Міністерство освіти і науки України
Кам’янець-Подільський національний університет імені Івана Огієнка
Історичний факультет
Кафедра політології та філософії

Кваліфікаційна робота
рівень вищої освіти – другий (магістерський)
з теми: **«ІНФОРМАЦІЙНА ПОЛІТИКА В УМОВАХ ВІЙСЬКОВО-ПОЛІТИЧНИХ КОНФЛІКТІВ»**

Виконав: студент 2 курсу, групи Р1-М23
напряму підготовки (спеціальності)
052 Політологія
Олексійчук Дмитро

Керівник: **Чабанов В.Г.,**
кандидат філософських наук, доцент

Кам’янець-Подільський – 2024

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Розвиток інформаційних технологій та розширення інформаційного просто впливає на всіх рівнях життя суспільства сьогодні. Наразі неможливо увити свою буденність без гаджета та новин про те, що відбувається у світі. Сучасна епоха характеризується інтенсивним розвитком і використанням різноманітних інформаційних ресурсів, які впливають на процеси управління та суспільний розвиток. Зокрема, впровадження новітніх технологій створює нові виклики в політичній сфері, де стабільність і функціонування залежать від якості та швидкості інформації, яку отримує політична еліта, а також від реакції системи управління на цю інформацію.

З прогресивним розвитком інформаційної сфери засоби масової інформації слід розглядати не тільки як посередника для передачі тієї чи іншої інформації, а й учасником комунікації між суспільством та владою. ЗМІ сьогодні активно використовуються для маніпулювання, навіювання, спотворення реальності тощо. Тому, безпека інформаційного середовища є одним з важливих секторів державного регулювання та удосконалення.

Розвиток інформаційної політики розпочався у ХХ століття, перші прояви застосування її були під час Першої та Другої світових війн. Інформуючи суспільство не правдивою інформацією, тоталітарна влада досягала своїх цілей.

Інформаційна політика – це сукупність певних державних законів та правил, які покликані захистити медіапростір від фейків, агресивної інформаційної атаки особистих даних тощо.

З початком повномасштабного вторгнення Росії в Україну питання бойових дій та заходів безпеки в контексті інформаційної війни стали як ніколи актуальними, адже в сучасному світі інформація поширюється досить швидко. Тому, для України сьогодні є важливим функціонування інформаційної політики

на вищому рівні, тому що в умовах війни українське суспільство піддається впливу різноманітних інформаційних потоків і інформація не завжди правдива і реальна, часто ворог використовує джерела інформації для дезінформації, щоб послабити підтримку населення дій керівництва держави, збільшити паніку тощо.

Наразі є важливим питанням формування незалежних ЗМІ, удосконалення системи інформаційної політики, доповнення нормативно-правової бази тощо.

Мета дослідження полягає у розкритті особливостей інформаційної політики в умовах військово-політичних конфліктів.

Визначена мета зумовила постановку таких **завдань**:

1. Визначити поняття «інформаційна політика» та її сутність.
2. Розглянути нормативно-правове регулювання інформаційної політики в Україні.
3. Розкрити роль та функції засобів масової інформації в умовах військово-політичних конфліктів.
4. Охарактеризувати методи та засоби ведення інформаційних війн у XXI столітті.
5. Проаналізувати досвід розвитку інформаційної політики в США та Європі.
6. Дати характеристику інформаційній політиці України в умовах воєнного стану та визначити шляхи її вдосконалення.

Об’єктом дослідження є феномен інформаційної політики.

Предметом дослідження виступає інформаційна політика в умовах військових та політичних конфліктів.

Для вирішення поставлених завдань в магістерській роботі використовувалися загальнонаукові та фундаментальні **методи дослідження:** методом аналізу було здійснено характеристику поняття «інформаційна політика» та розглянута її сутність, розглянуто нормативно-правове забезпечення інформаційної політики в Україні, а також охарактеризовано роль та функції

засобів масової інформації під час воєнних та політичних конфліктів, особливості інформаційної війни в Україні; за допомогою системного підходу розглянуто та сформовано методи та засоби ведення інформаційних війн у XX столітті; порівняльним методом, індукції та дедукції викладено висновки в ході дослідження наукової теми.

Джерельна база дослідження складається з Законів України, законодавчих актів, збірників, науково-практичних статей та доповідей, монографій тощо. Наприклад: О. Жадька «Гібридна війна і журналістика. Проблеми інформаційної безпеки» – у роботі висвітлюється суть та складові сучасних протистоянь, їхній психологічний та інформаційний аспект, пояснюють засоби та методи інформаційних війн; С. Глобенко досліджувала становлення та розвиток правового забезпечення України щодо захисту інформаційного простору держави; робота А. Крупнової також зосереджувалася на вивчені правового поля інформаційної безпеки України; Ю. Ніколаєць вивчала інформаційну політику в Україні в умовах війни та російський вплив на мас-медіа; І. Проноза висвітлила вплив ЗМІ на суспільну думку в умовах війни; зарубіжний досвід ведення інформаційної політики досліджували О. Топчій, Є. Таран, Н. Ржевська, М. Багмет, Є. Булана та інші. У роботі також використовувалися аналітичні дані досліджень організації ОПОРА та USAID-Internews.

Наукова новизна одержаних результатів. Інформаційна політика знаходиться на етапі дослідження та є актуальним питанням в умовах політично-військових конфліктів. Особливим чином стосується України після повномасштабного вторгнення. В ході магістерського дослідження ми отримали результати, які містять елементи наукової новизни, а саме визначено шляхи вдосконалення інформаційної політики України на базі зарубіжного досвіду в конфліктних чи військових умовах.

Практичні значення отриманих результатів. Основні теоретичні положення та висновки під час дослідження роботи можуть використовуватися

студентами під час написання дипломної чи магістерської роботи, при підготовці матеріалів для науково-практичних конференцій, складання навчально-методичних матеріалів тощо.

Структура й обсяг роботи. Магістерська робота складається з 3 розділів, 8 підрозділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи становить 89 сторінок.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ПОНЯТТЯ «ІНФОРМАЦІЙНА ПОЛІТИКА»

1.1 Сутність та основні ознаки інформаційної політики

У ході дослідження поняття «інформаційна політика» ми зіштовхуємося з такими термінами, як «інформатизація суспільства», «інформаційна безпека» тощо. Ці терміни тісно взаємопов'язані та доповнюють одне одного.

Сучасний політичний процес характеризується широкою участю інститутів громадянського суспільства у формуванні політичних рішень та залученням засобів масової інформації до їх обговорення та дебатів. Внутрішня і зовнішня політика держав зазнає все більшого тиску з боку громадськості як всередині країни, так і за її межами. Цьому сприяє процес глобалізації інформаційних потоків, які майже безперешкодно циркулюють у світі. Фактично в наш час завершується процес інформатизації соціально-економічного життя та формування глобального інформаційного простору [89, с. 391].

Сьогодні практика здійснення державної інформаційної політики потребує її нового теоретичного переосмислення. Цей процес знаходиться в прямій залежності від процесів наукової обґрунтованості та ефективності реалізації інформаційної політики держави, її світоглядного забезпечення. Як відомо, ці проблеми ще недостатньо розроблені адміністративно-правовою та управлінською наукою. Подібне спостерігається і в інформаційній сфері: державна інформаційна політика, як правило, розглядається як допоміжна для обслуговування корпоративних інтересів державної влади, а ЗМІ (як офіційні, так і неофіційні) як своєрідна сполучна тканина між державою і громадянським суспільство. Це суперечить об'єктивному факту, який відображає самодостатність ЗМІ (преси) як носія інформаційної влади [50, с. 72].

Інформатизація суспільства – це глобальний соціальний процес, особливістю якого є те, що основним видом діяльності у сфері суспільного виробництва є збирання, накопичення, виробництво, обробка, зберігання, передача та використання інформації, що здійснюється на основі сучасних засобів мікропроцесорної та обчислювальної техніки, а також на основі різноманітних засобів обміну інформацією. Інформатизація суспільства забезпечує:

– активне використання постійно зростаючого інтелектуального потенціалу суспільства, зосередженого в друкованому фонді, наукової, виробничої та іншої діяльності його учасників;

– інтеграція інформаційних технологій у наукову та виробничу діяльність, ініціювання розвитку всіх сфер суспільного виробництва, інтелектуалізація трудової діяльності;

– високий рівень інформаційного обслуговування, доступ будь-якого члена суспільства до джерел достовірної інформації, візуалізація представленої інформації, суттєвість використаних даних [31, с. 10].

Використання відкритих інформаційних систем, призначених для використання всієї маси інформації, доступної суспільству на даний момент, у певній його сфері дозволяє вдосконалювати механізми управління соціальною системою, сприяє гуманізації та демократизації суспільства, підвищує рівень добробуту її учасників. Процеси, що відбуваються у зв’язку з інформатизацією суспільства, сприяють не тільки прискоренню науково-технічного прогресу, інтелектуалізації всіх видів людської діяльності, а й створенню якісно нового інформаційного середовища суспільства, що забезпечує розвиток творчого потенціалу особистості [31, с. 10].

Цікаве визначення державної інформаційної політики через категорію «влада», запропоноване В. Степановим, виходячи з твердження про те, що влада як явище характеризується здатністю та можливістю окремих суб’єктів здійснювати вирішальний вплив на діяльність і поведінку іншими предметами за

допомогою різних засобів. А тому з позицій системного підходу інформаційна політика визначається як діяльність органів державної влади за певними напрямками [84, с. 82].

У своїй праці українські дослідники О. Ляшенко та І. Дацків згадують британських вчених, які дали таке визначення інформаційній політиці: «це особлива сфера життя людей (політиків, аналітиків, журналістів, слухачів, читачів тощо), пов'язана з відтворенням та поширенням інформації, яка задовольняє інтереси держави та громадянського суспільства і спрямована на забезпечення творчого, конструктивного діалогу між ними та їх представниками. Важливу роль у формуванні інформаційної політики відіграють засоби масової інформації. На думку деяких зарубіжних авторів, інформація, що поширюється медіаканалами, впливає на населення в трьох напрямках: «дає їм можливість стежити за тим, що відбувається у світі», «розподіляє основні політичні теми за ступенем важливості» і «формує політичні уподобання людей»» [41, с. 212].

На думку українського дослідника Ю. Іванченка, державна інформаційна політика – це сукупність основних напрямів і методів діяльності держави щодо отримання, використання, поширення та зберігання інформації [32, с. 1].

Існує два аспекти державної інформаційної політики:

– технологічний (регулювання процесу розвитку компонентів інформаційного середовища);

– змістовні (пріоритети комунікаційної діяльності учасників суспільно-політичного процесу) [4, с. 5].

Об'єктом державної інформаційної політики є інформаційна сфера суспільства в широкому її розумінні. До нього входить уся сукупність інформації, інформаційна інфраструктура, суб'єкти, які збирають, формують, поширюють і використовують інформацію, а також система регулювання суспільних відносин, що з цього приводу виникають [33, с. 52].

Метою інформаційної політики є забезпечення переходу до нового етапу розвитку України – побудови демократичного інформаційного суспільства та входження нашої держави у світову інформаційну спільноту. Основою такого переходу є створення єдиного інформаційно-телекомунікаційного простору країни як основи вирішення завдань соціально-економічного, політичного і культурного розвитку країни та забезпечення її безпеки [33, с. 53].

Основними завданнями державної інформаційної політики є:

– створення необхідної нормативно-правової бази для побудови інформаційного суспільства;

– модернізація інформаційно-телекомунікаційної інфраструктури;

– розвиток інформаційно-телекомунікаційних технологій;

– підготовка людини до життя і праці в нову інформаційну епоху;

– ефективне формування та використання національних інформаційних ресурсів та забезпечення широкого, вільного доступу до них;

– забезпечення громадян соціально значущою інформацією та розвиток незалежних ЗМІ тощо [33, с. 53].

Ми погоджуємося з думкою В. Терещенка, що теоретико-методологічна база формування ідеології інформаційної політики в умовах війни має ґрунтуватися на сучасних уявленнях про державну інформаційну політику як про систему ідей, установок, цілей, методів та засобів, за допомогою яких держава (в особі своїх органів та посадових осіб) здійснює нормативно-правове регулювання відносин між громадянським суспільством та інформаційною системою держави, яка володіє власним потенціалом влади та впливу на суспільні процеси. Засоби масової інформації орієнтовані на потреби особистості – суб’єкта (споживача інформації), забезпечуючи їй доступ до необхідної інформації, яка має допомогти їй свідомо брати участь у процесі суспільних перетворень, впливати на соціальну практику. Завданням держави в таких умовах є розробка адекватної чинним

суспільним умовам високоефективної нормативно-правової бази, яка б задала основні параметри та регулятори інформаційної політики держави, структуруючи як її взаємодію із засобами масової інформації, так і взаємодію ЗМІ з громадянським суспільством. Центральним принципом цієї політики є доступ до інформації та водночас захист власних інтересів держави від зловживань з боку приватних ЗМІ, насамперед через законодавство [89, с. 392].

Інформаційна політика в сучасному її розумінні є інструментом забезпечення безпеки людини, суспільства, держави, світової спільноти. У багатьох країнах і міжнародних об'єднаннях існують спеціальні структури, які здійснюють інформаційну діяльність [89, с. 392].

Крім того, активну участь у цій діяльності беруть перші особи держави, реалізуючи найважливіші інтереси у сфері національної та міжнародної безпеки. Потужні структури для реалізації інформаційної політики існують як в авторитарних державах, так і в країнах з демократичним режимом. Таким чином, адміністративно забезпечена та концептуально структурована інформаційна політика дозволяє вирішувати низку найважливіших національних і міжнародних завдань. Важливими завданнями інформаційної політики в умовах війни має бути розв'язання проблеми балансу суспільних інтересів, отримання об'єктивної та своєчасної інформації та необхідності дотримання вимог секретності в умовах ведення широкомасштабних військових дій. Виконання збройними силами та іншими воєнізованими формуваннями різноманітних завдань щодо відбиття агресії противника [89, с. 393].

Аналізуючи вищевикладене, слід зробити висновок, що захист інформації є одним із важливих і актуальних аспектів регулювання інформаційної політики. В. Ліпкан виділяє кілька підходів до класифікації поняття «інформаційна безпека»:

– стан безпеки інформаційного простору;

– процес управління загрозами та небезпеками, що забезпечує інформаційний суверенітет країни;

– стан захищеності національних інтересів країни в інформаційному середовищі або в інформаційній сфері;

– безпека встановлених законом правил, за якими відбуваються інформаційні процеси в державі;

– суспільні відносини, пов’язані із захистом життєво важливих інтересів людини та громадянина, суспільства і держави від реальних і потенційних загроз в інформаційному просторі;

– складовою частиною політичної, економічної, оборонної та інших складових національної безпеки [39, с. 25-30].

В. Негодченко зазначає, що для забезпечення інформаційної безпеки держави спочатку визначаються загрози такій безпеці, формується певний правовий інструментарій, який застосовуватиметься для подолання цих загроз з обов’язковим пріоритетом прав і свобод людини та громадянина, формується певний вектор розвитку інформаційних відносин. Тобто формується стратегія, доктрина, яка називається «державна інформаційна політика» і являє собою певну правову позицію, яка полягає у визначенні правових інструментів, за допомогою яких держава підтримує баланс інтересів особи, суспільства і держави в інформаційній сфері та забезпечує інформаційну безпеку [43, с. 78].

Підходи до трактування поняття «інформаційна безпека» за О. Бордук сформовано на Рисунку 1.1:

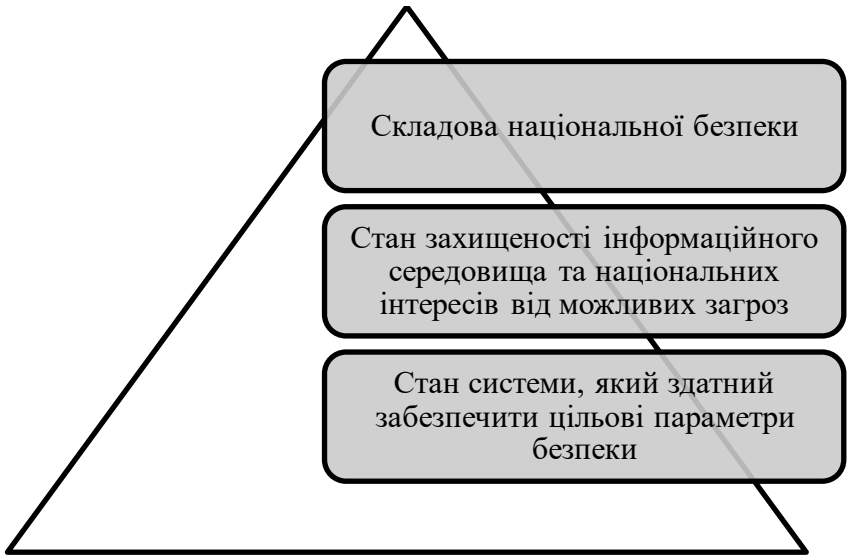

Рис. 1.1 Підходи до трактування поняття «інформаційна безпека» [5]

Отже, інформаційна політика – це певна організація комунікації в інформаційній сфері між владою та суспільством, що регулюється законами та актами створенні владою. Інформаційна політика в умовах війни – це певне система заходів, що реалізуються державою спільно з інститутами громадянського суспільства, спрямованих на регулювання інформаційних процесів, формування та розвиток інформаційного суспільства, де пріоритетним завданням є захист інформаційного середовища від впливу ворога.

