УДК *351.862.4:[004:355.4*
DOI: *10.31673/2786-7412.2025.040705*

Володимир КОЗАКОВ
доктор наук з державного управління, професор,
професор кафедри публічного управління та адміністрування
Державного університету інформаційно-комунікаційних технологій, м. Київ
ORCID ID: 0000-0003-1330-5244
e-mail: v.kozakov@ukr.net

Volodymyr KOZAKOV
Doctor of Science in Public Administration, Professor,
Professor of the Department of Public Administration and Administration
State University of Information and Communication Technologies, Kyiv
ORCID ID: 0000-0003-1330-5244
e-mail: v.kozakov@ukr.net

Юрій СТАДНИК
здобувач другого (магістерського) рівня вищої освіти
Державного університету інформаційно-комунікаційних технологій, м. Київ
ORCID ID:0009-0006-3023-7721
e-mail: mag9039693@stud.duikt.edu.ua

Yurii STADNIC
applicant of the second (master's) level of higher education
State University of Information and Communication Technologies, Kyiv
ORCID ID:0009-0006-3023-7721
e-mail: mag9039693@stud.duikt.edu.ua

ДЕРЖАВНО-УПРАВЛІНСЬКІ СТРАТЕГІЇ В ІНФОРМАЦІЙНІЙ ВІЙНІ З АГРЕСОРОМ

STATE AND ADMINISTRATIVE STRATEGIES IN INFORMATION WAR WITH THE AGGRESSOR

Анотація. *Формування ефективної системи інформаційної безпеки передбачає три взаємопов'язані напрями: розвиток державних стратегій і нормативно-правової бази, активну участь громадянського суспільства та підвищення рівня інформаційної культури населення. Лише за умови гармонійної взаємодії цих компонентів Україна зможе забезпечити власну стійкість у глобальному інформаційному середовищі та стати прикладом демократичної держави, здатної протистояти викликам XXI століття.*

Успішність цієї політики полягає у поєднанні технологічних і гуманітарних підходів. З одного боку, розвиваються інструменти кіберзахисту, створюються алгоритми виявлення фейків, удосконалюється система раннього попередження. З іншого – держава активно інвестує в освіту, формує програми цифрової грамотності, підтримує незалежні фактчекінгові ініціативи. Значне місце

посідає співпраця з Європейським Союзом і НАТО у сфері кібербезпеки, що дозволяє впроваджувати міжнародні стандарти та зміцнювати інтеграційні процеси.

Доведено, що ефективна протидія інформаційній агресії потребує системного та стратегічного підходу. Перш за все, слід удосконалити нормативно-правову базу у сфері інформаційної безпеки, створивши дієві механізми запобігання поширенню дезінформації та ворожих наративів. Другою ключовою умовою є формування довгострокової державної стратегії розвитку інтелектуального потенціалу суспільства–освітнього, культурного й аналітичного рівня громадян, що забезпечить стійкість до маніпулятивних впливів.

Отже, від ефективності державних і суспільних механізмів протидії інформаційній війні залежить здатність українського народу захищати власну незалежність та національну ідентичність у світі.

***Ключові слова**: інформаційна війна, державна політика, державно-управлінські стратегії, цифрові технології Цифрові технології, соціальні мережі*

***Abstract**. The formation of an effective information security system involves three interrelated areas: the development of state strategies and regulatory framework, active participation of civil society and increasing the level of information culture of the population. Only under the condition of harmonious interaction of these components will Ukraine be able to ensure its own stability in the global information environment and become an example of a democratic state capable of confronting the challenges of the 21st century.*

The success of this policy lies in the combination of technological and humanitarian approaches. On the one hand, cyber defense tools are being developed, algorithms for detecting fakes are being created, and the early warning system is being improved. On the other hand, the state is actively investing in education, forming digital literacy programs, and supporting independent fact-checking initiatives. Cooperation with the European Union and NATO in the field of cybersecurity plays a significant role, which allows for the implementation of international standards and strengthening integration processes.

It has been proven that effective counteraction to information aggression requires a systemic and strategic approach. First of all, it is necessary to improve the regulatory framework in the field of information security, creating effective mechanisms to prevent the spread of disinformation and hostile narratives. The second key condition is the formation of a long-term state strategy for the development of the intellectual potential of society – the educational, cultural and analytical level of citizens, which will ensure resistance to manipulative influences. Therefore, the ability of the Ukrainian people to defend their own independence and national identity in the world depends on the effectiveness of state and public mechanisms for countering information warfare.

***Keywords**: information warfare, state policy, state management strategies, digital technologies Digital technologies, social networks.*

Постановка проблеми. Інформація стала стратегічним ресурсом, а боротьба за неї одним із головних напрямів політичного, економічного й ідеологічного протистояння. Саме тому інформаційні війни посідають центральне місце у структурі сучасної міжнародної та внутрішньополітичної динаміки. Біьш того, в умовах цифровізації, глобальної комунікації та розвитку штучного інтелекту

інформаційні технології стали не лише засобом комунікації, а й інструментом впливу, маніпуляції та контролю. Інформаційні війни сьогодні ведуться без оголошення, без фронтів і чітких меж, охоплюючи політичну, економічну, культурну, і в першу чергу психологічну сфери суспільного життя. Актуальність дослідження зумовлена потребою наукового осмислення інформаційних війн як комплексного соціально-політичного явища, виявлення їхніх механізмів, інструментів і наслідків, а також визначення шляхів підвищення інформаційної стійкості держави та суспільства.

