УДК 327:351.862.4(477):[004:355.4
DOI: 10.31673/2786-7412.2025.031608

Дмитро ШУЛЬГА
аспірант кафедри публічного управління та адміністрування
Державного університету інформаційно-комунікаційних технологій, м. Київ
ORCID ID: 0009-0008-8321-013X
e-mail: d.shulha@stud.duikt.edu.ua

Dmytro SHULHA
graduate student of the Department of Public Administration,
State University of Information and Communication Technologies, Kyiv
ORCID ID: 0009-0008-8321-013X
e-mail: d.shulha@stud.duikt.edu.ua

АНАЛІЗ ЗАРУБІЖНОГО ДОСВІДУ РЕАЛІЗАЦІЇ ДЕРЖАВНИХ СТРАТЕГІЙ УКРАЇНИ В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ

ANALYSIS OF FOREIGN EXPERIENCE IN THE IMPLEMENTATION OF STATE STRATEGIES OF UKRAINE IN THE CONDITIONS OF INFORMATION WAR

Анотація. *Стаття присвячена вивченню зарубіжного досвіду у сфері забезпечення інформаційної безпеки, оскільки останнім часом інформаційна сфера перетворилась на арену протиборства. Адже, держава-агресор використовує нові інформаційні технології впливу на свідомість громадян, розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом, посягання на суверенітет і територіальну цілісність України. З метою протидії таким проявам варто вивчати відповідний позитивний досвід інших країн у цій сфері.*

Повномасштабне вторгнення РФ в Україну зумовило серйозне переосмислення концептуальних підходів щодо перспектив забезпечення безпеки та оборони Європейського континенту, розробки нових пріоритетів та підходів до реалізації зовнішньої політики, що знайшло відображення в дослідженнях провідних аналітичних центрів.

Розглянуто основні підходи щодо забезпечення інформаційній протидії у національній безпеці Європейського Союзу, Великої Британії, Франції, Німеччини тощо.

Особливий акцент зроблено на забезпеченню інформаційної безпеки у США, першою країною, яка почала розбудову інформаційного суспільства, перетворивши інформаційну галузь на стратегічний ресурс. У США питання інформаційної безпеки тісно пов'язані між собою, інформаційна політка в цій державі є

пріоритетною для забезпечення національної безпеки. Директива Міністерства оборони США «Інформаційна війна» окреслила політику щодо захисту інформаційних ресурсів і надала відповідної значимості самому поняттю «інформаційна війна». Директива охоплювала різні аспекти інформаційної безпеки, зокрема, психологічний вплив на супротивника, оперативну безпеку, електронне втручання, інформаційну розвідку, інформаційний захист та інші. Задля гарантування інформаційної безпеки у США велике значення приділяється управлінню інформаційними ресурсами. Основна мета цього – убезпечення власної системи інформаційної безпеки та вплив на інформаційно-безпекову систему потенційного супротивника. Американська модель забезпечення інформаційної безпеки цілком допускає ведення інформаційних війн, що включає у себе планування і проведення активних інформаційно-психологічних операцій як інструменту зовнішньої політики.

Ключові слова: *державне управління, інформаційна політика, інформаційна війна, інформаційна безпека, державна стратегія.*

Abstract. *The article is devoted to the study of foreign experience in the field of ensuring information security, since recently the information sphere has turned into an arena of confrontation. After all, the aggressor state uses new information technologies to influence the consciousness of citizens, incite national and religious hatred, propagate aggressive war, change the constitutional order by force, encroach on the sovereignty and territorial integrity of Ukraine. In order to counteract such manifestations, it is worth studying the relevant positive experience of other countries in this area.*

The full-scale invasion of the Russian Federation into Ukraine led to a serious rethinking of conceptual approaches to the prospects for ensuring the security and defense of the European continent, the development of new priorities and approaches to the implementation of foreign policy, which was reflected in the research of leading analytical centers.

The main approaches to ensuring information countermeasures in the national security of the European Union, Great Britain, France, Germany, etc. are considered. Particular emphasis is placed on ensuring information security in the USA, the first country to begin building an information society, turning the information industry into a strategic resource. In the USA, information security issues are closely interconnected, information policy in this country is a priority for ensuring national security. The US Department of Defense Directive «Information Warfare» outlined a policy for protecting information resources and gave appropriate importance to the concept of «information warfare». The directive covered various aspects of information security, in particular, psychological impact on the enemy, operational security, electronic interference, information intelligence, information protection and others. In order to guarantee information security in the USA, great importance is attached to the management of information resources. The main goal of this is to secure its own information security system and influence the information security system of a potential enemy. The American model of ensuring information security fully allows for the conduct of information

warfare, which includes planning and conducting active information and psychological operations as a foreign policy tool.