1.2 Стан розробленості питання та нормативно-правове регулювання інформаційної політики

Сьогодні ми живемо в час новітніх технологій, час розвитку та прогресивних змін, що є загальновідомим фактом для всіх. Будь-який вид діяльності зараз не може функціонувати без інформації, технологій передачі інформації чи інформаційного впливу на певне коло осіб. Тому дослідження інформаційної політики та її безпеки, на нашу думку, має велике значення для її майбутнього функціонування. Термін «інформаційна політика» з’явився в

науковій літературі не так давно, але з його завданням ми вже зустрічалися раніше.

Такі дослідники, як М. Дурман і Я. Лінецька у своїй праці вказує на те, що з другої половини XX століття в середовищі соціологів і соціальних філософів Заходу почалася дискусія про перехід найбільш розвинутих країн до стадії постіндустріального суспільства. Так з'явилося поняття «інформаційне суспільство», головну роль в якому відіграють інформаційні технології. Основним продуктом виробництва в такому суспільстві є інформація та знання. Таким чином, формування нового інформаційного суспільства є результатом повільної інформаційної еволюції, внаслідок якої напрям прогресу зміщується не стільки до збільшення кількості та якості суспільних благ, скільки до зміни ставлення до людини, до свого існування та усвідомлення нею свого місця в новому просторі. І цей простір вже неможливо уявити без використання інформаційних технологій у різних сферах суспільного життя, в тому числі у сфері державного управління, що включає державне управління, місцеве самоврядування та діяльність різних видів громадських організацій і процесів взаємодії між ними [22, с. 3].

Ідея інформаційного суспільства була сформульована в Японії на початку 60-х років XX століття. Термін «інформаційне суспільство» був запропонований професором Токійського технологічного інституту Ю. Хаяші, а його узагальнене визначення увійшло до доповідей японського уряду: «інформаційне суспільство – це суспільство, в якому процес комп'ютеризації надає людям доступ до надійних джерел інформації, звільняє їх від рутинної роботи та забезпечує високий рівень автоматизації виробництва» [23, с. 8].

На рубежі XX-XXI століття людство зробило крок до радикальних технологічних перетворень, пов'язаних з появою нового ряду значних небезпек і ризиків. Сьогодні інформаційні технології, які розглядаються як фактор, що спричиняє величезний вплив на глобальний розвиток суспільства та формування інформаційної реальності, вплинули на свідомість людини та її можливості,

змінили життя суспільства, трансформували пріоритети та цінності. На загальному тлі деформації системи цінностей інформаційна сфера виявилася ядром економічних, соціальних, політичних та інших конфліктів у суспільстві. Так, О. Панченко виокремлює реальну загрозу «інформаційного розшарування», розквіт комп'ютерної злочинності, потенційну загрозу дегуманізації праці та реальну загрозу техностресу, виробництва нових видів інформаційної зброї, загрозу інформаційного колоніалізму, розвиток різного роду захворювань, загроза маніпуляції людською свідомістю, що призводить до психічної та соціальної дезадаптації людини [48, с. 136].

Відповідно до вищесказаного можна зробити висновок, що інформаційна влада має велике значення в суспільстві. На думку І. Антошина, інформаційна влада здійснює широкий вплив на формування поведінки особистості та суспільства загалом, вміло маніпулює свідомістю людей за допомогою цілеспрямованого впливу інформації або блокування певної інформації, пропагандистських та агітаційних матеріалів, інформації, яку ми не сприймаємо як примус [1, с. 2].

Найважливішим фактором, що визначає ефективність державної влади, є рівень її інформаційного забезпечення, ступінь оснащеності сучасними технічними, технологічними та телекомунікаційними системами. Отже, інформаційне забезпечення органів державної влади – це система понять, методів і засобів, за допомогою яких працівники органів влади забезпечуються інформацією. Головною стратегічною метою державної інформаційної політики України є забезпечення переходу на новий етап розвитку нашої держави, побудова інформаційного суспільства та входження її у світове інформаційне товариство. Визначено, що інформаційні технології започаткували трансформацію державного управління з метою його адаптації до інформаційної ери. За допомогою інформаційних технологій прискорюється процес прийняття рішень та їх

реалізації, вивільняється частина робочого часу, з'являються механізми інформаційного забезпечення під час реалізації державної політики [40, с. 5].

На нашу думку, інформаційна влада з одного боку демонструє прозорість та легітимність своєї діяльності, а з іншого боку має потужний інструмент впливу на суспільство, що може супроводжуватися інформаційними війнами та конфліктами.

Інформаційні війни супроводжують всю історію людства. Спочатку вони були релігійно-ідеологічними, а для боротьби з носіями чужих поглядів використовувалися всі види репресій. У далекому минулому інквізиція або репресивні апарати тоталітарних держав XX століття вели активну боротьбу з носіями чужих ідей [101, с. 1].

Досліджуючи розвиток інформаційної політики, більшість дослідників згадують у своїх працях відомого китайського стратега VI ст. до н. е. Сунь Цзи. Його рекомендації щодо психологічних та інформаційних засобів завоювання фактично актуальні й сьогодні. Так, зокрема, він радив:

1) послабити міць військ противника шляхом перешкоджання нормальному забезпеченню і підтриманню порядку;

2) послабити країну-жертву в цілому шляхом дискредитації її традицій, віри, лідерів, позитивних процесів, розбещення населення, провокування внутрішніх конфліктів [15, с. 66].

Цього, на думку Сунь Цзи, можна досягти такими методами:

– шляхом купівлі інформації та спільників;

– втягувати опонентів у злочин з метою подальшого шантажу та вербування;

– залучати до співпраці негідників;

– використовувати дезінформацію, залякування, психологічний тиск, образи, глузування;

– перешкоджати ефективній роботі уряду опонента та заохочувати до хабарництва [15, с. 66].

Найефективнішим методом ведення війни полководець вважав дезінформацію.

Сунь Цзи написав першу фундаментальну працю в цій галузі під назвою «Мистецтво війни», в якій, серед іншого, говорилося, що якщо передовий правитель або мудрий полководець перемагає своїх ворогів щоразу, коли вони беруть участь у битві, це відбувається завдяки попередній інформації. Так звану попередню інформацію неможливо отримати від духів чи божеств ні за аналогією з минулими подіями, ні за допомогою розрахунків. Воно повинно виходити від людини, знайомої з ситуацією ворога. Концепція Сунь Цзи базується на теорії оволодіння ворогом, якого заманюють в пастки перевагами, позбавленого хоробрості, ослабленого і виснаженого перед атакою [87, с. 90].

Використання технологій впливу на ворога за допомогою слова було типовим явищем і для Стародавньої Греції.

1. По-перше, було популярно поширювати чутки про кількісні та якісні переваги свого війська в таборі ворога.

2. По-друге, під час владних протистоянь створювали кам’яні написи із закликами до опонентів – тодішні аналоги сучасних листівок.

3. По-третє, збереглися також свідчення застосування психологічного тиску на опонента [15, с. 66].

Як зазначає Г. Почепцов, за допомогою певних засобів (наприклад, промова командира перед боєм) підтримувався бойовий дух воїнів; зображувалася також концепція «справедливої війни» («щоб війна була успішною, вона мала вважатися справедливою»); крім того, «значний пропагандистський ефект мали тріумфи, які супроводжували перемоги римських імператорів» [49, с. 572-573].

Потужним центром розвитку технологій інформаційного впливу на союзників і ворогів у середньовічній Європі, безсумнівно, був Ватикан. Яскравим

підтвердженням цього є розвиток концепції «священної війни» і сама організація хрестових походів [15, с. 67].

З XV століття в Європі працює друкарський верстат. Цю технологію глобального впливу на маси використовував Мартін Лютер. Він боровся з папським престолом головним чином доступними для народу виданнями Біблії, перекладеною німецькою мовою, а також своїми тезами та брошурами, які друкувалися величезними тиражами й миттєво ставали популярними [15, с. 68].

Здійснення інформаційних впливів із застосуванням інформаційної зброї (приховування інформації; надання її частково, у певному ракурсі; перебільшення наслідків) зафіксовано літописцями на території України ще за Київської Русі. Так, факт подорожі княгині Ольги до Константинополя загальновідомий, але ні візантійські, ні руські джерела не висвітлюють причину та мету подолання такої тривалої подорожі. Войовничий князь Святослав заздалегідь повідомив ворога про свій похід, але напрямок і сили, які планувалося застосувати, залишилися в таємниці. Це дало змогу викликати паніку в стані військ і швидко розгромити ворога [16, с. 18].

Отже, феномен інформаційної політики існує вже досить тривалий час, проте його активний розвиток набув з кінця XX століття, що свідчить про те, що дане питання не є розглянуте дослідниками та науковцями в повному обсязі й перебуває на етапі дослідження.

Важливе місце в рамках забезпечення національної безпеки кожної держави посідає правове регулювання забезпечення інформаційної безпеки. Це пояснюється не тільки тим, що інформація є фундаментальним елементом життєдіяльності сучасних соціальних систем, а й тим, що інформація, як і рух енергії та речовини, визначає функціонування біологічних і технічних систем і є рушійна сила сучасного світу. Правове регулювання інформаційної безпеки в Україні – це складна система законів різної юридичної сили, які регулюють відносини у сфері протидії загрозам в інформаційній сфері. Ця система також

включає активну діяльність органів державної влади та місцевого самоврядування, спрямовану на постійний розвиток та вдосконалення сфери інформаційної безпеки [34, с. 349].

Якщо звернутися до нормативного визначення інформаційної безпеки, то слід зазначити, що чинне законодавство України не містить розгорнутого тлумачення цього поняття. Проте нормативні акти, що стосуються питань інформаційної безпеки, природно розглядають її в контексті більш загального поняття національної безпеки [88, с. 67].

Після проголошення Україною незалежності розпочався новий етап розвитку та становлення національного законодавства, у тому числі у сфері забезпечення інформаційної безпеки. Аналізуючи закони, як джерело регулювання суспільних відносин у досліджуваній сфері, варто зазначити, що основними нормативно-правовими актами є закони установчого спрямування, які визначають важливі положення забезпечення національної безпеки в інформаційній сфері. Закони регулюють особливості взаємовідносин суб'єктів інформаційної безпеки, визначають їх права, обов'язки та відповідальність, визначають дії суб'єктів інформаційної безпеки на всіх рівнях (людини, суспільства, держави), а також організаційні засади їх діяльності, встановлюють порядок застосування різних сил і засобів забезпечення інформаційної безпеки [83, с. 87].

Систему правових актів, що становлять основу правового регулювання забезпечення інформаційної безпеки в Україні, українська дослідниця А. Крупнова поділила і класифікувала їх наступним чином:

1. Залежно від обсягу приписів, які містяться в актах, ступеня і характеру регульованих відносин:

– акти, що не містять прямих регламентуючих положень, щодо забезпечення інформаційної безпеки, проте прямо або опосередковано регулюють інформаційні відносини;

– акти, які безпосередньо регламентують забезпечення інформаційної безпеки в Україні.

2. Залежно від юридичної сили актів:

– Конституція України;

– Закони України, в тому числі «Про інформацію» [53], «Про захист інформації в інформаційно-комунікаційних системах» [54], «Про національну безпеку України» [55], «Про захист персональних даних» [56] тощо;

– підзаконні акти – це нормативні акти Президента України, Кабінету Міністрів України, Державної служби спеціального зв'язку та захисту інформації України тощо;

– нормативні документи в галузі технічного захисту інформації та державні стандарти України стосовно створення і функціонування комплексної системи захисту інформації;

– міжнародні акти [34, с. 349].

Серед таких актів та документів основними є:

1. Закони України:

– «Про інформацію» [53];

– «Про медіа» [61];

– «Про науково-технічну інформацію» [68];

– «Про державну таємницю» [69];

– «Про рекламу» [70];

– «Про Концепцію Національної програми інформатизації» [71];

– «Про доступ до публічної інформації» [72], де описано засади опублікування і поширення певних категорій інформації її розпорядниками, права на активний і пасивний доступ користувачів до інформації тощо;

– «Про основні засади забезпечення кібербезпеки України» [59], який спрямований на визначення правових та організаційних основ забезпечення

інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основних цілей, напрямів та принципів державної політики у сфері кібербезпеки України [95, с. 61]

2. Постанови Верховної ради України та Кабінету Міністрів України щодо розглядуваної тематики:

– «Про підсумки парламентських слухань «Інформаційна політика України: стан і перспективи» [73];

– «Про підсумки парламентських слухань «Проблеми інформаційної діяльності, свободи слова, дотримання законності та стану інформаційної безпеки України» [74];

– «Про парламентські слухання «Суспільство, засоби масової інформації, влада: свобода слова та цензура в Україні» [75].

3. Розпорядження Кабінету Міністрів України.

4. Укази Президента України щодо державної інформаційної політики:

– «Про першочергові заходи щодо забезпечення доступу до публічної інформації в допоміжних органах, створених Президентом України» [76];

– «Питання забезпечення органами виконавчої влади доступу до публічної інформації» [77];

– «Про введення воєнного стану в Україні» [62];

– «Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану»» [64].

Відповідно до останнього, РНБО України вирішила, що в умовах воєнного стану реалізація єдиної інформаційної політики є пріоритетним питанням національної безпеки, забезпечення якої реалізується через об’єднання всіх загальнонаціональних телеканалів, програмний контент якого складають переважно інформаційні та/або інформаційно-аналітичні програми на єдиній

інформаційній платформі стратегічної комунікації – цілодобовому інформаційному марафоні «Єдині Новини #UAразом» [95, с. 62].

Періодизацію розвитку та становлення інформаційної політики в Україні запропонував науковець В. Дрешпак. Отже, він виділив такі етапи:

Перший період (1991-1994 рр.) характеризується процесами формування правових засад регулювання інформаційної сфери України, визначенням основних напрямів державної інформаційної політики, певним плюралізмом суб'єктів її діяльності та реалізації, виникнення та подолання проблем перехідного етапу, інтенсивного розвитку інформаційного простору держави, насамперед сфери масових комунікацій, де значно збільшилася кількість друкованих ЗМІ переважно ділового та розважального спрямування. Нормативно-правове регулювання інформаційної сфери деякий час здійснювалося на основі прийнятого в червні 1990 р. Закону СРСР «Про друк та інші засоби масової інформації» та інших актів радянського періоду. Згодом важливим кроком до формування власної інформаційної політики стало прийняття Закону України «Про інформацію» [53].

Другий період (1995-1999 рр.) визначався процесами конституційного унормування основоположних принципів у сфері інформації та свободи слова, прийняттям нових законів, що регулюють найрізноманітніші аспекти інформаційних відносин, і внесенням змін до раніше прийнятих законів, створення нових державних органів, таких як: Національна рада України з питань телебачення і радіомовлення, Мінцифри, якісні зміни в інформаційному просторі держави за рахунок значних зростання впливу недержавних ЗМІ та інтенсивне розширення сфери застосування нових інформаційно-комунікаційних технологій. Пріоритетне завдання державної інформаційної політики цього періоду – регулювання (впорядкування) сфери інформаційних відносин – буквально ніде не було визначено, але чітко простежувалось у діях як центральних, так і місцевих органів влади. Посилилися багатовекторні впливи на інформаційну сферу як

безпосередньо з боку держави, так і через наближені до неї політико-економічні групи [24, с. 43].

Третій період (2000-2004 рр.) характеризується спробами уніфікації нормативно-правової бази у сфері інформаційних відносин та конкретизації напрямів і завдань державної інформаційної політики України, в умовах звуження державного сектору масових комунікацій. Держава намагається сприяти діяльності державних і комунальних ЗМІ, в першу чергу регіональних і місцевих, розширюється сфера застосування інформаційно-комунікаційних технологій, початок формування електронного уряду. У цей період відбувалося інтенсивне становлення, розвиток та впровадження основних складових електронного урядування: прийняття законодавчої бази, створення урядового веб-порталу, запровадження автоматизованого обліку та контролю виконавчої державної влади та розвитку телекомунікаційної інфраструктури.

Четвертий період (2005-2010 рр.) характеризується значним зниженням темпів законотворчості в інформаційній сфері, відсутністю кардинальних змін у системі управління галузями інформаційної сфери, намаганнями лібералізувати комунікативну політику органів публічної влади, наблизити до європейських стандартів державну політику у сфері ЗМІ, інтенсивною роботою з визначення основних напрямів і формуванням основ розвитку інформаційного суспільства та впровадження електронного урядування в Україні. У контексті розвитку електронного урядування за цей період удосконалюється урядовий веб-портал щодо надання послуг громадянам та представникам бізнесу, уніфікуються системи електронного документообігу органів виконавчої влади, створюється інфраструктура електронного цифрового підпису, триває об’єднання центральних органів виконавчої влади в єдину захищену мережу спеціального зв’язку [24, с. 44].

П’ятий період (з 2011 р.) характеризується передусім процесами модернізації інформаційної сфери в цілому, що вимагатиме постійного

вдосконалення її правового регулювання та змін у системі управління її галузями. До кінця цього періоду стало актуальним питання зміни структури державного управління в інформаційній галузі через зміни структури інформаційної сфери в цілому та розпорошення функцій у сфері інформатизації, яка почала динамічно розвиватися [24, с. 45].