Аналіз останніх досліджень і публікацій. Серед найбільш відомих вітчизняних вчених визначимо праці: Г. Почепцова «Сучасні інформаційні війни», в якій системно викладено історію виникнення і розвитку методології інформаційних воєн та військових протистоянь [15]; В. Горбуліна [3], який детально аналізує причини та передумови російської агресії проти України, її стратегічні цілі, а також особливості ведення гібридної війни у різних вимірах: воєнному, політичному, економічному, соціальному, гуманітарному, інформаційному; О. Данильян, О. Дзьобань [4], А. Сіленко [14] аналізують інформаційну війну у медіапросторі сучасного суспільства; основні моделі організації інформаційних війн та їх різновиди досліджують М. Білоусов, В. Алєйник [1] та ін. У сучасному науковому дискурсі поняття «інформаційна війна» має різноманітні трактування, що зумовлено складністю та багатогранністю цього феномену. Інший дослідник, О. Марунченко у своїй дисертації «Інформаційна війна в сучасному політичному просторі» визначає інформаційну війну як специфічну форму організації інформаційної взаємодії, що забезпечує найвищу ефективність при реалізації політичних завдань. На думку автора, її результативність напряму залежить від постійного підтримання інформаційного впливу та комунікаційного тиску [11, с. 28].

Серед іноземних авторів варто зазначити роботи М. Бангеманна, М. Лібікі, Д. Лайона, Г. Лассуелла, М. Маклюена, А. Манойла, А. Мерсьє, Е. Тоффлера, П. Дракера та ін.

Незважаючи на те що, дослідники аналізують ріні аспекти в сфері інформаційного протистояння між України та агресором сьогодні існує потреба у дослідженні, яке б основні визначило стратегії державної політики України щодо протидії інформаційним загрозам.

Мета статті полягає у аналізі стратегії державної політики України щодо протидії в інформаційній війні.

Виклад основного матеріалу. У сучасному світі, на тлі технологічного прориву та глобальних геополітичних змін, інформація перетворилася на стратегічний ресурс. Вона стала інструментом впливу, за допомогою якого держава, соціальні групи чи окремі особи можуть формувати громадську думку, зміцнювати свої позиції або нав’язувати власну інтерпретацію подій на внутрішньому та міжнародному рівнях.

Особливістю інформаційної епохи є надзвичайна швидкість поширення відомостей. Якщо раніше передача новин здійснювалася через друковані ЗМІ, поштові служби чи усне спілкування, що вимагало значного часу, то нині, завдяки цифровим технологіям, інтернету та соціальним мережам, інформація розповсюджується майже миттєво, охоплюючи величезні аудиторії у глобальному масштабі.

Інформаційні потоки охоплюють усі сфери життя – від економіки та політики до освіти, науки та культури. Унаслідок цього вони можуть безпосередньо впливати на внутрішні процеси в державі, формуючи настрої громадян і навіть змінюючи політичну динаміку. У певних випадках інтенсивний інформаційний вплив набуває ознак цілеспрямованої агресії –інформаційної війни. Саме тому потреба у побудові комплексної системи захисту національного інформаційного простору стала стратегічним завданням для України [12, с. 89].

Отже, протидія дезінформації та маніпуляціям у період війни стає не просто елементом інформаційної політики, а стратегічним напрямом забезпечення обороноздатності. Контроль над поширенням фейкових повідомлень, оперативне спростування ворожих наративів і своєчасне інформування суспільства є невід'ємними складовими сучасної боротьби на інформаційному фронті.

Вироблення державної стратегії у протидії у інформаційній війні з РФ набула для України виняткової актуальності, адже російська агресія, носить цілеспрямований характер і покликана підірвати міжнародну репутацію України та ускладнити реалізацію зовнішньополітичних і стратегічних інтересів нашої держави. Ворожі інформаційні кампанії є складовою масштабної гібридної стратегії, спрямованої на руйнування довіри, створення хаосу в суспільній свідомості та деморалізацію українського населення [5, с. 77].

Російська агресія проти України мала наслідком не лише дестабілізацію внутрішньої ситуації, а й глибокі зрушення у сфері європейської та глобальної безпеки. Сам факт російсько-українського конфлікту продемонстрував системні слабкості у механізмах інформаційного захисту на міжнародному рівні. Інструменти, що мали б гарантувати безпеку державного інформаційного простору, протидіяти дезінформаційним кампаніям та зміцнювати кіберстійкість, виявилися фрагментарними й недостатньо ефективними. У багатьох країнах бракує узгоджених стратегій реагування, міжінституційної координації та міжнародної співпраці, що створює численні «вікна вразливості» у глобальній інформаційній системі.

