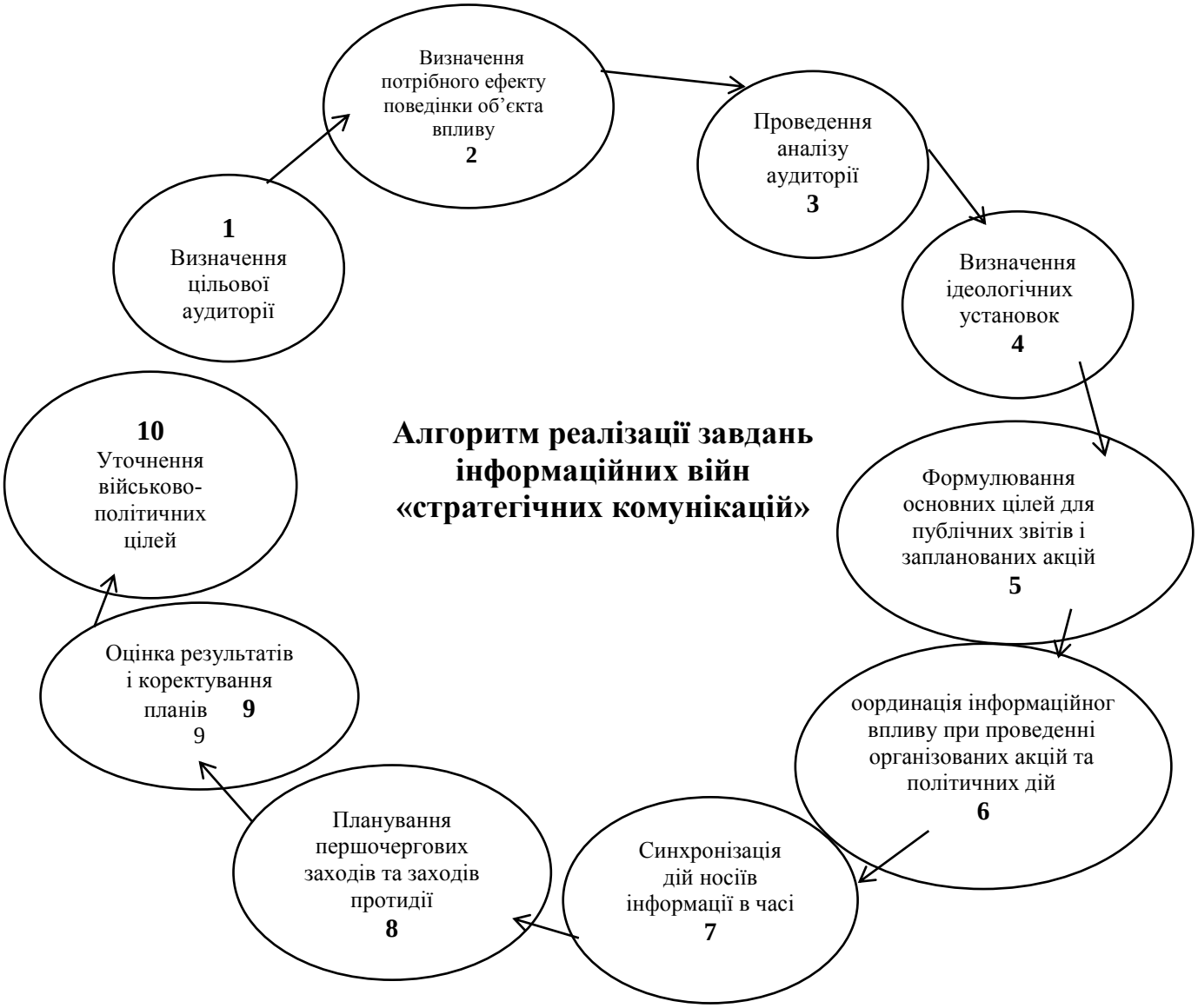
Додаток 13

КОНЦЕПЦІЯ КОНСЦІЄНТАЛЬНОЇ ВІЙНИ. ОСНОВНІ СПОСОБИ «РОЗМИВАННЯ» ІНДИВІДУАЛЬНОЇ ТА КОЛЕКТИВНОЇ СВІДОМОСТІ

№ з/п	Мета	Механізми впливу	Наслідки
1.	Ураження нейромозкового субстрату	Дія хімічних речовин, зараження повітря, радіоактивний вплив	Зниження ефективності функціонування мозку
2.	Пониження організації інформаційно-комунікативного середовища	Розбалансування, дезінтеграція, примітивізація інформаційно-комунікаційного середовища	Дезорієнтація свідомості
3.	Насадження бажаних форм мислення	Вплив за допомогою практики окультизму	Нейтралізація (параліч) свідомості
4.	Інтенсифікація атак на свідомість	Спеціальне розповсюдження по каналах комунікації потрібних образів і текстів	Руйнування свідомості
5.	Зруйнування форм ідентифікації особистості відносно фіксованих спільнот	Комплексна дія усіх форм і механізмів впливу	Зміна форм самовизначення та деперсоналізація