На нашу думку, запропоновану періодизацію слід доповнити шостим періодом, адже до 2024 року інформаційна політика суттєво змінилася, що характеризується початком воєнних дій на території України. В цей період збільшилося вагоме значення засобів масової інформації, впливу комунікаційних каналів на суспільство, поява агресивних технологій комунікації, доповнення нормативно-правової бази щодо інформаційної політики тощо.

Для більш детального розуміння нормативно-правового забезпечення державної інформаційної політики України, слід розглянути основні Закони, акти та документи.

У Законі України «Про національну безпеку України» зазначається, що відповідна державна політика «спрямовується на забезпечення. інформаційної, ... кібербезпеки України та на інші її напрями» [55]. Згадані напрями конкретизовано у Стратегії національної безпеки України [57], де зазначено про критичні проблеми в інформаційній сфері, посилення інструментів національної сили (зокрема, інформаційно-психологічних та кіберзасобів), інформаційну зброю, констатовано відсутність цілісної інформаційної політики держави. Інформаційна безпека передбачає захист інформаційного простору країни від зовнішнього впливу, дезінформації та інших загроз, які можуть завдати шкоди суспільству та державі. Забезпечення всіх складових національної безпеки потребує спільних зусиль держави та громадян, а також передбачає розроблення ефективної стратегії та політики у цих сферах [14, с. 67].

Указом Президента України підписано рішення «Про Стратегію інформаційної безпеки» [58], в якому висвітлено стратегічні цілі та завдання захисту інформації до 2025 року, описано основні виклики та загрози інформаційній безпеці, приділено увагу інформаційній політиці російської федерації, що впливає на демократичні інституції та поглиблює протиріччя в демократичних державах шляхом спеціальних інформаційних операцій та гібридної війни. У документі згадуються такі поняття, як «інформаційна загроза», «інформаційні заходи захисту держави», «антикризові комунікації», «кризові комунікації», «стратегічні комунікації», «стратегічний наратив», «урядові комунікації». Згідно з документом, інформаційна безпека України – це «невід'ємна частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, в якому конституційні права і свободи особи на збір, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, діє ефективна система захисту та протидії шкоді внаслідок поширення негативної інформації, у тому числі скоординоване поширення недостовірної інформації, деструктивна пропаганда, інші інформаційні операції, несанкціоноване поширення, використання та порушення цілісності інформації з обмеженим доступом» [67].

Закон України «Про основні засади забезпечення кібербезпеки України» дає пояснення таким термінам як «інцидент кібербезпеки», «кібератака», «кібербезпека», «кіберзагроза» тощо. В документі йдеться про основні принципи застосування закону, пояснення суб'єктів та об'єктів кібербезпеки, принципи, міжнародне співробітництво тощо [59].

Згідно зі Стратегією кібербезпеки України, затвердженою відповідним Указом Президента України [60], яка, зокрема, ґрунтується на положеннях Закону України «Про основні засади забезпечення кібербезпеки України» [59],

розглянуто актуальність забезпечення кібербезпеки як одного із пріоритетів національної безпеки України; відзначено роль інформаційних технологій та кіберпростору в сучасному світі та наголошено на ризиках щодо їх використання; підкреслено значення захисту від новітніх кіберзагроз в аспекті активізації кібертероризму, значущість захисту об'єктів критичної інформаційної інфраструктури та інших інфраструктурних об'єктів від кібератак.

Закон України «Про медіа» спрямований: «на забезпечення реалізації права на свободу вираження поглядів, права на отримання різнобічної, достовірної та оперативної інформації, на забезпечення плюралізму думок і вільного поширення інформації, на захист національних інтересів України та прав користувачів медіа-сервісів, регулювання діяльності у сфері медіа відповідно до принципів прозорості, справедливості та неупередженості, стимулювання конкурентного середовища, рівноправності і незалежності медіа та визначає правовий статус, порядок формування, діяльності та повноваження Національної ради України з питань телебачення і радіомовлення» [61].

В даному законі [61] розглядаються такі аспекти, як: загальні положення, суб'єкти медіа, публічні аудіовізуальні медіа, вимоги до змісту інформації та її поширення, обгрунтовуються повноваження Національної ради України з питань телебачення та радіомовлення, розглядається відповідальність за порушення законодавства в сфері медіа, а також зазначені особливості правового регулювання діяльності медіа в умовах збройної агресії.

На думку М. Шевчук, у сучасних умовах наявність і доступність достовірної інформації про стан і динаміку економічних, політичних, соціальних та інших процесів у суспільстві критично визначають здатність влади та суспільства в цілому розробляти та реалізовувати ефективні рішення в геополітичній, військовій стратегічній, науково-освітній, культурно-історичній та екологічній сферах, а також в умовах інтелектуалізації та інформатизації суспільства інформація та

інформаційні комунікації стають факторами, які можуть або забезпечать безпеку суспільства [98, с. 137].

Сьогодні діє єдиний орган виконавчої влади, який має реалізовувати, контролювати та реалізовувати завдання з реалізації державної інформаційної політики – Міністерство інформаційної політики. У своїй діяльності Міністерство інформаційної політики України базується на принципах захисту свободи слова та переконань, захисту прав громадян на вираження своєї позиції. При Міністерстві інформаційної політики створено Громадську раду, до складу якої увійшли представники громадських організацій, ЗМІ та медіа експерти. Головною метою створення цієї ради є здійснення контролю за діяльністю міністерства.

Основними завданнями Міністерства є:

– розробка стратегії інформаційної політики України та концепції інформаційної безпеки держави;

– координація роботи органів влади у сфері комунікації

– поширення інформації [6, с. 22].

Стан нормативно-правового регулювання захисту інформаційного простору України є складним і потребує постійного оновлення та вдосконалення відповідно до сучасних викликів і загроз, які з часом урізноманітнюються та ускладнюються. Україна має досить потужну законодавчу базу, яка регулює різні аспекти цього явища, однак, як показує практика, існує низка недоліків і не узгодженостей у законодавстві, а також проблемних питань щодо його практичної реалізації [14, с. 77].

Отже, нормативно-правове регулювання в Україні почало здійснюватися після прийняття незалежності. Основним кроком до забезпечення інформаційної безпеки було прийняття Закону «Про інформацію». Згодом інформаційна політика України поступово почала розвиватися та розширювати нормативну базу. Проте, на нашу думку, інформаційна політики України потребує більш детального вивчення та вдосконалення для захисту країни. Забезпечення інформаційної

безпеки України, безпеки її національних інтересів в інформаційній сфері передбачає пріоритетний розвиток системи нормативно-правового регулювання відносин у цій сфері, протидію загрозам цим інтересам та впорядкування відповідного правотворчого процесу.

РОЗДІЛ 2. РОЗВИТОК ІНФОРМАЦІЙНОЇ ПОЛІТИКИ В УМОВАХ ВІЙСЬКОВО-ПОЛІТИЧНИХ КОНФЛІКТІВ

2.1 Роль та функції засобів масової інформації в умовах військово-політичних конфліктів

Вивчаючи поняття засобів масової інформації, В. Войчук зазначає, що це розгалужена мережа інституцій, які займаються збором, обробкою та розповсюдженням інформації. До цієї мережі входять телевізійні та радіопрограми, газети, журнали, книговидавництва, радіо, інформаційні агентства, документальні фільми тощо. Крім того, сьогодні українське суспільство все активніше використовує Інтернет, що дає змогу органам державної влади налагоджувати зворотній зв'язок із громадянами. Преса, радіо і телебачення являють собою своєрідний «тріумвірат» засобів масової інформації, кожне з яких має ряд особливостей щодо характеру і способів донесення інформації до аудиторії. Проте, поряд із наявністю специфічних властивостей, усі види засобів масової інформації мають дещо спільне – це здатність більш-менш швидко доносити до масової аудиторії вербально-понятійну та емоційно-образну інформацію [12, с. 18].

Характерними рисами засобів масової інформації є:

– публічність (необмежене, знеособлене коло споживачів);

– наявність спеціальних технічних засобів;

– опосередкована, розрізнена в просторі та часі взаємодія партнерів по спілкуванню;

– непостійний характер аудиторії;

– переважний односпрямований вплив від комунікатора до реципієнта [47, с. 390].

Основним завданням ЗМІ є передача інформації споживачам, що відбувається різними способами (преса, радіо, телебачення). Основна мета засобів масової інформації – оперативне інформування окремих людей, соціальні групи населення в цілому про події та явища у світі, конкретній країні, конкретному регіоні. Цієї мети вони досягають шляхом виконання властивих їм соціальних функцій [47, с. 390].

У другій половині XX століття розвинені демократичні країни пережили дві революції у сфері доступу громадян до інформації, результатом яких стала масова освіта та масове телебачення. Значну роль у трансформації політичного простору відіграла поява на інформаційно-політичному ринку електронних ЗМІ, поява діалогічних методів політичної комунікації, різке збільшення швидкості передачі повідомлень, формування «електронних спільнот» (наприклад, користувачів Інтернету) тощо. Ці та пов’язані з ними явища та факти якісно змінили умови та можливості конкуренції за державну владу [51, с. 65].

Сьогодні медіа активно використовуються для розпалювання ненависті, а також критики висловлюваних думок та їх залякування. Інформаційні війни в Інтернеті небезпечні і часто отримують серйозне фінансування від влади. Пропаганда на таких сайтах набагато витонченіша і часто виступає у формі аналітичних, історичних публікацій, новинних публікацій, які нібито надають фактичні докази. Отже, медіа-інструменти в руках дипломатів можуть впливати на динаміку конфліктів і на сприйняття суспільства, впливати на формування колективної ідентичності та політичного курсу в цілому [100, с. 51].

Маніпулюючи суспільною свідомістю через засоби масової інформації, влада досягає своїх цілей. Політична маніпуляція є одним із способів (методів) усунення внутрішньополітичних конфліктів. У широкому розумінні – це дії політичної влади, що використовуються нею для забезпечення її стабільного

функціонування. У вузькому розумінні політичне маніпулювання означає цілеспрямований вплив на суспільну свідомість, насамперед через канали масової комунікації. Зазвичай газети, радіо і телебачення знаходяться переважно в руках політичних сил, які панують у цьому суспільстві. Тому їхні дії спрямовані на стабілізацію існуючої політичної системи. Велика роль засобів масової інформації в реалізації такого прийому усунення конфліктів, як «створення образу ворога». Він полягає в перекладанні відповідальності за невирішені проблеми на інші політичні сили (часто опозиційні, а іноді й міфічні) та відволіканні уваги населення від гострих політичних і соціальних проблем [52, с. 226].

Сучасні ЗМІ мають величезний вплив на свідомість і вчинки людини. З одного боку, ЗМІ публікують інформацію, яка викликає інтерес у аудиторії. З іншого боку, вони транслюють різні цінності, стереотипи, формують громадську думку, будучи основним засобом зміни масової свідомості. Вплив на свідомість людей відбувається не під час безпосереднього контакту, а через засоби масової інформації, які створюють ілюзію об'єктивного подання інформації, а тому мають високий ступінь переконливості [51, с. 66].

У наш час навіть поява таких понять, як «інформаційна війна», «медіа-агресія», «інформаційна безпека» свідчить не лише про тісний зв'язок ЗМІ з конфліктними ситуаціями, а й про те, що в сучасних збройних конфліктах боротьба за інформаційне поле не менш важливе, ніж безпосередні військові дії. Якщо донедавна війна торкалася переважно інформаційної сфери, зокрема журналістики (наприклад, Перша світова війна стала поштовхом для появи та розвитку аналітичної журналістики в США, оскільки американці не могли зрозуміти, як вбивство ерцгерцога Фердинанда спричинив такий конфлікт), то останній іноді спостерігається зворотний зв'язок, причому як на макро-, так і на мікрорівні [51, с. 66].

Сьогодні засоби масової інформації стали найпотужнішим елементом механізму цілеспрямованого конструювання політичних порядків, засобом

побудови необхідних зв'язків і відносин із громадськістю. Інформація, яку надають ЗМІ, ніколи не буває нейтральною, вона репрезентує спроби правлячих еліт створити такий імідж реальності, який їм вигідний і «виправдовує» їхню практичну політику, «упаковану» в стереотипні точки зору, які є вигідними владі та висвітлили лише частину того, що насправді відбувається [36, с. 113].

На нашу думку, вагомий вклад у дослідження засобів масової інформації в конфліктних ситуаціях вклала українська дослідниця О. Гарматій. У свої роботі вона виділила стратегії роботи засобів масової інформації під час конфліктних ситуацій. На її думку, засоби масової інформації – насамперед електронні ЗМІ, телебачення – стали потужною і часто використовуваною зброєю в управлінні збройними конфліктами. Інформаційний аспект сучасних конфліктів планується так само ретельно, як і військовий. ЗМІ відіграють все більшу роль як у виникненні конфліктів, так і в їх перебігу та припиненні. Таким чином, війна – у сенсі максимальної ескалації конфліктної маси – ведеться не лише на землі, а й на сторінках та екранах ЗМІ [17, с. 206].

Однак справжнє протистояння і протистояння, представлене в ЗМІ, не одне і те ж. На практиці існує розбіжність між реальним конфліктом і його відображенням у ЗМІ. Поряд з обов'язковим перенесенням у журналістські матеріали основних характеристик протистояння, конфлікт, відтворений у засобах масової інформації, і життєвий конфлікт відрізнятимуться динамікою та структурою. Вимушена однолінійність конфлікту в мас-медіа компенсується активністю його соціальної функції. Це досягається шляхом взяття всього найсуттєвішого, найхарактернішого і конкретного з подій реального життя. Завдання журналістики – на конкретних життєвих прикладах швидко помітити реальні протиріччя, сформулювати практичну проблему, яка потребує вирішення, вивчення, дослідження, обговорення [17, с. 207].

Досліджуючи дане питання О. Гарматій згадала у роботі теоретика і практика української журналістики В. Здоровега, який відзначав, що чим швидше

будуть помічені суперечності і чим точніше і чесніше відтворені засобами масової інформації, тим більша надія на їх розв'язання й уникнення соціальних, економічних, політичних катаклізмів. У цьому прогностична, «лікувальна» функція мас-медіа. Інше питання, зазначає вчений, чи суспільство хоче прислухатися до цих сигналів преси [28, с. 102].

Майже всі публікації конфліктної тематики мають розгорнуту по дієву сторону, для них характерне детальне викладення конфліктних процесів. Це безпосередньо пов'язано з тим, що конфлікт не працює в «чистому» вигляді: він передається через дії і вчинки сторін. Тому журналістські матеріали про конфлікти фіксують зміну подій, показують динаміку протистоянь. У більшості медіа текстів відтворюється хронологічно послідовне розгортання суперечливих дій і пов'язаних з ними роздумів автора. Стратегія ЗМІ в конфліктних процесах визначається виконанням важливого завдання як посередника між суспільством, громадськими організаціями, окремими громадянами, державними, політичними та владними інститутами – ефективно впливати на свою аудиторію [17, с. 208].

У роботі ЗМІ з конфліктами важливою є тактика запобігання. Вона передбачає обговорення проблеми, оприлюднення точок зору опонентів і думок аудиторії, діалог із читачем, полеміку, надання трибуни спеціалістам, здатним кваліфіковано попередити громадян про можливе протистояння, ця тактика також покликана посилити соціальну компетентність населення [17, с. 210].

ЗМІ використовують такі прийоми вирішення конфліктів:

– розробка власних варіантів управління конфліктом;

– залучення арбітрів – відомих і високоморальних особистостей, спеціалістів;

– надмірне акцентування параметрів конфлікту;

– розгляд конфлікту як частини соціального організму;

– перенесення конфлікту в морально-духовну площину [17, с. 212].

Діяльність засобів масової інформації в рамках вирішення конфліктів спрямована на інформування громадськості про програму антикризових дій у конфліктній сфері, оприлюднення важливих для налагодження відносин документів. Використовуючи концепцію врегулювання, ЗМІ також слідкують за практичними кроками влади, учасників конфлікту, аутсайдерів та всіх причетних, спрямованих на нормалізацію відносин. У рамках цієї тактики ЗМІ також звертаються до констатації конфліктів. Зрозуміло, що потенціал впливу журналістики не повністю реалізується в медійних текстах, які це підтверджують. Проте вони доречні при ознайомленні аудиторії з додатковими деталями вже відомих конфліктних процесів [17, с. 213].

Тактика придушення передбачає силове вирішення конфліктів, а також уникнення конфліктів за об'єктивними критеріями. Такий спосіб дій доцільно використовувати, коли неможливо успішно подолати протидію. Принциповим у реалізації такої тактики є те, що ЗМІ рідко йдуть на придушення конфліктів. Звісно, така тактика управління конфліктом не потребує особливих творчих зусиль журналістів. Проте запропонований шлях може виявитися раціональним з огляду на специфіку конкретного протиріччя. Придушення конфлікту також відбувається шляхом свідомого применшення значення протистояння в ЗМІ. Це може бути за умови, що ЗМІ не ігнорують об'єктивний факт (оскільки, наприклад, подають інформаційні повідомлення про протистояння), а дистанціюються від конфлікту, не подаючи власної інтерпретації події [17, с. 213].

Засоби масової інформації дуже часто працюють і протилежно попередньому – тактиці роздмухування конфліктів. А вплив на розвиток конфліктної ситуації за рахунок такої активності ЗМІ відбуватиметься за принципом «підливання масла у вогонь». Преса, радіо, телебачення, Інтернет-ЗМІ можуть активізувати конфліктні процеси, даючи їм позитивну оцінку – пряму чи приховану. Наприклад, сучасні ЗМІ зазвичай схвалюють різного роду акції протесту, підтримують тих, хто шукає вихід шляхом соціального протесту.