Використовуючи класичні військові дії лише як один із інструментів впливу, Росія паралельно розгортає політичний, економічний, дипломатичний і медійний тиск. Саме тому термін «гібридна війна» найточніше описує суть її деструктивної політики. В межах цієї війни інформаційний простір стає повноцінним полем бою, де кожне повідомлення, пост чи відео може перетворитися на зброю впливу.

Сьогодні інформаційна безпека України є не лише елементом державної політики, а визначальним чинником стійкості держави.

Внутрішні загрози пов'язані з низьким рівнем медіаграмотності серед частини громадян, що сприяє швидкому поширенню дезінформації. До цього додається активність політичних груп, блогерів та медійних осіб, які, нерідко підсилюють ворожі наративи, розпалюють суспільні суперечності та сприяють політичній поляризації. Значний ризик становлять анонімні джерела у цифровому середовищі – передусім у месенджері Telegram, який поєднує функцію новинної платформи з можливістю неконтрольованого поширення фейкової інформації [10, с. 81].

В таких умовах формування ефективних державно-управлінських стратегій є критично важливим завданням для збереження державної стійкості. Вивчення механізмів протидії дезінформації, підвищення рівня медіаосвіти

населення та вдосконалення нормативно-правової бази мають стати основними напрямами розвитку в цій сфері.

Цифрові технології та соціальні мережі суттєво змінили характер комунікації, перетворивши інформаційний простір на відкриту систему, де новини (як правдиві, так і фейкові) поширюються з блискавичною швидкістю. У таких умовах ключовими стають навички перевірки фактів і критичного мислення. Проте навіть перевірка достовірності інформації вимагає часу й професійних ресурсів, що не завжди можливо в умовах стрімкого інформаційного потоку. Навіть коли фейк спростовано, завдана шкода – дипломатична, економічна чи моральна – уже встигає проявитися.

Інформаційні атаки провокують загострення політичних конфліктів, підривають демократичні процеси, знижують довіру до державних інституцій і створюють хаос у громадській свідомості. До найнебезпечніших загроз інформаційній безпеці України належать: дезінформація, маніпулятивна пропаганда, кібератаки, цифрове шпигунство, штучно створені фейки та психологічні операції.

Дезінформація. Сучасні алгоритми штучного інтелекту дають змогу миттєво створювати та поширювати неправдиві повідомлення, що підривають суспільну довіру, дестабілізують політичні процеси та провокують панічні настрої. РФ системно використовує дезінформаційні технології як інструмент психологічного впливу на українське суспільство. Мета таких кампаній – посіяти зневіру, розколоти суспільство й знизити довіру до державних інституцій. Яскравими прикладами стали хвилі фейкових повідомлень 2022 року, коли поширювалися вигадки про «негайну капітуляцію України», «втечу уряду з Києва» та «розпад української армії». У 2023 році інформаційний простір заполонили фейки про «зраду військового командування під час боїв за Бахмут», а вже у 2024 році – вигадані «скандали» про «затримки у постачанні зброї» чи «масштабні корупційні зловживання у сфері військової допомоги». Усі ці кампанії були спрямовані на послаблення довіри громадян і партнерів до української влади та зменшення обсягів міжнародної підтримки.

Пропаганда. Російська пропагандистська машина системно використовує засоби масової інформації, соціальні мережі та цифрові платформи для спотворення іміджу України у світовому просторі. Противник просуває вигадані концепти на кшталт «денацифікації», «визволення від націоналістів» чи «нелегітимності української державності». Такі меседжі спрямовані на створення розколу всередині суспільства, провокування недовіри до влади та формування страху серед населення. Починаючи ще з 2014 року, російські медіа розгорнули масштабну інформаційну кампанію, що поєднує традиційні медійні ресурси та технології штучного інтелекту. Зокрема, у межах проєкту *Doppelgänger* створювалися клоновані сайти міжнародних медіа (*Le Monde*, *Fox News* тощо), які публікували вигадані матеріали з проросійським підтекстом. Використовувалися також AI-генеровані зображення, тексти та коментарі різними мовами для поширення вигідних Кремлю наративів. У 2024 році частину таких операцій було викрито компанією *OpenAI*, що підтвердило масштаби застосування штучного інтелекту в дезінформаційній діяльності.

Фейкові новини. Навмисно створені фальшиві повідомлення поширюються через месенджери, соціальні мережі та онлайн-платформи. Їхня головна мета – маніпулювання масовою свідомістю, дискредитація державних структур і

посилення внутрішньополітичного протистояння. У контексті війни фейкові новини стали повноцінним елементом гібридної агресії, що дозволяє агресору дистанційно керувати громадськими настроями, посилювати паніку, провокувати соціальну нестабільність і послаблювати волю до опору. Такі вкиди часто супроводжуються емоційними заголовками, «ексклюзивними» фото чи відео, що стимулює масове поширення та ускладнює спростування [10, с. 73].

