УДК 342.9(477)

КАЧИНСЬКИЙ А.Б., *доктор технічних наук, професор,*
аналітик Департаменту протидії інформаційним загрозам
Центру протидії дезінформації при Раді національної безпеки
і оборони України.
ORCID: http://orcid.org/0000-0001-9642-7006.

СИСТЕМНА МОДЕЛЬ ОРГАНІЗАЦІЇ, ЩО ЗАБЕЗПЕЧУЄ ІНФОРМАЦІЙНУ Й ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНУ БЕЗПЕКУ

Анотація. *У статті інформація розглядається як критично важливий ресурс, що суттєво позначається на стані національної безпеки нашої держави і потребує розробки як теоретичних основ, так і практичних методів державної політики інформаційної безпеки. Ця політика реалізується відповідними організаціями й інституціями держави на основі результатів системних досліджень. Вирішення даної проблеми має базуватися на загальних принципах системного аналізу: розробка та використання засобів формування й аналізу цілей і функцій організації щодо забезпечення інформаційної й інформаційно-психологічної безпеки має бути заснована на багатоешелонній моделі структури контрпропагандистської організації. Акцентується на тому, що при розробці структурної моделі контрпропагандистської організації виникає проблема: необхідно знайти компроміс між простотою опису її структури і докладним описом процесу пропаганди, як форми комунікації. Модель вирізняється як різноманіттям типів елементів і типів відношень між ними. Системний підхід розглядає структуру контрпропагандистської організації як сукупність відносно незалежних, взаємодіючих між собою підсистем; при цьому деякі (або всі) підсистеми мають право ухвалення рішень, а їх ієрархічне розташування визначається тим, що деякі з підсистем знаходяться під впливом або керуються вищими. Така модель структури організації протидії дезінформації передбачає виконання наступних функцій: затвердження завдань й перевірку їх узгодженості, а також виконання та співвиконання цих завдань. Ці функції спрямовані на адекватну реакцію і збереження цілісності організації до постійних змін, що відбуваються в безпековому середовищі.*

Ключові слова: *системний підхід, організація, інформаційна, інформаційно-психологічна безпека, котрпропаганда, модель структури, інформаційні війни, інформаційна зброя.*

Summary. *The article considers information as a critically important resource that significantly affects the state of national security of our country and requires the development of both theoretical foundations and practical methods of state information security policy. This policy is implemented by relevant state organizations and institutions, based on the results of systematic research. The solution to this problem should be based on the general principles of system analysis: the development and use of means of formation and analysis of the organization's goals and functions to ensure information and information-psychological security should be based on a multi-echelon model of the structure of a counter-propaganda organization. Emphasizes that a problem arises when developing a structural model of a counter-propaganda organization: it is necessary to find a compromise between the simplicity of the description of its structure and the detailed description of the propaganda process as a form of communication. The model is distinguished by the variety of types of elements and types of relations between them. The systemic approach considers the structure of a counter-propaganda organization as a set of relatively independent, interacting subsystems; while some (or all) subsystems have the right to make decisions, and their hierarchical location is determined by the fact that some of the subsystems are influenced or controlled by higher ones. This model of the structure of the disinformation countermeasures organization provides for the following functions: approving tasks and checking their coherence, as well as execution and co-execution of these tasks. These functions are*

aimed at an adequate reaction and preservation of the integrity of the organization to the constant changes occurring in the security environment.

Keywords: *system approach, organization, information, information and psychological security, counter-propaganda, structure model, information wars, information weapons.*

Постановка проблеми. Інформаційне протиборство є невід'ємною складовою сучасного світопорядку з огляду на гостру геополітичну конкуренцію між різними центрами сили. Наразі війна, що триває не лише на фронті, а й в інформаційному просторі, перетворює інформацію на критично важливий ресурс, який суттєво позначається на стані національної безпеки нашої держави.

Головним джерелом загроз національним інтересам України в інформаційній сфері є агресивна україножобська політика путінської Росії.

Для успішного протистояння інформаційній експансії РФ необхідно розробити теоретичні основи й практичні методи державної політики інформаційної безпеки, що реалізуються відповідними організаціями й інституціями держави та базуються на результатах системних досліджень.