реалізація тактики розпалювання конфлікту може мати дві принципово різні мети. Якщо ЗМІ є однією зі сторін конфлікту, то воно однозначно стурбоване вирішенням конфлікту на свою користь. Натомість для медіа, які опосередковано беруть участь у конфлікті, важливо не усунення фактичної основи конфлікту, а досягнення власної мети, для реалізації якої протистояння є лише середовищем, тлом [17, с. 214].

Соціальні мережі, або, як їх ще називають новітні ЗМІ, відіграють все більшу роль у конфліктах і політичних суперечках. Політики, лідери, повстанці та протестувальники – усі вони використовують соціальні мережі як інструмент для спілкування та поширення інформації. У той же час соціальні медіа зменшують витрати на спілкування, збільшують швидкість і поширення інформації. Нові дані, що надаються соціальними мережами, є не тільки важливим ресурсом, але й принципово змінюють інформацію, доступну учасникам конфлікту, тим самим формуючи сам конфлікт [37, с. 146]

Низка міжнародних організацій розглядає конструктивну роль ЗМІ у вирішенні конфліктів. Все більше визнається, що ефективні ЗМІ є складовою запобігання конфліктам. З'явилося кілька проектів та ініціатив, спрямованих на популяризацію «журналістики миру». Але це створює ситуацію, коли ЗМІ не просто висвітлюють події, а стають їх частиною. Представники ЗМІ стверджують, що суспільство потребує інформації, обміну ідеями та думками в публічній сфері, і що ЗМІ мають бути вільними грати будь-яку роль, яку вони обирають у виконанні цього обов'язку. Твердження про те, що ЗМІ сприяють миру, дає їм відчуття ідеологічно заангажованої журналістики, що нагадує старий Радянський Союз (який завжди прагнув сприяти «миру» у власному розумінні цього терміну) [37, с. 147].

Важко не погодитися з думкою Л. Богуш, що роль ЗМІ полягає саме в тому, щоб зрозуміти конфлікт, пояснити його, повідомити обставини та знайти інші точки зору, а не просто звернутися до тих самих старих джерел і повторити.

однакові причини невдоволення. Журналісти повинні розуміти, чого прагнуть усі сторони конфлікту, які можливі варіанти деескалації, компромісу чи навіть можливого врегулювання конфлікту [9, с. 294].

Отже, слід окреслити основні функції, які виконують ЗМІ у висвітленні військово-політичних конфліктів у світі:

1. Посередницька (ЗМІ можуть виступати посередниками між сторонами конфлікту, допомагаючи вирішувати різні конфлікти, а також налагоджувати контакт між сторонами).

2. Функція об’єктивного висвітлення подій (ЗМІ повинні об’єктивно висвітлювати воєнно-політичні протистояння, досконало розуміючи хід їх подій і позицію супротивників).

3. Моніторингова (завдяки присутності «на місці подій» ЗМІ можуть стежити за кожним кроком учасників конфлікту).

4. Функція формування думок (ЗМІ можуть впливати на суспільні оцінки та думки щодо конфлікту залежно від їх об’єктивності та збалансованості висвітлення подій).

5. Інформаційна підтримка (ЗМІ можуть сприяти поширенню інформації про різноманітні програми та ініціативи, спрямовані на вирішення конфліктів).

6. Маніпулятивна (ЗМІ можуть бути використані для маніпулювання громадською думкою та поширення такої інформації, яка може призвести до подальшої ескалації конфлікту).

7. Функція підтримки сторін конфлікту (ЗМІ можуть підтримувати одну зі сторін конфлікту, повідомляючи новини, які негативно впливають на інших учасників конфлікту) [85, с. 106].

Роль ЗМІ у ретрансляції військово-політичних конфліктів визначається низкою факторів, серед яких можна виділити:

1. Інформаційний запит суспільства. Громадяни мають право на інформацію про події, що відбуваються у світі, зокрема, про військові конфлікти. ЗМІ дають можливість отримати цю інформацію [85, с. 106]

2. Важливість суспільного розуміння подій, що відбуваються. Військово-політичні конфлікти можуть мати великий вплив на життя людей, тому розуміння їх природи є важливим.

3. Важливість об'єктивної та достовірної інформації. Військові конфлікти можуть мати значні наслідки, тому важливо, щоб інформація, яку отримують громадяни, була об'єктивною та достовірною.

4. Важливість публічності. ЗМІ можуть відігравати важливу роль у забезпеченні гласності та прозорості військових конфліктів.

5. Важливість контролю над владою. ЗМІ можуть бути важливим інструментом контролю за владою та її діяльністю в умовах військового конфлікту.

6. Роль ЗМІ у формуванні громадської думки. ЗМІ можуть впливати на громадську думку щодо військових конфліктів та їх вирішення.

7. Медіа як засіб ведення діалогу та вирішення конфліктів. ЗМІ можуть стати важливим інструментом залучення різних сторін конфлікту до діалогу та вирішення проблем на умовах мирного врегулювання [85, с. 107].

Вивчаючи подану проблематику слід згадати про довіру суспільства засобам масової інформації. В демократичному середовищі питання незалежності ЗМІ, відсутність впливу та контролю влади на журналістів є край важливим аспектом. В країнах, де ЗМІ є залежними від влади чи певних партійних організацій зіштовхуються з контролем їх діяльності та низькою довірою серед громадян.

В Україні у 2023 році було проведено соціологічне опитування USAID-Internews щодо споживання українського медіа, ставлення та довіру серед населення. Дослідження проводило InMind на замовлення міжнародної організації Internews, яка реалізує проект «Медійна програма в Україні» за фінансової

підтримки Агентства США з міжнародного розвитку (USAID). У 2023 році споживання новин майже в усіх видах ЗМІ залишилося на рівні минулого року, за винятком споживання ТБ, яке продовжує скорочуватися. 47% українців використовують кілька джерел новин. Ті, хто користується лише одним джерелом, як правило, віддають перевагу соціальним мережам. У 2023 році зріс рівень довіри як до національного, так і до регіонального радіо та друкованих ЗМІ. Основними причинами зростання довіри до радіо є зникнення проросійських станцій, відсутність російської музики та збільшення присутності новинного контенту на музичних станціях [93]. Більш детальна інформація щодо довіри медіа зображено графічно в додатку А; основна аудиторія різних каналів медіа та рівень медіаграмотності графічно зображено в Додатку Б.

Як повідомляє Громадська мережа ОПОРА, результати соціологічного дослідження «Медіаспоживання українців: третій рік повномасштабної війни» містять такі результати:

– у 2023 році рівень довіри до більшості джерел інформації поступово зростав, але в 2024 році люди стали менше довіряти всім джерелам;

– зростає кількість респондентів, які не довіряють жодному джерелу інформації (5,2% у 2022 році; 7,7% у 2023 році; 15,2% у 2024 році);

– найбільше втратили довіру громадян телебачення (34,1% у 2024 році проти 61,1% у 2023 році) та радіо (24,2% проти 41%);

– довіра до друкованих ЗМІ знизилася з 30,3% у 2023 році до 18% у 2024 році;

– найбільше українці довіряють новинам із соціальних мереж (47,3%), але довіра до них теж знизилася (з 60% у 2023 році до 47,3% у 2024 році);

– інтернету без соціальних мереж довіряють 43% українців (на 5,8% менше, ніж у 2022 році) [44].

У тому ж опитуванні ОПОРИ йдеться, що 73,4% українців використовують соціальні мережі як джерело новин. Це на 4,5% менше, ніж минулого року. Найпопулярнішими є Telegram (78,1%), YouTube (59,5%) і Facebook (44,6%) [44].

Отже, засоби масової інформації є сполучною ланкою між суспільством та державою для комунікації та передання інформації, ЗМІ інформує суспільство про ті чи інші процеси в країні та світі. Засоби масової інформації подають новини на запит суспільства про різні події, трактують мало зрозумілі факти, формують та висловлюють громадську думку, а також можуть бути важливим інструментом для діалогу між ворогуючими сторонами.

2.2 Методи та засоби ведення інформаційних війн в XXI столітті

Інформаційні війни ведуться з використанням певних засобів, способів, прийомів, технологій тощо, але обов'язково множинних, спільних, на різних рівнях, оскільки інформаційне середовище з його інформаційними потоками та різними видами інформаційних впливів характеризується низкою динамічних факторів, які мають прямий вплив на людину або можуть мати непрямі, негайні чи відстрочені наслідки. ЗМІ стали особливими каталізаторами та носіями інформаційних війн. Критичний дискурс щодо цієї нової медіа реальності, інспірований державами, які підтримують агресивну геополітику, також базується на досягненнях психології, представленому нею комплексі знань про модифікацію психіки людини-адресата, маніпулятивні техніки як складову комунікаційних технологій [25, с. 189].

Інформація завжди відігравала ключову роль у житті суспільства і держави. З давніх-давен могутні державні діячі розуміли, що володіння інформацією дає перевагу над іншими, уможливлює перемогу, підкорення та ефективний контроль. На сьогоднішній день реальна влада належить тому, хто формує інформаційні потоки та керує ними. В епоху XX століття інформаційні війни виходять на

перший план не тільки у військовому, а й у мирному житті, і якщо, за визначенням Клаузевіца, війна – це продовження політики іншими засобами, то сьогодні ми маємо політику як продовження війни іншими засобами. Інформаційний простір став полем великих баталій між країнами, політичними групами тощо [13, с. 37].

Поняття «інформаційна війна» трактується як «широкомасштабна боротьба в інформаційному просторі із застосуванням методів, прийомів, методів, каналів і засобів маніпулювання психікою людей, насамперед їх індивідуальною та суспільною свідомістю та колективним несвідомим, з метою досягнення цілей і вирішення завдань суб'єкта впливу через трансформацію світогляду мас» [29, с. 35].

З'явившись наприкінці 1980-х років термін «інформаційна війна» швидко набув популярності. З часом виникла велика кількість трактувань інформаційної війни, що призвело до плутанини в розумінні цього явища. Термін «інформаційна війна» зазнав значної еволюції, часто піддаючись спробам адаптувати його до конкретних інформаційних атак бойовиків. Тому актуалізується проблема з'ясування поняття інформаційної війни в умовах повномасштабної війни російської федерації проти України [86, с. 3].

Українські дослідники М. Кіца та Г. Свинаренко стверджують, що інформаційну війну слід трактувати як форму інформаційної боротьби між різними суб'єктами (державами, неурядовими, економічними чи іншими структурами), яка передбачає здійснення комплексу заходів із заподіяння шкоди інформаційній сфері протилежної сторони та захистити власну інформаційну безпеку. Вони висвітлюють відмінності в поняттях «інформаційна війна» та «інформаційний конфлікт».

У широкому розумінні інформаційна війна – це форма боротьби, яка поєднує в собі сукупність спеціальних (політичних, економічних, дипломатичних, технологічних, військових та інших) способів, способів і засобів благотворного

впливу на інформаційну сферу об’єкта інтересу та захисту власного в інтересах досягнення поставлених цілей [38, с. 71].

У вужчому розумінні інформаційна війна (у військовій та оборонній сферах) – це комплекс інформаційних заходів, що здійснюються з метою захоплення та утримання стратегічної ініціативи, досягнення інформаційної переваги над противником і створення сприятливої пропагандистської бази під час підготовки ведення бойових та інших заходів збройних сил.

Інформаційний конфлікт дослідники називають «війною без оголошеної лінії фронту», оскільки він складається з комплексу операцій, які практично неможливо відстежити та виявити. Таким чином, поняття інформаційного конфлікту є ширшим, і поняття інформаційної війни включається як одна з двох його складових [38, с. 71].

В. Антонюк вважає, що цілями інформаційної війни можуть бути:

– запобігання можливому військовому конфлікту;

– ослаблення морального духу особового складу збройних сил і мирного населення противника;

– впровадження у суспільну та індивідуальну свідомість ворожих, шкідливих ідей і поглядів;

– дезорієнтація і дезорганізація мас, внесення безладу в інформаційну мережу противника;

– послаблення патріотичних переконань і національних традицій;

– провокація та підбурювання до відмови від участі в бойових діях;

– залякування свого народу «образом ворога»;

– залякування опонента своєю владою;

– створення передумов для досягнення намічених військово-політичних цілей з мінімальними людськими та матеріальними втратами [2, с. 4].

Основними принципами інформаційної війни є:

– відповідність його цілей і завдань політичним цілям війни;

– необхідність зосередження сил у вирішальному місці і у вирішальний момент;

– всебічна та завчасна підготовка сил і засобів інформаційної боротьби;

– принцип високої активності та рішучості в ході інформаційної боротьби;

– принцип узгодженого спільного застосування різних видів сил і засобів інформаційної боротьби;

– принцип раптових інформаційних шоків;

– постійна готовність сил і засобів інформаційної боротьби до захисту власної інформації та руйнівного впливу на інформаційне середовище противника;

– безперервність інформаційної війни;

– ведення інформаційної війни з напругою, необхідною для виконання поставлених завдань;

– своєчасне маневрування силами та засобами інформаційної боротьби;

– врахування духовного чинника в інтересах виконання поставлених завдань;

– комплексне розгортання, забезпечення боєздатності та своєчасне відновлення Збройних Сил і засобів інформаційної боротьби;

– стійкість і безперервність управління силами і засобами інформаційної боротьби;

– наполегливість у досягненні поставлених цілей;

– виконання рішень і поставлених завдань [92, с. 287-291].

До основних інструментів гібридної війни належать такі інформаційні заходи:

– засоби військово-політичної дезорієнтації противника;

– дезінформація про власні ресурси;

– дії, спрямовані на розгром або блокування каналів передачі даних з метою дезорієнтації та дезорганізації;

– створення атмосфери напруги в суспільстві від постійного очікування ударів і масованого наступу по всій лінії фронту;

– вплив на масову свідомість з метою деморалізації та поширення паніки [94, с. 70].

Найпоширенішим методом є пропаганда, яка передбачає поширення в масах і роз'яснення будь-яких вірувань, ідей, вчень, знань. До основних прийомів пропаганди відносяться: формування в масовій свідомості образу жертви з діяча, який насправді є злочинцем, перекладання відповідальності та приписування власних злочинів супернику, ігнорування фактів і таврування всіх, хто не погоджується з пропагандою [94, с. 71].

До основних методів деструктивного інформаційного впливу зазвичай відносять: фізичне блокування систем зв'язку та телекомунікацій, дезінформацію, маніпулювання, навіювання, пропаганду, диверсифікацію громадської думки, залякування, психологічний та психотропний тиск, поширення чуток [15, с. 86].

До основних засобів інформаційної боротьби відносяться:

1) приховування інформації;

2) спотворення інформації;

3) кількісне збільшення повідомлень певного типу;

4) відволікання уваги від важливого на неважливе [15, с. 87].

Кожен із цих інструментів має велику кількість варіантів застосування та по-різному використовується в текстових або відео- та аудіоповідомленнях.

Інформаційні впливи за допомогою текстових повідомлень здійснюються таким чином:

1. Замовчування.

2. Подання неправдивого факту, поєднання правдивих і неправдивих фактів і коментарів.

3. Представлення випадкових явищ як типових і системних.

4. Зміщення акцентів у повідомленні шляхом пропусків, виділення маніпулятивних рубрик, заголовків, виділених цитат.

5. Введення в оману шляхом некоректного посилання на джерела повідомлення (наприклад, завуальовані натяки на авторитет – «інформація отримана з достовірних джерел»), оприлюднення фактів, отриманих з неофіційних та недостовірних джерел.

6. Використання розбіжностей у часі (використання фактів про минулі події для підтвердження повідомлень про сучасні реалії; згадування фактів минулого та їх перекручування на підставі того, що ніхто не пам’ятає деталей; спотворення хронології подій).

7. Замовчування повідомлень про важливі факти другорядними або створення строкатої мозаїки повідомлень про актуальні та неактуальні події з метою ускладнення формування пріоритетів реципієнтом.

8. Збільшення частоти відтворення повідомлень на одну і ту ж тему.

9. Використання певних дратівливих слів із виразною позитивною чи негативною конотацією – «правда», «свобода», «демократія», «патріотизм», «зрада», «фашизм», «корупція»; звернення до почуттів та спекуляції на очікуваннях – «благополуччя вдома», «стабільність», «впевненість у завтрашньому дні», «гордість за батьківщину».

10. Використання штампів (наприклад, «глобальні проблеми», «захист інтересів»).

11. Навішування ярликів (наприклад, «хунта», «країна, що не відбулася»).

12. Приховування змістовності чи потенційно небезпечного змісту повідомлення за допомогою поетизмів – метафор, порівнянь, гіпербол, риторичних запитань, окличних речень, емоційно забарвленої лексики.

13. Використання дієслівних форм, наприклад дієслів наказового способу, для спонукання до прямої дії («голосуй», «не спи», «вирішуй») [15, с. 87].

14. «Гіпнотизування» реципієнтів термінами, неологізмами, запозиченнями, точне значення яких часто не відоме не лише широкій аудиторії, а й самим ораторам.

15. Нав'язливе обговорення протягом певного часу обмеженої кількості топ-тем (їх називають «ідея дня», «топ-теми тижня», «медіа-порядок денний» тощо).

16. Змішання художніх образів і дійсності (апелювання до відомих літературних творів, фільмів, творів мас-медійної культури) або використання ментальних стереотипів, національних символів тощо.