Deepfakes. Технології глибокої підробки стали новим етапом інформаційної зброї. Вони дозволяють створювати правдоподібні відео- та аудіофайли, які візуально майже неможливо відрізнити від реальних. Deepfake-контент активно використовується для маніпуляцій, дискредитації політичних діячів і шантажу, підриваючи довіру до офіційних джерел інформації. Так, у березні 2022 року Центр стратегічних комунікацій України попередив про ймовірність поширення змонтованого відео, на якому президент Володимир Зеленський нібито закликає військових скласти зброю. Уже 16 березня у соціальних мережах з'явився відповідний фейковий ролик, який швидко поширився у Facebook, Telegram та YouTube. Завдяки оперативній реакції української влади та адміністрацій платформ відео було видалено, проте сам факт його появи засвідчив, наскільки глибокі фейки становлять загрозу для національної безпеки та міжнародної репутації України.

Отже, сучасні інформаційні виклики – від дезінформаційних кампаній до технологій глибокої підробки – формують нову реальність війни, у якій інформація стає не просто засобом впливу, а повноцінною зброєю, здатною змінювати хід подій і впливати на глобальну безпеку [12, с. 68].

Окрім всього, ворог активно залучає і сучасні інструменти інформаційно-комугікаційних технологій.

Кібератаки. У сучасних умовах цифрової війни саме кібератаки перетворилися на один із найнебезпечніших інструментів ведення інформаційної війни. Вони спрямовані на порушення роботи державних чи приватних систем, викрадення конфіденційних даних, блокування функціонування критичної інфраструктури або руйнування мережевих ресурсів. Найчастіше використовуються атаки типу DDoS, коли хакери штучно перевантажують сервери, що призводить до повного або часткового паралічу їхньої діяльності. Такі дії можуть вивести з ладу урядові сайти, банківські сервіси, засоби масової інформації чи транспортні системи. У грудні 2024 року масштабна хакерська атака на державні електронні реєстри, зокрема портал «Дія» та сервіси Міністерства юстиції, спричинила їхнє тимчасове відключення. Відповідальність за цю кіберагресію взяла на себе угруповання XakNet Team, що пов'язується зі спецслужбами РФ.

Фішинг. Одним із найпідступніших способів кібератак є фішингові операції, засновані на методах соціальної інженерії. Зловмисники створюють підроблені вебресурси або розсилають електронні листи, які зовні повністю копіюють офіційні повідомлення від банків, державних структур чи поштових сервісів. Мета таких атак – викрадення паролів, фінансових реквізитів і персональних даних громадян. У період війни фішингові кампанії часто маскуються під «інструкції з безпеки», «повідомлення про виплати» або «оновлення державних сервісів», що робить їх особливо небезпечними. Восени 2023 року фахівці CERT-UA зафіксували хвилю атак із використанням PDF-файлів, які містили шкідливі посилання для встановлення шпигунських і руйнівних програм – PicassoLoader, njRAT, RoarBAT (операція UAC-0165 / Sandworm).

Цифрове шпигунство. Цей тип діяльності спрямований на збір стратегічно важливої інформації з урядових, військових та промислових систем. Шпигунське програмне забезпечення дає змогу отримувати доступ до електронних листів, зламувати захищені канали комунікацій, відстежувати переміщення інформаційних потоків або навіть перехоплювати аудіоповідомлення. Здобуті дані використовуються для політичного шантажу, дестабілізації економічних процесів чи підготовки наступальних операцій. У травні 2025 року група APT28 (Fancy Bear), що належить до російського ГРУ, здійснила масштабну хакерську атаку на системи спостереження вздовж українського кордону. У результаті було зламано понад 10 000 камер відеонагляду на залізничних станціях та митних переходах, що дозволило противнику відстежувати логістичні маршрути постачання міжнародної допомоги Україні [6, с. 78].

Злом баз даних. Такі інциденти мають потенційно катастрофічні наслідки, адже витік персональної, фінансової чи службової інформації може призвести до серйозних загроз для державної безпеки. Викрадені дані нерідко потрапляють на «чорний ринок», де їх використовують для шахрайства, підробки документів або вербування інформаторів. Особливо небезпечним є втручання у системи критичної інфраструктури – енергетику, транспорт, фінансовий сектор. Улітку 2023 року хакери угруповання Sandworm (UAC-0165) здійснили атаку із застосуванням шкідливих програм RoarBAT та PicassoLoader, які видаляли або викрадали дані державних установ, знищуючи серверні файли та паралізуючи їхню роботу.

Штучний інтелект у кіберпросторі. Хоча технології ШІ мають величезний потенціал для побудови систем кіберзахисту, їх дедалі частіше використовують зловмисники. Алгоритми машинного навчання допомагають аналізувати вразливості, адаптувати шкідливий код і проводити атаки з високим рівнем персоналізації. Найбільшу небезпеку становить автоматизація шпигунства та цілеспрямованих атак, що істотно підвищує ризики для національної безпеки. У 2023 році дослідники виявили мережі акаунтів, керованих штучним інтелектом, які масово генерували псевдоновинні матеріали англійською та німецькою мовами, поширюючи антиукраїнські наративи. У відповідь Україна та її союзники впроваджують системи на основі ШІ для виявлення ботів, ідентифікації підробленого контенту й миттєвого реагування на інформаційні атаки.

