МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ЕКОНОМІКИ І ТЕХНОЛОГІЙ

ННІ/факультет	Навчально-науковий інститут економіки та бізнес-освіти
Кафедра	міжнародних відносин
Спеціальність	291 Міжнародні відносини, суспільні комунікації та регіональні студії
Форма навчання	денна

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

Малько Катерини Сергіївни

(прізвище, ім'я, по батькові здобувача)

на тему: **Інформаційна безпека в стратегіях комунікації держав: виклики та тенденції**

(повна назва теми)

за матеріалами

(повна назва бази дослідження)

науковий керівник к.і.н. _____ **Н.ШЕЛУДЯКОВА**
(наук. ступінь, вчене звання) *(підпис)* *(прізвище, ініціали)*

Робота допущена до захисту в ЕК
Протокол засідання кафедри
від "10" червня 2025 р. № 12

Завідувач кафедри _____
(підпис)

д.е.н., доцент І. МАКСИМОВА
Наук. ступінь, вчене звання *Ініціали, прізвище*

Кривий Ріг – 2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ЕКОНОМІКИ І ТЕХНОЛОГІЙ

ННІ/факультет	Навчально-науковий інститут економіки та бізнес-освіти
Кафедра	міжнародних відносин
Спеціальність	291 Міжнародні відносини, суспільні комунікації та регіональні студії
Форма навчання	денна

«ЗАТВЕРДЖУЮ»

Завідувач кафедри _____ І. МАКСИМОВА
(підпис) (Прізвище, ініціали)
«16» червня 2025 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ БАКАЛАВРСЬКУ РОБОТУ
Малько Катерина Сергіївна

1. Тема роботи Інформаційна безпека в статегіях комунікації держав: виклики та тенденції
Керівник роботи Шелудякова Наталія Андріївна, к.і.н.
затверджено наказом закладу вищої освіти від «04» квітня 2025 р. № 236-ст

2. Строк подання здобувачем роботи «16» червня 2025 р.

3. Зміст кваліфікаційної магістерської роботи, об'єкт, предмет та мета дослідження:

Розділ 1. Теоретичні засади інформаційної безпеки в контексті державних комунікацій
Базові поняття, моделі та парадигми інформаційної безпеки в контексті державних комунікацій, стратегічні комунікації як інструмент політики

Розділ 2. Сучасні виклики та тенденції в сфері інформаційної безпеки
Актуальні загрози інформаційній безпеці держав, такі як кібератаки, дезінформація, цифрове шпигунство та нові виклики, пов'язані зі штучним інтелектом

Розділ 3. Використання стратегічних комунікацій в інформаційній безпеці
Практичне застосування стратегічних комунікацій для зміцнення інформаційної безпеки, з прикладами кампаній та механізмів державної взаємодії з аудиторіями

Об'єкт дослідження: державна система комунікацій та інформаційного захисту.

Предмет дослідження: механізми, інструменти та стратегії забезпечення інформаційної безпеки у державних комунікаціях.

Мета кваліфікаційної бакалаврської роботи: дослідження концепції інформаційної безпеки в контексті державних комунікаційних стратегій, аналіз сучасних викликів та тенденцій, а також вивченні практичного досвіду країн світу у протидії інформаційним загрозам.

5. Дата видачі завдання "04" квітня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної магістерської роботи	Строк виконання етапів роботи	Відмітка керівника про виконання етапів (дата, підпис)
1	Підготовка розділу 1	14.04.2025 р.	28.04.2025 р.
2	Підготовка розділу 2	12.05.2025 р.	12.05.2025 р.
3.	Підготовка розділу 3	21.05.2025 р.	02.06.2025 р.
4	Перевірка кваліфікаційної бакалаврської роботи на наявність ознак академічного плагіату за допомогою програм UNICHECK / StrikePlagiarism	до 04.06.2025 р.	04.06.2025 р.
5	Отримання відгуку від наукового керівника	до 16.06.2025 р.	16.06.2025 р.
6	Подання кваліфікаційної роботи на перегляд завідувачу кафедри	до 16.06.2025 р.	16.06.2025 р.
7	Реєстрація завершеної кваліфікаційної роботи	16.06.2025 р.	Реєстраційний № ___ «16» червня 2025 р.
8	Попередній захист кваліфікаційної роботи на кафедрі	16.06.2025 р.	16.06.2025 р.
9	Підготовка до захисту в ЕК	до 18.06.2025 р.	до 18.06.2025 р.

