МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ МІЖНАРОДНИХ ВІДНОСИН
КАФЕДРА МІЖНАРОДНИХ ВІДНОСИН, ІНФОРМАЦІЇ ТА РЕГІОНАЛЬНИХ СТУДІЙ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____Ніна РЖЕВСЬКА
«20» 12 2023 р.

КВАЛІФІКАЦІЙНА РОБОТА
ЗДОБУВАЧА ВИЩОЇ ОСВІТИ ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРА
СПЕЦІАЛЬНОСТІ 291 «МІЖНАРОДНІ ВІДНОСИНИ, СУСПІЛЬНІ КОМУНІКАЦІЇ ТА РЕГІОНАЛЬНІ СТУДІЇ»
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
«МІЖНАРОДНА ІНФОРМАЦІЯ»

Тема: «ІНФОРМАЦІЙНА ПОЛІТИКА США В СУЧАСНИХ МІЖНАРОДНИХ ВІДНОСИНАХ»

Виконавець: здобувачка вищої освіти 2 курсу, 208-М групи Сидоркевич Анастасія Дмитрівна

Керівник: к.іст.н., доцент кафедри міжнародних відносин, інформації та регіональних студій, Дерев'янко Ігор Петрович

Нормоконтролер _____ Сергій ТРОЯН
(підпис)

КИЇВ 2023

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ВСТУП……..3

РОЗДІЛ 1. ТЕОРЕТИЧНИЙ АСПЕКТ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ В МІЖНАРОДНИХ ВІДНОСИНАХ……...…….……6

1.1. Поняття інформаційної політики та її аспекти……..….....6

1.2. Теоретичні підходи до аналізу інформаційної політики в міжнародних відносинах…….……11

1.3. Інструменти інформаційної політики США.....18

РОЗДІЛ 2. ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЗОВНІШНЬОПОЛІТИЧНОЇ ДІЯЛЬНОСТІ США

2.1. Нормативно-правова база інформаційної політики США

2.2. Базові принципи, політичні пріоритети інформаційної політики США

2.3. Концепція національної інформаційної політики США

РОЗДІЛ 3. ІНФОРМАЦІЙНА ПОЛІТИКА США В КОНТЕКСТІ ЗБРОЙНОЇ АГРЕСІЇ РОСІЇ…….

3.1. Специфіка використання інформаційних технологій та ЗМІ США в умовах російської агресії……..

3.2.Протидія російській пропаганді та маніпуляціям як частина сучасної інформаційної стратегії США

ВИСНОВКИ

СПИСОК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

ДОДАТКИ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІБ – інформаційна безпека

ІТТ – інформаційно-телекомунікаційні технології

МЗС – Міністерство закордонних справ

НАТО – North Atlantic Treaty Organization

ОБСЄ – Організація з безпеки та співробітництва Європи

ООН – Організація Об'єднаних Націй

РЕМ – радіоелектронних засобів

BBC – British Broadcasting Corporation

CISA – Certified Information Systems Auditor

CNN – Cable News Network

DHS – Department of Homeland Security

DISA – Direct Inward System Access

FEMA – The Federal Emergency Management Agency

IEC – International Electrotechnical Commission

ISO – International Organization for Standardization

NSA – National Security Agency

NSS – Network Security Services

RFE – Radio Free Europe

RL – Radio Liberty

USCERT – United States Computer Emergency Readiness Team

VOA – Voice of America

ВСТУП

Актуальність даного дослідження визначається передусім сучасним станом міжнародних відносин і виникненням конфліктів між окремими країнами. Розгляд інформаційної політики США у сучасних міжнародних відносинах є важливою темою, яка залежить від багатьох чинників. США з різних причин вже починаючи з минулого століття стали одним із найбільш помітних гравців на міжнародній арені у питаннях, так чи інакше пов'язаних з інформаційною діяльністю (та інформаційними війнами, як їх проявом), формуванням дискурсу та громадської думки (і протистояння за право та можливість їх формувати), а також з публічною дипломатією, яка так чи інакше має точки дотику з усім вище переліченим. У сучасному світі, де інформація стала найбільш цінним ресурсом, країни змагаються за лідерство в цьому аспекті. Роль інформаційної політики США виявляється важливою в рамках їхньої зовнішньої політики та має значущий вплив на міжнародну сцену.

Інформаційна політика, яку проводять США, є величезним комплексом завдань і проблем, і повинна постійно підлаштовуватися під сучасне суспільство. Інформаційний простір зростає разом з інформаційним суспільством, утворюючи глобальний процес трансформації засобів масової інформації відповідно до потреб суспільства. Ця інформація здатна впливати на всі основні сфери життя держави.

З розвитком інформаційних технологій доступ до отримання інформації значно спрощується, оскільки розвивається концепція міжнародного мовлення, мережа Інтернет дає відкритий доступ до практично будь-якого виду інформації, телевізійне мовлення розширює межі свого мовлення, здійснюючи його в інших державах. За допомогою соціальних мереж жителі різних держав можуть бути ближчими один до одного, а політики відразу можуть спостерігати трансформацію громадської думки щодо тієї чи іншої політичної дії. Американська інформаційна політика розвиває досить широку мережу свого мовлення у вигляді різних новин на каналах, а й шляхом мовлення через популярні платформи та соціальні мережі. Зацікавлені користувачі мережі Інтернет, які стежать за політичними діями США, відразу можуть бути в курсі всіх подій, що відбуваються у світі, оновлюючи, наприклад новини в Twitter.

Міжнародне мовлення об'єднує у собі багато інструментів, утворюючи цілу мережу, поширену у своїй державі, а й у світі. Засоби масової інформації, які є основним механізмом міжнародного мовлення, здатні здійснити багато політичних завдань. Привернення уваги народу залежить від грамотного розподілу обов'язків між різними видами ЗМІ. У цю мережу входить, безумовно, вся мережа Інтернет, включаючи канали новин, а також телевізійне мовлення. Сполучені Штати намагаються сформувати позитивний образ про себе, намагаючись просувати виключно позитивні новини про життя у своїй країні і про політику, що проводиться. Інформаційна політика, як Сполучених Штатів розвивається у межах будь-якої концепції. Інформація часто розглядається як інструмент політики м'якої сили, що здійснюється з боку держави.

Інформаційна політика США, як ключовий компонент їхньої зовнішньої стратегії, пройнята багатьма вимірами, включаючи дипломатію, економіку, безпеку та вплив на громадську думку. Дослідження цього аспекту дозволяє краще розуміти, як країна використовує інформаційні ресурси для формування свого образу, впливу на події в світі та досягнення своїх стратегічних цілей.

Війна, яку розгорнула Росія проти України визначила основного союзника України у протистоянні російській агресії. Тиждень перед повномасштабним вторгненням, Сполучені Штати оприлюднили конфіденційні дані розвідки та попередили Україну про можливий наступ. Саме США активно просували ідею підтримки іншими країнами економічних санкцій проти Росії, з метою визнання її агресорського статусу та відокремлення її від міжнародного співтовариства. В інформаційній сфері всі американські ЗМІ з самого початку активно транслюють новини та останні події в Україні, стосовно біженців, гуманітарної кризи, постачання військового обладнання, обстрілів мирних мешканців та наслідків руйнування інфраструктури. Суттєву роль відіграє антипропагандистська стратегія США у соціальних мережах та телебаченні, спрямована на блокування розповсюдження дезінформації серед російських громадян і активне відвернення від фейкових новин, які можуть негативно впливати на репутацію України та президента Зеленського.

Мета – проведення аналізу і дослідження інформаційної політики Сполучених Штатів в контексті сучасних міжнародних відносин.

Відповідно до поставленої мети було сформульовано низку завдань:

1. Визначити поняття інформаційної політики та її аспекти;
2. Виявити теоретичні підходи до аналізу інформаційної політики в міжнародних відносинах;
3. Розкрити інструменти інформаційної політики США;
4. На основі комплексного аналізу офіційних документів виявити особливості нормативно-правових баз інформаційної політики США;
5. Визначити концепцію національної інформаційної політики США;
6. Дослідити роль інформаційної сфери США в умовах російської збройної агресії проти України.

Об'єкт дослідження – інформаційна політика.

Предметом дослідження є інформаційна політика США на сучасному етапі розвитку міжнародних відносин.

Методологічна основа дослідження. Функціональний метод був використаний задля вивчення поняття «інформаційна політика», виявлення її аспектів та функцій. Системний метод дозволив комплексно підійти до розуміння проблем інформаційної політики США відносно Росії та України в умовах війни.

Наукова новизна отриманих результатів. Наукова новизна полягає в проведенні аналізу інформаційної політики США в контексті російської агресії проти України саме в 2022-2023 роках.

Практичне значення отриманих результатів. Результати дослідження кваліфікаційної роботи можуть стати в нагоді для написання статей, тез, курсових робіт студентів в галузі інформаційної політики, кібербезпеки США. У цілому, наукова робота з даної теми може слугувати основою для подальших розробок та

удосконалень наукових робіт в контексті майбутнього розвитку інформаційної політики США в умовах сучасних міжнародних відносин.

Особистий внесок випускника.

Структурно кваліфікаційна робота складається зі вступу, трьох розділів, висновків і списку використаних інформаційних джерел.

Отже, в даній роботі підкреслюється всепроникаюча роль американських засобів і підтверджується їхнє значне місце у системі впливу суспільних настроїв. Крім того, засоби масової інформації в США відіграють значну роль у процесі зовнішньої політики, вносячи свій внесок як спостерігачі, учасники і каталізатори. Отже, обрана тема дипломної роботи є актуальною проблемою світової та міжнародної політики.

РОЗДІЛ 1. ТЕОРЕТИЧНИЙ АСПЕКТ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ В МІЖНАРОДНИХ ВІДНОСИНАХ

1.1 Поняття інформаційної політики та її аспекти

Основна тенденція розвитку світової спільноти наприкінці XX століття – це інтенсивний перехід до нового типу демократичного суспільства – відкритого інформаційного суспільства. Революційні зміни в галузі інформаційно-телекомунікаційних технологій (ІТТ) зумовлюють той факт, що інформація, інформаційні процеси та ІТТ, що забезпечують їх, в даний час відіграють визначальну роль у всіх сферах діяльності суспільства і держави.

Інформаційні процеси мають значний, а часом і визначальний вплив не тільки на економічний, соціальний, політичний, науково-технічний та культурний розвиток суспільства, а й на зміну світогляду людей, морально-психологічні та поведінкові аспекти їх життєдіяльності, державний устрій та функціонування державного механізму, загалом на інфраструктуру міжособистісних, суспільних, усередині та міждержавних відносин. Інформаційна сфера стає одним із найважливіших об'єктів державного управління, а її регулювання у багатьох країнах визнано не лише актуальним, а й пріоритетним завданням державного управління.

Основний інструмент державного управління інформаційною сферою, що визначає зміст такого управління – державна інформаційна політика.

В даний час саме інформація є основним фактором для розвитку суспільства та держави, а інформаційні процеси вважаються найважливішою складовою всіх внутрішньополітичних та зовнішньополітичних процесів життєдіяльності країни. Державну інформаційну політику слід розглядати як сукупність:

– цілей, що відображають національні інтереси в інформаційній сфері;

– стратегії та тактики управлінських рішень та методів їх реалізації, що розробляються та реалізуються державною владою для регулювання та

вдосконалення як безпосередньо процесів інформаційної взаємодії у всіх сферах життєдіяльності суспільства та держави, так і процесів (у широкому сенсі) технологічного забезпечення такої взаємодії.

Інформаційна політика полягає у використанні ресурсів державної влади для знаходження ефективних шляхів вирішення найактуальніших проблем розвитку інформаційної сфери.

До таких проблем можна віднести такі:

– Покращення життєвого рівня всіх членів суспільства;

– зміцнення гарантій держави щодо прав та свобод людини і громадянина у сфері інформаційної діяльності;

– активізація процесу переходу суспільства у фазу інформаційного (постіндустріального) розвитку;

– створення промисловості конкурентоспроможних інформаційних технологій;

– забезпечення безпеки інформаційних та комунікаційних систем критично важливих об'єктів;
– збереження цінностей культури та моралі.

Вищезазначені проблеми мають певний ступінь соціальної значущості і можуть стати об'єктом інтересів політичних сил суспільства, а діяльність з їх вирішення – скласти один із аспектів інформаційної політики.

Державна інформаційна політика – це здатність та можливість суб'єктів політики впливати на свідомість, психіку людей, їх поведінку та діяльність за допомогою інформації на користь держави та громадянського суспільства.

У більш широкому значенні – це особлива сфера життєдіяльності людей, пов'язана з відтворенням та поширенням інформації, що задовольняє інтереси держави та громадянського суспільства, та спрямована на забезпечення творчого, конструктивного діалогу між ними та їх представниками.

Держава займає особливу увагу серед суб'єктів інформаційної політики. Це зумовлено його специфічною роллю у забезпеченні функціонування політичної системи суспільства.

Сутність державної інформаційної політики у суспільному вимірі полягає у створенні умов для розвитку інформаційної сфери, що забезпечують ефективне функціонування держави та її сталий розвиток, а також для залучення людей до об'єднання заради розвитку культурних та збереження моральних цінностей суспільства, що становлять духовну основу її існування.

Об'єктами державної інформаційної політики є політична свідомість та громадська думка, а предметом – методи та засоби державного впливу на політичну свідомість та громадську думку з метою залучення громадян до підтримки заходів державної політики, до участі у цих заходах, а також методи та засоби протидії «інформаційному тиску» на державу та суспільство з боку нелегітимних політичних сил суспільства та політичних сил зарубіжних держав. Поняття «інформаційна політика» останнім часом стало досить популярним. Воно використовується як юридичний термін, широко застосовується у засобах масової інформації, у політичній, юридичній, соціологічній літературі. Разом про те саме поняття залишається недостатньо певним. У нього часто вкладається різний зміст та зміст. В умовах, коли інформація та інформаційні технології стають одним із ключових факторів суспільного життя, розуміння сутності та змісту поняття «інформаційна політика» є дуже актуальним.

Питання, що стосуються теоретичних та практичних аспектів інформаційної політики, розглядали багато авторів. Видається важливим виділити праці Ж. Бодрійяра, П. Бурдьє, Т. А. Ван Дейка, М. Кастельса, У. Ліппманна, Н. Лумана, М. Фуко, У. Еко, М. М. Грачова, А .В. Манойло , В. Д. Попова та ін., присвячені проблемам політичної комунікації, дискурсивного характеру владних взаємин, процесам медіатизації та віртуалізації сучасної політики. З українських авторів варто виділити роботи І. В. Аристової («Державна інформаційна політика: організаційно-правові аспекти», «Еволюційний розвиток поняття інформаційна сфера»), Г. Г.

Почепцова «Сучасні інформаційні війни», «Як працюють механізми інформаційної війни»), С. А. Чукут («Інформаційна політика»), Ю. П. Сурміна та ін.

Інформаційна політика може бути описана як сукупність законів, правил і політичних рішень, які визначають, сприяють або обмежують процеси створення, використання, зберігання, доступу до інформації та її передачу і поширення. Взагалі інформаційна політика включає три головні напрямки:

Громадська інформація. Цей напрямок включає діяльність уряду щодо створення та поширення інформації, включаючи фінансування досліджень і розробок, публікацію законодавства та адміністративних рішень, а також матеріали культурного характеру та інше.

Інфраструктура інформації. Цей напрямок включає в себе регулювання сфери телекомунікацій та мовлення, забезпечення інфраструктури для навчальних закладів та бібліотек, збереження безпеки та цілісності інфраструктури та інші аспекти.

Інституційна та юридична інфраструктура. Цей напрямок включає участь держави в міжнародних договорах та організаціях, встановлення правил конфіденційності, антимонопольної політики, захисту інтелектуальної власності та інші правові аспекти.

В розвинених країнах інформаційна політика включає в себе дії компетентних органів держави, які контролюють, регулюють та планують процеси у сфері отримання, зберігання, обробки, використання та поширення інформації. Ці країни активно впроваджують правові норми для впорядкування відносин у національному інформаційному просторі та модернізують органи влади, що відповідають за інформаційну політику. В таблиці 1.1 зображено порівняльну характеристику державної інформаційної політики розвинених країн.