Key words: *public administration, information policy, information warfare, information security, state strategy.*

Постановка проблеми. Широкомасштабна війна РФ проти України відзначається не тільки воєнними діями, а й здійсненням спеціальних інформаційних операцій, спрямованих на підрив обороноздатності країни, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів. Більш того, інформаційна експансія держави-агресора та контрольованих нею структур, націлена не тільки на Україну, але й зокрема, шляхом розширення власної інформаційної інфраструктури і в інших державах.

Чи готові зарубіжні країни протистояти цим проявам агресії в інформаційній сфері? Які основні тренди інформаційних війн XXI століття? Який досвід зарубіжних країн у цій сфері може слугувати цінним джерелом знань для розробки нових механізмів забезпечення інформаційної безпеки України. На ці та інші питання зарубіжного досвіду реалізації державних стратегій в умовах інформаційних війн буде присвячена ця стаття.

Аналіз останніх досліджень і публікацій. Проблема інформаційних війн привертала увагу багатьох закордонних науковців, експертної спільноти, зокрема, Мартін Лібікі [1], (якого уважають однин із провідних теоретиків у галузі інформаційних війн), Дороти Деннінг [2]. У книзі «Decisive Force: The new American Way of War» Ф. Хоффман уважає за необхідним включення проблем інформаційної війни у воєнний план країн як невід'ємної частини ведення сьогоднішньої війни [3].

Серед вітчизняних дослідників можна виділити ґрунтовні праці Горбуліна В. П. [4], Курбан О.В. [5], Марунченко О. П. [6], Семен Н. Ф. [7] та ін.

Мета статті полягає у аналізі зарубіжного досвіду реалізації державних стратегій в протистоянні інформаційним війнам XX1 ст.

Виклад основного матеріалу. У XX ст. під поняттям «інформаційна війна» розуміли систему «спеціальних інформаційних операцій», що мали деморалізувати противника та схилити його до капітуляції під час конвенційних бойових дій. З приходом епохи постіндустріалізму поняття «інформаційна війна» розширилося за межі свого традиційного предмету. Інформаційна війна є одним з найбільших викликів сучасного світу. Її наслідки можуть бути руйнівними для будь-якого суспільства, економіки та політичної стабільності.

Мартін Лібікі – у своїй книзі «Що таке інформаційна війна?», визначає 7 форм інформаційної війни [1]:

1) командно-управлінська (націлена на знищення каналів зв'язку між командуванням і виконавцями);

2) розвідувальна (збір важливої та захист власної інформації);

3) психологічна (пропаганда, інформаційна обробка населення, деморалізація);

4) хакерська (диверсійні дії та атаки проти ворога шляхом створення спеціальних програм);

5) економічна (інформаційна блокада й інформаційний імперіалізм);

6) електронна (спрямована проти засобів електронних комунікацій – радіозв'язку, радарів, комп'ютерних мереж);

7) кібервійна.

Потрібно визначити, інформаційні війни – це особливий виклик для сучасної загальнолюдської системи цінностей, адже всі війни прикриваючись великою метою – патріотизмом, справедливістю, захистом прав та свобод людини, боротьбою з тероризмом тощо, а у підсумку все це закінчується військовою агресією, збройним конфліктом, суттєвим людським жертвам.

Європейська комісія сформулювала внутрішню та зовнішню мету інформаційної політики щодо захисту внутрішнього комунікаційного простору Європейського Союзу від зовнішнього впливу. Базові цінності інформаційної політики ЄС та її принципи можна поділити на три групи прийнявши за основний критерій інтереси та цінності трьох ключових сторін: суспільства загалом, національних держав і Європейського Союзу. Ці принципи визначаються:

- соціально-політичними цінностями, прийнятими в об'єднаній Європі (закріплені загальноєвропейськими законами, прийнятими ЄС);
- інтересами Європейського Союзу (сформульовані законами та директивами ЄС, заснованими на нормах міжнародного права);
- національними інтересами країн-членів ЄС (сформульовані законодавчою базою країн-членів, що відповідають нормам міжнародного права та законодавству Європейського Союзу).

Безпека інформаційних та комунікаційних систем є сьогодні невід'ємною частиною національних оборонних стратегій. Адже, протидія інформаційній агресії стає п'ятою сферою ведення війни після суші, моря, повітря та космосу. У США забезпечення інформаційної безпеки держави визнано одним із головних національних пріоритетів, Пентагон створив Кіберком, нове військове командування для захисту американських військових інформаційних мереж та розвитку своїх наступальних можливостей.

Повномасштабне вторгнення РФ в Україну зумовило серйозне переосмислення концептуальних підходів щодо перспектив забезпечення безпеки та оборони Європейського континенту, розробки нових пріоритетів та підходів до реалізації зовнішньої політики, що знайшло відображення в дослідженнях провідних аналітичних центрів.