Завдання підготував науковий керівник Н. ШЕЛУДЯКОВА
(прізвище та ініціали)

Завдання одержав К.МАЛЬКО
(прізвище та ініціали)

Декларація
про дотримання академічної доброчесності під час написання кваліфікаційної бакалаврської роботи
здобувачем вищої освіти
Державного університету економіки і технологій

Я, Малько Катерина Сергіївна студентка 4 курсу, групи МВС-21 Державного університету економіки і технологій розумію і підтримую політику закладу із академічної доброчесності. Я не надавала і не одержувала заборонену допомогу під час підготовки цієї роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

10.06.2025  **К. МАЛЬКО**

АНОТАЦІЯ

Малько Катерина Сергіївна. Інформаційна безпека в стратегіях комунікації держав: виклики і тенденції. Кваліфікаційна бакалаврська робота. Спеціальність 291 — Міжнародні відносини, суспільні комунікації та регіональні студії. Державний університет економіки та технологій. Кривий Ріг, 2025.

У роботі досліджено теоретичні засади та практичні аспекти забезпечення інформаційної безпеки в стратегіях комунікації держав. Проаналізовано сучасні виклики та загрози, пов'язані з інформаційною безпекою, зокрема кібератаки, дезінформація, інформаційний тероризм, шпигунство.

Розглянуто роль стратегічних комунікацій як інструмента державної політики у зміцненні стійкості суспільства, захисті інформаційного простору та протидії гібридних загрозам. Узагальнено міжнародний досвід США, ЄС, Естонії та Тайваню та визначено можливості його адаптації в Україну.

На основі проведеного аналізу запропоновано практичні рекомендації щодо посилення інформаційної безпеки держави, розвитку комунікаційних стратегій та формування культури населення.

Ключові слова: інформаційна безпека, дезінформація, кібератаки, гібридна війна, кібербезпека, стратегічні комунікації, медіаграмотність, держава, комунікаційні стратегії.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ЗМІ – Засоби масової інформації

КНР – Китайська Народна Республіка

РФ – Російська Федерація

США – Сполучені Штати Америки

ШІ –Штучний інтелект

ACL – Access Control List (Список контролю доступу)

CRRTs – Cyber Rapid Reaction Teams (Кібергрупи швидкого реагування)

DDoS – Distributed Denial of Service (Розподілена атака на відмову в обслуговуванні)

ENISA – European Union Agency for Cybersecurity (Агентство ЄС з кібербезпеки)

EU – European Union (Європейський Союз)

GAN – Generative Adversarial Network (Генеративно-змагальна мережа)

ISMS – Information Security Management System (Система управління інформаційною безпекою)

NATO – North Atlantic Treaty Organization (Організація Північноатлантичного договору)

PR – Public Relations (Зв’язки з громадськістю)

RBAC – Role-Based Access Control (Рольовий контроль доступу)

SIEM – Security Information and Event Management (Система управління інформацією про безпеку та подіями)

SSH – Secure Shell (Протокол безпечного доступу)

StratCom – Strategic Communications (Стратегічні комунікації)

TLS – Transport Layer Security (Протокол захищеної передачі даних)

UEBA – User and Entity Behavior Analytics (Аналітика поведінки користувачів та об’єктів)

VPN – Virtual Private Network (Віртуальна приватна мережа)

ВСТУП

Сучасний інформаційний простір набуває першочергового значення, оскільки розвиток цифрових технологій, глобалізація інформаційних потоків та посилення гібридних загроз створюють нові виклики для держав, суспільства та кожного окремого громадянина. В еру інформаційного суспільства доступ до даних та можливість впливу на інформаційну сферу стають важливими інструментами забезпечення національних інтересів, формування громадської думки, зміцнення довіри до державних інституцій та протидії зовнішнім загрозам.