17. Домінування негативних чи трагічних новин, залякування небезпеками військового, екологічного, економічного характеру [15, с. 88].

Інформаційні впливи за допомогою зображень, відео чи аудіозаписів здійснюються у такий спосіб:

1) з використанням фрагментів записів минулих років або будь-яких матеріалів про події в іншій країні для ілюстрації актуальних новин у країні – жертві інформаційної агресії (наприклад, реальні висловлювання політиків щодо подій 2010 року подаються як актуальний коментар до подій 2018 року; так само і з репортажами про події);

2) подання правдивого фрагмента запису як ілюстрації маніпулятивного коментаря;

3) спотворення змісту шляхом вилучення окремих фрагментів;

4) накладання на відеоряд дубляжу, перекладу, титрів, які містять текст, який насправді не проголошувався [15, с. 88].

Методи впливу росії на Україну в інформаційному просторі досліджували О. Джус. У своїй роботі він приділив увагу поширенню ідей російської політики щодо інформаційної політики, а саме впливу на міжнародні ЗМІ на період 2017-

2030 років. Серед основних завдань ведення інформаційної боротьби виділяються: створення умов для популяризації російської культури і науки за кордоном, у тому числі для протидії спробам спотворення і фальсифікації історичних та інших фактів; налагоджувати стійкі культурно-освітні зв'язки з сучасниками, які проживають за кордоном як іноземні громадяни та особи без громадянства, для яких російська мова є рідною, у тому числі на основі інформаційно-комунікаційних технологій. На практиці це означає використання пропагандистських ЗМІ за кордоном для поширення спотвореної кремлівської ідеології. Ця політика росії була досить успішною у східних областях України та Криму. росія завжди покладала на ЗМІ особливу місію, розглядаючи їх як інструмент підтримки своїх інтересів. Телебачення, кіностудії, радіо та інші засоби масової інформації вважалися важливими складовими національної безпеки. Про це свідчить, зокрема, створення так званого Центру інформаційної боротьби – управління в структурі окупаційних військ російської федерації в Україні, створеного керівництвом генштабу російської федерації для посилення ефективність інформаційної війни проти України. Основними напрямами діяльності цього центру були: дискредитація політичного керівництва та командування Збройних Сил України, формування до них недовіри; формування думки про поширення расизму та міжнаціональної нетерпимості в Україні; переконати міжнародне співтовариство в систематичному порушенні українською владою режиму припинення вогню та прихованому нарощуванні сил і засобів Збройних Сил України вздовж лінії розмежування з метою відновлення активних бойових дій; деморалізація українських військовослужбовців; формування антиукраїнських настроїв у населення тимчасово окупованих територій України [25, с. 194-195].

Отже, методи та засоби інформаційної війни покликані створити сприятливі умови для досягнення своїй цілей на інформаційному полі. Часто в інформаційному протистоянні використовують такі методи як: замовчування,

навіювання, дезінформація, залякування, пропаганда, поширення чуток тощо. Вдало вибрані засоби та методи дають можливість переваги впливу на суспільство на державну владу. Таким чином, питання забезпечення інформаційної безпеки стає критично важливим для сучасної України, особливо в умовах триваючої війни. Сьогодні Україна стала так званим «полігоном» для застосування новітніх форм та методів інформаційних війн з боку росії. Тому важливо не лише вміло протистояти наявним загрозам, а й вміти передбачати можливий розвиток подій.

РОЗДІЛ 3. ЗАРУБІЖНИЙ ТА УКРАЇНСЬКИЙ ДОСВІД ЩОДО ПОБУДОВИ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ ТА ШЛЯХИ ЇЇ ВДОСКОНАЛЕННЯ

3.1 Досвід розвитку інформаційної політики та її безпеки на прикладі США

В аспекті забезпечення інформаційної безпеки США можна вважати піонерами, адже це не лише держава, яка вперше у світі запровадила електронне урядування з використанням новітніх інформаційних технологій, а й створила спеціальну систему захисту національного інформаційного суверенітету та безпеки інформаційних ресурсів.

Переходячи безпосередньо до характеристики системи американської моделі управління інформаційною безпекою, слід зазначити, що в США існує кілька інституцій із забезпечення інформаційної безпеки: Агентство національної безпеки (NSA), Національне управління кібербезпеки США, Міністерство внутрішньої безпеки США, Федеральне бюро розслідувань (ФБР), Центральне розвідувальне управління (ЦРУ). Слід зазначити, що серед державних інституцій із забезпечення інформаційної безпеки АНБ також розвиває партнерство з приватним сектором та науковими інституціями у формі планування заходів протидії загрозам у недержавних комп'ютерних мережах (таким чином держава бере участь у захисті найважливіших приватних телекомунікаційних, електричних, банківських мереж (телекомунікації, електромережі, банківські мережі, Інтернет-провайдери). АНБ залучає приватні установи та громадські організації (CERT, ISACA, CSX, CCSIS) [102, с. 108].

Слід зазначити, що вже на початку нинішнього століття гарантуванням інформаційної безпеки займається понад 150 державних організацій та багато приватних структур США. Усі ці заходи координує АНБ, але головною

інституцією, відповідальною за державне регулювання інформаційної безпеки, є президент [82, с. 77].

Сучасна організаційно-правова база збереження інформаційної безпеки США, яка гарантує безпеку інформаційно-оборонної системи, з'явилася після Другої світової війни, саме тоді, коли американська інформаційна система стала об'єктом деструктивного впливу радянської пропаганди. Ця правова база охоплює федеральні закони та закони штату. Незважаючи на відмінності між цими законами, в США існує загальне розуміння того, що інформаційна безпека держави є важливою для безпеки кожного громадянина [82, с. 77].

Досить ґрунтовно в законодавстві врегульовано питання щодо:

– забезпечення безпеки інформації в державних комп'ютерних системах (Закон «Про комп'ютерну безпеку», Закон «Про удосконалення рівня інформаційної безпеки»);

– протидії комп'ютерній злочинності (Закон «Про комп'ютерне шахрайство та зловживання», Закон «Про зловживання комп'ютерами»);

– регулювання співвідношення прав громадян на отримання інформації (Закон «Про свободу інформації», Закон «Про висвітлення діяльності уряду», «Про право на фінансову таємницю»);

– конфіденційності їх приватного життя (Закон «Про охорону особистих таємниць», «Про таємницю») [30, с. 99].

У монографії І. Арістова автор аналізує розвиток інформаційної безпеки після Другої світової війни. З його роботи доречно виділити той факт, що в США після Другої світової війни розвиток мереж здійснювався з ініціативи адміністрації президента та за значної фінансової підтримки з коштів державного бюджету. У сучасних умовах за ініціативи американського президента розгортається новий виток розвитку національної інформаційної інфраструктури, який викликаний прагненням зміцнити позиції США як найбільш розвиненого

інформаційного суспільства у світі. Основна проблема, з якою довелося зіткнутися американцям у сфері інформаційної концепції, це відповідальність, тобто у визначенні суб'єкта, відповідального за надання інформації. Основною ідеєю, на якій базується американська інформаційна концепція, є «наповнення» інформацією ЗМІ. І з цим важко не погодитись. У Сполучених Штатах інформаційне право в основному є концептуальною основою для інтелектуальної власності та авторського права. Тобто одне з головних питань – хто має право на інформацію. І звідси логічно випливає така проблема: власник інформації має відповідати за неї [3, с. 137].

Інформаційну безпеку та інформаційне домінування по праву можна назвати ключовими напрямками економіко-технологічного, науково-промислового та військово-політичного лідерства США у світі. Державна політика США у сфері інформаційної безпеки пройшла тривалий еволюційний шлях, який складається з чотирьох етапів:

1 етап: виникнення – 1939-1947 рр.;

2 етап: становлення – 1947-1982 рр.;

3 етап: активний розвиток – 1983-2001 рр.;

4-й етап: фундаментальне вдосконалення – 2001-по теперішній час [96, с. 111].

Національна безпека США зазвичай визначається документом під назвою Стратегія національної безпеки США (далі – NSS), який розробляється окремо адміністрацією кожного нового президента та об'єднує зовнішню політику, національну оборону, міжнародні економічні відносини та політику допомоги у розвитку [96, с. 112].

У 1993 р. уряд США одним із перших оприлюднив доповідь про плани розвитку національної інформаційної інфраструктури (Agenda for Action). Для вивчення проблем, пов'язаних із розбудовою національної інформаційної

інфраструктури, було створено робочу групу з питань інформаційної інфраструктури (Information Infrastructure Task Force).

На той час основними принципами державного регулювання інформаційної інфраструктури були:

1) заохочення приватних інвестицій;
2) концепція загального доступу;
3) сприяння технологічним інноваціям;
4) забезпечення інтерактивного доступу;
5) захист особистого життя, безпека та надійність мереж;
6) покращення управління радіочастотним спектром;
7) захист прав інтелектуальної власності;
8) координація зусиль держави;
9) забезпечення доступу до державної інформації [97, с. 15].

З 2001 року, коли тодішній президент США Д. Буш під час виступу перед співробітниками ЦРУ вказував, що забезпечення інформаційної безпеки є головним пріоритетом у забезпеченні національної безпеки Сполучених Штатів, починається реалізація федеральних державних програм із захисту національного інформаційного середовища в комп'ютерних мережах країни. Метою таких програм є створення всебічно сприятливих умов для отримання та обробки спецслужбами інформації про загрози інформаційному потенціалу публічних адміністративних установ з боку інших держав та осіб. Окрім негласної інформаційної діяльності, значна увага приділяється систематичному аналізу відкритих джерел та вилученню інформації з конфіденційних баз даних за допомогою комп'ютерних технологій. Це призвело до формування нормативно-правової бази боротьби з кіберзлочинністю [102, с.109].

У 2003 р. було введено у дію Національну стратегію безпечного кіберпростору. Пізніше – Огляд політики кібербезпеки (2009 р.), Міжнародну стратегія для кіберпростору (2011 р.), Директива Президента США «Щодо

Проекту стратегії покращення кібербезпеки критично важливих об’єктів інфраструктури (2013 р.), Проект стратегії покращення кібербезпеки критично важливих об’єктів інфраструктури (2014 р.), Закон про кібербезпеку та обмін інформацією (2015 р.), Національна стратегія безпеки (2015 р.), Стратегія кібербезпеки Департаменту оборони (2015 р.) [102, с. 109].

За часів президентства Барака Обами цифрова інфраструктура США була оголошена «стратегічною національною цінністю», а захист цієї інфраструктури – національним пріоритетом [102, с. 109].

У 2010 році президент США підписав «Ініціативу зі всеосяжної національної кібербезпеки», яка органічно доповнювала Військову доктрину США. Розпочато створення універсальної федеральної мережі захищених каналів зв’язку, яка об’єднає всі центри оперативного реагування на кіберзагрози та хакерські атаки. Також у центральних урядових установах США були створені спеціальні підрозділи кіберконтррозвідки з метою виявлення посягань на державні інформаційні мережі та запобігання терористичним атакам. Також розроблено систему управління ризиками для прогнозування ймовірних наслідків несанкціонованого втручання в інформаційні мережі державних установ. Впроваджено роботу програми спеціальної програмної платформи «Einstein», яка призначена для виявлення втручання у державні інформаційні мережі [102, с. 110].

Політика захисту інформації спрямована навіть на захист відкритої інформації, яка доступна в соціальних мережах. У США хакерські атаки прирівнюються до оголошення війни цій країні, що тягне за собою жорсткі заходи відповідальності та негативні наслідки для країн, які намагаються зламати інформаційні системи США. Високий рівень захисту найважливіших об’єктів інфраструктури, задіяних в інформаційно-комунікаційній сфері [35, с. 8].

Враховуючи те, що інформаційна індустрія є основним стратегічним рушієм конкуренції та провідним сектором економіки, інформаційна політика Сполучених Штатів охоплює широкий спектр діяльності уряду, спрямованої на створення та

управління інформаційними технологіями. Одним із ключових напрямів розвитку американської інформаційної безпеки, як і в інших країнах, є гарантування національної безпеки та безпеки інформаційних систем «силових» відомств: збройних сил та зовнішньої розвідки [82, с. 79].

В рамках розпорядження президента від 11 травня 2017 року №13800 «Посилення кібербезпеки федеральних мереж і критичної інфраструктури» було розроблено нову Національну кіберстратегію (The National Cyber Strategy of the USA – далі NCS), яка була опублікована у вересні 2018 року. Даний документ містить цілі, подібні до тих, що поставлені у попередніх схожих документах: політикою у сфері кіберпростору адміністрації Б. Обами 2009 та Національною стратегію безпеки Дж. Буша 2002 щодо безпеки кіберпростору. Однак, незважаючи на схожість з планами попередніх адміністрацій, NCS Д. Трампа знову викликала критичні відгуки зі сторони його опонентів, оскільки замість того, щоб продовжувати концепцію зміцнення захисних технологій і мінімізувати вплив інформаційних загроз, адміністрація президента планувала посилити наступальні попереджувальні кібероперації та змусити інші країни боятися притягнення до відповідальності за свої дії у відповідь на такі кібератаки зі сторони США. Також критики звернули увагу на той факт, що дана стратегія жодним чином не вказує на можливості щодо захисту виборів від інформаційних загроз, що є надзвичайно актуальним в світлі подій 2016 р. [96, с. 112].

Остання редакція американської національної інформаційної стратегії відбулася у березні 2018 р.. У ній відповідальність за забезпечення критичної інфраструктури нації та управління ризиками кібербезпеки розподіляється між приватним сектором та Федеральним Урядом. У документі, визначено пріоритетність діяльності по зменшенню ризиків у семи ключових сферах: національна безпека (інформаційна безпека у т.ч.) енергетика та потужності, банківська справа і фінанси, охорона здоров’я і безпека, зв’язок, інформаційні технології та транспорт [18, с. 44-45].

Національна стратегія кібербезпеки США базується на п’яти принципах: захист, виявлення, реагування, обмін і відновлення. Для реалізації стратегії було засновано Центр кібербезпеки Національного інституту стандартів і технологій США та інші центри кібербезпеки для підтримки розробки стандартів, норм і методів безпеки. Наприклад, Федеральне агентство з кібербезпеки та інфраструктури (CISA) діє для забезпечення захисту інфраструктури США від кібератак, промислового шпигунства та інших загроз [10, с. 399].

У США велику увагу приділяють забезпеченню інформаційної безпеки неповнолітніх. Як відомо, діти та підлітки можуть мати більш підпорядкований маніпулятивний вплив, що свідчить про несформовану свідомість та необізнаність з певними аспектами політичних процесів, інформаційних ресурсів, фейкової інформації тощо. Тому захист дітей від негативного інформаційного впливу є однією з прерогатив усіх навчальних закладів. Особливо це видно на прикладі США. По-перше, Закон про захист дітей в Інтернеті (Children’s Internet Protection Act – скорочено CIPA) є обов’язковим для всіх шкіл, який вимагає від навчальних закладів використовувати спеціалізовані комп’ютерні програми, «фільтри» для блокування доступу шкільного обладнання до деяких загрозливих сайтів. Системним адміністраторам шкіл надано право контролювати відвідування сайтів і сторінок школярів з обов’язковим повідомленням адміністратора про інформаційні порушення. Використання особистих гаджетів під час занять у державній школі заборонено, а відповідальність за доступ учня до забороненої інформації покладається на батьків. По-друге, у ряді випадків адміністрація школи неповнолітній кваліфікується як особа, яка несе повну відповідальність за свої дії. На фоні стереотипних уявлень багатьох українців про демократію в США їх би здивував той факт, що в ряді шкіл Каліфорнії на початку навчального року кожен старшокласник дає розписку про те, що він усвідомлює сутність інформаційних злочинів, що він поінформований, що дозволено, а що заборонено робити в освітньому середовищі, що готовий понести покарання, в тому числі й за

рішенням суду, за порушення шкільного розпорядку та вчинення інформаційних проступків [91, с. 65].

Отже, інформаційна політика США має великий досвід свого становлення та розвитку, й продовжує надалі розвиватися і забезпечувати свою стабільність на інформаційному просторі. Адже, безпека інформаційного середовища – це безпека держави та кожного громадянина.

3.2 Європейський досвід інформаційної політики у військово-політичних умовах

Історію розвитку інформаційного суспільства в Європейському Співтоваристві можна почати з 1979 року, коли відбулася Європейська Рада в Страсбурзі, на якій вперше було заявлено, що інформаційні технології мають широкі соціальні та політичні наслідки для Співтовариства. Надалі Європейський Союз розпочав активну політику у сфері формування та регулювання інформаційного суспільства, встановлення норм і стандартів функціонування держав в інформаційному просторі [19, с. 93].

Основні пріоритети реалізації інформаційної політики Європейського Союзу:

– формування у громадян умінь використовувати нові інформаційні засоби та прикладні завдання;

– завчасне залучення громадян до розробки нових додатків і послуг, щоб вони стали корисними для них у повсякденному житті;

– використання нових технологій з метою залучення людей до процесів прийняття рішень і надання їм можливості знати, що робить їхній уряд, тим самим гарантуючи плюралізм і відкритий доступ до інформації [97, с. 18].