Результати аналізу наукових публікацій. Із вітчизняних дослідників, які приділяли увагу проблемі вивчення інформаційної й інформаційно-психологічної безпеки можна назвати такі прізвища, як Литвиненко О., Остроухов В., Петрик В., Присяжнюк М., Почепцов Г., Дубов Д. тощо. Становлення наукового напрямку інформаційних війн було також повя'зано з іменами таких учених, як Лайнбарджер П.М.Е., Джоует Г., О'Доннел В., Померанцев П., Грант Дж., Макдональд Г., Сінгер П., Бруклін Е., Патракаракос Д. тощо. На сьогодні існує значна кількість наукових публікацій і навчальної літератури з інформаційної й інформаційно-психологічної безпеки. Одначе питання розробки теоретичних засад організації зі забезпечення інформаційної й інформаційно-психологічної безпеки, що використовує теоретичні методи системного аналізу формування й аналізу її цілей і функцій, в літературі не розглядається.

Метою статті є розробка структурної моделі організації зі забезпечення інформаційної й інформаційно-психологічної безпеки. При цьому враховується той факт, що однією з принципових особливостей системного аналізу є розробка та використання засобів для формування й аналізу цілей і функцій організації.

Такий підхід створює перспективу розробки формалізованої моделі організації з інформаційного протиборства, дозволяє визначити її основні цілі і функції, забезпечити цілісність й адаптацію щодо змін, які відбуваються в оточуючому середовищі.

Виклад основного матеріалу. При розробці структурної моделі організації зі забезпечення інформаційної й інформаційно-психологічної безпеки виникає проблема: необхідно знайти компроміс між простотою опису її структури, що дозволяє скласти і зберегти цілісні уявлення про неї, і докладним описом процесу пропаганди, як форми комунікації [1; 2]. Модель вирізняється як різноманіттям типів елементів і типів відношень між ними.

Одним із способів вирішення даної проблеми є системний підхід, який розглядає складну систему як сукупність відносно незалежних, взаємодіючих між собою підсистем; при цьому деякі (або всі) підсистеми мають право ухвалення рішень, а їх ієрархічне розташування визначається тим, що деякі з підсистем знаходяться під впливом або керуються вищими [3; 4]. Рівні такої ієрархії називаються ешелонами [5].

На Рис. 1 наведена багатешелонна модель структури контрпропагандистської організації.