Інформаційна війна не обмежується традиційними воєнними конфліктами, а розгортається на полях соціальних мереж, медіа, комунікаційних каналів, де дезінформація, пропаганда, фейкові новини та інформаційні операції стають зброєю впливу на громадську свідомість і політичні процеси. Інформаційний простір перетворюється на арену боротьби за увагу, довіру та контроль суспільними настроями, що робить стратегії комунікації держав ключовим інструментом забезпечення безпеки та стійкості.

Розробка ефективних комунікаційних стратегій, здатних захистити державу від дезінформаційних атак, забезпечити стабільність, сформувати позитивний імідж на міжнародній арені та консолідувати суспільство навколо спільних цінностей — є актуальним завданням для сучасних держав. Особливої актуальності ця тема набуває для України, яка в умовах гібридної війни та зовнішньої агресії щодня стикається з викликами інформаційної безпеки, атакою на цифрові ресурси, маніпуляціями громадською думкою та спробами підірвати довіру до державних інституцій.

Актуальність теми обумовлена необхідністю формування цілісної та системної політики інформаційної безпеки в умовах глобальної нестабільності та загроз національному суверенітету. Дослідження сприятиме кращому розумінню ролі стратегічних комунікацій у забезпеченні інформаційного

суверенітету держави та розробці практичних рішень для ефективної протидії сучасним інформаційним загрозам.

Мета роботи полягає у комплексному дослідженні концепції інформаційної безпеки в контексті державних комунікаційних стратегій, аналізі сучасних викликів та тенденцій, а також вивченні практичного досвіду країн світу у протидії інформаційним загрозам.

Для досягення були поставлені такі досілдницькі завдання:

– проаналізувати теоретичні засади поняття інформаційної безпеки та її роль у сфері міжнародних відносин;

– з’ясувати сутність та особливості стратегічних комунікацій як інструменту державної політики;

– виявити сучасні загрози інформаційній безпеці, зокрема у контексті розвитку цифрових технологій, гібридної війни, дезінформаційних кампаній та кіберзлочинності;

– дослідити тенденції трансформації державних комунікаційних стратегій в умовах нових викликів;

– проаналізувати практичні приклади протидії інформаційним загрозам у таких країнах, як США, ЄС, Тайвань та Естонія;

– сформулювати рекомендації щодо підвищення інформаційної стійкості України та посилення її державної комунікаційної політики в умовах гібридної війни.

Об’єктом дослідження є державна система комунікацій та інформаційного захисту, яка формується у відповідь на сучасні загрози та виклики в інформаційному просторі. Це явище створює проблемну ситуацію в умовах глобалізації, цифровізації та гібридних загроз, що потребує наукового вивчення та розробки ефективних рішень.

Предметом дослідження є механізми, інструменти та стратегії забезпечення інформаційної безпеки у державних комунікаціях, а також економічні, соціальні та політичні аспекти функціонування інформаційної безпеки як складової державної політики в умовах гібридної війни.

У процесі дослідження було використано низку взаємодоповнюваних методів, що забезпечили всебічне розкриття теми. Зокрема, застосовано аналіз і синтез для структурного осмислення понять інформаційної безпеки, порівняльно-правовий та інституційний аналіз для зіставлення міжнародного досвіду (США, ЄС, Тайваню, Естонії), а також контент-аналіз державних комунікаційних кампаній, спрямованих на протидію дезінформації. Метод кейс-стаді дав змогу глибше вивчити конкретні приклади інформаційних загроз та відповідей на них. Крім того, дослідження базується на системному та міждисциплінарному підходах, що поєднують політичні, правові, технічні та комунікаційні аспекти забезпечення інформаційної безпеки в умовах гібридної війни та цифрових трансформацій.