Додаток 14

АЛГОРИТМ РЕАЛІЗАЦІЇ ЗАВДАНЬ ІНФОРМАЦІЙНИХ ВІЙН «СТРАТЕГІЧНИХ КОМУНІКАЦІЙ»



Додаток 15

СТРУКТУРА КЕРІВНИХ ОРГАНІВ НАТО З ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ

СТРУКТУРА КІБЕРКОМАНДУВАННЯ ЗС США

Командування бойових дій у кіберпросторі

УНБ
Надання розвідувальної інформації

Центр спільних операцій у кіберпросторі

УІС МО США
Надання технічної підтримки

Командування бойових дій у кіберпросторі СВ ЗС США (2-га Польова армія)

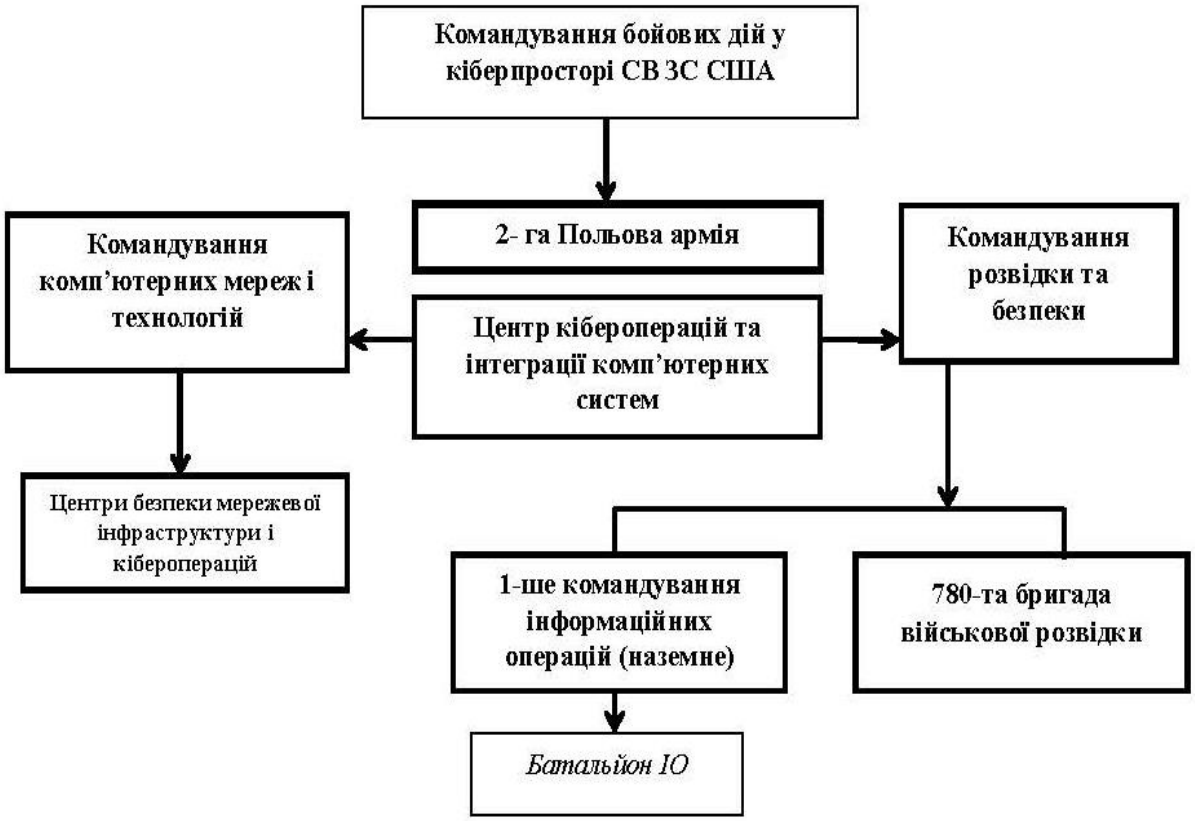
Командування бойових дій у кіберпросторі ВМС ЗС США (10-й оперативний флот)