Досвід зарубіжних країн щодо формування національних стратегій ефективної протидії в умовах інформаційних війн, кібербезпеки, подоланні ворожої пропаганди має величезне значення для удосконалення власних підходів до забезпечення інформаційної безпеки інформаційного простору України.

Аналітикі Чатем-Хаус (англ. Chatham House) – Королівського інституту міжнародних відносин (англ. The Royal Institute of International Affairs) з Великої

Британії визнали, що найбільший воєнний конфлікт у Європі з часів Другої світової війни радикально вплинув на експертні оцінки та аналітичні дослідження у сфері політики безпеки і зовнішньої політики. Якщо раніше європейська спільнота зосереджувалася на запобіганні конфліктів, збереженні миру та сприянні міжнародній безпековій співпраці, то нині фокус уваги змістився на нові питання: особливості організації територіальної оборони, безальтернативність НАТО і трансатлантичної системи для європейської оборони, примарність перспектив «стратегічної автономії» ЄС, необхідність визначення та оцінювання глобальних наслідків російської агресії [8].

Повномасштабне збройне вторгнення РФ в Україну в 2022 р. спричинило глобальний шок, тому що «ознаменувало собою різке закінчення тридцятирічного періоду глобалізації та системи міжнародного співробітництва» та призвело до виникнення найгострішої безпекової кризи у Європі з часів Другої світової війни. Наслідки російсько-української війни, які безпосередньо впливають на глобальні тенденції, спонукатимуть до створення засад нового європейського порядку. Інформаційна війна стали в 21-у столітті безпековим викликом для багатьох країн.

Для протидії дезінформаційній кампанії РФ, у 2015 році в ЄС була створена оперативна робоча група зі стратегічних комунікацій Європейського Союзу – East StratCom Task Force, підрозділ Європейської служби зовнішньополітичної діяльності (ЄСЗД) на підставі ухваленого на зустрічі Європейського Союзу 19-20 березня 2015 року рішення про необхідність «протистояти постійним дезінформаційним кампаніям з боку Росії» Служба покликана надавати підтримку делегаціям Європейського союзу в країнах Східної Європи (зокрема, в Азербайджані, Білорусі, Вірменії, Грузії, Молдові, Росії та Україні).

Головним продуктом роботи співробітників East StratCom Task Force є сайт EUvsDisinfo.eu, де оприлюднюється інформація про всі виявлені приклади дезінформаційних атак Росії. До основних функцій цієї групи увійшло: роз'яснення ключових аспектів політики Європейського Союзу, створення його позитивного іміджу та протидія дезінформації; ефективна комунікація та просування політики ЄС щодо Східного партнерства; загальний розвиток медійного простору в країнах Східного партнерства та країнах-членах ЄС, що передбачає сприяння незалежності ЗМІ; вдосконалення механізмів, що уможливлюють передбачення, оцінку та реагування ЄС на дезінформацію, яка поширюється зовнішніми акторами [9].

У 2001 р. Європейською комісією представлено перший документ під назвою «Мережева та інформаційна безпека: європейський політичний підхід», у якому окреслено європейський підхід до проблеми інформаційної безпеки, яка трактується як здатність мережі або інформаційної системи чинити опір випадковим подіям або зловмисним діям, що становлять загрозу доступності, автентичності, цілісності й конфіденційності даних, що зберігаються або передаються, а також послуг, що надаються через ці мережі та системи [10].

А, вже, у 2004 створено Європейське агентство з питань мережевої та інформаційної безпеки (ENISA), основна мета його діяльності забезпечувати виконання вимог інформаційної безпеки, контролювати дотримання чинного та

майбутнього законодавства ЄС. ENISA надає консультації як для держав-членів, так і для інституцій ЄС із питань, пов'язаних з інформаційною безпекою [5].

Україна з 2022 року розвиває співпрацю з Агентством ЄС з мережевої та інформаційної безпеки, а отримання нашою державою особливого статусу партнера стане надзвичайно важливим кроком на шляху євроінтеграції та необхідності гармонізації вітчизняного законодавства у сфері кібербезпеки з європейським. Національний координаційний центр кібербезпеки (НКЦК) при РНБО України та Адміністрація Державної служби спеціального зв'язку та захисту інформації України (ДССЗЗІ) уклали у 2023 р. Угоду про співробітництво з Агентством Європейського Союзу з мережевої та інформаційної безпеки (ENISA), спрямовану на розвиток можливостей, обмін кращими практиками і підвищення рівня поінформованості щодо ситуації в цій сфері [11].