Таблиця 1.1

Країна	Характеристика інформаційної політики
Великобританія	Головна мета полягає в поліпшенні умов конкуренції на інформаційному ринку, підвищенні результативності надання інформаційних послуг та впровадженні інформаційних технологій у сферу державного управління. Серед головних пріоритетів варто виділити освіту, охорону здоров'я і підтримку приватного сектору. Ця мета досягається через дотримання таких принципів, як технологічна нейтральність законів, підтримка міжнародного співробітництва та захист прав інтересів споживачів у сфері комп'ютерних систем і мереж.
Німеччина	Головна мета полягає у забезпеченні незавадного транскордонного обміну інформацією і забезпеченні свободи слова. Також метою є розвиток інформаційно-комп'ютерних технологій і телекомунікаційних мереж, створення умов для вільної конкуренції в інформаційній сфері і встановлення нових норм і принципів правового регулювання інформаційної діяльності в німецькому суспільстві. Ця ініціатива спрямована на підтримку реформування державного управління у зазначених країнах, їх участь у вільному транскордонному обміні інформацією, популяризацію цінностей європейської демократії, створення правової основи, технічного забезпечення сектору інформаційних технологій та підготовку кваліфікованих спеціалістів для національних та приватних корпорацій, організацій, фондів і т. д.

Франція	Головна мета цього завдання полягає у розвитку інфраструктури для інформаційних мереж, розширенні можливостей електронного ринку і банківської сфери, забезпеченні вільного доступу до комунікаційних засобів, перегляді інформаційного законодавства з метою внесення реформ, підтримці наукових досліджень у сфері інформаційних технологій, створенні систем безпеки інформації та запобіганні комп'ютерним злочинам. Уряд також утворив Фонд допомоги і співробітництва для підтримки впровадження вітчизняних інформаційних технологій.
Японія	Головна ціль полягає у створенні дієвого інформаційного суспільства, заснованого на доступі до засобів оптичного волокна для урядових інститутів, державних організацій і приватних підприємств, які потребують спеціалізованого програмного забезпечення.
США	Основна мета полягає у налагодженні контролю над інформаційними потоками в політичній, економічній, науковій та військовій сферах з метою забезпечення балансу між державним наглядом і свободою підприємницької діяльності. Основними пріоритетами є підтримка наукових досліджень і розробок в галузі інформатизації і телекомунікацій, сприяння обміну технологіями між університетами і фірмами, розвиток та покращення інформаційної інфраструктури, включаючи глобальну, збалансованість між основними інформаційними цінностями та впровадженням нових інформаційних технологій, а також вдосконалення

	державної політики у сфері інформатизації і телекомунікацій.
Європейський союз (ЄС)	Ця ініціатива ґрунтується на концепції єдиного загального підходу до інформаційної політики, яка втілюється у концепції співробітництва в Європейському просторі інформації та зв'язку. Вона розглядається та реалізується на різних рівнях - місцевому, регіональному, національному і наднаціональному, і всі ці рівні управління інтегровані в одну цілісну систему.

Сенс поняття «інформаційна політика» розкривається через розуміння доданків «інформаційна» та «політика». Поняття «політика» виступає тут як іменник, що підпорядковує поняття, а «інформаційна» – як прикметник, що характеризує основне поняття «політика». Тобто поняття «політика» ширше, ніж поняття «інформаційна політика» та перекриває останнє. Поняття «політика» має надзвичайно широке значення і охоплює всі види діяльності з самостійного керівництва (М.Вебер). Політика ґрунтується на владних взаємодіях, тобто відносинах між лідерством та підпорядкуванням. Традиційне визначення політичної діяльності – «мистецтво та наука управління». М.Вебер писав навіть про політику розумної дружини, яка прагне керувати своїм чоловіком. Політика є одним з різновидів управління, його окремим випадком. Але, перш за все, політика розуміється як сфера діяльності, пов'язана з відносинами між класами, націями та іншими соціальними групами, ядром якої є проблема завоювання, утримання та використання державної влади; діяльність державної влади у галузі управління та міжнародних відносин; діяльність того чи іншого суспільного угруповання, партії, класу, що визначається їх цілями та інтересами. Існує безліч способів визначення поняття «інформація», як і спроби взагалі відмовитися від його визначень. Кожне з визначень відбиває те що, що саме поняття мінливе. У зв'язку з цим поняття «інформація» визначається в кожній області та для кожної оригінальної задачі спеціальним чином. У будь-якому випадку

інформація – це результат зовнішнього знакового впливу та його інтерпретації, а не власного досвіду людини.

Інформаційна політика є використання інформації як засобу для досягнення політичних та інших цілей, інформаційний вплив політичних акторів один на одного. Влада – це інформаційна взаємодія між керуючим та керованим. В інформаційному суспільстві політика та інформація – взаємозалежні явища, що впливають один на одного у процесі соціального управління. Інформаційна політика є регулятором більшості сфер життєдіяльності людини.

2.1. Теоретичні підходи до аналізу інформаційної політики в міжнародних відносинах

Теоретичні підходи до аналізу інформаційної політики в міжнародних відносинах відображають різні школи думок і підходи до розуміння важливості і впливу інформації в міжнародній арені. Ось деякі з найважливіших теоретичних підходів:

Реалістичний підхід. Реалізм в міжнародних відносинах вважає держави основними акторами інтернаціональної системи, і його підхід до інформаційної політики акцентує на важливості інформації для збереження та розширення влади і впливу країн. Згідно з реалізмом, інформаційна політика може бути використана для розповсюдження пропаганди, дезінформації та маніпуляції з метою досягнення національних стратегічних цілей.

Реалістичний підхід до аналізу інформаційної політики в міжнародних відносинах базується на основних принципах реалізму як теоретичного підходу до міжнародних відносин. Цей підхід наголошує на ролі держав та їх стратегічних інтересах у міжнародній арені і розглядає інформаційну політику як інструмент

досягнення цих інтересів. Основні аспекти реалістичного аналізу інформаційної політики включають наступні:

Державна безпека та влада. Реалісти вважають, що головним завданням держави є забезпечення своєї безпеки та збільшення своєї влади у міжнародній системі. Інформаційна політика використовується для захисту національних інтересів і впливу на інших акторів.

Пропаганда і дезінформація. Науковці вважають, що держави використовують інформаційні засоби для поширення своєї пропаганди та дезінформації в інших країнах з метою підірвати довіру до конкуруючих держав та домогтися своїх цілей.

Баланс влади і стратегічний обмін інформацією. Інформаційну політику розглядають як одну з форм стратегічного взаємодії між державами. Інформація може бути використана для переваження у важливих міжнародних питаннях або для досягнення компромісів у випадку стратегічного обміну інформацією.

Інформаційна війна. В даному аспекті інформаційна політика – складова військових конфліктів. Реалісти визнають, що інформаційні атаки можуть супроводжувати або передувати військовим операціям і використовувати для дестабілізації противника та морального підриву.

Кібербезпека. Відзначають важливість кібербезпеки в інформаційній політиці. Інформаційні атаки на комп'ютерні мережі та інфраструктуру можуть бути використані для здійснення кібершпигунства, кібертероризму або кібервійни з метою зламати безпеку інших держав.

Реакція на інформаційні загрози. Науковці підкреслюють важливість здатності держави реагувати на інформаційні загрози шляхом створення силових або кібернетичних відповідей, а також захисту критично важливих інформаційних ресурсів.

Загалом, реалістичний підхід до аналізу інформаційної політики в міжнародних відносинах підкреслює жорстку конкуренцію та боротьбу за владу в міжнародній

системі, де інформація є ключовим ресурсом для досягнення стратегічних цілей держав.

Ліберальний підхід. Лібералізм вважає, що не тільки держави, але і інші актори, такі як міжнародні організації, неурядові організації та громадянське суспільство, мають роль у міжнародних відносинах. Ліберальний підхід до інформаційної політики розглядає акцент на важливості вільного обміну інформацією, відкритості та діалогу як інструментів для досягнення спільних цілей.

Ліберальний підхід до аналізу інформаційної політики в міжнародних відносинах базується на основних принципах лібералізму як теоретичного підходу до міжнародних відносин. Цей підхід наголошує на ролі різних акторів, включаючи держави, міжнародні організації, неурядові організації, громадянське суспільство та глобальну громадськість, у формуванні інформаційної політики та міжнародної спільноти. Основні аспекти ліберального аналізу інформаційної політики включають наступні:

Вільний обмін інформацією. Ліберальні вважають, що вільний обмін інформацією сприяє розвитку міжнародного співробітництва та сприяє врегулюванню міжнародних конфліктів. Вони підтримують принцип свободи преси, доступу до інформації та відкритості.

Неурядові організації та громадянське суспільство. Ліберальні вважають, що неурядові організації та громадянське суспільство мають важливу роль у формуванні інформаційної політики. Вони можуть брати участь у міжнародних діалогах, вносити пропозиції щодо розв'язання міжнародних проблем і впливати на прийняття рішень.

Міжнародні норми і права. Прихильники даного підходу підтримують ідею створення міжнародних норм і прав, які регулюють поведінку держав та акторів у сфері інформаційної політики. Основні документи, такі як Міжнародний пакт про громадянські та політичні права, підтримують права на свободу слова та інформаційну відкритість.

Міжнародний діалог і співробітництво. Науковці вірять у важливість діалогу та співробітництва між державами та акторами на міжнародній арені. Інформаційна політика може використовуватися для створення позитивних зв'язків та сприяння спільним ініціативам.

Громадська думка і міжнародна громадськість. В контексті даного аспекту вважається, що громадська думка та міжнародна громадськість можуть впливати на інформаційну політику держав і створювати тиск на владу для дотримання міжнародних норм і стандартів.

Довіра та співробітництво. В даному аспекті ліберального аналізу науковці вважають, що довіра та співробітництво між державами сприяють розвитку інформаційної політики та міжнародного співробітництва. Вони підтримують ініціативи з підвищення довіри між державами, такі як обмін інформацією про військові дії або кібербезпеку.

Загалом, ліберальний підхід до аналізу інформаційної політики в міжнародних відносинах підкреслює роль інформації як інструменту співробітництва, міжнародних норм та прав, а також важливість активної участі різних акторів у формуванні міжнародної інформаційної політики.

Конструктивний підхід. Конструктивізм акцентує на ролі ідентичності та ідеології в міжнародних відносинах і розглядає інформаційну політику як засіб для формування і зміни ідентичностей та переконань акторів. За цим підходом, інформація не просто впливає на рішення, вона може змінювати структуру системи через створення нових норм та ідентичностей.

Конструктивний підхід до аналізу інформаційної політики в міжнародних відносинах базується на ідеях конструктивізму як теоретичного підходу до міжнародних відносин. Цей підхід відзначається акцентом на ролі ідентичностей, ідеологій та соціальних конструкцій у формуванні інформаційної політики та міжнародних спільнот. Основні аспекти конструктивного аналізу інформаційної політики включають наступні:

Конструкція ідентичностей. Конструктивізм вважає, що ідентичності держав та акторів формуються та змінюються в процесі соціальної конструкції. Інформаційна політика може впливати на сприйняття та формування ідентичностей акторів на міжнародній арені.

Соціальні норми та цінності. В даному аспекті розглядається інформаційна політика як інструмент для поширення та закріплення соціальних норм і цінностей в міжнародних відносинах. Інформація може впливати на утвердження інтернаціональних норм та сприяти прийняттю спільних цінностей.

Інформаційна архітектура. Конструктивісти розглядають інформаційну архітектуру міжнародної системи, включаючи ЗМІ, соціальні мережі, освітні інституції та інші канали комунікації, як важливий фактор у формуванні міжнародної інформаційної політики.

Міжнародний епістемологічний спільний простір. Акцентується на створенні спільного культурного, епістемологічного та мовного простору, де держави та актори можуть взаємодіяти та обмінюватися інформацією. Це сприяє розвитку довіри та співробітництва.

Інформаційний обмін і діалог. Прихильники даного підходу підтримують інформаційний обмін та діалог як засоби для розв'язання міжнародних конфліктів і підтримки міжнародних домовленостей.

Прозорість і відкритість. Важливим аспектом конструктивного підходу є підтримка прозорості та відкритості в інформаційній політиці, що сприяє підвищенню довіри між державами та акторами.

Неореалізм і неолібералізм. Ці підходи поєднують аспекти реалізму і лібералізму, звертаючи увагу на важливість структури системи та інтересів держав. Вони розглядають інформаційну політику як важливий фактор, але аналізують її в контексті міжнародних структур і раціональних обчислень держав.

Теорія міжнародної комунікації. Ця теорія спеціалізується на дослідженні комунікаційних процесів між державами та іншими акторами в міжнародних відносинах. Вона досліджує вплив медіа, дипломатичних каналів комунікації та інших факторів на формування інформаційної політики. Основні аспекти теорії комунікації, які можна використовувати для аналізу інформаційної політики в міжнародних відносинах, включають наступні:

Мас-медіа та глобальна комунікація. Теорія комунікації допомагає розуміти вплив глобальних мас-медіа на міжнародну інформаційну політику. Вона дозволяє аналізувати, як мас-медіа формують глобальний інформаційний порядок, впливають на сприйняття подій та взаємовідносини між державами.

Міжнародна дипломатія та комунікація. Теорія комунікації допомагає розуміти роль комунікації у міжнародній дипломатії та переговорах. Вона дозволяє аналізувати способи спілкування між державами, обмін інформацією та використання мови в процесі вирішення міжнародних конфліктів і укладення міжнародних угод.

Символічна політика і імідж. Теорія комунікації допомагає розуміти важливість символів та іміджу для міжнародних держав. Вона дозволяє аналізувати, як держави конструюють свій імідж у світі через використання символів, логотипів, культурних обмінів і т. д.

Вплив інформаційної технології. Теорія комунікації розглядає вплив інформаційних технологій, зокрема інтернету і соціальних мереж, на міжнародну комунікацію. Вона допомагає аналізувати роль цих технологій у поширенні інформації, мобілізації громадян та організації глобальних кампаній.

Міжкультурна комунікація і мовна різноманітність. Теорія комунікації враховує міжкультурні аспекти інформаційної політики, де різні культури та мови взаємодіють. Вона допомагає розуміти, як мовна різноманітність може впливати на ефективність інформаційної комунікації між державами.

Дипломатична комунікація та кризовий менеджмент. Теорія комунікації може бути корисною для аналізу дипломатичної комунікації під час міжнародних криз та

конфліктів. Вона допомагає розуміти, як ефективна комунікація може допомогти у врегулюванні криз та запобіганні ескалації конфліктів.

Загалом, теорія комунікації надає важливий фреймворк для аналізу інформаційної політики в міжнародних відносинах, допомагаючи розуміти, як інформація впливає на сприйняття, взаємодію та поведінку держав та інших міжнародних акторів.

Геополітичний підхід. Геополітичний підхід аналізує інформаційну політику в контексті геостратегії та впливу географічних факторів на інформаційний обмін та вплив держав у міжнародних відносинах.

Кожен з цих теоретичних підходів надає відмінний погляд на інформаційну політику в міжнародних відносинах і допомагає розуміти, як інформація впливає на прийняття рішень, взаємодію між державами та розвиток міжнародної системи.

1.3. Інструменти інформаційної політики США

Регулювання сфери інформації стало пріоритетом американської державної політики раніше, ніж у інших країнах. Це зв’язано з тим, що саме США стали епіцентром інформаційної революції у другій половині XX століття. Після економічного буму 1990-х р., коли адміністрація У. Клінтона прагнула отримати максимум економічної вигоди від інформаційно-технологічної революції, відбулося різке посилення державного контролю. Пріоритетом адміністрації Дж. Буша-мол. була протидія тероризму, що потребувало посилення державного контролю за інформаційними ресурсами. Такі заходи викликали потужні протести з боку громадянського суспільства, під впливом яких ці рішення було переглянуто за адміністрації президента Б. Обами. Традиції індивідуалізму визначили генеральний підхід американської політичної системи до викликів інформаційної доби. Ключовий виклик у тому, щоб гарантувати рівні можливості виробництва та споживання

інформації кожному індивіду. У зв'язку з цим адміністрація Б. Обами прийняла «net neutrality» – принцип «нейтральності мережі», в основу якої були покладені роботи в галузі права американського професора права Тіма Ву. Американський правознавець стверджував, що інтернет має розвиватися згідно з принципом рівності, який виявляється у тому, що всі інформаційні мережі мають прагнути забезпечити рівний доступ усіх користувачів до будь-якого цифрового контенту.