Практична значущість роботи полягає у розробці рекомендацій та пропозицій щодо удосконалення державної інформаційної політики, зокрема стратегічних комунікацій, протидії дезінформації та забезпечення інформаційної безпеки в умовах сучасних загроз. Результати дослідження можуть бути впроваджені у діяльність державних установ, аналітичних центрів, комунікаційних підрозділів органів влади та приватних компаній, які здійснюють міжнародну економічну діяльність або є залученими до міждержавного співробітництва у сфері інформаційної безпеки. Зокрема, напрацьовані пропозиції можуть бути корисними для підвищення рівня інформаційної обізнаності, формування навичок медіаграмотності, посилення стійкості до інформаційних атак та підвищення ефективності державних комунікаційних стратегій.

Апробація результатів виконана під час міжнародної науково-практичної конференції “Журналістика XXI століття: виклики та перспективи”, за результатами якої опубліковано наукові результати “Сучасні тенденції в журналістиці”.

РОЗДІЛ 1 ТЕОРЕТИЧНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОНТЕКСТІ ДЕРЖАВНИХ КОМУНІКАЦІЙ

1.1 Поняття та сутність інформаційної безпеки у міжнародних відносинах

У світі глобалізації, численних конфліктів, диджиталізації інформаційна безпека має ключове значення для стабільності розвитку країни. Вона охоплює не лише технічні заходи захисту даних, а й формування стійкого до зовнішніх впливів інформаційного середовища, захист стратегічної інформації, захист державних комунікацій, іміджу країни, стратегічної інформації та інституцій від зовнішніх загроз.

Інформаційна безпека держави — стан захищеності та інформаційного розвитку, за якого інформаційні війни, операції, терористичні акти в інформаційному середовищі та комп'ютерна злочинність не завдають суттєвої шкоди національним інтересам. Потрібний рівень інформаційної безпеки країни забезпечується при створенні умов для гармонійного розвитку інформаційної інфраструктури держави, реалізації конституційних прав і свобод людини в інтересах держави: зміцнення суверенітету і територіальної цілісності країни, встановлення політичної і соціальної стабільності, економічного розвитку, безумовного виконання законів та міжнародного співробітництва [1].

До основних загроз інформаційній безпеці належать:

- **Акції інформаційно-психологічного впливу** — дії, які передбачають спланований вплив на свідомість і поведінку групи людей шляхом поширення упередженої, неповної або недостовірної інформації та інформаційно-технічну структуру об'єкта.
- **Комп'ютерна злочинність** — незаконне соціальне явище, яке полягає у використанні електрообчислювальних машин, систем та комп'ютерних мереж та мереж електрозв'язку.

Рис 1.1 Структура інформаційної безпеки держави

Примітка: розроблено автором

- **Інформаційний тероризм** — інформаційний вплив на соціальні групи, державні органи влади та управління, які пов'язані з поширенням інформації, що містить в собі погрози розправи, переслідування, вбивства, а також викривлення інформації, яка може спричинити виникненню кризової ситуації у країні.

Об’єктами інформаційної безпеки можуть бути:

- свідомість окремих осіб, групи або суспільства загалом;
- інформаційні ресурси (зокрема, конфіденційні або критично важливі для функціонування держави);
- інформаційно-телекомунікаційна інфраструктура (система створення, зберігання, поширення й передання даних).

Різні наукові підходи пояснюють механізми інформаційного впливу через концепції стратегічних комунікацій, «м’якої сили», інформаційних війн та когнітивного управління. Одним із ключових інструментів у цьому контексті є модель стратегічних комунікацій.