У квітні 2016 року Єврокомісія ухвалила «Спільні принципи протидії гібридним загрозам – відповідь Європейського Союзу» (Joint Framework on countering hybrid threats a European Union response): у Спільних принципах наголошується на необхідності вироблення державами-членами узгоджених механізмів реалізації стратегічних комунікацій для протидії дезінформації та публічного викриття гібридних загроз. У документі зазначається, що важливо захищати об'єкти критичної інфраструктури (наприклад транспорт і телекомунікації), оскільки гібридні атаки можуть призвести до серйозних економічних або соціальних порушень. Документ визначає, що діяльність у сфері стратегічних комунікацій передбачає тісну взаємодію з НАТО. Зазначається, що співпраця ЄС та НАТО дозволить обом організаціям більш ефективно реагувати на гібридні інформаційні загрози. Також у документі стверджується, що провокатори можуть систематично поширювати дезінформацію, у тому числі в межах цілеспрямованих кампаній у соціальних мережах, прагнучи радикалізації окремих індивідів та дестабілізації суспільства. Стратегічні комунікації мають сповна використовувати соціальні медіа, а також традиційні візуальні, аудіо та інтернет ЗМІ [12].

У листопаді 2016 року Європейський парламент ухвалив Резолюцію «Стратегічні комунікації Європейського Союзу як протидія пропаганді третіх сторін» [13].

Використання Росією інструментів інформаційного впливу як елементу агресії на міжнародній арені актуалізувало питання пошуку ефективних механізмів протидії розповсюдженню антиліберальних наративів російської пропаганди у країнах ЄС. Ключовими можна вважати наступні пункти цієї резолюції:

- стратегічні комунікації та інформаційна війна визнаються не тільки зовнішнім аспектом ЄС, але й внутрішнім;
- дезінформація та пропаганда визначаються складовими частинами гібридної війни;
- позитивні меседжі ЄС мають бути наступальними (offensive), а не захисними (defensive)»;
- Європарламент закликає інституції ЄС проводити моніторинг джерел фінансування антиєвропейської пропаганди;

- Європарламент закликає інституції ЄС збільшити видатки на підтримку свободи ЗМІ у країнах-сусідах ЄС;
- Європарламент підкреслює, що «розпалювання ненависті, насильства або війни не може «ховатися» за ширмою свободи висловлення думок»;
- Європарламент наголошує на існуванні різниці між пропагандою та критикою. (Однак не розкриває ці поняття і не встановлює межі між ними) Стратегічні комунікації Європейського Союзу як протидія пропаганді «третіх сторін».

У жовтні 2019 року Європейський парламент ухвалив резолюцію про дезінформацію і зовнішнє втручання у вибори до Європарламенту. Зокрема, у резолюції наголошується на фактах втручання іноземних держав у внутрішні справи ЄС шляхом фінансування європейських політичних партій. На думку євродепутатів, ключова роль у цьому належала саме РФ, оскільки було зафіксовано майже тисячу (998) випадків розповсюдження дезінформації з боку Росії. Крім того, у резолюції наголошується на необхідності посилення законодавчих рамок для попередження гібридних загроз.

Для посилення протидії дезінформації Європейська Комісія спрямовуватиме зусилля для перегляду Кодексу практики дезінформації (Code of Practice on Disinformation) у систему регулювання зобов'язань та підзвітності Інтернет-платформ відповідно до майбутнього Закону про цифрові послуги (Digital Services Act). У цілому, Європейська Комісія має на меті запровадити інструменти, які б дозволили збільшити відповідальність медіа та бенефіціарів інформаційних кампаній за розповсюдження дезінформації.

Аналізуючи перелік запроваджених у ЄС механізмів протидії дезінформації, зокрема, і антиліберальних інформаційний кампаній, можна дійти висновку, що політика ЄС у цій сфері полягає у підтримці якісної журналістики, посиленні законодавчих норм щодо збільшення прозорості фінансування ЗМІ та політичних партій тощо. Натомість, навіть попри численні факти втручання РФ у внутрішньополітичні справи як ЄС в цілому, так і її окремих країн, у Європейському Союзі не розглядаються можливості примусового обмеження чи повної заборони діяльності окремих медіа, які системно розповсюджують дезінформацію. Такий підхід ЄС зумовлений критичною важливістю для інституції забезпечити дотримання базових цінностей демократії, таких як свобода слова.

Можна наголосити на відносній інертності офіційної реакції ЄС на реальні загрози розповсюдження дезінформації та запровадженні ефективних механізмів протидії. Про недостатню ефективність відповідних дій з боку ЄС свідчить той факт, що іноземні держави, включно з Росією, продовжують здійснювати системні кампанії з дезінформації, що відзначали і у Європейській Комісії [14].

Протягом десятиліть російські олігархи вкладали гроші у *Великій Британії* – лише у нерухомість із 2016 по 2022 рік росіяни, пов'язані з Кремлем або підозрюванні у використанні корупційних схем для збагачення, вклали 1,5 мільярда фунтів. Фінансовий вплив, як зазначають дослідники, перетворився на інформаційний і політичний.