Серед основних документів, які регламентують цифрову трансформацію об’єднання, слід відзначити такі:

– «Європа і глобальне інформаційне суспільство» (The Bangemann Report, 1994 р.) [107], у якому вперше сформульовано напрями створення інформаційного суспільства, крім того, цей документ став основою для подальших стратегій і законодавчих актів, спрямованих на цифрову трансформацію;

– «Зелена книга» Living and Working in the Information Society: People First (1996) [106] окреслила підходи до подальшого розвитку інформаційного суспільства;

– ініціатива eEurope: An Information Society For All (2000) [104] була спрямована на прискорення цифровізації Європи, забезпечення доступу до Інтернету для всіх громадян, розвиток електронного урядування (e-governance) та підвищення цифрової грамотності;

– Директива про захист даних (1995) стала основоположним документом ЄС у сфері захисту персональних даних, у подальшому (2018 р.) була замінена на Загальний регламент про захист даних (GDPR);

– Стратегія i2010 (2005) передбачала заходи для створення єдиного європейського інформаційного простору;

– Europe2020: Цифровий порядок денний для Європи (2010 р.) визначав напрями подальшої цифрової трансформації [19, с. 25].

Основні принципи інформаційної політики ЄС можна умовно поділити на три групи, взявши за головний критерій інтереси та цінності трьох ключових сторін: суспільства в цілому, національних держав та 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)».

Окінавська хартія інформаційного суспільства 2000 р. стала документом, у якому світове співтовариство визнає міжнародну інформаційну безпеку необхідною умовою існування людства, закликаючи до розробки спільної стратегії побудови інформаційного суспільства, і це факт тепер поза сумнівом. Щодо поняття «інформаційна безпека» існує багато підходів і не вироблено жодного загальноприйнятого визначення [7, с. 31].

2000 рік став визначальним для ЄС, оскільки відбулися дві важливі події. Першим із них стало підписання у березні главами держав і урядів країн-учасниць Європейського Союзу Лісабонської стратегії (Lisbon Strategy), яка визначила мету перетворення Європейського Союзу на найбільш конкурентоспроможну економіку світу. Вирішення завдань, визначених цією Стратегією, передбачало використання потенціалу новітніх ІКТ. Для досягнення задекларованих цілей Лісабонської стратегії було прийнято два важливі документи ЄС [8, с. 518]

Другою подією став саміт «Великої вісімки» на Окінаві в липні 2000 року. На ньому вперше було офіційно оголошено про перехід світової спільноти до глобального інформаційного суспільства. Окінавська хартія глобального інформаційного суспільства встановлює загальні принципи входження держав у глобальне інформаційне суспільство і є найважливішим документом, покликаним «організувати та активізувати діяльність міжнародного співтовариства у сфері формування глобального інформаційного суспільства» [8, с. 519].

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. У документі використовується термін «мережева та інформаційна безпека», який 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 [90, с. 172].

10 березня 2004 р. створено Європейське агентство з питань мережевої та інформаційної безпеки (ENISA), яке є єдиним агентством у ЄС, якому визначено конкретний термін завершення його дії у 2020 р. Це агентство функціонувало з 1 вересня 2005 р., знаходилося в м. Іракліон, Крит, Греція. Метою ENISA було вдосконалення інформаційної та мережевої безпеки в ЄС. Воно допомагало Єврокомісії, державам-членам ЄС і приватному сектору забезпечувати виконання вимог інформаційної безпеки, контролювати дотримання чинного та майбутнього законодавства ЄС. ENISA надавало консультації як для держав-членів, так і для інституцій ЄС із питань, пов'язаних з інформаційною безпекою [90, с. 172].

Практичне формування автономної кіберполітики ЄС розпочалося лише після затвердження в лютому 2013 р. Стратегії кібербезпеки «Стратегія кібербезпеки Європейського Союзу: відкритий та безпечний кіберпростір». З тих пір розпочався інтенсивний розвиток політики ЄС щодо кіберпростору в усіх його вимірах:

- цифрова економіка;
- мережева та інформаційна безпека;
- боротьба з кіберзлочинністю;
- спільна зовнішня політика і політика безпеки;
- кіберзахист [20, с. 7].

Це стосується співпраці ЄС з іншими суб'єктами безпеки, насамперед з НАТО.

За результатами аналізу даних за 2019-2020 роки Агентство з кібербезпеки ЄС представило список із 15 основних типів кібератак (у порядку кількості виявлень). Серед суб'єктів кібератак Агентство з кібербезпеки ЄС включило

представників організованої злочинності (60% кібератак), держави (14%), інсайдерів (10%), системних адміністраторів (8%), користувачів (4%), інші (2%). Такі дані демонструють системний характер організації та реалізації кіберзлочинності на міжнародному рівні.

Національне законодавство країн зазвичай регулює такі питання: захист персональних даних (Нідерланди, Естонія, Швеція, Фінляндія, Іспанія); захист електронної комерції та безпека електронних транзакцій та платіжних інструментів (Польща, Естонія, Італія); безпека важливої інфраструктури та інформаційних систем (Франція). Кіберстратегія багатьох європейських держав допускає не тільки оборонні, а й наступальні дії в кіберпросторі.

Політика ЄС у сфері кібербезпеки, незважаючи на очевидний прогрес, досягнутий за останні роки, все ще має проблеми з функціонуванням. Перш за все, бракує необхідної координації. Це очевидно як на нормативному, так і на інституційному рівнях. ЄС зіткнувся з проблемою нестачі кваліфікованих спеціалістів у сфері ІКТ, особливо експертів у сфері кібербезпеки. У традиційному вимірі (так звана «жорстка сила») повна стратегічна автономія ЄС, пов'язана з наявністю власних можливостей кіберзахисту, досі не є нереалізованою. Держави-члени визнають необхідність зміцнення своїх ресурсів, але не хочуть ділитися своїми можливостями. Крім того, потенціал окремих держав дуже різноманітний. У сфері можливостей кіберзахисту європейські держави віддають перевагу співпраці та розподілу завдань між ЄС і НАТО, тоді як дії ЄС здебільшого вважаються взаємодоповнювальними [20, с. 7].

В умовах цілеспрямованої та послідовної атаки на свідомість громадян країн-членів Євросоюз був змушений активізувати свої дії в інформаційному полі та зміцнити захист від негативних зовнішніх впливів (зокрема росії). У вересні 2015 року Оперативна робоча група ЄС зі стратегічних комунікацій – East StratCom Task Force розпочала свою роботу, заснувавши проєкт EUvsDisinfo з метою підвищення обізнаності та розуміння громадськістю російських операцій з

дезінформації. У 2016 році Європейський центр цінностей запустив проєкт Kremlin Watch з метою щоденного моніторингу та аналізу дезінформації та її спростування. Саме ці ресурси регулярно виявляють дезінформаційні повідомлення та публікують їх спростування [7, с.32].

У квітні 2016 року Європейська комісія прийняла «Спільні принципи протидії гібридним загрозам – відповідь Європейського Союзу» (Joint Framework on countering hybrid challenges a European Union response):

1. Загальні принципи підкреслюють необхідність для держав-членів розробити узгоджені механізми впровадження стратегічних комунікацій для протидії дезінформації та публічного виявлення гібридних загроз.

2. У документі зазначено, що важливо захищати об’єкти критичної інфраструктури (такі як транспорт і телекомунікації), порушення гібридних атак можуть призвести до серйозних економічних чи соціальних зривів.

3. У документі йдеться, що діяльність у сфері стратегічних комунікацій передбачає тісну взаємодію з НАТО. Зазначається, що співпраця між ЄС і НАТО дозволяє організаціям ефективніше реагувати на гібридні загрози [103].

Протидія інформаційній війні та дезінформації в країнах ЄС здійснюється в рамках побудови відповідної системи стратегічних комунікацій, які є найефективнішим інструментом для досягнення цілей захисту інформаційного простору та інформаційної безпеки. У листопаді 2016 року Європарламент схвалив резолюцію під назвою «Стратегічна комунікація ЄС для протидії пропаганді, спрямованій проти нього третіми сторонами». У цьому документі серед загроз названі російські ЗМІ, зокрема: телеканал RT, агентство Sputnik, а також окремо згадані фонд «рускій мир» і «роспівробітництво». У документі міститься заклик розширити повноваження StratCom-East і перетворити його на повноцінний департамент Європейської служби закордонних справ. З вересня 2017 року у Фінляндії розпочав роботу Європейський центр протидії гібридним

загрозам (The European Centre of Excellence for Countering Hybrid Threats) [26, с. 50].

Зазначені резолюції були прийняті на тлі поширення росією дезінформації в Європі. В Європі Путіна називають «майстром» формування інформаційних стратегій для різних країн ЄС. Роками кремль створював мережу політиків у Європі, які стали його рупором для спілкування з внутрішньою аудиторією. Хоча в ЄС приймаються відповідні рішення щодо запобігання дезінформації та захисту інформаційної безпеки, кремль продовжує знаходити механізми впливу на ЗМІ [80].

«Наступальна інформаційна кампанія» російської федерації проти європейських держав базується на існуючій низці випробуваних і успішних тактик, до яких належать наступні:

– просування пропаганди та порядку денного російської федерації через підконтрольні державні ЗМІ (RT, «Супутник»), які намагаються обійти введені обмеження на роботу в країнах ЄС (наприклад, через VPN);

– діяльність фейкових мереж – клонів справжніх європейських ЗМІ (імітація таких ЗМІ як «Bild» у Німеччині, «20 minutes» у Франції, ANSA в Італії, «Guardian» у Великій Британії тощо);

– активність сплячих сайтів – неактивних веб-сторінок, які формують аудиторію за допомогою неполітичного контенту, а в міру набуття популярності починають поширювати дезінформацію [81];

– маніпуляції в соціальних мережах (зокрема, за допомогою масштабних російських ботофабрик);

– проведення кібератак і хакерських атак на критично важливі об’єкти та веб-сайти державних установ європейських держав (наприклад, робота російських хакерських угруповань «Advanced Persistent Threat 28» (APT 28) або «Fancy Bear», що входить до складу ГРУ РФ. Російська Федерація) тощо [81].

Протидія ЄС російській дезінформації передбачає:

– запуск у 2015 році платформи «EUvsDisinfo» – флагманського проекту Оперативної робочої групи зі стратегічних комунікацій Європейського Союзу (займається регулярним виявленням та аналізом випадків дезінформації в різних країнах Європи);

– оновлення від 2022 року Кодексу практики щодо дезінформації (ініціатива запроваджена для демонетизації поширення дезінформації в онлайн-середовищі; забезпечення прозорості політичної реклами; розширення можливостей користувачів тощо);

– удосконалення правового регулювання цифрових послуг (оновлення Закону про цифрові послуги, що передбачає встановлення чітких правил для онлайн-платформ, підвищення прозорості та підзвітності);

– посилення санкцій проти російських державних ЗМІ із забороною їхнього мовлення на території Європейського Союзу;

– проведення розслідувань на загальноєвропейському (на рівні інституцій ЄС) та національному рівнях щодо випадків іноземного втручання та операцій впливу третіх країн;

– впровадження проактивних заходів – запуск додаткових ініціатив фактчекінгу; підвищення рівня медіаграмотності населення; моніторинг та виявлення дезінформації на ранніх стадіях тощо [81].

У 2023 році Жозеп Боррель оголосив про створення «Центру обміну та аналізу інформації» Європейського Союзу для збору даних про загрози, пов’язані з дезінформацією та маніпуляціями ззовні. Це сприятиме обміну інформацією про основні причини, інциденти та загрози, а також обміну досвідом, знаннями та аналізом [11].

Масштабні технологічні перетворення залишаються пріоритетом створення умов для глобального впливу ЄС на світову геополітику й економіку.

Для цього Європейський Союз активно впроваджує сучасні цифрові ініціативи для розвитку інформаційного суспільства. Наприклад, «Європейський цифровий компас 2030» (Digital Compass 2030) [105] Комісія пропонує Цифровий компас для перенесення цифрових амбіцій ЄС на 2030 рік у конкретні терміни. Вони розвиваються навколо чотирьох основних моментів:

1. Громадяни, які мають цифрові навички та висококваліфіковані цифрові професіонали: до 2030 року принаймні 80% усіх дорослих повинні мати базові цифрові навички, а в ЄС має бути 20 мільйонів фахівців з ІКТ – і більше жінок повинні виконувати цю роботу.

2. Безпечна та стійка цифрова інфраструктура: до 2030 року всі домогосподарства ЄС повинні мати гігабітне з'єднання, а всі населені пункти мають бути покриті 5G; виробництво прогресивних і стабільних напівпровідників у Європі має становити 20% світового виробництва; у Європі також має бути свій перший квантовий комп'ютер.

3. Цифрова трансформація бізнесу: до 2030 року три з чотирьох компаній використовуватимуть сервіси хмарних обчислень, великих даних та штучного інтелекту [27].

4. Цифровізація державних послуг: до 2030 року всі ключові державні послуги мають бути доступні онлайн; всі громадяни мають доступ до своїх електронних медичних карт; і 80% громадян повинні використовувати рішення електронної ідентифікаційної картки (eID) [27].

Отже, найбільш продуктивна робота в сфері інформаційної політики в ЄС розпочалася після повномасштабного вторгнення росії в Україну. Це знаменувалося тим, що ЗМІ росії намагалися впливати на зарубіжні медіа та просувати свої політичні погляди, маніпулювати ситуацією в Європі тощо.

3.3 Інформаційна політика України в умовах воєнного стану та шляхи її вдосконалення

В умовах тривалої російсько-української війни Україна постала перед необхідністю гарантувати інформаційну безпеку держави, а повномасштабне військове вторгнення рф у 2022 році актуалізувало необхідність донесення до цивілізованого світу правдивої інформації про причини та характер збройного протистояння на українській території, суть агресивних планів росії та наявні й перспективні наслідки розв'язування нею найбільшої війни часів Другої світової війна. Значна перевага російської армії над Збройними Силами України в чисельності особового складу, озброєння та військової техніки поставила нашу державу в залежність від допомоги іноземних партнерів. Така залежність коригує напрямок державної інформаційної політики з метою забезпечення кількісного та якісного зростання зовнішньої допомоги.

Тривалість і характер ворожого вторгнення поставили на порядок денний мілітаризацію української економіки, збільшення масштабів мобілізації та збереження мотивації громадян продовжувати протистояння агресору. У таких умовах виникла необхідність комплексного аналізу державної інформаційної політики України в умовах повномасштабного російського військового вторгнення з метою визначення її ефективності та формування пропозицій щодо її модернізації. Перевірка вимагає припущення, що в сучасних умовах розвитку інформаційного суспільства обмеження джерел інформації «зверху» не забезпечує формування необхідного для влади інформаційного поля, а має наслідком його створення на за рахунок неофіційних джерел, як один із наслідків розширення горизонтальних зв'язків у суспільстві [45, с. 44].

Наприкінці лютого 2022 року розпочався новий етап російсько-української війни: повномасштабне вторгнення рф в Україну. Розгортання бойових дій на широкому фронті було зумовлене неможливістю втягнути Україну в орбіту

«руского міра» у 2014-2021 роках. Проте ліквідувати наслідки тривалого безперешкодного поширення російських наративів в українському медіапросторі не вдалося [46, с. 294-295].

З перших хвилин збройного нападу російської федерації 24 лютого відкрився інформаційний фронт, на якому наш Президент Володимир Зеленський всіляко привертав увагу лідерів усіх країн, просив допомоги та показував, що насправді відбувається і тим самим здобув певну перемогу над ворогом, тому що більшість нас підтримує. При цьому люди, блогери та інші діячі, які мали вплив на громадськість, намагалися якомога більше розповісти про події, що відбуваються, щоб світ дізнався правду, а не вигадану версію ворога. Наші громадяни, які проживали в інших країнах, і ті, хто виїхав у перші місяці після початку війни, організовують мітинги, які привертають увагу ЗМІ та урядів інших країн [42, с. 42].

Указом Президента 19 березня 2022 року «Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану» [11] введено в дію цілодобовий інформаційний марафон «Єдині новини #UAразом», який повністю об’єднав 11 українських телеканалів («UΛ:ПЕРШИЙ», «РАДА», «1+1», «ІНТЕР», «УКРАЇНА», «ICTV», «Україна 24», «ZOOM», «К2» «4», «УНІАН») ще 4 канали доєдналися частково (5 канал, ПРЯМИЙ, ЕСПРЕСО, телеканал «XSPORT»). Тобто саме через ці 15 телеканалів громадяни отримують основну інформацію про події в країні та світі [42, с. 43].

3 березня 2022 р. з’явився наказ головнокомандувача ЗСУ В. Залужного «Про організацію взаємодії між Збройними силами України, іншими складовими сил оборони та представниками засобів масової інформації на час дії правового режиму воєнного стану» [63]. Цей наказ визначив основні напрями взаємодії з медіа та окреслив перелік забороненої для поширення інформації. У роз’ясненні Генерального штабу містилася заборона на розголошення інформації про

постачання зброї для ЗСУ, місця розташування військових об'єктів та влучання ворожих ракет. Заборонявся також фактчекінг заяв і публікацій силових відомств та спецслужб. У роз'ясненні були також визначені умови акредитації представників засобів масової інформації під час дії правового режиму воєнного стану та правила їх роботи у районах ведення бойових дій [45, с. 51].

3 березня 2022 р. був ухвалений Закон України «Про внесення змін до деяких законодавчих актів України щодо встановлення кримінальної відповідальності за колабораційну діяльність» [66]. Покарання було передбачене для тих громадян України, які здійснювали пропаганду у закладах освіти задля сприяння вчиненню збройної агресії проти України, встановленню та утвердженню тимчасової окупації частини території України [45, с. 53].