24-та повітряна армія (бойових дій у кіберпросторі) ВПС

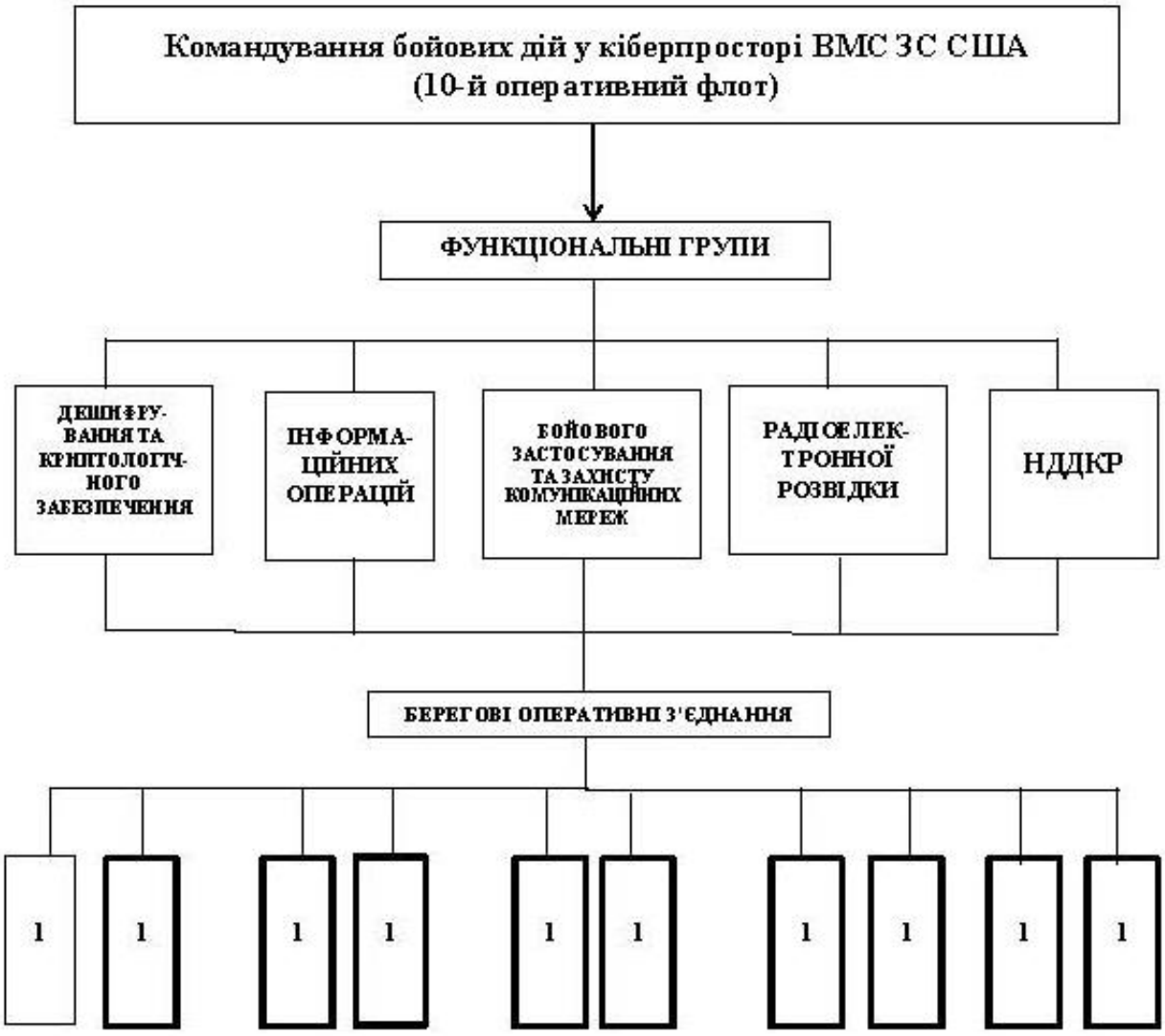
Командування бойових дій у кіберпросторі морської піхоти

Командування бойових дій у кіберпросторі берегової охорони (в перспективі)