Інформаційна політика Сполучених Штатів Америки включає в себе різні інструменти та засоби, які використовуються для досягнення своїх інтересів і впливу на міжнародні відносини. Деякі з основних інструментів інформаційної політики США включають:

1. Глобальні медіа

Глобальні медіа є одним з ключових інструментів інформаційної політики Сполучених Штатів Америки у міжнародних відносинах. Вони грають значущу роль у формуванні світової громадської думки, впливі на події в різних країнах і поширенні американської інформації та поглядів. Ось деякі способи, якими глобальні медіа використовуються як інструмент інформаційної політики США:

Поширення американських поглядів. Глобальні медіа, такі як CNN, BBC America, інтернаціональні видання The New York Times і The Washington Post, допомагають поширювати американську точку зору на міжнародному рівні. Це може включати в себе аналізи, коментарі та інтерв'ю з американськими експертами і представниками влади.

Засудження порушень прав людини. Глобальні медіа часто висвітлюють порушення прав людини у різних країнах та закликають до дій. Це може змушувати уряди приймати заходи або змінювати свою політику.

Покликання до демократії та свободи слова. Медіа, підтримувані США, часто акцентують важливість демократії та свободи слова. Це сприяє формуванню громадської думки та підтримці громадянського суспільства у різних країнах.

Інформація про події в США. Глобальні медіа висвітлюють події в США, що стосуються міжнародного співробітництва, зовнішньої політики та інших аспектів. Це допомагає сторонам у міжнародних відносинах бути в курсі подій та реагувати на них.

Публікація аналізів і досліджень. Глобальні медіа можуть публікувати аналітичні матеріали і дослідження, які стосуються міжнародних відносин і глобальних проблем. Це сприяє обговоренню важливих питань та розробці політики.

Висвітлення інтересів США. Глобальні медіа можуть використовувати інформаційні ресурси для висвітлення економічних, політичних та інших інтересів США в міжнародних відносинах. Загалом, глобальні медіа виступають як інструмент інформаційної політики США, сприяючи поширенню інформації, впливу та формуванню образу країни у світі.

2. Дипломатія та громадська дипломатія

Дипломатія і громадська дипломатія є важливими інструментами інформаційної політики Сполучених Штатів Америки (США) в міжнародних відносинах. Вони допомагають США сприяти своїм інтересам, встановлювати контакти з іншими країнами та впливати на глобальну арену. Ось докладніше про ці інструменти:

Дипломатія:

– Державні відділи зовнішніх справ. Дипломатичні представництва США у різних країнах та міжнародних організаціях використовуються для спілкування з урядами інших країн, проведення дипломатичних переговорів і вирішення міжнародних питань.

– Публічні виступи та прес-конференції. Дипломати США виступають перед міжнародними та національними ЗМІ, де коментують міжнародні події, відстоюють позиції США та пояснюють дії уряду.

– Дипломатичні ноти та листи. Ці документи використовуються для офіційних комунікацій між державами та для передачі офіційних повідомлень.

Громадська дипломатія:

– Культурна дипломатія. США використовують свою культурну спадщину, таку як музика, кіно, література та мистецтво, для сприяння міжнародному обміну та розумінню між країнами.

– Обмін студентами та академічні програми. Програми обміну, такі як програма «Фулбрайта» та інші, допомагають студентам та науковцям з інших країн навчатися в США та вивчати американську культуру.

– Інформаційні кампанії та освітні ініціативи. США запускають освітні ініціативи та інформаційні кампанії для поширення ідей демократії, прав людини і свободи слова.

Сприяння демократії і громадянському суспільству. США надають фінансову та технічну підтримку громадським організаціям, які працюють у сферах прав людини, демократії і громадянського суспільства.

Міжнародні програми та обміни. Програми, такі як Peace Corps, сприяють співпраці та взаєморозумінню між громадянами США і іншими країнами.

Економічна дипломатія. Залучення іноземних інвестицій, торгівля та економічне співробітництво також використовуються для досягнення зовнішньополітичних цілей США.

Громадська дипломатія та дипломатія разом із державними інструментами інформаційної політики створюють комплексний підхід для досягнення інтересів США та підтримки своїх цілей у міжнародних відносинах.

3. Пропаганда та інформаційна війна

Пропаганда і інформаційна війна можуть використовуватися як інструменти інформаційної політики Сполучених Штатів Америки у міжнародних відносинах, хоча це може бути спростовано або викрито іншими країнами та організаціями. Такі інструменти можуть бути використані:

Пропаганда:

– Інформація і комунікація. США можуть використовувати засоби масової інформації, соціальні медіа та інші канали для поширення певних інформаційних повідомлень та поглядів, що сприяють їхнім інтересам. Це може включати в себе висвітлення досягнень, ідеалів та цінностей, які підтримуються США.

– Дезінформація і контрпропаганда. Сполучені Штати можуть використовувати методи дезінформації, або навіть контрпропаганди, щоб заплутати або дискредитувати інші країни або групи, які вони вважають своїми ворогами або конкурентами.

– Підтримка опозиції та громадських рухів. США можуть підтримувати опозиційні рухи і громадські організації у країнах, де це відповідає їхнім інтересам і цілям. Це може включати в себе надання фінансової підтримки та розповсюдження інформації, яка сприяє зміні режимів або політики.

Інформаційна війна:

– Кібератаки і хакерські дії. США можуть використовувати кібератаки і хакерські дії для отримання інформації, впливу на системи зв'язку інших країн, або навіть знищення важливих об'єктів.

– Психологічні операції. Інформаційна війна може включати в себе психологічні операції для впливу на думку та переконання населення інших країн. Це може бути важливим для зміни ставлення до питань, які важливі для США.

– Захист власної інформації. США також здійснюють заходи для захисту своєї власної інформації та інфраструктури від можливих атак.

Важливо відзначити, що інформаційна війна та пропаганда можуть бути складними і спірними питаннями в міжнародних відносинах. Деякі дії можуть порушувати міжнародні стандарти і норми. Також інші країни і групи можуть вживати заходів для запобігання або відповіді на такі дії.

4. Міжнародне радіомовлення та телебачення

Міжнародне радіомовлення і телебачення є важливими інструментами інформаційної політики Сполучених Штатів Америки в міжнародних відносинах. Вони використовуються для впливу на громадську думку, формування образу країни, поширення ідеологій і цінностей, а також для надання інформації про події у світі. Засоби які використовують:

– Голос Америки (Voice of America, VOA). VOA є однією з найвідоміших міжнародних радіостанцій, що надає новини та інформацію в різних мовах. Вона спрямована на аудиторію в різних країнах і надає об'єктивні новини та аналіз подій.

– Радіо Свобода (Radio Free Europe/Radio Liberty, RFE/RL). RFE/RL надає інформацію для аудиторії в країнах, де інформаційна свобода обмежена. Вона допомагає поширювати альтернативні погляди та інформацію.

– Телеканал «Voice of America» (VOA TV). Це телевізійний канал, який також поширює новини та інформацію про США і світ у різних мовах.

– Трансляція через інтернет і соціальні медіа. США використовують онлайн-ресурси і соціальні медіа для висвітлення подій та поширення інформації. Це дозволяє доставляти контент до аудиторії у реальному часі.

– Надання технічної підтримки. США надають технічну підтримку для розвитку медіа та інформаційних ресурсів у країнах, де інформаційна інфраструктура слабка або обмежена.

– Поширення американської культури. Міжнародне радіомовлення і телебачення можуть поширювати американську культуру, музику, кіно та інші аспекти життя.

Ці засоби інформаційної політики допомагають США впливати на глобальну аудиторію, формувати образ країни та сприяти поширенню ідеалів, які вони визнають важливими. Однак важливо відзначити, що інформаційна політика має своєю метою надання об'єктивної інформації, а також забезпечення інформаційної свободи та правдивості в новинах.

5. Соціальні медіа

Соціальні медіа дозволяють США впливати на глобальну аудиторію, спілкуватися безпосередньо з громадськістю, поширювати ідеї та відстоювати позиції. Нижче наведено приклади, як соціальні медіа можуть бути використані в інформаційній політиці США.

Публікація новин та оновлень. Уряд США та посольства в інших країнах використовують соціальні медіа, такі як Twitter, Facebook, Instagram, і LinkedIn, для поширення новин, офіційних заяв і оновлень щодо подій у світі та діяльності США. Це дозволяє швидко і ефективно сповіщати громадськість та ЗМІ.

Дипломатична комунікація. Дипломатичні представництва США можуть використовувати соціальні медіа для спілкування з урядами і громадськістю інших країн. Це сприяє обміну інформацією та діалогу з партнерами.

Культурна дипломатія. Соціальні медіа використовуються для поширення американської культури, мистецтва, музики і інших аспектів американського життя. Це сприяє підтримці міжнародного обміну культурою та взаєморозумінню.

Кампанії проти дезінформації. Соціальні медіа використовуються для розповсюдження фактів і доказів, що спростовують дезінформацію та маніпуляцію. Це допомагає в боротьбі з дезінформацією та фейками.

Підтримка громадських рухів і прав людини. Соціальні медіа дозволяють публікувати інформацію про права людини, долю політв'язнів і громадські акції у країнах, де це важливо для інтересів США.

Прямий контакт з громадськістю. Сполучені Штати можуть взаємодіяти з громадськістю через коментарі, відповіді на запитання та дискусії на платформах соціальних медіа.

Сприяння обміну технологіями і знаннями. Соціальні медіа можуть бути використані для сприяння обміну технологіями, науковими дослідженнями та знаннями між США та іншими країнами.

Важливо відзначити, що соціальні медіа також мають свої виклики, такі як поширення дезінформації та приватність даних. Тому вони вимагають ретельного керівництва і контролю з боку влади для забезпечення об'єктивності та дотримання норм інформаційної політики.

6. Міжнародні організації

Міжнародні організації можуть бути важливим інструментом інформаційної безпеки Сполучених Штатів Америки в міжнародних відносинах, хоча їх роль головним чином полягає в співпраці та координації дій для забезпечення міжнародної стабільності та безпеки. Ось декілька способів, якими міжнародні організації можуть впливати на інформаційну безпеку США:

Стандарти та норми. Міжнародні організації можуть розробляти міжнародні стандарти та норми щодо інформаційної безпеки, кібербезпеки та обміну інформацією. Наприклад, Міжнародний стандарт ISO/IEC 27001 стосується управління інформаційною безпекою.

Співпраця в області кібербезпеки. Різні міжнародні організації, такі як ООН, ОБСЄ, НАТО, розвивають співпрацю в галузі кібербезпеки та інформаційної безпеки для обміну інформацією та виявлення загроз.

Обмін інформацією. Міжнародні організації можуть створювати механізми обміну інформацією про кіберзагрози та інші інформаційні загрози. Це допомагає країнам вчасно виявляти та реагувати на можливі загрози.

Лобіювання і вплив. США можуть використовувати свій вплив у міжнародних організаціях для встановлення стандартів та політик, які відповідають їхнім інтересам у сфері інформаційної безпеки.

Міжнародні договори та угоди. Міжнародні організації можуть сприяти укладенню міжнародних договорів та угод щодо кібербезпеки та інформаційної безпеки.

Кризовий менеджмент. Міжнародні організації можуть грати роль у кризовому менеджменті у випадку серйозних інформаційних або кібератак.

Доступ до ресурсів. Деякі міжнародні організації можуть надавати доступ до ресурсів, які допомагають в управлінні інформаційною безпекою та кіберзахистом.

Важливо відзначити, що міжнародна співпраця та координація є важливими аспектами інформаційної безпеки в світі, оскільки багато загроз є трансграничними і можуть впливати на багато країн одночасно. Міжнародні організації допомагають збалансовувати інтереси та забезпечувати безпеку в глобальному контексті.

7. Санкції та обмеження

Санкції і обмеження є одним із інструментів інформаційної безпеки, які використовуються Сполученими Штатами Америки для захисту своєї національної безпеки та інтересів в міжнародних відносинах. Ці інструменти можуть бути спрямовані проти країн, організацій або осіб, які сприяють загрозам для інформаційної безпеки США. Ось як вони можуть бути використані:

Економічні санкції. США можуть накладати економічні санкції на країни або організації, які здійснюють кібератаки або інші дії, що загрожують інформаційній безпеці. Це може включати замороження активів, обмеження торгівлі та фінансових операцій.

Заборона на ввезення програмного забезпечення і обладнання. Санкції можуть передбачати заборону на ввезення програмного забезпечення або обладнання з країн, які вважаються загрозою для кібербезпеки.

Санкції проти осіб та організацій. США можуть накладати санкції на індивідуальних хакерів, кіберзлочинців або організації, які здійснюють кібератаки або інші дії, що порушують інформаційну безпеку.

Законодавчі обмеження. США можуть приймати законодавчі акти, що обмежують доступ до деяких інформаційних ресурсів або забороняють співпрацю з країнами або організаціями, які загрожують інформаційній безпеці.

Співпраця з іншими країнами. США можуть співпрацювати з іншими країнами для спільного впровадження санкцій та обмежень, спрямованих на захист інформаційної безпеки.

Інформаційні кампанії. Поза санкціями, США також можуть вести інформаційні кампанії для розкриття загроз кібербезпеці та попередження атак.

Публічні звіти і засоби масової інформації. США можуть використовувати засоби масової інформації та публічні звіти для розкриття дій країн, які становлять загрозу для інформаційної безпеки.

Санкції і обмеження можуть бути ефективним інструментом у боротьбі з загрозами кібербезпеці та захисту інформаційної безпеки. Вони допомагають накладати відповідальність за кібератаки та забезпечують засоби для реагування на такі загрози. Однак важливо дотримуватися міжнародних норм і зобов'язань у процесі застосування санкцій і обмежень.

РОЗДІЛ 2. ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЗОВНІШНЬОПОЛІТИЧНОЇ ДІЯЛЬНОСТІ США

2.1. Нормативно-правова база інформаційної політики США

На сьогодні, нормативні документи, які визначають основні принципи національної безпеки та оборони, включаючи інформаційну політику (Доктрина інформаційної безпеки, Стратегічний оборонний бюлетень), передбачають, що співпраця з іноземними цивільними та військовими структурами, які підтримують обороноздатність та державну безпеку, є важливою гарантією зміцнення національної безпеки, включаючи інформаційну сферу. У відношенні до інформаційної політики та забезпечення інформаційної безпеки США можна розглядати як піонерів, оскільки це не лише держава, яка вперше в світі впровадила електронне управління з використанням сучасних інформаційних технологій, але і створила спеціальну систему захисту національного інформаційного суверенітету та безпеки інформаційних ресурсів.

Для розкриття стратегії інформаційної політики США необхідно проаналізувати ряд документів, законопроектів, ініціатив та стратегій, які визначили розвиток та формування сучасної концепції інформаційної політики та безпеки.

Початковим документом Пентагону, що стосується інформаційної безпеки (ІБ), є директива МО США Т3600.1 від 21 грудня 1992 року, під заголовком «Інформаційна війна». У 1993 році директива Комітету начальників штабів № 30 визначила основні принципи проведення інформаційної війни. Завершальним етапом визначення інформаційної війни стало визначення у 1997 році: «Дії, спрямовані на досягнення інформаційної переваги в рамках національної стратегії, і здійснювані за допомогою впливу на інформацію та інформаційні системи противника, при одночасному захисті власної інформації та інформаційних систем».

Перші основи військової стратегії інформаційної безпеки США були закладені в 1990-х роках. У 1995 році, за адміністрації Біла Клінтона, була опублікована

Стратегія національної безпеки, в якій було визначено завдання досягнення інформаційної переваги через наступальні та оборонні інформаційні операції.

У червні 1995 року Національний університет оборони у Вашингтоні випустив першу групу фахівців із інформаційної війни. Місяць пізніше військово-морський коледж у Ньюпорті завершив ігрове відпрацювання планів проведення інформаційних воєн. В січні – червні 1995 року в США було проведено командно-штабну військову гру (КШВІ), з участю представників усіх силових структур, мета якої полягала в розробці концепції стратегічної інформаційної війни.

Директива Президента № 63 «Про захист критичної інфраструктури», що була підписана президентом США у 1998 році, взяла на себе новий етап розвитку та була систематизована у формі «Національної стратегії безпеки кіберпростору». Також ця стратегія отримала визначення у Директиві Президента в галузі національної безпеки №7 «Про визначення, пріоритизацію та захист критично важливих елементів інфраструктури». В обох документах великий акцент був зроблений на створенні програми з мінімізації загроз у кіберпросторі.