Понад те, попри охолодження дипломатичних відносин протягом останніх десятиліть, російський вплив у Великій Британії зростав. Пропагандистські ресурси RT і Sputnik продовжували поширювати кремлівську дезінформацію у Сполученому Королівстві до повномасштабного вторгнення Росії в Україну 24 лютого 2022 року, після якого врешті-решт у країні заборонили мовлення російських каналів.

Британська дослідниця російської дезінформації Люсі Бірдж, яка захистила в Манчестерському університеті дисертацію про Sputnik відзначила в своєму досліджені, що Sputnik застосував звичайні прийоми у своєму наборі інструментів для захисту і нападу. По-перше, у прелюдії до війни Sputnik намагався скористатися невизначеністю щодо чи вторгнеться Росія в Україну шляхом обуреного заперечення. По-друге, на етапі новин Sputnik подвоїв офіційну позицію Росії, захистивши вторгнення і жорстоко атакувати західних гравців. По-третє, на етапі війни, статус великої держави Росії був підірваний її поганою військовою ефективністю [15].

Події останніх десятиріч (отруєння Олександра Литвиненка, намагання російської пропаганди втрутитися в референдум в Шотландії, спроби вбивства сім'ї Скрипалів та багато інших епізодів) призвели до того, що у 2020 році при МЗС Великої Британії було створено підрозділ із протидії дезінформації. Причиною такого рішення було поширення медичних фейків на тлі пандемії коронавірусної хвороби, але згодом робота була зосереджена на створенні стратегічних комунікацій проти російського інформаційного впливу у Британії.

Результатом цього став звіт комітету розвідки та безпеки парламенту Великої Британії під назвою «Росія», який було оприлюднено 21 липня 2020 року[16].

Повномасштабне вторгнення Росії в Україну призвело до більшої уваги до України з боку британців і усвідомлення того, що варто змінювати сприйняття Росії. Основна сюжетна лінія апарату російської пропаганди незмінна – це звинувачення Заходу в провокаціях проти Росії, яка начебто захищається, а країни Східної Європи населені «фашистами чи неонацистами».

Одним із наслідків 24 лютого (нападу на Україну) була заборона мовлення RT на території Сполученого Королівства. Медіарегулятор Ofcom 18 березня 2022 року оголосив про це на тлі 29 розслідувань щодо порушень висвітлення російського вторгнення в Україну.

У парламенті Великої Британії 23 травня 2022 р. був представлений проєкт рамкового закону «Про національну безпеку», підготовлений Міністерством внутрішніх справ країни на заміну попереднього законопроєкту «Про протидію загрозам державі». Метою документа є оновлення чинного законодавства у сфері національної безпеки, його адаптація до сучасних викликів та інформаційних загроз, особливо у контексті агресивної зовнішньої політики РФ та широкомасштабної російської агресії проти України.

Передбачена криміналізація таких правопорушень, як-от саботаж (включно з кібератаками на урядові та неурядові вебресурси, об'єкти критичної інфраструктури), а також неправомірне іноземне втручання у систему.

Крім цього, криміналізації підлягатимуть дії осіб ще на стадії підготовки до вчинення злочину проти держави, що дасть можливість запобігти заподіянню серйозної шкоди національній безпеці.

Для полегшення протидії прихованим загрозам державі у законопроєкті розширено повноваження слідчих органів щодо проведення обшуку та виїмки [17].

У жовтні 2023 року парламент Великої Британії прийняв закон про онлайн-безпеку. Закон зобов'язав онлайн-платформи стежити за наявністю шкідливого контенту, а медіарегулятор Ofcom має вживати кроків із його нейтралізації. Було також встановлено кримінальну відповідальність за поширення шкідливого контенту в інтернеті.

США. Сполучені Штати Америки стали першою країною, яка почала розбудову інформаційного суспільства, перетворивши інформаційну галузь на стратегічний ресурс. У США питання інформаційної безпеки тісно пов'язані між собою, інформаційна політка в цій державі є пріоритетною для забезпечення національної безпеки. Політикою в інформаційній сфері щодо гарантування національної безпеки та протидії інформаційної агресії третіх країн займаються відповідні державні інституції.

У 1992 році була введена в дію Директива Міністерства оборони США «Інформаційна війна», що окреслила політику щодо захисту інформаційних ресурсів і надала відповідної значимості самому поняттю «інформаційна війна». Задля гарантування інформаційної безпеки у США велике значення приділяється управлінню інформаційними ресурсами. Основна мета цього – убезпечення власної системи інформаційної безпеки та вплив на інформаційно-безпекову систему потенційного супротивника. Було визначено складові такого явища як «інформаційна війна»: психологічний вплив на супротивника, оперативна безпека, введення супротивника в оману, електронне втручання, інформаційна розвідка, виведення з ладу системи управління вірогідного супротивника, інформаційний захист власної системи управління під час бойових зіткнень. Фактично, введення цієї Директиви на юридичному рівні інформаційну безпеку прирівняло до військової безпеки. Американська модель забезпечення інформаційної безпеки цілком допускає ведення інформаційних війн, що включає у себе планування і проведення активних інформаційно-психологічних операцій як інструменту зовнішньої політики [17].