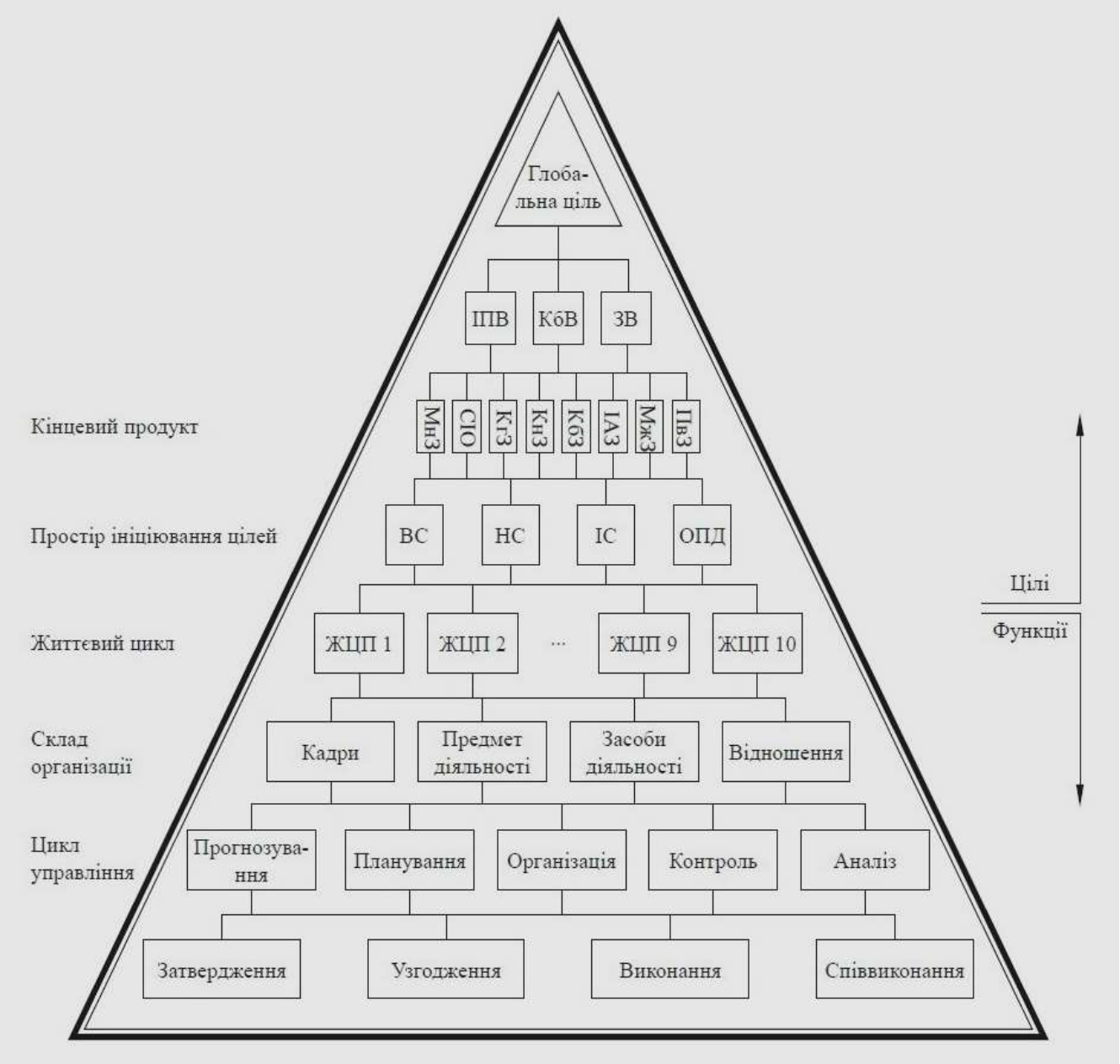

Рис. 1. Структурна модель організації протидії дезінформації,
що включає цілепокладання й її основні функції

Ешелон 1. *Визначення глобальної цілі.*

Успіх контрпропагандистських організацій, пов'язаний із сильним централізованим органом, що ухвалює рішення щодо досягнення визначених цілей. Цей орган передає чіткі команди по всій ієрархічній структурі організації. У даному випадку керівництво організації протидії дезінформації (далі – ОПД) формує глобальну ціль, визначену вищим органом або утворену за допомогою аналізу директивних документів.

Глобальна ціль має бути зорієнтована на кінцевий інформаційний продукт [6; 7].

Пропаганда віддзеркалює плани та наміри її авторів, що поступово проявляються в процесі аналізу. При формуванні глобальної цілі ОПД необхідно пам'ятати, що

наріжним каменем будь-якої пропаганди є свідомі та систематичні наміри добитися реакції, яка сприяє бажаному задуму пропагандиста.

Так, у передвоєнний час, або у мирний час ворожа пропаганда намагається негативно вплинути на бойовий дух і патріотичні настрої населення, виступити проти збройного опору ворогові, заразити населення занепадницькими і поразницькими настроями. Під час війни такі дії повинні наносити максимальні збитки ворогові: паніку серед населення, страйки й мітинги, скарги споживачів, розбрат серед політиків, недовіру до уряду, капітулянтські настрої.

За допомогою системного підходу аналітики організації протидії дезінформації можуть скласти повний список можливих цілей ворога. Про них завжди можна зробити висновки, аналізуючи досягнуті результати, незалежно від того скільки часу пройшло. після завершення тієї чи іншої операції [4].

Ешелон 2. *Декомпозиція цілей згідно критерія "кінцевий інформаційний продукт".*

Жорстке протиборство в глобальному інформаційному просторі призводить до повноцінних інформаційних війн. Наразі саме інформаційні війни нового покоління стали однією з рушійних сил геополітики.

Американські фахівці розглядають інформаційні й інформаційно-психологічні війни як сукупність різних форм, методів і засобів впливу на людей з метою зміни у бажаному напрямку їх психологічних характеристик (поглядів, думок, ціннісних орієнтацій, настроїв, мотивів, установок, стереотипів поведінки), а також групових норм, масових настроїв і громадської свідомості загалом [1; 2].

Існує багато класифікацій інформаційних війн. Ми розглядаємо три їх основних види: інформаційно-психологічні війни (ІПВ), кібернетичні війни (КбВ) й інформаційні війни змішаного типу (ЗВ).