СТРУКТУРА КОМАНДУВАННЯ БОЙОВИХ ДІЙ У КІБЕРПРОСТОРІ СВ ЗС США

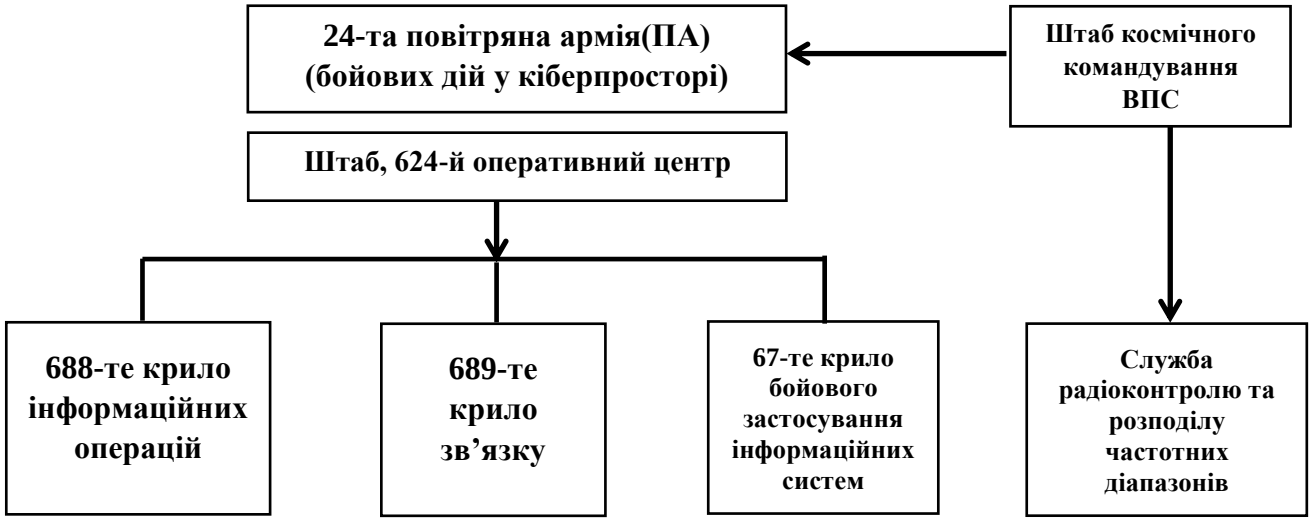


СТРУКТУРА КОМАНДУВАННЯ БОЙОВИХ ДІЙ У КІБЕРПРОСТОРІ ВІЙСЬКОВО-МОРСЬКИХ СИЛ ЗС США (10-Й ОПЕРАТИВНИЙ ФЛОТ (ОФ))