Російські кампанії дедалі частіше інтегрують штучний інтелект у свої стратегії дезінформації, використовуючи його для автоматичного створення коментарів, фейкових акаунтів, статей і відеоматеріалів у соціальних мережах – зокрема X (Twitter), Facebook, Telegram. Таким чином, кіберпростір стає не лише ареною технічних атак, а й простором тотальної інформаційної війни, де технологічна перевага може визначати долю державної безпеки [7, с. 52].

Серед механізмів протидії інформаційній війні РФ проти України особливе місце мають зайняти інституційно-організаційні механізми, серед яких виділяють державні та недержавні інституції, діяльність яких спрямована на формування та реалізацію інформаційної політики та національної безпеки України, а також міжнародні структури, діяльність яких спрямована на нейтралізації інформаційного впливу з боку Росії.

Тому, від того, як Україна інституційно та організаційно зможе об'єднати свої зусилля в інформаційній протидії агресору, залежить, власно кажучи, майбутнє країни, її незалежність.

Безперечно, особливе місце в протидії інформаційній війни в Україні належить Президенту України та відповідним структурним підрозділам, які формують саму політику спротиву інформаційній війні, яку проводить російський агресор проти України.

Рада національної безпеки і оборони України (РНБО) виступає центральним координатором у визначенні стратегічних напрямів політики держави у сфері національної безпеки, включно з інформаційною. Цей орган формує основи національної стратегії інформаційного захисту, прогнозує потенційні ризики, що виникають унаслідок технологічних і геополітичних змін, та ухвалює рішення, спрямовані на зміцнення інформаційного суверенітету держави.

Комітети Верховної Ради України, серед яких, Комітет з питань національної безпеки, оборони та розвідки виконує законодавчу функцію – розробляє, коригує й удосконалює правову базу, яка регламентує діяльність у сфері кібер- та інформаційної безпеки. Взаємодія між урядовими структурами, парламентом і РНБО забезпечує узгодженість державної політики, спрямованої на захист національних інтересів у цифровому просторі та зміцнення обороноздатності інформаційного середовища [10, с. 20].

Міністерство внутрішніх справ України виконує провідну функцію у сфері кібербезпеки, координуючи заходи із запобігання та розслідування кіберзлочинів. До його компетенції входить виявлення кіберзагроз, проведення аналітичних досліджень, нейтралізація хакерських атак та організація превентивних дій для мінімізації їхніх наслідків. Важливою складовою роботи є міжнародне співробітництво з іноземними правоохоронними структурами, кіберцентрами та приватними компаніями, що дозволяє інтегрувати українську систему безпеки у глобальну архітектуру кіберзахисту.

Міністерство цифрової трансформації України займає центральну роль у модернізації інформаційного простору держави, що є необхідним щодо ефективного протистояння у інформаційній війні, яку розв'язала РФ.

Служба безпеки України (СБУ) забезпечила захищеність інформаційного простору України, активізувала протидії спеціальним інформаційним операціям рф проти України в інформаційному полі держави-агресора.

Щодо діяльності цих інститутів державної влади та їх роль у вироблені стратегії інформаційної протидії було написано вже немало.

У сучасних умовах значну роль відіграє наукове осмислення механізмів інформаційного впливу. Дослідник А. Карп розглядає дезінформацію як інструмент руйнування демократичних процесів і державного управління, особливо в контексті російсько-української війни. Автор наголошує на її здатності спотворювати політичну реальність, впливати на громадську думку та підривати довіру до влади [8, с. 23].

Для ефективної протидії дезінформації та інформаційному впливу в Україні потрібно розвивати комплексний підхід, який охоплює кілька важливих сфер. Насамперед важливо вдосконалити інформаційне забезпечення зовнішньополітичного курсу України та створити умови для протидії дезінформації за кордоном. Це передбачає розробку стратегій для посилення міжнародного інформаційного впливу, а також удосконалення методів боротьби з порушенням прав громадян та юридичних осіб на території РФ [9, с. 58].

Система протидії у інформаційній війни проти Україні базується на кількох взаємопов'язаних складових: нормативно-правовій, організаційно-інституційній, технологічній, освітній та міжнародній. Її основою є стратегічні документи державного рівня, що визначають довгострокові цілі й принципи інформаційної безпеки, серед яких Стратегія кібербезпеки, Доктрина інформаційної безпеки та інші урядові програми. Вони узгоджуються між собою та забезпечують єдиний підхід до захисту інформаційного простору.

Ключовими елементами у формування державницької стратегії перемоги у інформаційній війні є низка інструментів на яких зупинимося нижче.