Невдовзі після терористичних подій 11 вересня 2001 року, що підкреслили вразливість національної безпеки, адміністрація Джорджа Буша посилила зусилля щодо розробки конкретних механізмів забезпечення інформаційної безпеки. У 2003 році була розроблена Національна стратегія забезпечення безпеки кіберпростору, де адміністрація Буша визначила ключові програми, спрямовані на забезпечення національної кібербезпеки, запобігання кібератакам та зменшення вразливості критичної інфраструктури. Стратегія також наголошувала на важливості досягнення переваги через наступальні та оборонні інформаційні операції. Міністерство оборони виділило три випадки їх застосування: у мирний час, у період кризи і під час конфлікту, що свідчить про вирішальність керівництва країни у підсиленні своїх зусиль в кіберсередовищі для готовності до інформаційної оборони.

Стратегія 2003 року знайшла відображення у 2008 році, коли було запроваджено Комплексну ініціативу з національної кібербезпеки. Ця ініціатива стала фундаментом для подальшого розвитку інформаційної безпеки країни, підтверджуючи, що майбутні кіберзагрози вимагатимуть ще більших зусиль уряду

для впровадження технічних та організаційних можливостей для більш ефективного протидії сучасним загрозам та вразливостям.

У грудні 2006 року Комітет начальників штабів (КНШ) підготував документ під назвою "Національна військова стратегія кібернетичних операцій", який визначав стратегічні пріоритети для забезпечення інформаційної безпеки США. Серед цих пріоритетів були:

– Досягнення та утримання ініціативи в ході операцій, проводжених противником під час циклу прийняття рішень.

– Забезпечення захисту власних комп'ютерних систем та проведення наступальних дій у комп'ютерних мережах противника.

– Включення кібероперацій у військове планування для всього спектра збройних конфліктів з метою розроблення методів проведення таких операцій у тісній взаємодії з різними видами Збройних Сил та управліннями Міністерства оборони, які, у свою чергу, повинні узгоджувати свої дії з іншими агентствами США, союзниками з коаліції та промисловими підрядниками.

– Створення в межах Міністерства оборони необхідних умов для проведення кібернетичних операцій, включаючи організаційні заходи, підготовку фахівців та розбудову відповідної інфраструктури.

– Оцінка ризиків мережевих операцій, пов'язаних з недостатньо ефективним виділенням коштів або використанням противником уразливих місць у кіберпросторі США, а також внаслідок побічного ефекту від проведення наступальних операцій.

За даними Пентагону, лише у 2007 році було зафіксовано майже 44 тисячі інцидентів, які були визнані кібернетичними злочинами, вчиненими іноземними арміями, спецслужбами та окремими хакерами. Один з найбільших випадків стосувався крадіжки декількох терабайт даних про багатоцільовий винищувач-бомбардувальник п'ятого покоління F-35 «Лайтнінг-2», розроблюваний в США. Вартість проекту цього бойового літака оцінюється приблизно в 300 мільярдів доларів. Ці дані були вкрадені з серверів компаній-підрядників.

Важливо відзначити, що, незважаючи на те, що проблеми інформаційної безпеки в США почали активно вивчатися ще в 90-х роках і продовжили свій розвиток у 2000-х, адміністрація Барака Обами відзначилася початком принципово нового етапу у цьому напрямку. Президент Обама визнав ІБ як одну з найбільш серйозних загроз для національної безпеки, зокрема в контексті економічної сфери. Після приходу Обами до посади, йому було доручено переглянути федеральні заходи з захисту американської інформаційної інфраструктури.

У травні 2011 року Білий дім представив світові Міжнародну стратегію в кіберпросторі, в якій акцентувалася увага на необхідності військового стримування та протистояння, а також створення мирного та стабільного глобального кіберпростору за умови міждержавного співробітництва. Документ визначав важливість адаптації до зростаючих військових потреб у безпечних та надійних мережах. Крім того, він визнавав важливість розширення військових союзів для протистояння потенційним загрозам у кіберпросторі. Ця стратегія підкреслювала готовність адміністрації до співпраці з іншими країнами та підкріплювала принципи, якими керується сама адміністрація.

У липні 2011 року, також за адміністрації Обами, була ухвалена Стратегія дій Міністерства оборони у Кіберпросторі, яка стала першим документом, що визначав політику Міністерства оборони у цьому напрямку. Документ підкреслював значення забезпечення безпеки та надійності нового простору ІБ, який повинен захищати основні свободи громадян, їхнє приватне життя і забезпечувати вільний потік інформації, необхідної для успішного ведення військових операцій.

Однією з ключових проблем інформаційної безпеки для США залишалося комерційне шпигунство з боку Китаю, і, незважаючи на видані укази, ситуація не покращувалася. Важливим кроком у вирішенні цієї проблеми стало прийняття у 2012 році Національної Стратегії обміну та захисту інформації. Цей документ визначив три ключові принципи політики США з інформаційної безпеки: розгляд інформації як національного надбання; обмін та захист інформації з акцентом на розподіл загальних ризиків; прийняття кращих рішень завдяки інформації. Ця стратегія визначалася

потребою у нових та інноваційних методах захисту інформаційних мереж та структур в умовах постійних кібератак.

На завершення усіх попередніх стратегій у ніч на 24 квітня 2015 року Міністерство оборони США представило оновлену стратегію інформаційної безпеки країни. Документ підтверджував намір стримувати будь-які кібератаки та максимально захищати Сполучені Штати від будь-яких супротивників та інформаційного вторгнення. Стратегія визначала три групи потенційних загроз у кіберпросторі: окремі держави (Китай, Росія, Іран, Північна Корея), недержавні актори (Ісламська держава) та кіберзлочинці.

У грудні 2017 року адміністрація Дональда Трампа опублікувала «Стратегію національної безпеки США», де Китай визначався одним із суперників. Проте вказувалося, що Китай прагне змінити глобальне розміщення сил на своє користування, що може становити загрозу для США. Реакція МЗС Китаю була вимогою відмовитися від застарілих концепцій.

Однією з ключових проблем інформаційної безпеки для США залишалося комерційне шпигунство з боку Китаю, і, незважаючи на видані укази, ситуація не покращувалася. Важливим кроком у вирішенні цієї проблеми стало прийняття у 2012 році Національної Стратегії обміну та захисту інформації. Цей документ визначив три ключові принципи політики США з інформаційної безпеки: розгляд інформації як національного надбання; обмін та захист інформації з акцентом на розподіл загальних ризиків; прийняття кращих рішень завдяки інформації. Ця стратегія визначалася потребою у нових та інноваційних методах захисту інформаційних мереж та структур в умовах постійних кібератак.

На завершення усіх попередніх стратегій у ніч на 24 квітня 2015 року Міністерство оборони США представило оновлену стратегію інформаційної безпеки країни. Документ підтверджував намір стримувати будь-які кібератаки та максимально захищати Сполучені Штати від будь-яких супротивників та інформаційного вторгнення. Стратегія визначала три групи потенційних загроз у кіберпросторі: окремі держави (Китай, Росія, Іран, Північна Корея), недержавні актори (Ісламська держава) та кіберзлочинці.

У грудні 2017 року адміністрація Дональда Трампа опублікувала «Стратегія національної безпеки США», де Китай визначений одним із суперників. Проте вказувалося, що Китай прагне змінити глобальне розміщення сил на своє користування, що може становити загрозу для США. Реакція МЗС Китаю була вимогою відмовитися від застарілих концепцій.

19 січня 2018 року Міністерство оборони США оприлюднило нову Стратегію національної оборони США, в якій стверджувалося, що основною загрозою національній безпеці є стратегічне суперництво між державами. Документ визначав чотири держави (Китай, Росія, Північна Корея, Іран) та активність терористичних груп як головні загрози для американської безпеки.

У березні 2021 року президент Джо Байден представив Тимчасову стратегію національної безпеки (NSS) на 2021 рік. Ця стратегія повторно засвідчила зобов'язання Сполучених Штатів альянсу НАТО та визначила глобальні пріоритети країни. Президент прийшов до висновку, що Сполучені Штати "повинні продемонструвати, що демократії можуть і надалі приносити користь нашому народу".

16 вересня 2022 року Міністерство внутрішньої безпеки США (DHS) оголосило про першу в історії програму грантів з кібербезпеки для Державних, місцевих та територіальних органів влади (SLT) по всій країні. Обсяг програми - $1 млрд. Агентство з кібербезпеки та інфраструктурної безпеки (CISA) та Федеральне агентство з управління у надзвичайних ситуаціях (FEMA) спільно управляють грантами, при цьому CISA визначило основні цілі фінансування:

Мета 1: Розробити та створити відповідні структури управління, включаючи розробку, впровадження або перегляд планів кібербезпеки, для покращення можливостей реагування на інциденти у сфері кібербезпеки та забезпечення безперервності операцій.

Мета 2: Визначити поточний стан структур кібербезпеки та напрями їх удосконалення на основі постійного тестування, оцінки та систематизованих оцінок.

Мета 3: Впроваджувати засоби захисту, які можна порівняти з ризиком.

Мета 4: Забезпечити належне навчання персоналу організацій у сфері кібербезпеки, що відповідає їхнім обов'язкам.

26 травня 2023 року Міністерство оборони США представило Конгресу секретну кіберстратегію. Документ, як стверджується, ґрунтується на багаторічному реальному досвіді проведення великих операцій в інформаційному просторі.

Однією з основних цілей стратегії на 2023 рік названо припинення «зловмисної кіберактивності», перш ніж вона зможе негативно вплинути на IT-інфраструктуру держави. В офіційному несекретному бюлетені, оприлюдненому Пентагоном, йдеться, що стратегія враховує геополітичну обстановку, що склалася, і те, як кіберможливості можуть використовуватися для впливу на противників в умовах великомасштабних конфліктів.

Включення функцій забезпечення інформаційної безпеки до компетенції Міністерства національної безпеки та інших подібних установ обумовлено тим, що атаки на інформаційну інфраструктуру можуть потенційно призвести до негативних наслідків для різних критичних сфер економіки США, таких як фінансовий сектор, енергетика, транспорт і інші.

Додатково, в межах окремих федеральних відомств та відомств були створені спеціальні підрозділи, які вирішують конкретні завдання в рамках загальної стратегії забезпечення інформаційної безпеки США:

1. Група готовності до надзвичайних ситуацій в інформаційних системах — United States Computer Emergency Readiness Team, US-CERT (підрозділ, що діє під час DHS).

2. Армійський центр безпеки та підтримки роботи глобальних мереж — Army Global Network Operations and Security Center, AGNOSC (підрозділ, що функціонує у складі Міністерства оборони США).

3. Агентство оборонних інформаційних систем Міністерства оборони США (DISA), до складу якого входить Об'єднаний центр забезпечення роботи комп'ютерних мереж — Joint Task Force for Computer Network Operations, JTF-CNO.

4. Центральна служба безпеки (Central Security Service, CSS) Агентства національної безпеки, National Security Agency — NSA.

Фактично ці документи можуть вважатися офіційною загальнонаціональною політикою США у сфері інформаційної безпеки, на основі якої будується система діяльності державної влади та структура державних органів, які забезпечують інформаційну безпеку в державі.

2.2. Базові принципи, політичні пріоритети інформаційної політики США

Організаційна структура державного управління в галузі інформаційної безпеки в США є високо складною, включає різноманітні автономні, але взаємозалежні компоненти, основні з яких проілюстровані на зображенні 2.3.

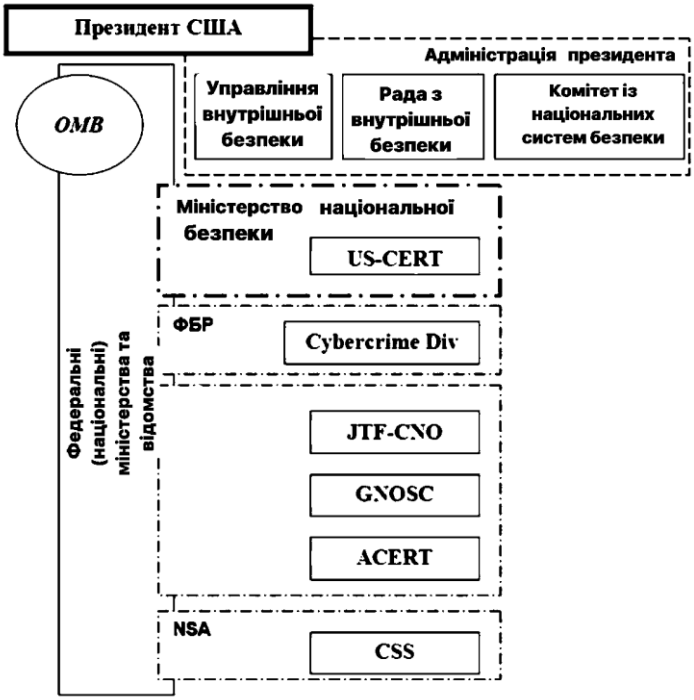

Рис. 2.1 Організаційна структура виконавчих органів, відповідальних за реалізацію завдань у сфері забезпечення інформаційної безпеки в США.

Комітет національних систем безпеки (Committee on National Security Systems, CNSS) складається із 21 члена та 11 спостерігачів, які представляють різні федеральні відомства. Робота комітету організована через кілька робочих груп і спрямована на

формування єдиної національної політики з питань технологій та методів, ключових для захисту інформаційної інфраструктури на рівні всієї країни. Ці робочі напрямки включають:

1. Управління ризиками.
2. Засоби ідентифікації користувачів та пристроїв.
3. Стійкість мережної інфраструктури.
4. Розвиток системи підготовки кадрів у галузі інформаційної безпеки.
5. Забезпечення надійності при розширенні спільного доступу до інформаційних ресурсів.

Основні засоби досягнення цих цілей включають:

1. Розробка національної політики в галузі інформаційної безпеки та стандартів.
2. Оцінка рівня розвиненості існуючих та використовуваних засобів захисту інформації.
3. Випуск директив, інструкцій та технічних бюлетенів з питань інформаційної безпеки.
4. Заснування нових урядових структур для розв'язання спеціалізованих завдань.
5. Участь у регулюванні експорту засобів захисту інформації.

Міністерство національної безпеки (Department of Homeland Security, DHS) було утворене в листопаді 2002 року в результаті значної реорганізації державного апарату, з метою створення постійно діючого автономного органу федеральної влади. Позначаючи свою роль у різних аспектах забезпечення національної безпеки, таких як протидія тероризму, зовнішні загрози та запобігання наслідкам природних катастроф, Міністерство має відповідальність виконувати ключові завдання у сфері інформаційної безпеки, включаючи:

1. Розробка та удосконалення плану національної безпеки, спрямованого на захист ключових ресурсів та складових інфраструктури Сполучених Штатів.
2. Керівництво в умовах кризових ситуацій під час атак на найважливіші інформаційні системи.

3. Надання технічної допомоги приватним компаніям і різним урядовим організаціям для вирішення наслідків відмов критично важливих інформаційних систем.

4. Координація заходів з федеральними структурами для своєчасного оповіщення різних підприємств та організацій про виникаючі загрози та необхідні заходи.

5. Виконання та фінансування науково-дослідницьких робіт, необхідних для вирішення завдань в області внутрішньої безпеки.

Функції забезпечення інформаційної безпеки покладені на Управління кібербезпеки та комунікацій (Office of Cyber Security and Communications). У цьому управлінні функціонує підрозділ, який прямо займається вирішенням проблем, пов'язаних із інформаційною безпекою – National Cyber Security Division, до якого включений USCERT.

Група готовності до надзвичайних ситуацій в інформаційних системах (United States Computer Emergency Readiness Team, US-CERT) є центральним цілодобово діючим органом, відповідальним за взаємодію з урядовими структурами (федеральними та місцевими), а також іншими суб'єктами у сфері захисту інформації. Основне завдання групи - збір та поширення інформації для реагування на інциденти, підвищення координації дій та зменшення рівня вразливості. Група включає п'ять підрозділів.

1. Відділ оперативної діяльності (Operations Branch) відповідає за обробку інформації про інциденти, координацію реагування на них, розповсюдження необхідної інформації та аналіз різноманітних даних для підвищення ефективності оцінки відомих чи нових загроз для ключових елементів національної інфраструктури, включаючи аналіз мережевої інфраструктури та шкідливого програмного забезпечення тощо.