Агентство національної безпеки – АНБ – є частиною Міністерства оборони США і відповідає за збір та аналіз іноземної розвідувальної інформації та за захист інформаційних систем і комп'ютерних мереж уряду США. Основний напрям дій – співпраця з приватним сектором і науковими установами у справах боротьби з загрозами неурядовим комп'ютерним мережам, захисту приватних телекомунікаційних, електронних та банківських мереж, а також – заходи, спільні разом із приватними установами і громадськими організаціями, з протидії тероризму [18].

Франція. Національна агенція з безпеки інформаційних систем (ANSSI, Agence nationale dela sécurité des systèmes d'information) являє собою міжвідомчу структуру, діяльність якої зосереджена на координації дій органів влади у сфері

кібербезпеки, визначенні урядової стратегії кіберзахисту та реалізації необхідних заходів разом з іншими органами влади [19].

Головною зоною відповідальності ANSSI є кібербезпека суб'єктів критичної інфраструктури та інформаційних систем.

До його повноважень належать:

- формування державної політики у сфері оборони та безпеки інформаційних систем;
- моніторинг, виявлення, оповіщення і реагування на кібератаки, спрямовані на державні інформаційно-телекомунікаційні системи;
- виявлення і реагування на вірусні атаки, реалізація адаптаційних механізмів захисту від них;
- систематичне інформування громадськості про загрози, зокрема, через урядовий вебпортал з питань ІБ;
- сертифікація комплексних систем захисту інформації.

Основний Закон, який націлений на боротьбу з інформаційною агресією проти країни, фейковими новинами став «Закон щодо протидії маніпулюванню інформацією» [20]. Цей закон включає в себе загальні правові норми та правові норми, які регулюють виборчий процес:

- прозорість цифрових платформ, що включає в себе зобов'язання повідомляти про спонсорований контент, вказуючи ім'я автора та сплачену суму. До того ж платформи мають надавати інформацію щодо використання персональних даних;
- у разі недотримання закону стягується штраф або призначається покарання одним роком тюремного ув'язнення;
- надання повноважень Вищій раді з аудіовізуальних питань переривати або призупиняти телевізійне мовлення, що контролюються іноземною державою, якщо вони поширюють фейкові новини;
- пришвидшення процедури розгляду судового позову задля оперативної реакції на поширення фейкових новин (на ухвалення рішення дається 48 год). Саме суддя має кваліфікувати «фейкові новини» відповідно до закону 1881 р. за такими критеріями: штучне та масове поширення, очевидність, явний вплив на вибір або порушення громадського спокою [21].

Забезпечення інформаційної безпеки *Німеччини* здійснюють Федеральні збройні сили Німеччини (Бундесвер), зокрема, «відділом інформаційних та комп'ютерних мережевих операцій командування стратегічної розвідки. Командування стратегічної розвідки також здійснює управління супутниковою розвідувальною системою SAR-Lupe, яка була запущена в грудні 2008 р».

За допомогою п'яти супутників система SAR-Lupe, яка «вважається однією з найдосконаліших систем у своєму роді, може передавати зображення з роздільною здатністю менше одного метра не залежно від денного світла і погоди. Таким чином, можна пояснити майже будь-яку точку на землі. Система збирає й оцінює інформацію про військово-політичну ситуацію в окремих країнах і альянсах потенційного або фактичного противника і його збройних сил». Основний закон в

галузі інформаційної безпеки в Німеччині – Закон «Про посилення безпеки систем інформаційних технологій».

Закон про безпеку IT від 25.07.2015 р. Закон відводить Федеральному відомству з безпеки в сфері інформаційних технологій (BSI) центральну роль в захисті критично важливих інфраструктур в Німеччині. Загалом забезпечення інформаційної безпеки Німеччини здійснюється Федеральними збройними силами Німеччини (Бундесвером), зокрема, відділом інформаційних та комп'ютерних мережевих операцій командування стратегічної розвідки [22].

Висновки. Аналіз зарубіжного досвіду дозволяє зробити деякі висновки:

1. Система забезпечення інформаційної безпеки європейських країн ґрунтується на усвідомленні ризиків і загроз, які зумовлюються швидким розвитком інформаційних та комунікаційних технологій. Тому політика цих країн у вказаній сфері є послідовною, засновується на компетентних оцінках та стратегіях та небезпек, які стоять перед країнами в сучасних умовах.
2. Сполучені Штати Америки стали першою країною, яка почала розбудову інформаційного суспільства, перетворивши інформаційну галузь на стратегічний ресурс. У США питання інформаційної безпеки тісно пов'язані між собою, інформаційна політка в цій державі є пріоритетною для забезпечення національної безпеки.
3. Позитивний досвід проаналізованих нами держав може бути корисним для України, практики забезпечення інформаційної безпеки в сучасних умовах, формування державних стратегій України в умовах інформаційної війни.