Додаток 19

СТРУКТУРА КОМАНДУВАННЯ БОЙОВИХ ДІЙ У КІБЕРПРОСТОРІ ВІЙСЬКОВО-ПОВІТРЯНИХ СИЛ ЗС США



Додаток 20

КОМАНДУВАННЯ БОЙОВИХ ДІЙ У КІБЕРПРОСТОРІ МОРСЬКОЇ ПІХОТИ

Додаток 21

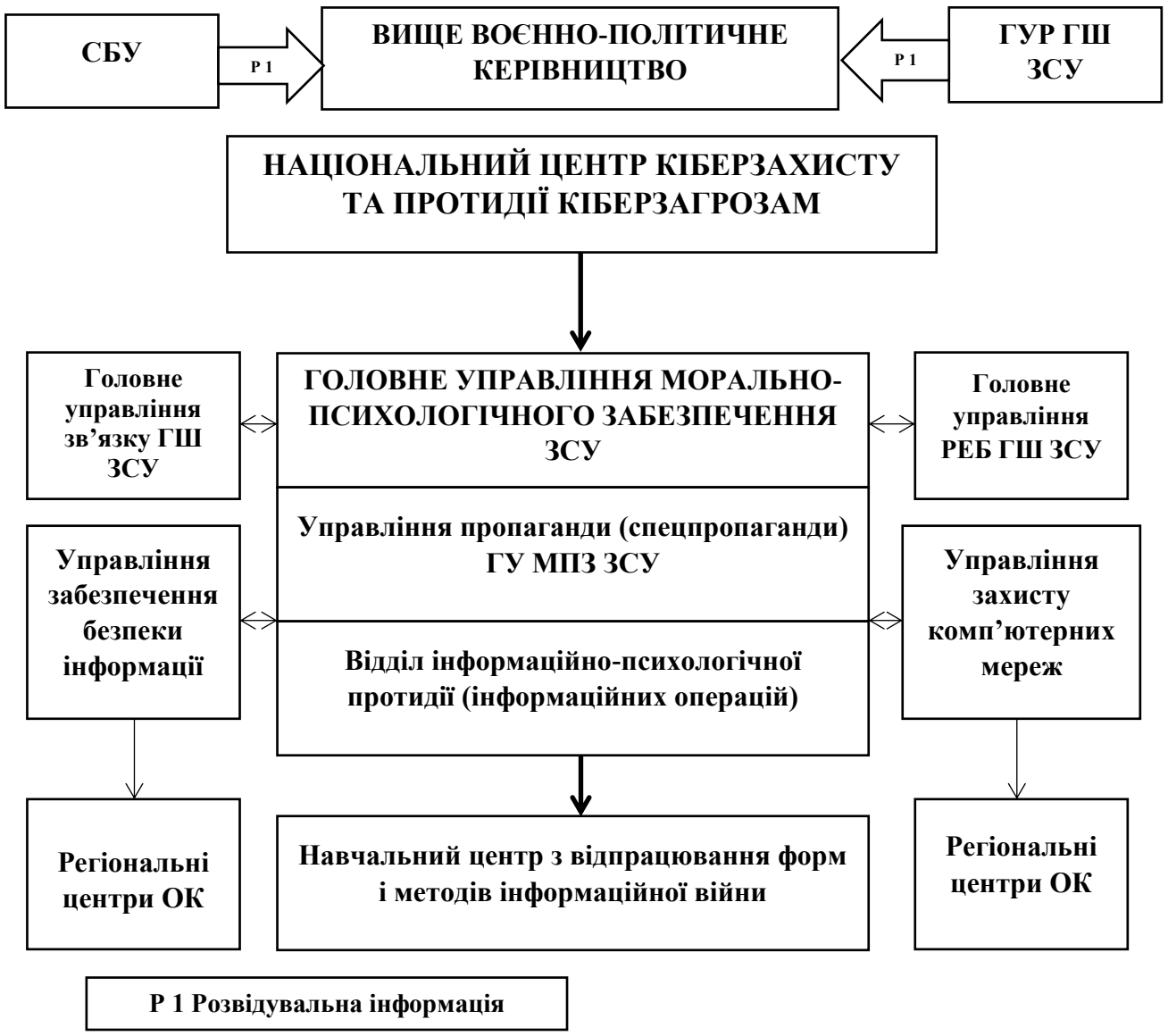
СТРУКТУРА КІБЕРВІЙСЬК ФРН

КОМАНДУВАННЯ

КОМАНДУВАННЯ СТРАТЕГІЧНОЇ РОЗВІДКИ	КОМАНДУВАННЯ ЗВ'ЯЗКУ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ	ЦЕНТР КІБЕРБЕЗПЕКИ
Ведення радіо, радіотехнічної, радіолокаційної, космічної разведки, РЕБ, оцінка воєнних потенціалів держав,картографічне забезпечення збройних сил	**Організація централізованого управління та зв'язку видів ЗС і міжвидових компонентів (до тактичної ланки), забезпечення функціонування АСУ та засобів комунікації, навчання фахівців**	**Захист ІТ систем від кібератак, сертифікація та установка програмного забезпечення на військових об'єктах**
Центри психологічних операцій, геоінформаційного забезпечення, обробки результатів космічної розвідки і оцінки радіоелектронної обстановки, батальйони РТВ, РЕБ	*Батальйони управління та зв'язку, центри обслуговування інформаційно-телекомунікаційних систем*	*Чисельність військовослужбовців і персоналу – 600 осіб*

Додаток 22

ОРГАНІЗАЦІЙНА СТРУКТУРА КІБЕРБЕЗПЕКИ ЗСУ (ВАРІАНТ)



Наукове видання

РУСЛАН ВОЛОДИМИРОВИЧ ГУЛА
ОЛЕКСАНДР ПЕТРОВИЧ ДЗЬОБАНЬ
ІРИНА ГРИГОРІЇВНА ПЕРЕДЕРІЙ
ОЛЕНА ОЛЕКСАНДРІВНА ПАВЛІЧЕНКО
ГРИГОРІЙ ОЛЕКСІЙОВИЧ ФІЛЬ

ІНФОРМАЦІЙНА ВІЙНА:
СОЦІАЛЬНО-ОНТОЛОГІЧНИЙ ТА МІЛІТАРНИЙ АСПЕКТИ

Монографія

Керівник видавничих проектів Ю. В. Піча

Підписано до друку 27.11.2019 р.
Формат 60х84/16. Папір офсетний.
Друк цифровий. Гарнітура Times New Roman.
Ум. друк. арк. 25,50. Обл.-вид. арк 25,85.

Видавництво «Каравела»,
просп. М. Рокоссовського, 8а, м. Київ, 04201, Україна.

Свідоцтво
про внесення суб'єкта видавничої справи
до Державного реєстру
видавців, виготівників і розповсюджувачів
видавничої продукції:
ДК №2035 від 16.12.2004 р.