2. Відділ обліку ситуацій (Situational Awareness Branch) відповідає за комплексний аналіз мережевої активності, визначення тенденцій та характеру змін у завантаженні магістральних мереж, а також інформує федеральні структури для

підвищення їхнього рівня захищеності, надаючи підтримку під час реагування на інциденти.

3. Відділ правоохоронної та розвідувальної роботи (Law Enforcement and Intelligence Branch) забезпечує взаємодію з правоохоронними органами при виявленні та розслідуванні протизаконних дій.

4. Відділ стратегічного розвитку (Future Operation Branch) відповідає за розробку перспективних планів, процедур і регламентів для забезпечення ефективного реагування US-CERT на інциденти.

5. Відділ підтримки місії (Mission Support Branch) забезпечує підтримку засобів зв'язку, необхідних для роботи USCERT, включаючи підтримку веб-сайту, а також відповідає за адміністративну підтримку, безпеку персоналу, постачання та інші допоміжні функції.

Агентство оборонних інформаційних систем (Defense Information Systems Agency, DISA) Міністерства оборони США виконує різноманітні завдання, спрямовані на підтримку інформаційних систем для потреб військових операцій, зокрема, вони стосуються забезпечення надійності та безпеки цих систем. Крім того, сили, які відповідають за інформаційну безпеку армії США, включають такі структури:

1. Перше командування інформаційними операціями американської армії (U.S. Army's 1st Information Operations Command (LAND) (1ST IOC[L])), раніше відоме як Підрозділ з наземних військових інформаційних операцій (Land Information Warfare Activity, LIWA).

2. Морське командування оборонними операціями у кіберпросторі (Navy Cyber Defense Operations Command).

3. Армійський центр реагування на небезпеку інформаційної безпеки (ACERT).

Поміж зазначених функцій федеральних органів, державна політика інформаційної безпеки також передбачає взаємодію з іншими установами для вирішення проблем у цій області:

1. Національний науковий фонд – забезпечення фінансової підтримки наукових досліджень в галузі інформаційної безпеки.

2. Державний департамент – надання допомоги різним органам у здійсненні міжнародного співробітництва у сфері інформаційної безпеки.

3. Центральне розвідувальне управління – протидія проникненню до інформаційних систем з-за кордону.

4. Національний інститут стандартів (NIST), Управління з комп'ютерної безпеки – розроблення стандартів у галузі інформаційної безпеки.

5. Міністерство оборони – технічна підтримка у розробці та впровадженні систем захисту інформації.

6. Міністерство юстиції та Федеральне бюро розслідувань – здійснення ефективного розслідування та припинення кіберзлочинів, а також надання юридичної підтримки органам федеральної влади у справах, пов'язаних з інформаційною безпекою.

У законодавчій гілці влади США, а саме в Конгресі, основним структурним підрозділом, що займається вирішенням питань інформаційної безпеки, є один із 22 постійних комітетів Палати представників – Спеціальний комітет національної безпеки (Select Committee on Homeland Security). Головним профільним підкомітетом є Підкомітет з нових загроз, кібербезпеки та науки (Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology). Його компетенція включає питання безпеки комп'ютерних систем, телекомунікацій, інформаційних технологій, систем автоматичного управління в промисловості, а також аспекти запобігання внутрішнім та зовнішнім атакам на урядові та приватні мережі, а також питання уникнення збитків, завданих цивільному населенню внаслідок атак на інформаційні системи.

Деякі слухання з питань інформаційної безпеки також може проводити Комітет з енергетики та торгівлі (Committee on Energy and Commerce). Зокрема, цими питаннями може займатися Підкомітет з питань телекомунікацій та мережі Інтернет (Subcommittee on Communications, Technologies, and the Internet).

Завдання Конгресу у сфері управління інформаційною безпекою, як і в усіх інших сферах державного управління, відповідно до Конституції країни включають:

1. Ухвалення законодавства.
2. Прийняття бюджету та управління фінансами.
3. Контроль за діяльністю урядових установ.
4. Виконання квазісудових функцій.
5. Формування структури виконавчої та судової влади.

Однією з основних форм роботи Конгресу, зокрема, Комітету з національної безпеки та Комітету з енергетики та торгівлі, є проведення спеціальних слухань та розслідувань. Ці слухання мають на меті визначення шляхів вдосконалення законодавства, виявлення та припинення недоробок та порушень у роботі органів виконавчої гілки влади і інше. Конгрес може розглядати питання, пов'язані як з національною та інформаційною безпекою державних структур, так і проблеми інформаційної безпеки приватного сектору та громадян країни. Для участі у слуханнях з різних питань, пов'язаних з інформаційною безпекою, до Конгресу, зазвичай, запрошуються керівники та експерти, представники різних сфер діяльності.

1. Представники органів влади, які відповідають за забезпечення інформаційної безпеки, наприклад, NSA та інші урядові установи.
2. Керівники провідних приватних компаній, що є лідерами у виробництві інформаційних систем та наданні інформаційних послуг, таких як Microsoft, ISS та інші.
3. Представники впливових науково-дослідних установ, консалтингових компаній, професійних та галузевих об'єднань, таких як Electronic Industries Alliance.

Окрім організації діяльності окремих відомств, важливим аспектом є підтримка програм спільної дії у галузі інформаційної безпеки всіма державними установами та приватними компаніями.

Однією з ключових ініціатив в цьому напрямі є Міжрегіональний Центр обміну та аналізу інформації, який об'єднує структури, відповідальні за інформаційну безпеку в урядах практично всіх штатів. Основні завдання цього об'єднання включають:

1. Обмін інформацією щодо інцидентів.

2. Розповсюдження перевірених методів і прийомів забезпечення безпеки.

3. Розповсюдження попереджень про нові загрози інформаційній безпеці.

Крім цього, однією з ініціатив на федеральному рівні є Національне партнерство з підвищення надійності інформації (National Information Assurance Partnership, NIAP), створене для сприяння розробці надійних IT-продуктів та валідації інформаційних систем щодо відповідності міжнародним стандартам у сфері інформаційної безпеки. Завдання цієї структури:

1. Ефективне управління витратами державних та приватних установ на оцінку інформаційних систем.

2. Сприяння створенню приватних структур, які спеціалізуються на перевірці безпеки інформаційних продуктів.

3. Покращення доступності інформаційних систем, які успішно пройшли перевірку відповідності сучасним стандартам.

Також серед програм загальнонаціонального характеру функціонує Інформаційна мережа для передбачення загроз критичній інфраструктурі (Critical Infrastructure Warning Information Network, CWIN). Основною метою цієї мережі є створення можливості обміну попередженнями та передачі сигналів тривоги між урядовими організаціями, приватними компаніями та певними зарубіжними партнерами. За задумом Міністерства національної безпеки, ця мережа призначена для забезпечення надійного зв'язку з різними суб'єктами, чиє участь є вирішальною для відновлення критично важливої інфраструктури у випадку подій національного масштабу.

Відповідно до стратегії інформаційної безпеки, ключовими пріоритетами держави в цій сфері є наступні аспекти:

1. Розвиток національної системи реагування на інциденти в галузі інформаційної безпеки.

2. Впровадження комплексу заходів з метою зменшення загроз інформаційній безпеці.

3. Підготовка фахівців у сфері комп'ютерної безпеки та підвищення рівня обізнаності населення щодо захисту інформації.

4. Забезпечення безпеки інформаційних систем, пов'язаних з діяльністю державних органів.

5. Розвиток різноманітних форм співпраці, включаючи міжнародну, у сфері забезпечення інформаційної безпеки.

Політика інформаційної безпеки США визначається такими пріоритетами:

– Підтримка досліджень і розробок в сфері інформації та комунікацій.

– Вплив на напрямок цих досліджень та сприяння поширенню технічних знань та можливостей в економіці.

– Поширення технологій між лабораторіями та фірмами, впровадження нововведень на ринках.

– Розвиток та поліпшення інфраструктури інформаційної сфери, а також дослідження впливу цієї інфраструктури на міжнародні, національні та приватні інтереси.

– Відновлення рівноваги між чотирма основними інформаційними цінностями: конфіденційність інформації, інформація як суспільне благо, інформація як товар, інформація як невіддільний компонент існування держави.

– Забезпечення недоторканності приватного життя та конфіденційності приватної інформації на різних рівнях і в різних сферах державного управління та приватного сектору.

– Розробка урядової політики в галузі інформації та комунікацій.

Політика інформаційної безпеки в США у різні періоди включає в себе різні аспекти, включаючи підтримку досліджень, контроль за розвитком інфраструктури, та забезпечення безпеки в інформаційних системах, особливо в сфері державних органів.

2.3. Концепція національної інформаційної політики США

Національна інформаційна політика США спрямована на організацію потоків інформації у сферах політики, економіки, науки і оборони з метою досягнення балансу між державним контролем і підприємницькою свободою. Інформація вважається одним із ключових національних ресурсів, і системи, що створюють, обробляють і поширюють інформацію, розглядаються як стратегічні фактори у розвитку індустрії інформації та будівництві інформаційної інфраструктури.

Концепція національної інформаційної політики передбачає необхідність розширення та покращення інформаційного середовища, зокрема, вплив на регіони, такі як країни Латинської Америки, Центральної і Західної Європи, Азійсько-Тихоокеанського регіону. Інформаційна політика включає комплекс законодавчих актів з боку держави, які сприяють та регулюють створення, використання, збереження, передачу і поширення інформації.

Головними пріоритетами цієї політики є:

– Підтримка наукових досліджень і розробок в галузі інформатизації та телекомунікацій, сприяння обміну технологіями між університетами і підприємствами.

– Створення та поліпшення інформаційної інфраструктури, включаючи глобальну інформаційну інфраструктуру.

– Забезпечення балансу між ключовими інформаційними цінностями, які можуть бути порушені внаслідок нових інформаційних технологій, такими як конфіденційність інформації, інформація як суспільне надбання і благо, інформація як товар, інформація як невід'ємна частина функціонування держави.

– Захист приватного життя та особистих даних в різних галузях державного управління та приватному секторі.

– Покращення державної політики в галузі інформатизації та телекомунікацій.

– Ця політика наділяє громадян США низку невід'ємних прав, таких як право на свободу інформації (зокрема у засобах масової інформації), публічні судові процеси, обвинувачувальна інформація, інтелектуальна власність, доступ до урядової інформації та захист і безпеку інформації.

Концепція інформаційної політики США включає в себе низку принципів і пріоритетів, які спрямовані на ефективне управління інформацією в країні. Основні аспекти концепції інформаційної політики США включають такі пункти:

Забезпечення національної безпеки. Однією з ключових мет цієї політики є захист національних інтересів та безпеки країни в інформаційній сфері. Це включає в себе заходи щодо захисту важливих інформаційних систем і мереж, а також боротьбу зі злочинами в інформаційній сфері.

Сприяння інноваціям та технологічному розвитку. США активно підтримують дослідження та розробки в галузі інформаційних технологій та телекомунікацій. Ця політика спрямована на стимулювання інновацій та розвиток галузі інформаційної технології.

Свобода інформації. США високо цінує свободу слова та свободу доступу до інформації. Концепція інформаційної політики США включає захист цих принципів та підтримку вільної передачі та обміну інформацією.

Приватність і захист даних. Забезпечення приватності громадян та захисту їх особистих даних є важливою частиною концепції інформаційної політики. Вона передбачає встановлення норм та стандартів для захисту особистих даних та конфіденційної інформації.

Розвиток глобальних зв'язків. США сприяє розвитку міжнародних інформаційних зв'язків та співпраці в галузі інформаційної технології та телекомунікацій. Це включає в себе співпрацю з іншими країнами та міжнародними організаціями.

Забезпечення доступу до інформації. Концепція інформаційної політики США включає заходи для забезпечення доступу до інформації для всіх громадян, включаючи тих, які можуть мати обмежений доступ через технічні або інші обставини.

Регулювання інформаційного простору. Забезпечення справедливого та ефективного регулювання інформаційного простору, включаючи аспекти якість та безпеку послуг, також входить до концепції інформаційної політики.

Ці аспекти допомагають створити фреймворк для розвитку та управління інформаційною сферою в США, забезпечуючи баланс між інтересами держави, громадян та бізнесу.

Політика США в сфері інформаційної безпеки спрямована на досягнення та утвердження американського домінування в глобальному інформаційному просторі. Ураховуючи важливість інформаційних ресурсів у всіх аспектах безпеки, інформаційне домінування стає ключовим для технологічного, економічного, військового та політичного переважання США над іншими державами.

Політика США у сфері інформаційної безпеки об'єднує ринкові інструменти лібералізації та регулювання інформаційної сфери, а також намагається встановити прямий державний контроль над інформаційними ресурсами, не лише на національному рівні, але й на міжнародному. Деякою мірою ці напрями можуть суперечити один одному.

Політика лібералізації інформаційної сфери включає такі заходи, як розсекречування воєнних технологій, їх використання у громадській сфері, зняття обмежень на експорт контрольованих товарів та податкові пільги. Держава намагається створювати сприятливі умови для розвитку інформаційного сектору економіки.

Одночасно використовуються механізми державного політичного контролю, такі як встановлення стандартів для інформаційної сфери, регулювання використання

комерційних технологій у державних органах та співпраця з приватними компаніями в розвідувальних та контррозвідувальних операціях.

У першому терміні адміністрації Клінтона більший акцент був зроблений на кримінальних аспектах інформаційної безпеки, зокрема на інформаційних злочинах та інших правопорушеннях, які використовували інформаційні технології. У цей час Федеральне бюро розслідування (ФБР) та Міністерство юстиції США відігравали центральну роль у системі забезпечення інформаційної безпеки.

Протягом другого терміну адміністрації Клінтона зросла роль воєнних аспектів політики США в інформаційній сфері. Реформа системи забезпечення інформаційної безпеки при адміністрації Дж. Буша спрямована на включення військових і розвідувальних органів у процес забезпечення інформаційної безпеки. Центральним елементом цієї системи було створення Міністерства внутрішньої безпеки у 2003 році, яке надало воєнним та розвідувальним органам значні повноваження в інформаційній сфері. Президент США Джордж Буш назвав головні загрози безпеці США, де на другому місці після тероризму зазначив інформаційну війну, а потім поширення засобів масового ураження та їх доставку.

Американська адміністрація вважає, що формування єдиної глобальної інформаційної інфраструктури під контролем США дозволить їм вирішити завдання стратегічного використання інформаційної зброї «аж до блокування телекомунікаційних мереж держав, які не визнають реалії сучасної міжнародної системи».

Слід зазначити, що у час застосування інформаційних технологій у військових цілях мало регулюється міжнародним правом. На думку зарубіжних експертів, ці питання мають розглядатися та вирішуватися на багатосторонній основі за участю всіх зацікавлених сторін. При цьому управління інформаційним простором необхідне для забезпечення не тільки національної безпеки абсолютного IT-лідера США, але й міжнародної безпеки в цілому. Проте з цих питань США займають особливу позицію і уникають домовленостей.

РОЗДІЛ 3. ІНФОРМАЦІЙНА ПОЛІТИКА США В КОНТЕКСТІ ЗБРОЙНОЇ АГРЕСІЇ РОСІЇ

3.1. Специфіка використання інформаційних технологій та ЗМІ США в умовах російської агресії

Технологія була рушійною силою соціального будівництва війни та миру. Вона відіграє вирішальну роль у сприянні комунікації, транспорту та торгівлі, а також впливає на наш спосіб мислення. У сучасну епоху нові технології відіграють значну роль у полегшенні передачі інформації і, як такі, вплинули на соціальне конструювання війни та миру. Прикладом того є використання соціальних мереж у повномасштабній війні, яку розгорнула Росія проти України 24 лютого 2022 року.

Використання інформаційних технологій та засобів масової інформації (ЗМІ) США в рамках збройної агресії характеризується високим рівнем технологічної розвиненості та стратегічного використання медіа. Соціальні мережі також використовувалися для поширення пропаганди з обох сторін конфлікту, сприяючи створенню середовища дезінформації. Крім того, спосіб роботи платформ змінився під час конфліктів.

Протягом багатьох років соціальні медіа піддавалися критиці за їх роль у поширенні дезінформації та пропаганди, і очевидно, що вони також відіграли значну роль у формуванні громадської думки про конфлікти. Як наслідок, соціальні медіа відіграли певну роль у соціальному створенні війни та миру.