1. Посилення нормативно-правової бази. За останні роки було вдосконалено законодавство у сфері кібербезпеки, захисту персональних даних, охорони критичної інформаційної інфраструктури та інформаційного простору загалом. Ці акти створюють правові умови для ефективної взаємодії державних органів, військових структур, правоохоронних відомств і приватного сектору у протидії кіберзагрозам. Значна увага приділяється гармонізації українського законодавства з європейськими директивами, зокрема у контексті майбутньої інтеграції України до спільної системи безпеки Європейського Союзу. [12, с. 67]. Але парадокс в тому, що ні в одному із законадавчих актів, нормативно-правових документах України ми не знаходимо саме поняття інформаційна війна.

2. Важливою складовою державної стратегії є захист критичної інформаційної інфраструктури. Йдеться про комп'ютерні системи, які забезпечують функціонування енергетики, транспорту, фінансів, охорони здоров'я, оборони та зв'язку. Для забезпечення їхньої безпеки створено механізм державного аудиту та сертифікації інформаційних систем, який передбачає перевірку стійкості до кіберзагроз. Крім того, активніше працювати над запровадженням формується єдиної організаційно-технічної модель кіберзахисту, яка базується на принципах міжнародного стандарту NIST Cybersecurity Framework. Ця модель визначає порядок виявлення, аналізу та реагування на загрози, а також правила обміну інформацією між відомствами.

3. Створення системи оперативного реагування на кіберінциденти. Центральним елементом має стати урядова команда реагування CERT-UA, що здійснює моніторинг кіберподій, проводить аналітичні розслідування та координує дії державних і приватних структур. У практичному вимірі діяльність CERT-UA дозволяє виявляти спроби втручання у державні інформаційні системи, зупиняти атаки та мінімізувати їхні наслідки.

4. Особливе місце у стратегії займає протидія дезінформації та маніпулятивним інформаційним впливам. Український уряд розробив комплекс заходів, спрямованих на підвищення рівня медіаграмотності населення, формування навичок критичного мислення та стійкості до пропаганди. На рівні держави створюються структури, що здійснюють моніторинг інформаційного

простору, виявляють фейки, інформаційні маніпуляції та координують дії з нейтралізації таких впливів. У Збройних Силах та інших силових відомствах діють підрозділи стратегічних комунікацій, які протидіють інформаційним операціям противника, формуючи достовірні наративи для громадськості. Підвищення медіаграмотності серед населення, дасть змогу громадянам краще орієнтуватися у величезному потоці інформації, критично ставитися до медіа та визначати маніпуляції. Важливою складовою цього є розробка методик, що сприятимуть формуванню критичного мислення серед громадян, здатності розпізнавати фейки та інші загрози. Загалом для успішної боротьби з дезінформацією важливо об'єднати зусилля держави, медіа, громадських організацій та міжнародних партнерів, активно впроваджуючи нові технології та методи для запобігання маніпуляціям і захисту національних інтересів.

5. Іншим важливим кроком є активна боротьба з фейковою інформацією через фактчекінг, медіамоніторинг і правове регулювання інформаційного простору. Потрібно посилити контроль за поширенням маніпулятивного контенту, запровадивши кримінальну відповідальність за створення та поширення дезінформації, особливо в умовах війни. Також слід впровадити механізми контролю за фейковими акаунтами й анонімними джерелами, які поширюють неправдиву інформацію в інтернеті.

6. Інформаційна стратегія держави також має передбачати активне використання кіберзахисту. Потрібно створити належну технічну базу для боротьби з кібератаками та дезінформацією в кіберпросторі. Для цього важливо забезпечити взаємодію між різними державними та приватними структурами, зокрема в рамках Ситуаційного центру кібербезпеки при СБУ. Виявлення фейкових новин і діпфейків потребує мобілізації спеціальних підрозділів у сфері кіберполіції та співпраці з громадськими ініціативами, як-от «КіберАрмія», для протидії інформаційним атакам з боку ворога [9, с. 56].

7. Велике значення має розвиток кадрового потенціалу. Державна політика передбачає підготовку спеціалістів з кібербезпеки, комунікаційної аналітики, інформаційної розвідки та стратегічних комунікацій. Університети, військові академії та освітні центри мають активно розробляти програми навчання, що базуються на міжнародних стандартах. Паралельно для працівників органів державної влади впроваджуються курси кібергігієни, у межах яких навчають безпечному користуванню цифровими технологіями, захисту персональних даних і реагуванню на кіберінциденти [10, с. 65].

8.Важливо також розвивати систему громадського нагляду за дотриманням етичних стандартів у сфері інформації. Це дозволить зменшити рівень політичного тиску на журналістику, водночас підвищивши професійну відповідальність. У поєднанні з медіаосвітою та підвищенням кваліфікації журналістів така система стане запорукою формування зрілого, стабільного медійного простору, який буде здатний самостійно протидіяти дезінформації.