Модель стратегічних комунікацій (Strategic Communications) передбачає скоординоване використання інформаційних ресурсів для формування сприятливого інформаційного середовища, зміцнення довіри, підвищення легітимності держави та впливу на зовнішню і внутрішню аудиторію. Вона

базується на синергії дипломатії, PR, психологічних операцій, культурної дипломатії та медіа [2].

Наприклад, ЄС та НАТО активно використовують стратегічні комунікації для протидії дезінформації з боку третіх країн [3]. Ця модель базується на системному, міждисциплінарному підході: вона поєднує знання з політології, соціології, психології та кібербезпеки. Стратегічні комунікації відрізняються від звичайної комунікації тим, що вони мають довгостроковий характер, прив'язані до стратегічних наративів і цінностей, а також тісно інтегровані у загальну політику національної безпеки [2, 7].

Ншою концепцією, яка розкриває потенціал інформаційного впливу у міжнародних відносинах, є теорія «м'якої сили», запроваджена Джозефом Найєм (Joseph Nye). Ця модель підкреслює здатність держави впливати на інші країни не силою чи тиском, а через привабливість її культури, політичних ідей та зовнішньої політики. В основі — здобуття згоди, а не примусу.

Класичним прикладом є вплив США через Голлівуд, англійську мову, університети та популярну культуру [4]. М'яка сила реалізується через ключові ресурси:

- Культура (у її привабливій формі, включаючи мистецтво, кінематограф, мову, музику);
- Політичні цінності (демократія, права людини, верховенство права — якщо дотримуються послідовно);
- Зовнішня політика (яка сприймається як легітимна і моральна).

Ця концепція безпосередньо пов'язана з інформаційною політикою, оскільки значна частина «м'якої сили» реалізується саме через інформаційні канали: ЗМІ, соціальні мережі, культурні інституції, публічну дипломатію, міжнародні мовники [4, 8].

Одним із важливих проявів деструктивного інформаційного впливу в сучасному світі є інформаційна війна — цілеспрямоване використання інформаційних технологій і засобів масової комунікації для деструктивного впливу на противника: зниження бойового духу, поширення паніки, підриву

довіри до влади. Інформаційна війна є складовою гібридної війни, що передбачає поєднання збройного протистояння та маніпулятивного впливу на інформаційний простір. Характерним прикладом виступає активне використання дезінформації та фейків у період збройних конфліктів або політичних криз. У межах цієї моделі інформація виступає не просто як канал комунікації, а як зброя, здатна змінювати реальність, впливаючи на сприйняття подій, дійсності й легітимності владних інститутів. [9]

Модель інформаційної війни охоплює широкий спектр методів, серед яких:

- поширення дезінформації;
- маніпуляція наративами та емоціями;
- психологічний тиск через медіа;
- створення інформаційного шуму та протиріч;
- використання бот-мереж і тролінгу;
- атаки на інформаційну інфраструктуру;
- імітаційна активність (deepfake, фейкові акаунти, псевдоновини).

У тісному зв’язку з інформаційною війною розвивається когнітивна модель впливу (Cognitive Warfare), яка зосереджена на втручанні у ментальні процеси цільової аудиторії — сприйняття, пам’ять, судження, емоції. Її мета — зміна рішень, поведінки, лояльності та цінностей цільової аудиторії. Основними інструментами когнітивного впливу є маніпулятивні наративи, алгоритми соцмереж, використання deepfake-технологій. Наприклад, таргетована політична реклама в соціальних мережах, яка використовує дані про психологічний профіль користувачів [5].

Когнітивна модель пояснює вплив інформації через призму психології та нейронаук, зосереджуючи увагу на зміні способу сприйняття, обробки та інтерпретації інформації суб’єктами. Ключовим завданням когнітивного впливу є трансформація мислення, емоційного стану, цінностей, рішень і поведінки цільової аудиторії. Такий вплив здійснюється за допомогою цілеспрямованої маніпуляції наративами, використання технологій алгоритмічного підбору

контенту в соціальних мережах, а також застосування гібридних інструментів, таких як deepfake-технології, боти тощо.