Одним з ключовим аспектом специфіки використання інформаційних технологій є ***кібербезпека.*** Уряд США продовжує докладати зусиль, щоб посилити кібербезпеку країни, а також посилити свою загальну стратегію управління технологіями. Джо Байден оприлюднив нову Національну стратегію кібербезпеки, в якій описано кроки, які вживає уряд для захисту кіберпростору та побудови стійкої цифрової екосистеми, яку легше захищати, ніж атакувати, і яка є відкритою та безпечною для всіх. Це включало зусилля щодо підвищення підзвітності

технологічних компаній , посилення захисту конфіденційності та забезпечення чесної конкуренції в Інтернеті.

Світ стає дедалі складнішим, а кіберзагрози стають все більш витонченими, а атаки програм-вимагачів призводять до економічних збитків у США на мільйони доларів. За даними IBM, у 2022 році середня вартість атаки програм-вимагачів становила понад 4,5 мільйона доларів. Тому стратегія США в кіберпросторі налічує 5 головних аспектів: захист критичної інфраструктури, демонтування загрозливих об'єктів, формування ринкової сили для забезпечення безпеки та стійкості, інвестиції в стійке майбутнє, налагодження міжнародних партнерств для досягнення спільних цілей.

Другим аспектом специфіки використання інформаційних технологій та ЗМІ США під час військового конфлікту є ***соціальні мережі та інтернет.*** Соціальні медіа відіграють важливу роль в американській політиці. Вони не лише надають платформу для спілкування політичних діячів із виборцями, а й стають інструментом впливу на громадську думку та формування політичних уподобань.

До повномасштабного вторгнення Росії в Україну основні інтернет-платформи продовжували захищатися від спроб уряду притягнути їх до відповідальності за вміст, який відображається в облікових записах користувачів. Вони продовжують стверджувати, що не несуть відповідальності за вміст, яким би мерзенним він не був, і цензурувати ці платформи неможливо. Однак ці компанії не могли продовжувати висувати такі аргументи. З початком війни в Україні концепція нейтралітету більше не керує роботою цих компаній. YouTube оголосив, що заблокував понад 1000 російських каналів і 15 000 відео. Facebook наслідував їхній приклад і заблокував доступ до офіційних російських видань RT і Sputnik в Європейському Союзі. Крім того, заборонили можливість російських ЗМІ поширювати інформацію через Facebook. Великі технологічні компанії, такі як Apple і Netflix, які призупинили свої послуги в Росії, вжили таких же заходів.

Як зазначає Є.Магда (український політолог, історик, журналіст, директор Інституту світової політики), завдяки відсутності державної цензури та комерційному характеру українських видань, радіостанцій і телеканалів Росія досить легко взяла під

контроль інформаційний простір України та наситила його інформаційною продукцією російського шоу-бізнесу. Крім того, Кремль завжди покладав на ЗМІ особливу місію, розглядаючи їх як інструмент підтримки своїх інтересів. Телебачення, кіностудії, радіо та інші засоби масової інформації розглядалися як важливі складові національної безпеки. У своїй практиці ведення інформаційної війни Росія використовує принципи пропагандистської концепції Геббельса, які зводяться до таких тез: пропаганда повинна плануватися і вестись з однієї інстанції; тільки авторитет може визначити, чи має бути результат пропаганди правдивим чи брехливим; чорна пропаганда має характеризувати події та людей характерними фразами чи гаслами; для кращого сприйняття пропаганда повинна викликати інтерес у аудиторії та транслюватися через привабливе комунікаційне середовище. Тому США і надалі приділятимуть велику увагу соціальним медіа та інтернету.

Третій аспект – ***електронна війна.*** Розвиток радіотехніки та засобів перехоплення чужих трансляцій йшли завжди пліч-о-пліч. Підслухати, що відбувається в ефірі у супротивника, було розумним бажанням будь-якої армії. Але поява нових видів радіотехніки, не пов'язаних із передачею інформації – радіолокаторів – штовхнула розвідки світу до нового незвичайного завдання: перехоплення сигналів ворожих локаторів.

Досягнення в галузі інформаційних технологій зробили використання засобів зв'язку важливою складовою у будь-якій військовій операції. Вони дозволяють скласти всеосяжну картину поля бою та ефективно координувати свої дії. Порушення роботи системи зв'язку противника обмежує його здатність керувати військами та оновлювати дані про зміни обстановки в ході бойових дій.

В даний час на озброєнні бронетанкових бойових бригадних груп та бойових бригадних груп «Страйкер» складається тактична система РЕБ TEWS, яка призначена для радіоелектронного забезпечення дій підрозділів бригадних груп та радіоелектронного придушення працюючих радіоелектронних засобів (РЕМ) супротивника.

Вона включає цифрове обладнання останнього покоління для швидкого широкосмугового перехоплення, постійного спостереження, пеленгації та створення

перешкод працюючим РЕМ противника в діапазонах HF (3–30 МГц), VHF (30–300 МГц) та UHF (300–3 000 МГц) на глибину до 30 км, а також апаратне та програмне забезпечення для його експлуатації.

У США розроблять комбіновану технологію радіоелектронної боротьби, радіотехнічної розвідки та кіберзахисту, якою оснащуватимуть броньовану техніку. Про це пише Defence News, посилаючись на керівника Управління армійської програми з розвідки, радіоелектронної боротьби та датчиків Марка Кітца.

За його словами, розробка нової технології розпочнеться цього року, а вже 2024 року армія США розраховує провести перші бойові демонстрації. Система РЕБ наземного рівня має забезпечити американським військовим велику обізнаність на полі бою, а також придушувати ворожі засоби зв'язку.

ВВС США отримають покращені літаки РЕБ EC-37B Compass Call, які розробили L3Harris Technologies, BAE Systems та Gulfstream. Він має забезпечити американських військових можливістю придушувати радари та усувати радіоелектронні перешкоди.

Створення та контроль наративу. Завдання наративів — сформувати певний світогляд. Саме наратив є стратегічно найважливішим, оскільки повідомлення можна змінювати, а наратив є постійною історією. Щоб створити якісний наратив, потрібні час і ресурси. Найпопулярнішим наративом Росії щодо України є твердження про «нездатну державу». Повідомлення, які наповнюють цей наратив, стосуються історії, корупції, культури, економіки тощо. Тобто все, що можна використати для підтримки оповіді. Іншим центральним наративом є твердження про «українських нацистів». Саме такий світогляд Росія використовує як одну з причин для повномасштабного вторгнення в Україну. Крім того, щоб підживити цей наратив, Кремль продовжує говорити про денацифікацію України як одну з вимог мирної угоди. Цей наратив також наповнений різними повідомленнями, що стосуються як української історії, так і сьогодення. Зокрема, що «в Україні при владі нацисти», «Україна забула про перемогу над нацизмом», «УПА – пособники Гітлера» чи що гасло «Слава Україні!» – це калька з нацистського гасла «Хайль Гітлер!». Цей список можна продовжувати. Отже, існує наратив, який складається з повідомлень, які живлять фейки, маніпуляції

та спекуляції. За словами О.Батрименка (професор кафедри політології Київського національного університету імені Тараса Шевченка), «по суті, представлені Росією та Україною наративи є діаметрально протилежними. Росія розглядає війну в Україні, яку В.Путін наполегливо трактує як «спеціальну військову операцію», як необхідний оборонний захід у відповідь на розширення НАТО у Східній Європі Президент РФ також називає військову кампанію необхідною для «денацифікації» України та припинення нібито геноциду, який українська влада здійснює проти російськомовного народу. Наратив України, навпаки, наполягає на тому, що війна є відкритою агресією Російської Федерації проти суверенної держави, відмінної від Росії, і зображує її громадян і збройні сили героями, які захищаються від невиправданого вторгнення».

Можна легко ідентифікувати російські фейки, але водночас піддаватися певним повідомленням російської дезінформації або взагалі вірити наративу. Важливо також пам'ятати, що інформаційно-психологічний вплив завжди здійснюється з метою зміни поведінки. Тобто кожен фейк, провокація чи спекуляція у своїй сукупності має спонукати до дії. Наприклад, голосувати за конкретну партію на виборах, йти чи не йти на акцію протесту. Тобто інструменти можуть бути різними, але смисли інформаційного впливу завжди будуються за принципом «наратив – повідомлення – фейки, маніпуляції, спекуляції». Саме тому для інформаційної політики США є важливим створення та контроль наративів, формування певного сприйняття подій, впливу на громадську думку та міжнародну спільноту.

Глобальна інформаційна присутність. США прагне мати сильну глобальну інформаційну присутність через міжнародні телеканали, новинні агентства та інші медіа-ресурси для впливу на міжнародну громадськість. Стратегія також закликає відновити дипломатичну присутність США в Україні, розширивши її за межі Києва та охопивши такі міста, як Львів, Одеса, Харків та Дніпро.

Глобальна інформаційна присутність Сполучених Штатів Америки визначається рядом стратегічних та геополітичних мет цієї країни. Тут розглянемо деякі з основних цілей та функцій глобальної інформаційної присутності США:

Дипломатичні цілі. Інформаційна присутність грає ключову роль у формуванні позитивного іміджу країни в міжнародному масштабі. Це допомагає зміцнювати дипломатичні відносини, підтримувати союзників та впливати на міжнародну політику.

Забезпечення національної безпеки. Інформаційна присутність використовується для розповсюдження інформації про стратегії та позиції США, яка може впливати на безпеку та стабільність у світі. Це включає протидію дезінформації та психологічну війну.

Формування глобального впливу. США використовує свою інформаційну присутність для зміцнення своєї ролі в світових справах. Це охоплює вплив на економіку, культуру, науку та технології.

Продаж товарів та послуг. Глобальна інформаційна присутність сприяє просуванню та продажу американських товарів, послуг, технологій та ідей на світовому ринку.

Підтримка демократії та цінностей. США використовує свою інформаційну присутність для підтримки демократичних цінностей, свободи слова та прав людини у світі. Це може включати публікацію інформації про демократичні досягнення та порушення прав людини в інших країнах.

Посилення образу країни. Глобальна інформаційна присутність сприяє формуванню позитивного образу країни як інноваційної, демократичної, культурно різноманітної та впливової нації. Ці цілі допомагають зміцнювати позиції США на світовій арені та впливати на ключові світові процеси в різних аспектах.

Підтримка демократії та цінностей. США використовує свою інформаційну присутність для підтримки демократичних цінностей, свободи слова та прав людини у світі. Це може включати публікацію інформації про демократичні досягнення та порушення прав людини в інших країнах.

9 вересня 2023 року Сполучені Штати Америки оголосили, що нададуть народові України додаткову допомогу вартістю понад $200 млн. на підтримку розвитку демократії та врядування і дотримання прав людини. Державний секретар США Ентоні Дж. Блінкен зробив відповідну заяву під час свого перебування в

Україні; цю допомогу буде надано по лінії Агентства США з міжнародного розвитку (USAID).

Додаткова допомога сприятиме зростанню прозорості та підзвітності інституцій в Україні, забезпечить підтримку реформ з метою протидії корупції та вдосконалення практики управління публічними фінансами відповідно до міжнародних стандартів, уможливить подальшу діяльність із адвокації для забезпечення підзвітності у сфері прав людини, сприятиме здійсненню судової реформи та наданню правової допомоги, а також зміцненню незалежних медіа та громадянського суспільства. Всі ці ініціативи є неодмінним елементом забезпечення демократичного майбутнього України та її прагнення увійти до складу ЄС.

На основі цього фінансування USAID забезпечить допомогу антикорупційним органам України – зокрема у втіленні таких заходів, як реалізація Державної антикорупційної програми. Кошти USAID сприятимуть подальшому зміцненню заходів у сфері судової реформи, що є необхідними для просування європейської інтеграції України – зокрема у співпраці з Вищою радою правосуддя, Вищою кваліфікаційною комісією суддів та Конституційним судом України. Підтримка з боку USAID також допоможе створити додаткову кількість центрів правосуддя, які працюють на місцевому рівні під орудою організацій громадянського суспільства; у тісній співпраці з системою надання безоплатної правової допомоги Міністерства юстиції України, вони надаватимуть підтримку потерпілим від війни українцям у вирішенні юридичних питань і відновленні джерел їхнього добробуту.

Психологічна операційна діяльність. Використання інформаційних технологій для психологічного впливу на ворога та населення в зоні конфлікту, а також для формування позитивного сприйняття власної сторони.

Психологічна операційна діяльність Сполучених Штатів у контексті збройної агресії Росії охоплює широкий спектр стратегій та заходів, спрямованих на вплив на психіку супротивника, громадську думку та інші ключові аспекти. Деякі аспекти цієї діяльності включають:

Інформаційна кампанія. США здійснюють активну інформаційну кампанію для формування образу Росії та впливу на громадську думку в Україні та світі. Це може включати розповсюдження інформації про російську агресію, порушення прав людини та інші аспекти конфлікту.

Психологічний вплив на супротивника. Спрямована на психологічний вплив на військовий та цивільний персонал Росії. Це може включати психологічні операції, спрямовані на зниження бойового духу та моралі супротивника.

Підтримка інформаційної свободи. США підтримують роботу незалежних ЗМІ та інтернет-платформ, які розкривають інформацію про події в регіоні, освітляють правдивий стан справ та протистоять дезінформації.

Проведення психологічних операцій в інтернеті. Використання соціальних мереж та інших онлайн-платформ для впливу на громадську думку та створення сприятливого образу країни в інтернет-просторі.

Робота з інформаційною інфраструктурою. Здійснення заходів для захисту та підтримки інформаційної інфраструктури, щоб утримати інформаційні атаки та забезпечити стабільність комунікацій.

Розвиток контрінформації. Створення контрінформаційних кампаній та реагування на дезінформацію, яка може виникати від російської сторони.

Отже, повномасштабне вторгнення Росії проти України є безпрецедентним явищем сучасних міжнародних відносин, яке здійснюється всупереч міжнародним нормам та інтересам стабільності на європейському континенті. Проте реалізація агресивних планів не була одноразовим рішенням російського керівництва, а виявилася втіленням довгострокового політичного курсу, невід'ємною складовою якого була і залишається інформаційна війна. Інформаційні війни реалізуються конкретними засобами, способами, технологіями тощо, але обов'язково у множині, спільно, на різних рівнях, оскільки інформаційне середовище з його інформаційними потоками та різного роду інформаційними впливами характеризується сукупністю динамічних фактори, здатні справляти прямий вплив на людину або опосередкований, негайний або відстрочений вплив. Особливими каталізаторами та носіями інформаційних війн стали ЗМІ. Критичний дискурс щодо цієї нової

медіареальності, інспірований державами, що підтримують агресивну геополітику, також спирається на досягнення психології, представлений нею комплекс знань щодо масовізації психіки особи-адресата, техніки маніпулювання як складової комунікації.

Специфіка використання інформаційних технологій та ЗМІ США в умовах російської збройної агресії проти України включає в себе ключові аспекти: кібербезпека, соціальні медіа та інтернет, електронна війна, створення та контроль наративу, глобальна інформаційна пристуність, психологічна операційна діяльність. Кожна з них відіграє ключову роль в інформаційній політиці США та розгортанню подальших подій.

3.2.Протидія російській пропаганді та маніпуляціям як частина сучасної інформаційної стратегії США

Протистояння російській пропаганді та маніпуляціям визначається як ключовий компонент сучасної інформаційної стратегії Сполучених Штатів Америки. Російська пропаганда відома своєю високою ефективністю та використанням різноманітних технологій та маніпуляцій, таких як фейкові новини, застосування соціальних мереж та ботів, а також створення медіакомплексів та впливових осіб.

В рамках цієї стратегії, США активно співпрацюють з партнерами в Європі та інших частинах світу, зокрема, для обміну інформацією та спільних заходів з протидії російській пропаганді. Однією з ініціатив у цьому напрямку є створення Global Engagement Center (Глобальний центр залучення), який визначає свою мету в боротьбі з дезінформацією та пропагандою, зокрема з боку Росії та її союзників.

Ця інформаційна стратегія США включає в себе не лише реагування на конкретні випадки пропаганди, але й акцентує на необхідності зміцнення медійної грамотності, розвитку критичного мислення суспільства та забезпечення прозорості в інформаційному просторі, щоб запобігти впливовій дезінформації.