9. Важливим елементом політики є створення комплексних систем моніторингу. Вони дозволяють у режимі реального часу відстежувати інформаційні атаки, аналізувати соціальні мережі, оцінювати рівень інформаційної безпеки та визначати потенційні вразливості.

Перспективним напрямом ефективної державної політики є створення Національного центру інформаційної стійкості – міжгалузевої платформи, що поєднає державні й недержавні структури для спільної роботи над аналізом інформаційних ризиків, розробкою сценаріїв реагування та проведенням навчань. Такий центр міг би забезпечити постійний моніторинг медіапростору, здійснювати оцінку ризиків і координувати дії у випадку масштабних інформаційних атак.

Висновки. Стратегія державної політики України щодо протидії РФ у інформаційній війні ґрунтується на принципах системності, міжвідомчої взаємодії, відкритості та адаптивності до нових викликів. Вона поєднує технічні, правові, освітні та соціальні інструменти, спрямовані на захист національного інформаційного простору. Впровадження цієї стратегії формує підґрунтя для стійкості держави перед сучасними інформаційними загрозами, забезпечує її інтеграцію у світову систему цифрової безпеки та сприяє зміцненню демократичних засад суспільства.

Україні потрібно впроваджувати активно свій власний проукраїнський дискурс, переходити від інформаційної оборони до контрнаступу. Ключем успішної стратегії контрпропаганди – є розбудова ефективних партнерств та колаборацій. Україна повинна формувати власний набір стратегій, принципів, стандартів і норм для комунікації та боротьби за інформаційний простір. Все це призведе до створення єдиної реальності, де замість спростування окремих елементів пропаганди вибудується цілісна альтернативна картина світу, в якій ворожі наративи програють та втрачають сенс.

ДЖЕРЕЛА ТА ЛІТЕРАТУРА

1. Білоусов М. В., Алєйник В. Г. Російська гібридна війна: загрози і кібервиклики для європейської інформаційної безпеки. *Регіональні студії*. 2023. № 33. С. 119–125.
2. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення. *Вісник Національної академії державного управління при Президентові України*. 2015. № 1. С. 136–141.
3. Горбулін В. П. (ред.) *Світова гібридна війна: український фронт* : монографія. Київ : НІСД, 2017. 496 с.
4. Данильян О. Г., Дзьобань О. П. Інформаційна війна у медіапросторі сучасного суспільства. *Вісник НЮУ імені Ярослава Мудрого. Серія «Філософія, філософія права, політологія, соціологія»*. 2022. № 3 (54). С. 11–29.
5. Клочко А. Загрози інформаційній безпеці України в умовах викликів сучасності. У: *Забезпечення інформаційної безпеки держави у воєнній сфері: проблеми та шляхи їх вирішення* : матеріали І міжвідомчої наук.-практ. конф. Київ, 2021. С. 180.
6. Кобільник Б. Ю., Гізун А. І. Роль інформаційно-психологічних впливів в інформаційній війні. У: *Актуальні задачі і досягнення в галузі кібербезпеки* : матеріали Всеукр. наук.-практ. конф. (Кропивницький, 23–26 листопада 2016 р.). URL: https://core.ac.uk/download/pdf/84825493.pdf.

7. Коруц У. Інформаційна війна як інструмент пропаганди війни: правові підстави протидії. *Підприємництво, господарство і право.* 2020. № 8. DOI: https://doi.org/10.32849/2663-5313/2020.8.55.
8. Крап А. Дезінформація як загроза демократії та державному управлінню. *Український політико-правовий дискурс*. 2025. № 9. URL: https://zenodo.org/records/15108404.
9. Курбан О. В. *Сучасні інформаційні війни в мережевому он-лайн просторі* : навч. посіб. Київ : ВІКНУ, 2016. 286 с.
10. Лісовський О. Кібербезпека та інформаційна війна: виклики та загрози. Львів : Магнолія, 2021. С. 16–23.
11. Марунченко О. П. *Інформаційна війна в сучасному політичному просторі* : дис. … канд. політ. наук : 23.00.02. Одеса : Південноукраїнський нац. пед. ун-т ім. К. Д. Ушинського, 2012. 208 с.
12. Рибак М. І., Атрохов А. В. До питання про інформаційні війни. *Наука і оборона*. 2018. № 2. С. 65–68.
13. Саприкін О. Інформаційна експансія, інформаційна війна та інформаційна атака у засобах масової інформації на прикладі Євро-2012. *Вісник Книжкової палати*. 2013. № 1. С. 40–43.
14. Сіленко А. О. Роль засобів масової інформації в інформаційній війні. У: *Сучасні політичні процеси: глобальний та національний виміри* : матеріали III Міжнар. наук.-практ. інтернет-конф. (Одеса, 30 листопада 2023 р.). Одеса, 2023.
15. Почепцов Г. Г. *Сучасні інформаційні війни*. Київ : Вид. дім «Києво-Могилянська академія», 2015. 495 с.