У свою чергу, новітні інформаційні технології, сучасні інформаційні й психологічні форми та способи впливу на особистість й суспільство породжують велику кількість різних видів інформаційної зброї [8 – 10].

Ми розглядаємо *ментальну зброю* (МнЗ), як зброю спрямовану на зміну ідентичності. В умовах сучасних інформаційних війн особливого значення набуває забезпечення безпеки національного культурного простору, його захист від ментальної зброї.

С*пеціальні інформаційні операції* (СІО) – це інформаційна зброя, що використовує не тільки медійні засоби, але й можливості культури й мистецтва, а також психотропні й психотронні методи ураження свідомості, що небезпечніше, – заміщення свідомості.

До інформаційної зброї, спрямованої на ураження свідомості відноситься й *когнітивна зброя* (КгЗ), що здатна заражати масову свідомість когнітивними вірусами на кшталт мемів. Проникаючи у свідомість, "перепрограмовуючи" її, меми-віруси, подібно інформаційній пандемії, поширюються у масовій свідомості.

Контентна зброя (КнЗ) – це зброя, що спрямована на зміну властивостей людського інтелекту. Головним її інструментом є зміст інформаційного повідомлення, вибудований спеціальним способом, і який може бути представлений у мультимедійному, текстовому або графічному форматі.

Кібернетична зброя (КбЗ) – це зброя, що використовує комп'ютерні мережі для здійснення різних політично орієнтованих кібератак, і використовуватися як окремими хакерами, терористичними групами, так і цілими державами. Тут особливу загрозу становлять віруси типу "логічних бомб" і "троянів".

Інформаційно-алгоритмічна зброя (ІАЗ) – це зброя, що за допомогою психофізичних методів вражає мозок людини через візуальні образи кіберпростору,

перетворює людей у провідники наперед заданих ідей-алгоритмів. Мета застосування даного виду зброї – корекція культурного коду.

Основу *мережевої зброї* (МзЗ) становить сукупність дій, спрямованих на формування задуманої моделі поведінки як окремих людей, так і окремих груп спільноти в умовах миру, кризи чи війни. Мережеві способи організації взаємодії й реалізації колективних дій змінюють наші спільноти. Здійснюється це за допомогою інформаційних технологій (від смартфона до Інтернету).

Поведінкова зброя (ПвЗ) – це нелетальний тип зброї, метою використання якої є зміна поведінки окремих груп людей або ворога загалом. Вона спрямована на створення спеціальних умов, коли людина віддає перевагу не самостійному ухваленню рішень, а автоматичному наслідуванню чужих звичок, стереотипів тощо.

Під кінець з погляду декомпозиції цілей згідно критерію "кінцевий інформаційний продукт" можна зазначити, що цілі інформаційних й інформаційно-психологічних війн суттєво відрізняються від війн у загальноприйнятному розумінні. Це не фізичне знищення противника: ліквідація його збройних сил, не знищення його важливих стратегічних й економічних об'єктів, а широкомасштабне порушення роботи інформаційних, комунікаційних мереж і систем, часткове порушення економічної інфраструктури, розробки технологій раннього розпізнавання інформаційної агресії та засобів її протидії.

***Ешелон 3*: *декомпозиція цілей згідно критерію "простір ініціювання цілей"*.** Цілепокладання на даному рівні здійснюється в залежності від змін, що відбуваються у зовнішньому інформаційному середовищі, і позначається на кінцевих інформаційних продуктах. При чому всі організовані системи (організації, відомства тощо), з якими взаємодіє система забезпечення інформаційної й інформаційно-психологічної безпеки діляться на чотири класи: вищестояща система (ВС), що визначає головні вимоги до кінцевого інформаційного продукту; нижчестоящі системи (НС), вимоги до яких визначають можливості підготовки якісних інформаційних продуктів, інформаційне середовище (ІС), організація протидії дезінформації (ОПД), яка ініціює власні підцілі, що відповідають стану захищеності держави від інформаційних й інформаційно-психологічних загроз [11; 12].