«Є правда, а є брехня. Брехня заради влади та прибутку. І кожен з нас має обов'язок і відповідальність – як громадян, як американців і особливо як лідерів,

лідерів, які зобов'язані шанувати нашу Конституцію та захищати наш народ – захищати правду і спростовувати брехню».

ДЖОЗЕФ БАЙДЕН

ПРЕЗИДЕНТ СПОЛУЧЕНИХ ШТАТІВ

Сполучені Штати, ЄС, інші країни Європи (зокрема Велика Британія, Норвегія та Швейцарія), Канада, Австралія, Нова Зеландія, Японія та Південна Корея, серед інших, відповіли на війну Росії проти України масштабними санкціями. Ці санкції розширюють і значно перевищують заходи, які Сполучені Штати, ЄС та інші раніше запровадили проти Росії у відповідь на вторгнення Москви в Україну в 2014 році, втручання у вибори в США в 2016 році та інші зловмисні дії. Санкції США, введені з лютого 2022 року, включають обмеження російського центрального банку на використання його резервів, номінованих у доларах, заборону більшості великих російських банків проводити операції в доларах США або з американськими особами, а також заборону на нові інвестиції США в Росію. Сполучені Штати також розширили контроль над експортом, що впливає на доступ Росії до чутливих або необхідних американських технологій, заборонили імпорт певних товарів із Росії та заборонили Росії використовувати повітряний простір і порти США. З лютого 2022 року Сполучені Штати запровадили економічні санкції проти близько 1900 російських фізичних та юридичних осіб і заборонили в’їзд до США кільком тисячам російських чиновників, військовослужбовців, бізнесменів, пов’язаних з урядом, та інших.

Протидія російській пропаганді та маніпуляціям становить суттєвий компонент сучасної інформаційної стратегії Сполучених Штатів, спрямованої на забезпечення свободи слова, точності та об'єктивності інформації, а також на протидію дезінформації. Вказівник свободи преси за світовим індексом (World Press Freedom Index), який визначає ступінь свободи та можливостей журналістів, підтверджує, що місцевість була сприятливою для посилення пропаганди з боку Росії (164 місце), яка впала ще на дев’ять позицій в Індексі 2023 року. У рекордно короткі терміни Москва створила новий медіа-арсенал, призначений для поширення меседжу Кремля на окупованих територіях півдня України, водночас жорсткіше, ніж будь-коли,

розправляючись із останніми незалежними російськими ЗМІ, які були заборонені, заблоковані та/або оголошені «іноземні агенти». Військові злочини Росії в Україні (79 місце) допомогли цій країні отримати один із найгірших показників Індексу безпеки.

Щодня десятки лояльних Росії матеріалів з'являються у провідних західних ЗМІ, просуваючи ідеї того, що Москву неможливо перемогти, що заради миру треба повернутися до переговорів, а ціна війни для Заходу надто велика.

Чи мають такі меседжі вплив на звичайних громадян? За рік у США зменшилася частка тих, хто вважає, що Україні потрібно давати більше зброї, йдеться в останніх дослідженнях Pew Research Center.

Чверть американців вважають, що підтримка України з боку США є надто великою. Хоча у вересні минулого року таких було лише 20%, а на початку війни – лише 7-15%.

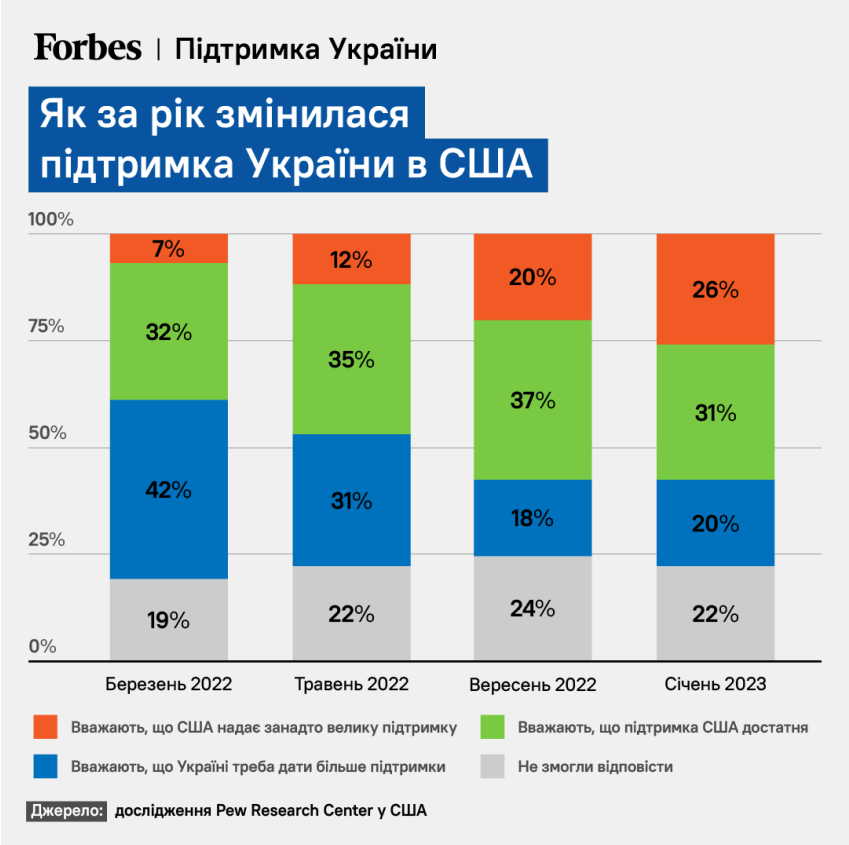

Рис. 3.1 Графік підтримки України в США

Найбільше підтримка України зменшується серед прихильників республіканської партії. Якщо на початку війни 49% із них вважали, що Україні треба дати більше зброї (тоді лише 38% прихильників демократів були такої самої думки), то зараз лише 17% республіканців підтримують розширення допомоги Україні.

Рис 3.2 Графік підтримки України серед прихильників демократів та республіканців США

Уряди намагаються прямо спростовувати неправдивий і оманливий контент і поширювати точний контент у рамках зусиль протистояти та зменшити успіх російської дезінформації. Перед вторгненням уряди США та Великої Британії завчасно обмінювалися розвідданими щодо передбачуваної військової діяльності Росії, викриваючи плановані атаки під «фальшивим прапором», спрямовані на розпалювання антиукраїнських настроїв (Bose, 2022). У листопаді 2021 року Сполучені Штати зазначили, що їм відомо про плани вторгнення, а на початку 2022

року Сполучені Штати та Велика Британія поділилися з союзниками розвідданими та публічно попередили про неминучий напад.

Хоча ці стратегічні комунікаційні зусилля не завадили Росії вторгнутися в Україну, оприлюднення розвідданих ускладнило уряду приховати свої наміри або заплутати громадський дискурс за допомогою кампаній дезінформації, і, ймовірно, підтримало швидку та відносно єдину відповідь (Carvin, 2022). Ця проактивна комунікація є яскравою ілюстрацією «попереднього спалювання», підходу, який має на меті прищепити громадськість до потенційної неправдивої та дезінформації. За своєю суттю, попереднє спалювання полягає в попередженні людей про можливість отримати маніпулятивну інформацію з ідеєю, що така діяльність зменшить сприйнятливість до неправдивої та дезінформації. (Roozenbeek and van derLinden, 2021).

Пакет екстрених витрат Конгресу США також включає 120 мільйонів доларів США на протидію російській дезінформації та пропаганді (Pallaro and Parlapiano, 2023). Подібним чином Глобальний центр взаємодії Сполучених Штатів відстежує та протидіє наративам дезінформації ще задовго до вторгнення Росії. На додаток до розвінчання наративів, пов'язаних з російським урядом, Global Engagement Center надає детальний аналітичний і роз'яснювальний контент щодо зусиль Росії (US Department of State, 2022).

Глобальний центр взаємодії (GEC) Державного департаменту ділиться інформацією з агентствами США та іноземними урядами про російську дезінформацію в соціальних мережах, новинних виданнях і російських проксі-сайтах, повідомив Reuters офіційний представник Держдепартаменту.

GEC підтримує регулярні контакти з компаніями соціальних медіа, «які повідомили департаменту про свої дії щодо припинення монетизації російських осіб, які перебувають під санкціями, на своїх платформах», — сказав чиновник.

Хоча GEC не вимагає видалення чи позначення вмісту, він ділиться своїми аналізами з платформами для виявлення та протидії російській дезінформації.

Крім стратегічних комунікаційних заходів для реагування на певний контент, уряд США докладає зусиль, щоб використовувати ширші можливості для поширення

інформації через ЗМІ та соціальні медіа. Наприклад, фінансують треті сторони та журналістів, як-от BBC та незалежних журналістів в Україні та Росії, щоб допомогти забезпечити та розширити постійну доставку неупереджених новин, щоб допомогти громадянам уникнути російських обмежень на місцеві та соціальні медіа (GOV.UK, 2022).

Адміністрація Байдена використовує унікальний підхід до боротьби зі сплеском російської дезінформації та пропаганди. На відміну від своїх європейських союзників, Білий дім безпосередньо не наполягає на гігантських американських технологічних і соціальних медіа-компаніях, які контролюють потік інформації для мільярдів людей, знищувати дезінформацію або облікові записи, які її поширюють. Натомість офіційні особи США зосереджуються на тому, щоб звинуватити проросійські ЗМІ у поширенні дезінформації, швидкому обміні розвідданими про військові дії та пропаганду Росії та викритті того, що вони називають планами Москви влаштувати атаки під «фальшивим прапором», спрямовані на провокацію настроїв проти України.

«Ми активно оприлюднюємо інформацію про зібрані нами розвідувальні дані, те, що ми бачимо, розвінчуючи твердження, які є неправдивими, переконуючись у тому, що наші союзники та партнери мають правильну інформацію», — повідомило одне з таких джерел. «Ідея полягає в тому, щоб протистояти російським наративам і змусити людей зрозуміти, що те, що їм нав'язують, є дезінформацією».

Це продовження стратегії оприлюднення інформації розвідки США про скупчення російських військ поблизу України перед вторгненням. «Випереджати те, що росіяни робили, вказувати на речі та бути сміливим у тому, як адміністрація розкривала розвідувальні дані, було дуже цінно», — сказав Брайан Мерфі, колишній керівник відділу розвідки Міністерства внутрішньої безпеки, а нині віце-президент зі стратегічних операцій у Logically, фірма, яка пропонує послуги зі зменшення поширення дезінформації.

Представник Ради національної безпеки (NSC) Білого дому заявив, що адміністрація «надзвичайно обережна» з тим, що розсекречує, але «є цінність для громадськості» у викритті операцій з дезінформації.

Такі технічні платформи, як Alphabet (GOOGL.O), YouTube, Twitter (TWTR.N) і Facebook (FB.O), стали віртуальним полем битви під час російського вторгнення, оскільки підтримувані Кремлем ЗМІ публікують інформацію, яка часто суперечить повідомленням інформаційних агентств, що базуються на фактах на землі в Україні.

Власник Facebook Мета заблокував російські державні ЗМІ доступ до стрічок користувачів у Європі під тиском чиновників ЄС. Twitter та інші соціальні медіа в Росії обмежені, і технічні компанії стикаються з новими штрафними санкціями. Кілька технологічних гігантів також обмежують російські державні ЗМІ в отриманні прибутку від реклами на своїх платформах, а Meta знижує посаду публікацій із пов'язаних із Кремлем ресурсів.

Адміністрація Байдена виявила ЗМІ, які публікують інформацію, яку, на її думку, є російською пропагандою через облікові записи з мільйонами підписників, але не тиснула на технологічні компанії, щоб вони заблокували або видалили їх.

Наприклад, консервативний веб-сайт фінансових новин ZeroHedge був названий американською розвідкою одним із таких засобів. Видання все ще твітує інформацію для понад мільйона підписників.

За словами технічної компанії, обліковий запис не порушує правил обслуговування Twitter, і Білий дім не наполягає на забороні, кажуть джерела. Це викликало б питання щодо свободи американської преси, свободи слова та могло б почати боротьбу з технологічними гігантами, чого не хоче адміністрація.

За словами джерел, Білий дім також дивиться на російську дезінформацію інакше, ніж, наприклад, на поширення дезінформації про вакцини, яка вбивала американців і підштовхнула Байдена боротися з компаніями соціальних мереж. У цьому випадку Державний департамент, Міністерство внутрішньої безпеки (DHS) і ФБР співпрацюють з NSC, щоб зупинити Москву в поширенні неправдивих наративів про Україну.

У США застосовують систему на основі штучного інтелекту для виявлення та збору російської дезінформації в інтернеті. Про це розповів державний секретар США Ентоні Блінкен. «Державний департамент розробив онлайн-агрегатор контенту про Україну з підтримкою штучного інтелекту, щоб збирати російську дезінформацію,

яку можна перевірити, а потім ділитися нею з партнерами по всьому світу. Ми просуваємо незалежні ЗМІ та цифрову грамотність. Ми працюємо з партнерами в академічних колах, щоб надійно виявляти фальшивий текст, створений російськими чатботами», — сказав Блінкен під час церемонії Freedom House 9 травня 2023 року у Вашингтоні. Росія продовжує поширювати невпинний потік дезінформації про свою агресивну війну проти України, щоб приховати «жахливі зловживання, які вона вчинила», або виправдати свої злочини, додав Ентоні Блінкен. За його словами, уряд США співпрацює з науковцями, «щоб надійно виявляти фейковий текст, створений російськими чатботами». Державний секретар США також попередив, що технологія штучного інтелекту може мати зворотний ефект, якщо потрапить у «погані руки». «Це також загрожує зміцненню авторитарних урядів, зокрема, може дозволити їм ще ефективніше використовувати соціальні медіа, щоб маніпулювати своїми народами й сіяти розкол серед своїх супротивників», — зазначив керівник Держдепу США.

Росія продовжує проштовхувати постійний, невпинний потік дезінформації про свою агресивну війну проти України, щоб брехати та приховувати жахливі злочини, які вона вчинила, намагаючись виправдати вчинення інших. Отже, інформаційна політика США грає важливу роль у подальшій долі вирішення конфлікту та розгортання подій. США активно використовують усі належні ресурси для протидії російській пропаганді та маніпуляціям.

ВИСНОВКИ

В процесі написання кваліфікаційної роботи було досліджено, що інформаційна політика Сполучених Штатів Америки включає в себе різні інструменти та засоби, які використовуються для досягнення своїх інтересів і впливу на міжнародні відносини. Деякі з основних інструментів інформаційної політики США включають: глобальні медіа, дипломатія та громадська дипломатія, пропаганда та інформаційна війна, міжнародне радіомовлення та телебачення, соціальні медіа, міжнародні організації, санкції та обмеження.

Для розкриття стратегії інформаційної політики США було проаналізовано ряд документів, законопроектів, ініціатив та стратегій, які визначили розвиток та формування сучасної концепції інформаційної політики та безпеки. Однією з основних цілей стратегії на 2023 рік названо припинення «зловмисної кіберактивності», перш ніж вона зможе негативно вплинути на ІТ-інфраструктуру держави. В офіційному несекретному бюлетені, оприлюдненому Пентагоном, йдеться, що стратегія враховує геополітичну обстановку, що склалася, і те, як кіберможливості можуть використовуватися для впливу на противників в умовах великомасштабних конфліктів.

Національна інформаційна політика США спрямована на організацію потоків інформації у сферах політики, економіки, науки і оборони з метою досягнення балансу між державним контролем і підприємницькою свободою.

Концепція інформаційної політики США включає в себе низку принципів і пріоритетів, які спрямовані на ефективне управління інформацією в країні. Основні аспекти концепції інформаційної політики США включають такі пункти: Забезпечення національної безпеки. Сприяння інноваціям та технологічному розвитку, свобода інформації, приватність і захист даних, розвиток глобальних зв’язків, забезпечення доступу до інформації, регулювання інформаційного простору.

Політика США в сфері інформаційної безпеки спрямована на досягнення та утвердження американського домінування в глобальному інформаційному просторі. Ураховуючи важливість інформаційних ресурсів у всіх аспектах безпеки, інформаційне домінування стає ключовим для технологічного, економічного, військового та політичного переважання США над іншими державами.

Інформаційна політика США об'єднує ринкові інструменти лібералізації та регулювання інформаційної сфери, а також намагається встановити прямий державний контроль над інформаційними ресурсами, не лише на національному рівні, але й на міжнародному. Деякою мірою ці напрями можуть суперечити один одному.