ДЖЕРЕЛА ТА ЛІТЕРАТУРА

1. Libicki M. C. What Is Information Warfare? [e-book]. Washington : National Defense University, 1995. URL: http://www.dtic.mil/get-tr-doc/pdf?AD=ADA367662.
2. Denning D. E. R. Information Warfare and Security. Addison-Wesley Professional, 1998.
3. Hoffman F. G. Decisive Force: The New American Way of War. Potomac Books, Inc., 1994. 233 p.
4. Molander R. C. Strategic Information Warfare: A New Face of War. RAND, 1996. 355 p.
5. Горбулін В. П. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу. *Стратегічні пріоритети* : Національний інститут стратегічних досліджень, 2014. № 4 (33). С. 5–10.
6. Курбан О. В. Сучасні інформаційні війни в мережевому он-лайн просторі. Київ : ВІКНУ, 2016. 286 с.
7. Марунченко О. П. Інформаційна війна в сучасному політичному просторі : дис. ... канд. політ. наук : 23.00.02 / Південноукраїнський національний педагогічний університет ім. К. Д. Ушинського. Одеса, 2012. 208 с.
8. Семен Н. Ф. Російські інтернет-ресурси як чинник інформаційної війни проти України (на прикладі сайтів «Правда. Ру» та «Российский диалог») :

дис. ... канд. соц. наук. Міжнародний економіко-гуманітарний університет імені акад. С. Дем'янчука. Рівне, 2018. 260 с.
9. Chatham House, The Royal Institute of International Affairs. Seven ways Russia's war on Ukraine has changed the world. 20 February 2023. URL: https://www.chathamhouse.org/2023/02/seven-ways-russias-war-ukraine-has.
10. East StratCom Task Force. URL: https://en.wikipedia.org/wiki/East_StratCom_Task_Force.
11. European Union. Network and information security: proposal for a European policy approach : adopted by the European Commission on 6 June 2001. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52001DC0298.
12. НКЦК уклав угоду про співпрацю з Агентством ЄС з мережевої та інформаційної безпеки. URL: https://interfax.com.ua/news/general/947334.html.
13. European Union. Joint Framework on countering hybrid threats: a European Union response. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016JC0018.
14. European Parliament. EU strategic communication to counteract propaganda against it by third parties. URL: https://www.europarl.europa.eu/doceo/document/A-8-2016-0290_EN.html.
15. Як Євросоюз протидіє російській пропаганді. URL: https://icps.com.ua/yak-vrosoyuz-protydi-rosiyskiy-propahandi.
16. Birge L. Sputnik and the «Information War»: Projecting Russia in the Digital Age : thesis submitted to The University of Manchester for the degree of Doctor of Philosophy. URL: https://pure.manchester.ac.uk/ws/portalfiles/portal/234007181/FULL_TEXT.PDF.
17. Intelligence and Security Committee of Parliament. Russia. URL: https://isc.independent.gov.uk/wp-content/uploads/2021/03/CCS207_CCS0221966010-001_Russia-Report-v02-Web_Accessible.pdf.
18. Велика Британія оновлює законодавство у сфері національної безпеки. URL: https://niss.gov.ua/doslidzhennya/mizhnarodni-vidnosyny/velyka-brytaniya-onovlyuye-zakonodavstvo-u-sferi-natsionalnoyi.
19. The White House. The Administration's Priorities on Cybersecurity. URL: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity#section-protect-critical-infrastructure (дата звернення: 04.03.2019).
20. Агентство національної безпеки (АНБ). URL: https://uk.wikipedia.org/wiki/.
21. Commission de la défense nationale et des forces armées. Assemblée Nationale, 2017. URL: http://www.assemblee-nationale.fr/14/cr-cdef/16-17/c1617024.asp.
22. Agence nationale de la sécurité des systèmes d'information. L'édito du directeur général. URL: https://www.ssi.gouv.fr/agence/missions/ledito-du-dg/.
23. Gouvernement français. Fake news : une proposition de loi pour lutter contre la manipulation de l'information. 2018. URL: https://www.gouvernement.fr/argumentaire/fake-news-une-propos-ition-de-loi-pour-lutter-contre-la-manipulation-de-l-information.

24. Beck-community. IT-Sicherheitsgesetz (IT-SiG) 2.0 – die wichtigsten Änderungen des Referentenentwurfs im Schnellüberblick. 03.04.2019. URL: https://community.beck.de/2019/04/03/it-sicherheitsgesetz-it-sig-20-die-wichtigsten-aenderungen-des-referentenentwurfs-im-schnellueberblick.