У такий спосіб ОПД – це цілеспрямована система, яка може сприймати виклики й загрози, зовнішні щодо неї, та формувати цілі, адекватні інформаційні безпеці держави, ефективно протидіяти деструктивним інформаційним впливам і пропаганді. При чому ОПД може змінювати функції, властивості і навіть структуру як функціональних елементів, так і системи загалом, здійснюючи при цьому доцільний вибір альтернативних дій для досягнення цілей за наявних умов [13; 14].

***Ешелон 4*: *декомпозиція цілей згідно критерію "життєвий цикл"*.**

На даному рівні визначаються послідовні кроки отримання кінцевих інформаційних продуктів – від визначення джерела дезінформації до постановки конкретних завдань: визначення ідеології та мети (ЖЦП1); визначення контексту (ЖЦП2); визначення пропагандиста (ЖЦП3); дослідження структури пропагандистської організації (ЖЦП4); визначення цільової аудиторії (ЖЦП5); розуміння методів використання інструментів пропаганди (ЖЦП6); аналіз спеціальних методів для максимального впливу (ЖЦП7); аналіз реакції аудиторії (ЖЦП8); виявлення й аналіз контрпропаганди (ЖЦП9); завершення оцінки й завдання (ЖЦП10) .

У такий спосіб ОПД буде здійснювати погоджену, цілеспрямовану, керовану з єдиного центру державну політику інформаційного протиборства, спрямовану на захист державних інтересів і забезпечення інформаційної й інформаційно-психологічної

безпеки особистості, суспільства і держави в умовах інформаційно-психологічної агресії [15].

Ешелон 5*: *декомпозиція цілей згідно складу системи забезпечення інформаційної й інформаційно-психологічної безпеки, у результаті якої формуються функції щодо вироблення основного інформаційного продукту. Вони випливають із потреб основних елементів організації протидії дезінформації і об'єднуються у три основні групи кадри (К), протидія дезінформації як предмет діяльності (ПД) і засоби діяльності (ЗД).

Проблема професійного відбору та супроводження фахівців у сфері інформаційної безпеки у процесі їх професійної діяльності є достатньо актуальною для багатьох держав світу. Що стосується України, то загалом можна стверджувати, що нарощення кількісних показників розвитку підготовки фахівців мережею вищих навчальних закладів в останні роки забезпечило певні якісні перетворення, зокрема на рівні прийняття рішень органів державного і міжнародного управління.

На думку [16], з огляду на підвищену загрозу сучасного арсеналу сил, засобів і методів інформаційної війни акції інформаційно-психологічної агресії та операції інформаційно-психологічної війни необхідно виявляти і припиняти на ранніх стадіях їх підготовки. Систему заходів ОПД протидії акціям інформаційно-психологічної агресії та операціям інформаційно-психологічної війни на ранніх стадіях можна умовно розподілити на три складові: попередження акцій інформаційно-психологічної агресії та операцій інформаційно-психологічної війни; виявлення акцій інформаційно-психологічної агресії та операцій інформаційно-психологічної війни; припинення інформаційно-психологічної агресії та операцій інформаційно-психологічної війни.

Основними засобами, за допомогою яких ОПД здійснює свою діяльність, є сукупність знань, умінь та навичок. Вони є основними продуктивними елементами її діяльності.

Ешелон 6*: *декомпозиція цілей згідно критерію "управлінський цикл".

Використовуючи методику структуризації цілей, на даному рівні декомпозиції можна виділити наступні організаційні заходи системи забезбечення інформаційної й інформаційно-психологічної безпеки: прогнозування (Пр), планування (Пл), організацію (Ор), контроль (Ко) й аналіз результатів її діяльності (Ан) [17].

Усі ці заходи передбачають виконання наступних функцій організації протидії дезінформації: затвердження завдань й перевірку їх узгодженості, а також виконання та співвиконання цих завдань. Ці функції спрямовані на адекватну реакцію і збереження цілісності організації до постійних змін, що відбуваються в оточуючому середовищі.

Попри те, що успішна діяльність будь-якої організації залежить від її фінансових та організаційних можливостей, ОПД має працювати незалежно від внутрішньополітичної кон'юктури в державі, а також стану її окремих елементів.

Висновки.