У кваліфікаційній роботі було досліджено специфіку використання інформаційних технологій та ЗМІ США в умовах російської агресії.

Одним з ключовим аспектом специфіки використання інформаційних технологій є кібербезпека. Уряд США продовжує докладати зусиль, щоб посилити кібербезпеку країни, а також посилити свою загальну стратегію управління технологіями. Другим аспектом було виявлено соціальні мережі та інтернет. Третій – інформаційна війна. Наступними аспектами є створення та контроль наративу, глобальна інформаційна присутність, психологічна операційна діяльність та підтримка демократії та цінностей. Кожна з них відіграє ключову роль в інформаційній політиці США та розгортанню подальших подій.

Протидія російській пропаганді та маніпуляціям становить суттєвий компонент сучасної інформаційної стратегії Сполучених Штатів, спрямованої на забезпечення свободи слова, точності та об'єктивності інформації, а також на протидію дезінформації. В ході написання роботи було досліджено дії США в даному контексті: пакет екстрених витрат Конгресу США на 120 мільйонів доларів на протидію російській дезінформації та пропаганді; Глобальний центр взаємодії (GEC) Державного департаменту ділиться інформацією з агентствами США та іноземними урядами про російську дезінформацію в соціальних мережах, новинних виданнях і

російських проксі-сайтах; блокування доступу російських користувачів; санкції; запровадження системи штучного інтелекту інтелекту для виявлення та збору російської дезінформації в інтернеті.

В процесі дипломної роботи були досягнені всі цілі та розкрита мета, а саме – проведено аналіз і досліджено інформаційну політику Сполучених Штатів в контексті сучасних міжнародних відносин. Відповідно до поставленої мети було сформульовано та виконано всі завдання.

У теоретичній частині викладено теоретичні підходи до аналізу інформаційної політики в міжнародних відносинах, інструменти, базові принципи, політичні пріоритети, концепцію інформаційної політики США.

Практичний розділ містить специфіку використання інформаційних технологій та ЗМІ США в умовах російської агресії та тактику протидії російській пропаганді та маніпуляціям як частина сучасної інформаційної стратегії США.

Отже, в виконаній кваліфікаційній роботі акцентується на всеосяжній ролі американських засобів масової інформації, підтверджуючи їхнє значуще місце у системі формування суспільних настроїв. Крім того, в США ЗМІ відіграють вагому роль у зовнішній політиці, діючи як спостерігачі, учасники і каталізатори. Таким чином, обрана тема дипломної роботи є актуальною у контексті глобальної та міжнародної політики, а також в умовах повномасштабного вторгнення Росії в Україну.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аристова І. В. Еволюційний розвиток поняття «інформаційна сфера» / Вісник Національного університету внутрішніх справ. – 2005. – Вип. 31. – с. 228–245.
2. Баранов О. А. Правове забезпечення інформаційної сфери: теорія, методологія і практика / О. А. Баранов. – К. : Едельвейс, 2014. – 434 с.
3. Бармен Скотт , М. Вільямс Розробка правил інформаційної безпеки. – 2002. — 208 с.
4. Батрименко О.В. Роль соціальних медіа у російсько-українській інформаційній війні. Політологіічний вісник: збірник наукових праць. Київ: ТОВ «Вадекс», 2022. Вип. 89. С. 124-132.
5. Батрименко, О.В. (2022). Роль соціальних медіа в російсько-українській інформаційній війні. Політологічний вісник: збірник наукових праць. Київ: ТОВ «Вадекс», Вип.89, с. 124-132.
6. Боднар І.Р. Інформаційна безпека як основа національної безпеки. Механізм регулювання економіки, 2014. № 1. с. 68–75.
7. Боднар І.Р. Інформаційна безпека як основа національної безпеки. Механізм регулювання економіки. 2014. № 1. С. 68–75.
8. Бурило Ю. П. Інформаційна сфера як сфера господарювання: теоретично-правовий аспект / Ю. П. Бурило // Правова інформатика. – 2012. – № 4 (36). – С. 18–28.
9. В. Пашков. Інформаційна безпека США. Зарубіжний військовий огляд № 10/ 2010, с. 3-13.
10. Вайнгартен Ф. Основи федеральної інформаційної політики: Погляд конгресу США – 1996 р.
11. Волошин Ю.О. Legal globalization and interstate integration as a leading factor of the formation of state security and sovereignty. Atlantic Press. 2nd International Conference on Social, Economic and Academic Leadership. – 2018, № 11. – P. 351-358.

12. Горовий В. М. Національні інформаційні процеси в умовах глобалізації / В. М. Горовий. – К. : НБУВ, 2015. – 332 с.
8. Національний інформаційний комплекс і його роль у глобальному інформаційному просторі / О. С. Онищенко, В. М. Горовий, В. І. Попик та ін. – К. : НБУВ, 2014. – 218 с.
13. Д. Устинов. Сутність інформаційної безпеки. URL: https://cyberleninka.ru/article/n/suschnost-informatsionnoy-bezopasnosti/viewer (дата звернення: 19.05.2023)
14. Ділай А. Війна за Україну: від інформаційних операцій до прямого вторгнення. Вісн. Львів. ун-ту. Серія : Журналістика. 2019. № 45. С. 13-20.
15. Інформаційна війна проти України та засоби її ведення / Ю. О. Горбань // Вісник Національної академії державного управління при Президентові України. - 2015. - № 1. - С. 136-141.
16. Інформаційна політика держави як фактор реформування суспільства. URL: http://dspace.onua.edu.ua/handle/11300/1585 (дата звернення: 13.10.2023)
17. Інформаційна політика протидії російської пропаганди в Україні. URL: http://publications.lnu.edu.ua/bulletins/index.php/intrel/article/view/10364 (дата звернення: 13.10.2023)
18. Лібікі М. Що таке інформаційна війна? URL: http://viysko.com.ua/texnologiji-voyen/martin-libiki-shhotake-informacijna-vijna/ (дата звернення: 12.09.2023)
19. Магда Є.В. Гібридна війна: вижити і перемогти. Харків: Віват, 2015. 304 с.
20. Маковський І. Ю. Етапи становлення та значення інформаційної безпеки для ефективного функціонування підприємств, 2017. URL: https://conf.ztu.edu.ua/wp-content/uploads/2019/12/554.pdf (дата звернення: 17.05.2023)
21. Міжнародна інформаційна політика: структура, тенденції, перспективи. URL: https://elib.nakkkim.edu.ua/handle/123456789/2968 (дата звернення: 13.06.2023)

22. Національний інформаційний суверенітет у контексті розвитку новітніх інформаційних технологій / О. С. Онищенко, В. М. Горовий, В. І. Попик та ін. – К. : НБУВ, 2011. – 160 с.

23. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. Юридичний журнал. 2009. № 5. С. 122–134.

24. Почепцов Г. Г., Чукут С. А. Інформаційна політика. / Київ: Знання, 2006. 659с.

25. Почепцова Г. Г. Сучасні інформаційні війни. / Київ: Києво-Могилянська академія, 2015. 250 с.

26. Про сучасну інформаційну політику. URL: https://ippi.org.ua/sites/default/files/09bvmsip.pdf (дата звернення: 13.07.2023)

27. Роговської Є. Розвиток інформаційного сектора США на початок XXI століття // США – Канада – 2002 р. - №4

28. Російська пропаганда в Україні як інформаційна складова конфлікту. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3332 (дата звернення: 13.10.2023)

29. Росія втричі збільшила витрати на пропаганду під час війни з Україною, – ЗМІ. URL: https://focus.ua/world/512231-rossiya-vtroe-uvelichila-rashody-na-propagandu-vo-vremya-voyny-s-ukrainoysmi (дата звернення 25.05.2023)

30. Секрет успіху США у сфері інформаційної безпеки. URL: https://relint.vnu.edu.ua/index.php/relint/article/view/28 (дата звернення 22.04.2023)

31. Урсул А. Д. Информатизация общества. Введение в социальную информатику / А. Д. Урсул. – М. : Акад.общественных наук, 1990. – 192 с.

32. Юдін О. К, Богуш В. М. Інформаційна безпека держави. – Харків: Консум, 2005. – 506 с.

33. Burchill S, Theories of International Relations (R Devetak and J True eds, 6th edn, Bloomsbury Publishing), 2022.

34. Castells M. The Rise of the Network Society / M. Castells. – Oxford : Blackwell Publishers Ltd., 1996. – 556 p. – (The Information Age : Economy, Society and Culture, Vol. I).

35. Cloud Computing and Information Policy: Computing in a Policy Cloud. URL: https://www.tandfonline.com/doi/full/10.1080/19331680802425479 (дата звернення: 13.07.2023)

36. Freedom of Information Act. URL: https://home.treasury.gov/footer/freedom-of-information-act (дата звернення 25.08.2023)

37. High-tech sanctions and restrictions against Russia. URL: https://tadviser.com/index.php/Article:High-tech_sanctions_and_restrictions_against_Russia?ysclid=lpl6s2ftim450832209 (дата звернення 28.04.2023)

38. Historical Trends in Federal R&D. American Association for the Advancement of Science. 2020. URL: https://www.aaas.org/programs/r-d-budget-and-policy/ historical-rd-data (дата зверненя: 11.09.2023).

39. Information policy analysis features Russian aggression. URL: http://apir.iir.edu.ua/index.php/apmv/article/view/1146 (дата звернення: 13.10.2023)

40. Information Policy. The White House. URL: https://www.whitehouse.gov/omb/information-regulatory-affairs/information-policy/ (дата звернення 18.10.2023)

41. Information Warfare in Russia's War in Ukraine. The Role of Social Media and Artificial Intelligence in Shaping Global Narratives. URL: https://foreignpolicy.com/2022/08/22/information-warfare-in-russias-war-in-ukraine/ (дата звернення 02.02.2023)

42. Information warfare is not only about fakes. URL: https://ms.detector.media/propaganda-ta-vplivi/post/ 29264/2022-03-31-informatsiyna-viyna-tse-ne-tilky-feyky/ (дата звернення 07.04.2023)

43. International Information Security in US-Russian Bilateral Relations. URL: https://moderndiplomacy.eu/2023/05/22/international-information-security-in-us-russian-bilateral-relations/ (дата звернення 07.07.2023)

44. Karl Maria Michael de Leeuw, Jan Bergstra. The History of Information Security: A Comprehensive Handbook 1st Edition. (October 16, 2007).

45. Key indicators of information warfare Russia against Ukraine. URL: file:///C:/Users/%D0%9D%D0%B0%D1%81%D1%82%D1%8F/Downloads/14103-%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-28054-1-10-20230726.pdf (дата звернення: 12.09.2023)

46. Margulies P, 'Sovereignty and Cyber-Attacks: Technology's Challenge to the Law of State Responsibility' (2013) 14 (2) Melbourne Journal of International Law 496.

47. Michael Cox, Doug Stokes. US Foreign Policy 3e, 2020.

48. Michael Lind. The American Way of Strategy: U.S. Foreign Policy and the American Way of Life, 2018.

49. National Security Strategy of the United States of America / Seal of the President of the United States. December 2017 // The White House. URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf (дата звернення: 16.05.2023)

50. Niemeyer K and others, 'The Russian Invasion Shows How Digital Technologies Have Become Involved in All Aspects of War' (The Conversation, 28 March 2022). URL: https://theconversation.com/the-russian-invasion-shows-how-digital-technologies-have-become-involved-in-allaspects-of-war-179918 (дата звернення: 16.05.2023)

51. Perloff H. S., Dunn A. S. Information policy of the US government in the fi eld of R&D. Main fi nancial and institutional instruments // The American Economic Review. 2018. Vol. 108, № 12. P. 3622–3658.

52. Pillars of Russia's Disinformation and Propaganda Ecosystem. URL: https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf (дата звернення: 21.05.2023)

53. Should the U.S. help Ukraine? How does the Russia and Ukraine war affect the U.S.? URL: https://cvafoundation.org/should-the-us-help-ukraine-and-how-do-russia-and-ukraine-affect-the-us/ (дата звернення 27.08.2023)

54. The Emergent Global Information Policy Regime. URL: https://link.springer.com/chapter/10.1057/9780230377684_2 (дата звернення: 24.02.2023)

55. The impact of digital technology on international relations: the case of the war between Russia and Ukraine. URL: https://ajee-journal.com/upload/attaches/att_1679412084.pdf (дата звернення: 13.08.2023)

56. The Media : An Introduction / ed. by A. Briggs, P. Cobley. – 2nd ed. – Harlow : Pearson Education Ltd, 2002. – 500 p.

57. U.S. Security Cooperation with Ukraine. URL: https://www.state.gov/u-s-security-cooperation-with-ukraine/ (дата звернення 22.04.2023)

58. U.S. Security Cooperation with Ukraine. URL: https://www.state.gov/u-s-security-cooperation-with-ukraine/ (дата звернення 27.10.2023)

59. Ukraine and Russia. URL: https://www.state.gov/ukraine-and-russia/ (дата звернення 27.04.2023)

60. US Imposes Russia-Related Sanctions on 37 Individuals, 192 Entities. URL: https://sputnikglobe.com/20231102/us-imposes-russia-related-sanctions-on-37-individuals-192-entities-1114669434.html?ysclid=lpl6nwojw5470758521 (дата звернення 01.05.2023)

61. Why the US and NATO want war with Russia. URL: https://www.wsws.org/en/articles/2022/01/25/pers-j25.html (дата звернення 18.10.2023)

ДОДАТКИ

Таблиця 1.1 Характеристика інформаційної політики в контексті країн

Країна	Характеристика інформаційної політики
Великобританія	Головна мета полягає в поліпшенні умов конкуренції на інформаційному ринку, підвищенні результативності надання інформаційних послуг та впровадженні інформаційних технологій у сферу державного управління. Серед головних пріоритетів варто виділити освіту, охорону здоров'я і підтримку приватного сектору. Ця мета досягається через дотримання таких принципів, як технологічна нейтральність законів, підтримка міжнародного співробітництва та захист прав інтересів споживачів у сфері комп'ютерних систем і мереж.
Німеччина	Головна мета полягає у забезпеченні незавадного транскордонного обміну інформацією і забезпеченні свободи слова. Також метою є розвиток інформаційно-комп'ютерних технологій і телекомунікаційних мереж, створення умов для вільної конкуренції в інформаційній сфері і встановлення нових норм і принципів правового регулювання інформаційної діяльності в німецькому суспільстві. Ця ініціатива спрямована на підтримку реформування державного управління у зазначених країнах, їх участь у вільному транскордонному обміні інформацією, популяризацію цінностей європейської демократії, створення правової основи, технічного забезпечення сектору інформаційних технологій та підготовку кваліфікованих спеціалістів для національних та приватних корпорацій, організацій, фондів і т. д.

Франція	Головна мета цього завдання полягає у розвитку інфраструктури для інформаційних мереж, розширенні можливостей електронного ринку і банківської сфери, забезпеченні вільного доступу до комунікаційних засобів, перегляді інформаційного законодавства з метою внесення реформ, підтримці наукових досліджень у сфері інформаційних технологій, створенні систем безпеки інформації та запобіганні комп'ютерним злочинам. Уряд також утворив Фонд допомоги і співробітництва для підтримки впровадження вітчизняних інформаційних технологій.
Японія	Головна ціль полягає у створенні дієвого інформаційного суспільства, заснованого на доступі до засобів оптичного волокна для урядових інститутів, державних організацій і приватних підприємств, які потребують спеціалізованого програмного забезпечення.
США	Основна мета полягає у налагодженні контролю над інформаційними потоками в політичній, економічній, науковій та військовій сферах з метою забезпечення балансу між державним наглядом і свободою підприємницької діяльності. Основними пріоритетами є підтримка наукових досліджень і розробок в галузі інформатизації і телекомунікацій, сприяння обміну технологіями між університетами і фірмами, розвиток та покращення інформаційної інфраструктури, включаючи глобальну, збалансованість між основними інформаційними цінностями та впровадженням нових інформаційних технологій, а також вдосконалення

	державної політики у сфері інформатизації і телекомунікацій.
Європейський союз (ЄС)	Ця ініціатива ґрунтується на концепції єдиного загального підходу до інформаційної політики, яка втілюється у концепції співробітництва в Європейському просторі інформації та зв'язку. Вона розглядається та реалізується на різних рівнях - місцевому, регіональному, національному і наднаціональному, і всі ці рівні управління інтегровані в одну цілісну систему.