Сьогодні внутрішнє медіа-поле України має передусім вирішити три фундаментальні завдання:

1. Нейтралізація наслідків впливу російської дезінформації/пропаганди на цільові українські аудиторії.

2. Оптимізація національного українського медійного дискурсу принаймні на підконтрольних уряду України територіях.

3. Вирішення комплексу комунікаційних та медійних проблем окремих районів Донецької та Луганської областей (постійне джерело інформаційних приводів для ворожої пропаганди, «штаб» низки антиукраїнських журналістів та ЗМІ, місце проживання Громадяни України, яким у майбутньому доведеться реінтегруватися в загальноукраїнський життєвий контекст) [99, с. 135].

У державі створено необхідне законодавство, спрямоване на забезпечення інформаційної безпеки. Разом з цим, в умовах війни та існуючих загроз інформаційній безпеці держави законодавча база має бути здатною до змін та забезпечувати належний рівень нормативного регулювання у сфері забезпечення інформаційної безпеки та функціонування відповідних суб'єктів. Не менш гостро стоїть питання кібербезпеки в умовах гібридної війни. У сучасному світі

кіберпростір все частіше використовується для проведення широкого спектру підривних операцій: від викрадення цінної інформації до актів кібертероризму. Тому сьогодні існує потреба у належному правовому регулюванні та здійсненні державою відповідних заходів, спрямованих на усунення та ліквідацію кібератак, підвищення стану безпеки відповідних інформаційно-телекомунікаційних систем [78, с. 304-305].

Отже, вдосконалення забезпечення інформаційної безпеки вимагає цілеспрямованого вивчення зарубіжного досвіду організації та проведення інформаційних операцій, методів і засобів проведення кібератак, а також моделювання інформаційних атак. Система захисту інформації повинна бути міжвідомчою та ієрархічно організованою. Її структура та організація мають відповідати структурі державного управління з чіткою координацією дій окремих сегментів. Організація ефективної системи інформаційної безпеки передбачає централізоване управління з окремими відомчими адміністративними функціями, які забезпечують моніторинг і контроль усіх складових національного інформаційного простору. Система захисту інформації повинна в будь-якій ситуації скоординованої багатосторонньої та різнобічної інформаційної роботи мати здатність зберігати важливі параметри свого функціонування, тобто підтримувати стан гомеостазу [39, с. 176].

З. Гбур роглянув важливі заходи щодо забезпечення ефективної діяльності у сфері державного управління інформаційною безпекою. Серед них:

– розробка показників ефективності систем захисту державної інформації;

– моніторинг та виявлення виникнення дестабілізуючих факторів і загроз;

– організація фундаментальних та прикладних наукових досліджень у сфері захисту інформації;

– розробка відповідної законодавчої бази;

– протидіяти загрозі інформаційної війни [21, с. 870].

Інформаційна безпека є важливою функцією держави, повинна передбачати, насамперед, формування відповідними державними органами політики організаційно-правових механізмів в галузі інформаційної безпеки (див. Додаток В). Важлива роль в даному напрямі належить державним органам, які відповідно до наданих повноважень в сферах своєї відповідальності повинні здійснювати організаційне, нормативно-правове, матеріально-технічне та фінансове забезпечення реалізації державної політики інформаційної безпеки [21, с. 870].

Ми погоджуємося з думкою З. Гбура щодо основними напрямами щодо реалізації та захисту національних інтересів на сучасному етапі розвитку України в інформаційній сфері, серед них є наступні:

– розроблення та прийняття довгострокової програми забезпечення виходу на рівень провідних країн світу у сфері створення систем інформатизації та управління на основі новітніх інформаційних технологій;

– забезпечення свободи отримання та поширення інформації громадянами та іншими суб’єктами суспільних відносин в інтересах формування громадянського суспільства, демократичної правової держави, розвитку науки і культури;

– забезпечення надійного захисту інформаційного потенціалу України від його протиправного використання;

– здійснення контролю за вивезенням з держави інтелектуальної продукції, а також інформаційних банків даних;

– організація ефективної системи підготовки та підвищення кваліфікації кадрів у сфері забезпечення інформаційної безпеки;

– розвиток взаємодії державних і комерційних систем інформаційного забезпечення з метою більш ефективного використання інформаційних ресурсів держави [21, с. 872].

В умовах війни органи державної влади повинні продемонструвати високий рівень інформаційної взаємодії не лише з суспільством, а й з іншими країнами цивілізованого світу. Достовірні та досконалі промови як Президента України, так і інших представників влади перед парламентами або представниками іноземних держав чи міжнародних організацій та іншими мають містити лише факти та твори та роботи заяви які будуть прийматись суспільством України, цей запит за роки війни став найчастішим серед громадян України [79, с. 61].

Можна виділити кілька важливих напрямків підвищення медіаграмотності населення. До таких напрямів можна віднести:

– формування негативного ставлення до будь-якої анонімної інформації;

– необґрунтованість висновків в інформаційних повідомленнях, які містять оціночні судження;

– коментування чуток і неперевіреної інформації зі створенням на їх основі певних висновків;

– поширення повідомлень з неназваних джерел або джерел, походження яких автор повідомлення відмовляється розкрити;

– читання змісту повідомлень, джерела яких не можуть бути підтверджені відповідними посиланнями.

Слід формувати обережне ставлення до раптової появи нових джерел контенту, які поширюють інсайдерську інформацію; до джерел, що подають інформацію не збалансовано, а також до інформації експертів, походження знань, умінь і навичок яких неможливо встановити або чиї прогнози здебільшого не відповідають дійсності. Важливо переконати громадян у тому, що джерелом аналітики мають бути насамперед визнані експерти-науковці [45, с. 58].

Основні та найважливіші нормативно правові документи щодо інформаційної політики з 24 лютого 2022 року:

– Указ Президента України від 24 лютого 2022 року № 64/2022 «Про введення воєнного стану в Україні» [62];

– Наказ Головнокомандувача Збройних Сил України від 03 березня 2022 року № 73 «Про організацію взаємодії між Збройними Силами України, іншими складовими сил оборони та представниками засобів масової інформації на час дії правового режиму воєнного стану» [63];

– Указ Президента України «Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану» [64];

– Закон України «Про медіа» від 13 грудня 2022 року № 2849-IX [61];

– Розпорядження Кабінету Міністрів України «Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року» від 30 березня 2023 року № 272-р [65].

Саме ці нормативно-правові документи найбільше вплинули і продовжують впливати на інформаційну політику з початку війни, але не зважаючи на це залишається ряд питань які потребують розгляду та подальшого вдосконалення.

ВИСНОВКИ

В рамках магістерського дослідження були виконані та розглянуті наступні завдання:

1. Визначено поняття «інформаційна політика» та її сутність. Під час дослідження поданого питання, ми розглянули роботи М. Дурманова, В. Данил'янова, О. Панченко, В. Терещенка тощо. Державна інформаційна політика, як правило, розглядається як допоміжна для досягнення інтересів державної влади, а засоби масової інформації (як офіційні, так і неофіційні) як своєрідна сполучна тканина між державою і громадянським суспільством. Таким чином, державна інформаційна політика – це сукупність основних напрямів і методів діяльності держави щодо отримання, використання, поширення та зберігання інформації. Інформаційна політика не тільки регулює відносини між суспільством та державою, а й забезпечує створення необхідної нормативно-правової бази щодо розвитку інформаційного суспільства; виконає завдання розвитку та модернізації комунікативно-інформаційних технологій; забезпечує громадян доступом до важливої інформації тощо. Інформаційна політика в сучасному її розумінні є інструментом забезпечення безпеки людини, суспільства, держави, світової спільноти.

2. Розглянуто нормативно-правове регулювання інформаційної політики в Україні. Правове регулювання інформаційної безпеки в Україні – це комплексна система актів різної юридичної сили, які регулюють відносини у сфері протидії загрозам в інформаційній сфері. Під час дослідження, ми дійшли висновку, що систему правових актів, які регулюють інформаційну сферу можна поділити наступним чином:

– Залежно від обсягу приписів, які містяться в актах, ступеня і характеру регульованих відносин: акти, що не містять прямих регламентуючих

положень, щодо забезпечення інформаційної безпеки, проте прямо або опосередковано регулюють інформаційні відносини; акти, які безпосередньо регламентують забезпечення інформаційної безпеки в Україні.

– Залежно від юридичної сили актів: Конституція України; Закони України, в тому числі «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про національну безпеку України», «Про захист персональних даних» тощо; підзаконні акти – це нормативні акти Президента України, Кабінету Міністрів України, Державної служби спеціального зв'язку та захисту інформації України тощо; нормативні документи в галузі технічного захисту інформації та державні стандарти України стосовно створення і функціонування комплексної системи захисту інформації; міжнародні акти.

Також у роботі були розглянуті й інші державні акти, не менш важливі, які визначають завдання інформаційної політики.

3. Розкрили роль та функції засобів масової інформації в умовах військово-політичних конфліктів. Основна мета та завдання засобів масової інформації швидко та точно інформувати громадян про ті чи інші події, які відбуваються на території країни чи у світі. Серед основних функцій є: інформаційна, посередницька, функція об'єктивного висвітлення подій, спостереження, формування думок щодо подій, маніпулятивна. Засоби масової інформації подають новини на запит суспільства про різні події, трактують мало зрозумілі факти, формують та висловлюють громадську думку, а також можуть бути важливим інструментом для діалогу між сторонами, які ворогують.

4. Охарактеризовано методи та засоби ведення інформаційних війн у XXI столітті. Інформаційна війна – це комплекс заходів для підриву інформаційної сфери противника та збереження й утримання власної політики. До завдань інформаційної війни можна віднести: підрив якості інформації противника та перешкоджання можливості противника збирати інформацію; збір тактичної

інформації; гарантування безпеки власних інформаційних ресурсів; поширення пропаганди або дезінформації з метою деморалізації ворожих сил і населення.

У роботі ми розглянули такі засоби інформаційної війни: приховування та спотворення інформації; збільшення повідомлень певного типу чи за певним інформаційним змістом; відволікання уваги на не важливі теми тощо.

До методів інформаційної війни відносять: дезінформацію, маніпулювання, навіювання, пропаганду, залякування, психологічний тиск, поширення чуток тощо.

5. Проаналізовано досвід розвитку інформаційної політики в США та Європі. В США існує кілька інституцій із забезпечення інформаційної безпеки: Агентство національної безпеки, Національне управління кібербезпеки США, Міністерство внутрішньої безпеки США, Федеральне бюро розслідувань, Центральне розвідувальне управління. Інформаційну безпеку США розглядає як важливою для безпеки кожного громадянина. Національна безпека США зосереджена в документі під назвою Стратегія національної безпеки США, який розробляється окремо адміністрацією кожного нового президента та об’єднує зовнішню політику, національну оборону сферу, міжнародні економічні відносини тощо. Остання редакція американської національної інформаційної стратегії відбулася у березні 2018 р.. Велику увагу США приділяє кібербезпеці та інформативній безпеці молодшого покоління.

Розвиток інформаційної політики Європейського Союзу розпочався з 1979 року. Основні пріоритети реалізації інформаційної політики Європейського Союзу це формування у громадян умінь використовувати нові інформаційні засоби та прикладні завдання; завчасне залучення громадян до розробки нових додатків і послуг; використання нових технологій з метою залучення людей до процесів прийняття рішень і надання їм можливості знати, що робить їхній уряд, тим самим гарантуючи плюралізм і відкритий доступ до інформації. У роботі розглянуто

стратегії та інші важливі документи, які приймалися Європою щодо забезпечення безпеки інформаційного простору та протидії дезінформації.

6. Подано характеристику інформаційній політиці України в умовах воєнного стану та визначено шляхи її вдосконалення. Початок гібридної війни в інформаційному просторі проти України розпочало новий етап формування інформаційної політики в країні. Війна змінила ставлення до медіаресурсів, піднялося питання правдивості інформації, протиборство дезінформації та фейкам. З перших хвилин збройного нападу російської федерації відкрився інформаційний фронт, на якому Президент Володимир Зеленський всіляко привертав увагу лідерів усіх країн, просив допомоги та показував, що насправді відбувається і тим самим здобув певну перемогу над ворогом, тому що більшість країн почало нас підтримувати. Від 24 лютого 2022 року основними документами, які регулюють інформаційну безпеку України є: Указ Президента України «Про введення воєнного стану в Україні»; Указ Президента України «Про рішення Ради національної безпеки і оборони України»; Закон України «Про медіа» тощо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Антошин І. В. Інформаційна влада : актуалізація дослідження // Вчені записки ТНУ імені В. І. Вернадського. Серія: юридичні науки. Т. 31 (70). Київ, 2020. № 3. С. 1-6.

2. Антонюк В. В. Інформаційна війна в структурі сучасного геополітичного протиборства: нові контексти та інтерпретації // Державне управління: удосконалення та розвиток. 2021. № 7. 8 с.

3. Арістова І. В. Державна інформаційна політика: організаційно-правові аспекти / За загальною редакцією д-ра юрид. наук, проф. Бандурки О.М. : монографія. Харків : Вид-во Ун-ту внутр. справ, 2000. 368 с.

4. Бондаренко Д. Є. Інформаційна політика Польщі в умовах міжнародних відносин. Київ, 2020. 60 с.

5. Бодрук О. С. Структури воєнної безпеки: національний та міжнародний аспекти : монографія. Київ : НІПМБ, 2001. 300 с.

6. Булавіна О. С., Хлівнюк Т. П. Нормативно-правове забезпечення інформаційної політики в Україні: особливості та суперечливості // Політикус : науковий журнал. Вип. 4. 2018. С. 21-24.

7. Булана Є. А., Паніна І. Г. Європейський Союз та інформаційні впливи російської федерації // Вісник студентського наукового товариства ДонНУ імені Василя Стуса. 2020. С. 31-34.

8. Багмет М. О., Гаркуша А. М. Досвід країн ЄС відносно розроблення та реалізації моделей державної інформаційної політики // Публічне управління та регіональний розвиток. 2020. № 8. С. 515-539.

9. Богуш Л. А. Роль засобів масової інформації у висвітлені збройних конфліктів у світі: теоретичний підхід // Вчені записки ТНУ імені В. І. Вернадського. Серія: Філологія. Журналістика. Т. 32 (71). Ч. 3. 2021. № 4. С. 291-295.

10. Батько І., Павленко Д. Міжнародний досвід формування та становлення інституту інформаційної безпеки як невід'ємної складової сучасної держави // Аналітично-порівняльне правознавство. Львів, 2023. № 6. С. 397-401.

11. «Брехня у промислових масштабах»: як росія атакує ЄС. 2023. URL: https://www.dw.com/uk/brehna-u-promislovih-masstabah-ak-rosia-atakue-es/a-64644725 (дата звернення: 06.11.2024).

12. Войчук В. Роль засобів масової інформації у демократичному політичному режимі // Наукові праці Міжрегіональної академії управління персоналом. Вип. 2 (12). 2024. С. 17-21.

13. Валюшко І. О. Основні виклики і загрози в епоху інформаційних війн // Зовнішня політика і дипломатія: традиції, тренди, досвід : науковий вісник Дипломатичної академії України Ч. 2. Серія «Політичні науки». 2016. С. 142-147.

14. Глобенко С. Становлення й розвиток правового поля України щодо захисту інформаційного простору держави // Державне управління : науковий вісник. 2023. № 2. С. 64-79.

15. Гібридна війна і журналістика. Проблеми інформаційної безпеки : навчальний посібник / за заг. ред. В. О. Жадька ; ред.-упор. : О. І. Харитоненко, Ю. С. Полтавець. Київ : Вид-во НПУ імені М. П. Драгоманова, 2018. 356 с.

16. Гуз А. М. Історія захисту інформації в Україні та провідних країнах світу : навчальний посіб. Київ : КНТ, 2007. 260 с.

17. Гарматій О. Конфліктологічний менеджмент мас-медіа в сучасному українському соціумі // Україна. Конфлікт, трансформація, інтеграція : монографія / редакція : К. Сигідус, О. Горбач, Д. Мосьціцка, В. Котович. Львів : ПП Сорока Тарас Богданович, 2016. С. 203-216.

18. Грубі Т. В. Світові та вітчизняні практики в сфері кібербезпеки: виклики сучасності // Збірник матеріалів Міжнародної науково-практичної конференції «Інформаційна безпека: сучасний стан, проблеми та перспективи» [Електронний ресурс] / [за заг. ред. О. В. Віннічук]. Кам'янець-Подільський :

Кам’янець-Подільський національний університет імені Івана Огієнка, 2023. С. 42-46.

19. Грень Р. Т. Інтеграція України в єдиний цифровий простір ЄС // Науковий вісник Ужгородського національного університету. Серія : Міжнародні економічні відносини та світове господарство. Вип. 47. 2023. С. 25-29.

20. Грубінко А. Особливості формування політики кібербезпеки Європейського Союзу: правові аспекти // Актуальні проблеми правознавства. 2021. № 1 (25). С. 5-10.

21. Гбур З. В. Основи інформаційної безпеки держави в умовах війни // Russian-Ukrainian war (2014-2022): historical, political, cultural-educational, religious, economic and legal aspects: a scientific monograph. Riga, Latvia : Baltija Publishing, 2022. P. 868-872.

22. Дурман М. О., Дурман О. Л., Лінецька Я. М. Стан наукової розробленості проблематики запровадження інформаційних технологій у державне управління // Державне управління: удосконалення та розвиток. 2022. № 1. 9 с.