REFERENCES

1. Bilousov, M. V., & Aleinyk, V. H. (2023). Rosiiska hibrydna viina: zahrozy i kibervyklyky dlia yevropeiskoi informatsiinoi bezpeky [Russian hybrid war: threats and cyber challenges to European information security]. *Rehionalni studii – Regional Studies*, 33, 119–125 [in Ukrainian].
2. Horban, Yu. O. (2015). Informatsiina viina proty Ukrainy ta zasoby yii vedennia [Information war against Ukraine and the means of its implementation]. *Visnyk NADU pry Prezydentovi Ukrainy – Bulletin of the National Academy of Public Administration*, 1, 136–141 [in Ukrainian].
3. Horbulin, V. P. (Ed.). (2017). *Svitova hibrydna viina: ukrainskyi front* [World Hybrid War: Ukrainian Front]. Kyiv: NISD [in Ukrainian].
4. Danylian, O. H., & Dzoban, O. P. (2022). Informatsiina viina u mediaprostori suchasnoho suspilstva [Information war in the media space of modern society]. *Visnyk NYUU imeni Yaroslava Mudroho. Seriia «Filosofiia, filosofiia prava, politolohiia, sotsiolohiia» – Bulletin of Yaroslav Mudryi National Law University. Series «Philosophy, Philosophy of Law, Political Science, Sociology»*, 3(54), 11–29 [in Ukrainian].

5. Klochko, A. (2021). Zahrozy informatsiinii bezpetsi Ukrainy v umovakh vyklykiv suchasnosti [Threats to Ukraine's information security under modern challenges]. In *Zabezpechennia informatsiinoi bezpeky derzhavy u voiennii sferi: problemy ta shliakhy yikh vyrishennia – Ensuring Information Security of the State in the Military Sphere: Problems and Solutions*, Proceedings of the 1st Interagency Scientific and Practical Conference (p. 180). Kyiv [in Ukrainian].
6. Kobilnyk, B. Yu., & Hizun, A. I. (2016). Rol informatsiino-psykholohichnykh vplyviv v informatsiinii viini [The role of information-psychological influences in information warfare]. *Aktualni zadachi i dosiahnennia v haluzi kiberbezpeky – Current Issues and Achievements in Cybersecurity*, Proceedings of the All-Ukrainian Scientific and Practical Conference (Kropyvnytskyi, November 23–26, 2016). Retrieved from https://core.ac.uk/download/pdf/84825493.pdf [in Ukrainian].
7. Koruts, U. (2020). Informatsiina viina yak instrument propahandy viiny: pravovi pidstavy protydii [Information war as an instrument of war propaganda: legal grounds for counteraction]. *Pidpryiemnytstvo, hospodarstvo i pravo – Entrepreneurship, Economy and Law*, 8. https://doi.org/10.32849/2663-5313/2020.8.55 [in Ukrainian].
8. Krap, A. (2025). Dezinformatsiia yak zahroza demokratii ta derzhavnomu upravlinniu [Disinformation as a threat to democracy and public administration]. *Ukrainskyi polityko-pravovyi dyskurs – Ukrainian Political and Legal Discourse*, 9. Retrieved from https://zenodo.org/records/15108404 [in Ukrainian].
9. Kurban, O. V. (2016). *Suchasni informatsiini viiny v merezhevomu on-lain prostori* [Modern information wars in the online networked space]. Kyiv: VIKNU. [in Ukrainian].
10. Lisovskyi, O. (2021). Kiberbezpeka ta informatsiina viina: vyklyky ta zahrozy [Cybersecurity and information warfare: challenges and threats]. Lviv: Mahnoliia, 16–23 [in Ukrainian].
11. Marunchenko, O. P. (2012). *Informatsiina viina v suchasnomu politychnomu prostori* [Information war in the modern political space]. Candidate's thesis. Odesa: Pivdennoukrainskyi nats. ped. universytet im. K. D. Ushynskoho [in Ukrainian].
12. Rybak, M. I., & Atrokhov, A. V. (2018). Do pytannia pro informatsiini viiny [On the issue of information wars]. *Nauka i oborona – Science and Defense*, 2, 65–68 [in Ukrainian].
13. Saprykin, O. (2013). Informatsiina ekspansiia, informatsiina viina ta informatsiina ataka u zasobakh masovoi informatsii na prykladi Yevro-2012 [Information expansion, information war and information attack in mass media on the example of Euro-2012]. *Visnyk Knyzhkovoi palaty – Bulletin of the Book Chamber*, 1, 40–43. [in Ukrainian].
14. Silenko, A. O. (2023). Rol zasobiv masovoi informatsii v informatsiinii viini [The role of mass media in information war]. In *Suchasni politychni protsesy: hlobalnyi ta natsionalnyi vymiry – Modern Political Processes: Global and National Dimensions*, Proceedings of the 3rd International Scientific and Practical Internet Conference (Odesa, November 30, 2023) [in Ukrainian].
15. Pocheptsov, H. H. (2015). *Suchasni informatsiini viiny* [Modern Information Wars]. Kyiv: Vydavnychyi dim «Kyievo-Mohylianska akademiia» [in Ukrainian].