Окремим проявом цього впливу є когнітивні операції (COGOPS) — латентні дії, які можуть маскуватися під «звичайні» інформаційні потоки та бути непомітними для широкого загалу. Саме ця прихованість і здатність досягати стратегічних цілей, уникаючи прямої конфронтації, робить COGOPS дедалі більш популярними серед держав і недержавних акторів [6]

Ширшим за своїм аналітичним охопленням є підхід, що базується на моделі інформаційного суспільства (Information Society). Це соціологічна модель, яка розглядає інформацію як центральний ресурс розвитку. У такому суспільстві знання, інформаційні технології та мережеві комунікації стають головним чинником впливу на політичні, економічні й соціальні процеси. Прикладами є зростання політичної активності у соціальних мережах, розвиток електронного урядування чи цифрової дипломатії. Модель інформаційного суспільства описує сучасний етап розвитку людства, в якому виробництво, обробка, зберігання та поширення інформації стають ключовими факторами соціального, економічного та політичного розвитку. В інформаційному суспільстві **інформація та знання** виступають основними ресурсами, подібно до того, як у попередніх історичних етапах такими були праця, земля або капітал [10].

Інформаційне суспільство сприяє підвищенню прозорості державних процесів, розвитку електронної демократії, зростанню ролі громадянського суспільства. Проте воно також породжує нові виклики для інформаційної безпеки, зокрема:

- вразливість до кібератак;
- розповсюдження дезінформації;
- монополізацію цифрового простору транснаціональними корпораціями;
- загрозу маніпуляцій суспільною свідомістю через алгоритми платформ.

Через це, розвиток інформаційної безпеки утворив три головні теоретико-методологічні моделі: технічна, ідеологічна та правова.

У статті О. Тихомирова «Інформаційна безпека: соціотехнічна парадигма» запропоновано трирівневу модель інформаційної безпеки, що включає *технічну*, правову та психологічну складові на індивідуальному та суспільному рівнях [11]. Технічна парадигма зосереджується на застосуванні технологій із метою захисту інформації. Це включає криптографію, мережеві заходи безпеки, системи виявлення вторгнень і т.д. Основні складові включають в себе:

- Криптографічний захист інформації (шифрування, цифровий підпис, хешування [12], протоколи безпечної передачі TLS, VPN, SSH [13])
- Контроль доступу (аутентифікація, авторизація, механізми обмеження доступу ALC, RBAC [14])
- Захист кінцевих пристроїв (антивірусні програми, антишпигунські засоби, патч-менеджмент [15], засоби контролю USB та портів)
- Моніторинг та аудит (системи логування SIEM [16], аналіз поведінки користувачів UEBA [17])
- Резервне копіювання та відновлення (стратегії резервного копіювання, відновлення після аварій)

Криптографічний захист реалізується через використання таких інструментів, як хешування — процес перетворення вхідних даних (таких як текст або фрагменти тексту) у випадковий набір байтів фіксованої довжини за допомогою хеш-функцій [12]; **протоколи захищеної передачі даних — зокрема TLS (Transport Layer Security)**, що забезпечує шифрування трафіку між клієнтом і сервером; **VPN (Virtual Private Network)**, який створює захищене з'єднання між користувачем і мережею, приховуючи IP-адресу і шифруючи весь трафік; і **SSH (Secure Shell)** — протокол для безпечного віддаленого доступу до серверів і комп’ютерів через мережу. [13]

Контроль доступу здійснюється за допомогою таких мехінзімів, як **ACL (Access Control List)** — список, який вказує, хто і які дії може виконувати над конкретним об’єктом (наприклад, «користувач А може читати, але не змінювати

файл») та **RBAC (Role-Based Access Control)** — доступ надається не окремим користувачам, а ролям (наприклад, «роль *адміністратор* має повний доступ, роль *користувач* — лише читання»), а потім користувачі прив’язуються до ролей [14].