23. Данил’ян В. О. Інформаційне суспільство та перспективи його розвитку в Україні (соціально-філософський аналіз) : монографія. Харків : Право, 2008. 184 с.

24. Дрешпак В. М. Концептуальні основи періодизації державної інформаційної політики України // Аспекти публічного управління. Київ, 2013. № 2. С. 41-47.

25. Джус О. А. Концептуальні основи ведення інформаційної війни в сучасних умовах збройної агресії РФ проти України // Політологічний вісник. 2022. № 88. С. 189-201.

26. Денисюк Ж. З. Пропаганда та контрпропаганда в контексті стратегій державної інформаційної політики // Вчені записки ТНУ В. І. Вернадського. Серія: державне управління. Т. 32 (71). 2021. № 2. С. 46-51.

27. Європейське цифрове десятиліття: встановлення курсу на Європу з цифровими можливостями до 2030 року. EU4Digital. URL: https://eufordigital.eu/uk/europes-digital-decade-setting-the-course-towards-a-digitally-empowered-europe-by-2030/ (дата звернення: 06.11.2024).

28. Здоровега В. Й. Теорія і методика журналістської творчості : підручник. 3-тє видання. Львів : ПАІС, 2008. 276 с.

29. Зеленін В. В. По той бік правди: нейролінгвістичне програмування як зброя інформаційно-пропагандистської війни: навч. посіб. Т. 1. Київ : Люта справа, 2015. 384 с.

30. Захаренко К. В. Міжнародний досвід інформаційної безпеки // Сучасне суспільство, політичні науки, соціологічні науки, культурологічні науки. 2019. № 1 (17). С. 95-109.

31. Інформаційна політика в Україні : конспект лекцій / укладачі В. О. Шведун, Т. О. Луценко. Харків : НУЦЗУ, 2016. 40 с.

32. Іванченко Ю. М. Сутність, головні напрями та способи державної інформаційної політики в Україні // Державне управління: теорія та практика. 2005. 5 с.

33. Козьміних А. В. Інформаційна політика в умовах демократичного транзиту // Політичне життя. 2020. № 3. С. 51-57.

34. Крупнова А. О. Правове регулювання сфери забезпечення інформаційної безпеки в Україні. Аналітичне-порівняльне правознавство / редкол.: Ю. М. Бисага (голов. ред.), В. В. Заборовський, Д. М. Бєлов, С. Б. Булеца та ін. Ужгород : ДВНЗ «УжНУ», 2023. № 5. С. 348-354

35. Ківалов С. В. Інформаційно-комунікаційний чинник сучасної політики та його роль у сфері освіти // Актуальні проблеми політики. Вип. 66. 2020. С. 5-10.

36. Кондратюк М. О. Інформаційна війна та роль мас-медіа в міжнародних конфліктах // Вісник Харківської державної академії культури. Вип. 41. Харків, 2013. С. 108-113.

37. Корнат Л. Я., Сенчакевич Н. В. Роль засобів масової інформації у врегулюванні міжнародних конфліктів XXI ст. // Політикус : науковий журнал. Вип. 5. 2023. С. 145-149.

38. Кіца М., Свинаренко Г. Теоретичні та практичні аспекти ведення інформаційної війни у ЗМІ // Львівська політехніка : вісник Національного університету. Серія: Журналістські науки. Львів : Видавництво Львівської політехніки, 2019. № 3. С. 69-75.

39. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції : навчальний посібник. Київ : КНТ, 2006. 280 с.

40. Луценко С. М. Механізми інформаційного забезпечення публічної влади в Україні : автореф. дис. … к.держ.упр.: 25.00.02 «Механізми державного управління». Запоріжжя, 2011. 20 с.

41. Ляшенко О., Дацків І. Концептуальні засади формування інформаційної політики країни: світовий досвід // Україна-Європа-Світ : міжнародний збірник наукових праць. Серія: історія, міжнародні відносини. Вип. 15. Тернопіль : ТНПУ ім. В. Гнатюка, 2015. С. 211-224.

42. Мирошниченко А. І. Інформаційна політика в умовах воєнного стану // Вчені записки ТНУ імені В. І. Вернадського. Серія: публічне управління та адміністрування. Т. 34 (73). 2023. № 4. С. 41-45.

43. Негодченко В. Основні напрями державної інформаційної політики в Україні // Підприємництво, господарство і право. Харків, 2016. № 4. С. 77-81.

44. Новинам із яких джерел українці найбільше довіряють – дослідження ОПОРИ. Новини Суспільне. 2024. URL: https://suspilne.media/792121-novinam-iz-akih-dzerel-ukrainci-najbilse-doviraut-doslidzenna-opori/ (дата звернення: 04.11.2024).

45. Ніколаєць Ю. Державна інформаційна політика України в умовах повномасштабного воєнного вторгнення російської федерації: суспільно-

мобілізаційний потенціал і ефективність // Політичні студії. 2024. № 1 (7). С. 42-67.

46. Ніколаєць, Ю. Вплив медійного дискурсу на формування політичних цінностей населення Сходу і Півдня України // Ієрархія цінностей населення Сходу та Півдня України: етнополітичний аспект в умовах російської агресії : монографія. Київ : ІПіЕнД ім. І. Ф. Кураса НАН України, 2021. С. 245-295.

47. Основи демократії : навчальний посібник для студентів вищих навчальних закладів / Авт. колектив: М. Бессонова, О. Бірюков, С. Бондарук та ін. ; За заг. ред. А. Колодій ; М-во освіти і науки України, Ін-т вищої освіти АПН України, Укр.-Канад. проект «Демократична освіта», Інститут вищої освіти. Київ : «Ай-Бі», 2002. 684 с.

48. Панченко О. А. Інформаційна безпека держави як складник розвитку суспільних відносин // Публічне управління та адміністрування в Україні. Вип. 17. 2020. С. 135-139.

49. Почепцов Г. Г. Інформаційна політика / Г. Г. Почепцов, С. А. Чукут. 2-ге вид., стер. Київ : Знання, 2008. 663 с.

50. Пунда О. О., Добрянська О. Д., Новицька Н. Б. Принципи інформаційної політики в умовах війни та їх нормативно-правове закріплення // Соціологія права. 2022. №1-2. С. 71-76.

51. Проноза І. І. Засоби масової інформації та комунікації в інформаційній війні як сучасна політична практика // Політикус : науковий журнал. Вип. 3. 2020. С. 65-69.

52. Петрінко В. С. Конфліктологія: курс лекцій, енциклопедія, програма, таблиці : навчальний посібник. Ужгород: УжНУ «Говерла», 2020. 360 с.

53. Про інформацію : Закон України від 1992 р. 2657-XII ; поточна редакція від 27.07.2023. *Офіційний портал Верховної ради України*. 1992. № 48. Ст. 650.

54. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 1994 р. 80/95-ВР ; поточна редакція від 26.08.2024. *Офіційний портал Верховної ради України*. 1994. № 31. Ст. 286.

55. Про національну безпеку України : Закон України від 2018 р. 2469-VIII ; поточна редакція 09.08.2024. *Офіційний портал Верховної ради України*. 2018. № 31. Ст. 241.

56. Про захист персональних даних : Закон України від 2010 р. 2297-VI ; поточна редакція 27.04.204. *Офіційний портал Верховної ради України*. 2010. № 34. Ст. 481.

57. Про Стратегію національної безпеки України : Указ Президента України від 14.09.2020 р. № 392/2020. Офіційний вісник України. 2020. № 75. С. 127.

58. Про Стратегію інформаційної безпеки : Указ Президента України від 28.12.2021 р. № 685/2021. Офіційний вісник України. 2022. № 3. С. 22.

59. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. *Офіційний портал Верховної ради України*. 2017. № 45. Ст. 403.

60. Про Стратегію кібербезпеки України : Указ Президента України від 26.08.2021 р. № 447/2021. Офіційний вісник України. 2021. № 70. С. 42

61. Про медіа : Закон України від 13.12.2022 р. № 2849-IX. *Офіційний портал Верховної ради України*. 2023. № 47-50. Ст. 120.

62. Про введення воєнного стану в Україні : Указ Президента України від 24 лютого 2022 р. № 64/2022. *Офіційний портал Верховної ради України*. 2022.

63. Про організацію взаємодії між Збройними Силами України, іншими складовими сил оборони та представниками засобів масової інформації на час дії правового режиму воєнного стану : Наказ Головнокомандувача Збройних Сил України від 03 березня 2022 року № 73. 2022. URL: https://ips.ligazakon.net/document/MUS36785?an=2 (дата звернення: 07.11.2024).

64. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану» : Указ Президента України від 19 березня 2022 р. № 152/2022. *Офіційний портал Верховної ради України*. 2022.

65. Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року: Розпорядження Кабінету Міністрів від 30 березня 2023 року № 272-р. *Офіційний портал Верховної ради України*. 2023.

66. Про внесення змін до деяких законодавчих актів України щодо встановлення кримінальної відповідальності за колабораційну діяльність : Закон України від 3 березня 2022 р. №2108-IX. *Офіційний портал Верховної ради України*. 2022.

67. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28 грудня 2021 р. № 658/2021. *Офіційний портал Верховної ради України*. 2021.

68. Про науково-технічну інформацію : Закон України від 1993 р. № 3322-XII ; поточна редакція від 19.04.2014. *Офіційний портал Верховної ради України*. 1993. № 33. Ст. 345.

69. Про державну таємницю : Закон України від 1994 р. № 3855-XII ; поточна редакція від 30.10.2024. *Офіційний портал Верховної ради України*. 1994. № 16. Ст. 93.

70. Про рекламу : Закон України від 1996 р. № 270/96 ; поточна редакція від 27.04.2024. *Офіційний портал Верховної ради України*. 1996. № 39. Ст. 181.

71. Про Концепцію Національної програми інформатизації : Закон України від 1998 ; поточна редакція від 01.01.2022. *Офіційний портал Верховної ради України*. 1997. № 27-28. Ст. 182.

72. Про доступ до публічної інформації : Закон України від 2011 р. № 2939-VI ; поточна редакція від 08.10.2023. *Офіційний портал Верховної ради України*. 2011. № 32. Ст. 314.

73. Про підсумки парламентських слухань «Інформаційна політика України: стан і перспективи : Постанова Верховної Ради України від 2 червня 1999 р. № 705-XIV. *Офіційний портал Верховної ради України*. 1999.

74. Про підсумки парламентських слухань «Проблеми інформаційної діяльності, свободи слова, дотримання законності та стану інформаційної безпеки України» : Постанова Верховної Ради України від 7 червня 2001 р. № 3498-III. *Офіційний портал Верховної ради України*. 2001.

75. Про парламентські слухання «Суспільство, засоби масової інформації, влада: свобода слова та цензура в Україні» : Постанова Верховної Ради України від 23 жовтня 2002 р. № 190-IV. *Офіційний портал Верховної ради України*. 2002.

76. Про першочергові заходи щодо забезпечення доступу до публічної інформації в допоміжних органах, створених Президентом України : Указ Президента України від 2019 р. № 606/2019. *Офіційний портал Верховної ради України*. 2019.

77. Питання забезпечення органами виконавчої влади доступу до публічної інформації : Указ Президента України від 5 травня 2011 р. № 547/2011. *Офіційний портал Верховної ради України*. 2011.

78. Ряполов А. П. Окремі напрями удосконалення забезпечення інформаційної безпеки в умовах війни // Proceedings of the 14th International Scientific and Practical Conference «Science and Practice: Implementation to Modern Society». Manchester, 2023. P. 303-307.

79. Русакевич А. Інформаційна безпека в умовах воєнного стану у аспекті захисту інформаційних прав громадян // Law. State. Tehnology. 2024. № 2. P. 58-62.

80. Росія почала інформаційну війну: як ЄС перед виборами бореться з фейками. URL: http://surl.li/kgczwo (дата звернення: 06.11.2024).

81. Російські дезінформаційні кампанії в Європі. URL: https://niss.gov.ua/doslidzhennya/mizhnarodni-vidnosyny/rosiyski-dezinformatsiyni-kampaniyi-v-yevropi (дата звернення: 06.11.2024).

82. Ржевська Н. Сучасна інформаційна політика: досвід США для України // Політичні студії. 2024. № 1 (7). С. 68-85.

83. Ситніченко О. М. Окремі аспекти нормативно-правового регулювання забезпечення інформаційної безпеки // Вчені записки ТНУ імені В. І. Вернадського. Серія : юридичні науки. Т. 32 (71). Київ, 2021. С. 86-90.

84. Степанов В. Ю. Визначення поняття державної інформаційної політики // Інвестиції: практика та досвід. 2012. № 21. С. 81-84.

85. Стахнік Р. Роль медіа у якості ретранслятора військово-політичних конфліктів у світі // Магістерський науковий вісник Тернопільського національного педагогічного університету імені Володимира Гнатюка. Вип. 40. Тернопіль : ТНПУ ім. В. Гнатюка, 2023. С. 106-108.

86. Семен Н. Ф. Російські інтернет-ресурси як чинник інформаційної війни проти України : дис. к. соц. к. Міжнародний економіко-гуманітарний університет імені акад. С. Дем'янчука. Рівне. 2018. 260 с.

87. Ткачук Т. Ю., Довгань О. Д. Система інформаційної безпеки України: онтологічні виміри // Інформація і право : науковий журнал. 2018. № 1 (24). С. 89-104.

88. Ткачук Т. Ю. Правове забезпечення інформаційної безпеки в умовах інтеграції України : дис. ... док. юрид. наук : 12.00.07. Ужгород, 2019. 487 с.

89. Терещенко В. В. Особливості державної інформаційної політики в умовах війни // Юридичний науковий електронний журнал. 2023. № 2. С. 391-395.

90. Таран Є. Політика забезпечення інформаційної безпеки у США та ЄС: досвід для України // Вісник Львівського університету. Серія філософського-політологічні студії. Вип. 25. 2019. С. 170-175.

91. Топчій О. Зарубіжний досвід забезпечення інформаційної безпеки неповнолітніх // Теорія і практика : національний юридичний журнал. 2019. С. 63-67.

92. Требін М. П. Армія та суспільство: соціально-філософський аналіз взаємодії в умовах трансформації. Харків : Видавничий дім «Інжек», 2004. 404 с.

93. Українські медіа, ставлення та довіра у 2023 році. Опитування USAID-Internews щодо споживання медіа. 2023. URL: https://internews.in.ua/wp-content/uploads/2023/10/Ukrainski-media-stavlennia-ta-dovira-2023r.pdf (дата звернення: 04.11.2024).

94. Феськов І. В. Основні методи ведення гібридної війни в сучасному інформаційному суспільстві // Актуальні проблеми політики. Вип. 58. 2016. С. 66-76.

95. Хахановський В. Г., Корнейко О. В. Актуальні питання інформаційного права : навч. посіб. Київ : Нац. акад. внутр. справ, 2024. 258 с.

96. Черновол І. О., Чарських І. Ю. Інформаційна безпека США: проблеми та виклики в добу Дональда Трампа // Вісник студентського наукового товариства Донецького національного університету імені Василя Стуса. Вип. 12. Т. 1. Вінниця, 2020. С. 110-115.

97. Чукут С. А., Джига Т. В. Інформаційна політика в Україні (опорний конспект лекцій до нормативного курсу) : навчальний посібник. Київ, 2016. 94 с.

98. Шевчук М. О. До питання генези поняття інформаційної безпеки як складової національної безпеки // Науковий вісник Ужгородського національного університету. Вип. 78, Ч. 2. Ужгород, 2023. С. 134-139.

99. Шиманова-Стифанишин О. Інформаційна політика в Україні у контексті українсько-російських відносин: політологічний аналіз // Вісник Львівського державного університету. Львів, 2023. С. 123-136.

100. Юнак А. Роль медіа дипломатії у зовнішньополітичних стратегіях України // Політологія. Соціологія. Право : вісник НТУУ «КПІ». Вип. 3 (19). Київ, 2013. С. 48-52.

101. Яковчук В. С., Малець Б. І. Інформаційні війни в сучасному світі. Захист інформації в інформаційно-комунікаційних системах : збірних тез доповідей IV Всеукраїнської науково-практичної конференції молодих вчених, курсантів та студентів. Львів : ЛДУ БЖД, 2020. 3 с.

102. Яковлєв П. О. Досвід державного регулювання забезпечення інформаційної безпеки зарубіжних держав (на прикладі Сполучених Штатів Америки, Канади, Німеччини, Франції) // Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Право». Вип. 30. Харків, 2020. С. 106-113.

103. Як Євросоюз протидіє російські пропаганді. URL https://icps.com.ua/yak-vrosoyuz-protydi-rosiyskiy-propahandi/ (дата звернення: 06.11.2024).

104. An Information Society For All. 2000. URL: https://www.researchgate.net/publication/247750421_An_Information_Society_for_Everyone (дата звернення: 08.11.2024).

105. Communication from the commission to the european parliament, the council, the European economic and social committee and the committee of the regions. Brussel, 2021. URL: https://eufordigital.eu/wp-content/uploads/2021/03/2030-Digital-Compass-the-European-way-for-the-Digital-Decade.pdf (дата звернення: 06.11.2024).

106. Living and Working in the Information Society: People First. Green Paper. Belgium, 1996. URL: https://aei.pitt.edu/80911/1/1996.3.pdf (дата звернення: 08.11.2024).

107. Report on Europe and the global information society. Brussels, 1994. URL: https://aei.pitt.edu/1199/1/info_society_bangeman_report.pdf (дата звернення: 08.11.2024).