На разі інформація є критично важливим ресурсом, що суттєво позначається на стані національної безпеки держави. Жорстке протиборство в глобальному інформаційному просторі призвело до виникнення інформаційних війн нового покоління, серед них основними є: інформаційно-психологічні війни, кібернетичні війни й інформаційні війни змішаного типу. Водночас новітні інформаційні технології, сучасні інформаційні й психологічні форми та способи впливу на особистість й суспільство породжують велику кількість різних видів інформаційної зброї.

Успішне інформаційне й інформаційно-психологічне протиборство має базуватися на загальних принципах системного аналізу. При цьому розробка та використання засобів формування й аналізу цілей і функцій організації, що забезпечують

інформаційну й інформаційно-психологічну безпеку має бути заснована на багатоешелонній моделі структури контрпропагандистської.

Такий підхід щодо вибору моделі структури контрпропагандистської організації дає змогу кожному рівню ієрархії формувати свої конкретні цілі і засоби їх досягнення. Крім того, для окремих завдань можуть розглядатися як спеціальні цілі, так і засоби їх досягнення, що допомагає підсистемам усіх рівнів робити вибір власних рішень. Таким чином, надання підсистемам організації протидії дезінформації свободи дій при ухваленні рішень всім ешелонам ієрархічної структури загалом підвищує ефективність її функціонування, а також здійснювати погоджену, цілеспрямовану, керовану з єдиного центру державну політику інформаційного протиборства, спрямовану на захист державних інтересів і забезпечення інформаційної й інформаційно-психологічної безпеки особистості, суспільства і держави в умовах інформаційно-психологічної агресії.

Використана література

1. Джоуэт Г., О'Доннел В. Пропаганда и убеждение ; пер. с англ. О.И. Ткаченко. Харьков: "Гумманитарный центр", 2021. 496 с.

2. Померанцев П. Це не пропаганда. Подорож на війну проти реальності ; пер. з англ. О. Форостина. Київ: Yakaboo, 2020. 285 с.

3. Волкова В., Денисов А. Теория систем. Москва: Высшая школа, 2006, 511 с.

4. Ильичев А.В. Начала системной безопасности. Москва: Научный мир, 2003, 456 с.

5. Мессарович М. Теория иерархических многоуровневых систем. Москва: Мир, 1973, 344 с.

6. Лайнбарджер П.М.Э. Психологическая война. Теория и практика обработки массового сознания ; пер. с англ. Е.В. Ламановой. Москва: ЗАО Центрполиграф, 2013. 445 с.

7. Петрик В.М., Кузьменко А.М., Остроухов В.В. та ін. Соціально-правові основи інформаційної безпеки: навч. посіб. / за ред. В.В. Остроухова. Київ: Росава, 2007. 496 с.

8. Литвиненко О. Інформаційні впливи та операції. Теоретико-аналітичні нариси. Київ: НІСД, 2003. 240 с.

9. Воронова О., Трушин А. Современные информационные войны: стратегии, типы, методы, приемы. Москва: Издательство "Аспект Пресс", 2021. 176 с.

10. Патрикаракос Д. Війна у 140 знаках. Як соціальні медіа змінюють військовий конфлікт XXI століття. Київ: Yakaboo, 2019. 352 с.

11. Почепцов Г. Информационные войны. Новый инструмент политики. Москва: Алгоритм, 2015, 256 с.

12. Уєбстер Ф. Теория информационного общества. Москва: Аспект Пресс, 2004. 398 с.

13. Остроухов В.В., Петрик В.М., Присяжнюк М.М. та ін. Інформаційна безпека (соціально-правові аспекти): підручник / за заг. ред. Є.Д. Скулиша. Київ: КНТ, 2010. 776 с.

14. Грант Дж. Не верю. Как увидеть правду в море дезинформации. 12 уроков здорового скепсиса ; пер. с англ. Е. Бакушева. Москва: Альпина Паблишер, 2017. 296 с.

15. Макдональд Г. Правда. Как политики, корпорации и медиа формируют нашу реальность, выставляя факты в выгодном свете ; пер. с англ. Н. Мезина. Москва: Альпина Паблишер, 2019. 368 с.

16. Сінгер П., Бруклін Е. Війна лайків. Зброя в руках соціальних мереж. Харків: Книжковий клуб "Клуб сімейного дозвілля", 2019. 319 с.

17. Бухарин С.Н., Цыганов В.В. Методы и технологии информационных войн. Москва: Академический Проект, 2007. 382 с.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~