REFERENCES

1. Libicki, M. C. (1995). *What is Information Warfare?* [e-book]. Washington, DC: National Defense University. Retrieved from http://www.dtic.mil/get-tr-doc/pdf?AD=ADA367662
2. Denning, D. E. R. (1998). *Information Warfare and Security.* Addison-Wesley Professional.
3. Hoffman, F. G. (1994). *Decisive Force: The New American Way of War.* Potomac Books, Inc.
4. Molander, R. C. (1996). *Strategic Information Warfare: A New Face of War.* RAND Corporation.
5. Horbulin, V. P. (2014). «Hybrid war» as a key instrument of Russian geostrategic revenge. *Strategic Priorities*, (4[33]), 5–10.
6. Kurban, O. V. (2016). *Modern Information Wars in the Online Network Space.* Kyiv: VIKNU.
7. Marunchenko, O. P. (2012). *Information War in the Modern Political Space* (Candidate of Political Sciences dissertation, South Ukrainian National Pedagogical University named after K. D. Ushynsky). Odesa.
8. Semen, N. F. (2018). *Russian Internet Resources as a Factor of Information Warfare against Ukraine (Case Study of «Pravda.ru» and «Rossiiskii Dialog» Websites)* (Candidate of Social Sciences dissertation, International Economic and Humanities University named after Academician S. Demianchuk). Rivne.
9. Chatham House – The Royal Institute of International Affairs. (2023, February 20). *Seven Ways Russia's War on Ukraine Has Changed the World.* Retrieved from https://www.chathamhouse.org/2023/02/seven-ways-russias-war-ukraine-has
10. East StratCom Task Force. (n.d.). Retrieved from https://en.wikipedia.org/wiki/East_StratCom_Task_Force
11. European Union. (2001). *Network and Information Security: Proposal for a European Policy Approach* (adopted by the European Commission on 6 June 2001). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52001DC0298
12. National Coordination Center for Cybersecurity (NCCC). (2023). *NCCC Signed a Cooperation Agreement with the EU Agency for Network and Information Security.* Retrieved from https://interfax.com.ua/news/general/947334.html
13. European Union. (2016). *Joint Framework on Countering Hybrid Threats: A European Union Response.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016JC0018

14. European Parliament. (2016). *EU Strategic Communication to Counteract Propaganda Against It by Third Parties.* Retrieved from https://www.europarl.europa.eu/doceo/document/A-8-2016-0290_EN.html
15. ICPS. (n.d.). *How the European Union Counters Russian Propaganda.* Retrieved from https://icps.com.ua/yak-vrosoyuz-protydi-rosiyskiy-propahandi
16. Birge, L. (2021). *Sputnik and the «Information War»: Projecting Russia in the Digital Age* (Doctoral dissertation, The University of Manchester). Retrieved from https://pure.manchester.ac.uk/ws/portalfiles/portal/234007181/FULL_TEXT.PDF
17. Intelligence and Security Committee of Parliament. (2021). *Russia Report.* Retrieved from https://isc.independent.gov.uk/wp-content/uploads/2021/03/CCS207_CCS0221966010-001_Russia-Report-v02-Web_Accessible.pdf
18. National Institute for Strategic Studies (NISS). (2023). *United Kingdom Updates National Security Legislation.* Retrieved from https://niss.gov.ua/doslidzhennya/mizhnarodni-vidnosyny/velyka-brytaniya-onovlyuye-zakonodavstvo-u-sferi-natsionalnoyi
19. The White House. (2019). *The Administration's Priorities on Cybersecurity.* Retrieved March 4, 2019, from https://www.whitehouse.gov/issues/foreign-policy/cybersecurity#section-protect-critical-infrastructure
20. National Security Agency (NSA). (n.d.). Retrieved from https://uk.wikipedia.org/wiki/
21. Commission de la Défense Nationale et des Forces Armées. (2017). *Assemblée Nationale.* Retrieved from http://www.assemblee-nationale.fr/14/cr-cdef/16-17/c1617024.asp
22. Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). (n.d.). *L'édito du Directeur Général.* Retrieved from https://www.ssi.gouv.fr/agence/missions/ledito-du-dg/
23. Gouvernement Français. (2018). *Fake News: A Bill to Combat the Manipulation of Information.* Retrieved from https://www.gouvernement.fr/argumentaire/fake-news-une-propos-ition-de-loi-pour-lutter-contre-la-manipulation-de-l-information
24. Beck Community. (2019, April 3). *IT-Sicherheitsgesetz (IT-SiG) 2.0 – Die Wichtigsten Änderungen des Referentenentwurfs im Schnellüberblick.* Retrieved from https://community.beck.de/2019/04/03/it-sicherheitsgesetz-it-sig-20-die-wichtigsten-aenderungen-des-referentenentwurfs-im-schnellueberblick