Захист кінцевих пристроїв передбачає використання антивірусних і антишпигунських програм, а також **патч-менеджменту** — процесу оновлення програмного забезпечення шляхом встановлення патчів (виправлень), щоб усунути вразливості, покращити функціональність або виправити помилки [15].

Моніторинг та аудит інформаційних систем забезпечуються через **системи логування** — засоби збору, зберігання та аналізу журналів (логів) подій у системах, щоб відстежувати дії, помилки чи підозрілу активність [16]. Додатково застосовується **UEBA (User and Entity Behavior Analytics)** — це технологія, яка аналізує поведінку користувачів і об'єктів (наприклад, комп’ютерів, акаунтів) у системі, щоб виявити аномалії, які можуть свідчити про загрози (наприклад, злам аккаунта або внутрішню атаку) [17].

Ідеологічна парадигма висвітлена у статті С.Єсімової «Методологічні основи дослідження інформаційної безпеки», де проаналізовано міждисциплінарні підходи до дослідження інформаційної безпеки, включаючи філософські та *соціологічні* аспекти [18]. **Ідеологічна парадигма інформаційної безпеки** — це концептуальний підхід, що акцентує увагу на людському факторі, інформаційній культурі та ідеологічному впливі як ключових складниках захисту інформації в суспільстві. Ця парадигма розглядає безпеку не лише як технологічне чи юридичне явище, а як психологічну категорію. Головні аспекти ідеологічної культури запроваджують:

- Розвиток інформаційної культури [19] (усвідомлення значення захисту інформації на рівні особистості, організації, держави; формування навичок безпечної поведінки в інформаційному середовищі; виховання критичного мислення щодо інформаційних джерел);

- Протидія маніпуляціям, фейкам, дезінформації (захист від інформаційного стресу, залежності та когнітивного перевантаження; інформаційна гігієна, як усвідомлене споживання інформації [20]);
- Навчання та просвіта (включення тем інформаційної безпеки до шкільних і університетських програм; проведення тренінгів, кампаній з кібергігієни, популяризація теми через ЗМІ).

Люди — найвразливіша ланка в інформаційній безпеці. Жодна система не захистить від наслідків, якщо користувач легко піддається фейкам, розголошує дані чи стає мішенню для соціальної інженерії.

Правова парадигма інформаційної безпеки розглядає захист інформаційного простору як сферу, що регулюється юридичними механізмами — через закони, підзаконні акти, державну політику та міжнародні зобов'язання. Стаття «Інформаційна безпека: правовий та культурологічний виміри» Бикова О.М. [21], розглядає інформаційну безпеку як соціокультурне явище, зосереджуючись на її *правових* аспектах у контексті українського суспільства. **Правова парадигма інформаційної безпеки** покликана створити юридичну основу, яка визначає права, обов'язки, заборони та відповідальність усіх учасників інформаційного простору та складає [23]:

- Нормативно-правове регулювання (конституційні положення; закони про захист персональних даних, державну таємницю, кібербезпеку, інформацію; адміністративна, кримінальна та цивільна відповідальність за порушення інформаційної безпеки);
- Міжнародне право та співпраця (конвенція про кіберзлочинність (Будапештська конвенція); рекомендації ООН, Ради Європи, ЄС щодо цифрових прав і свобод; участь у міждержавних ініціативах);
- Захист прав суб'єктів інформаційних відносин (право на інформацію та право на її захист; регулювання обробки персональних даних (GDPR — в ЄС, ЗУ «Про захист персональних даних» — в Україні);

- Інституційне забезпечення (органи, відповідальні за інформаційну безпеку (СБУ, Держспецзв'язок, Нацполіція, "сині" хакери [22]); національні стратегії та концепції інформаційної безпеки);

Види правової відповідальності у сфері інформаційної безпеки [23]:

- Кримінальна: за кіберзлочини, неправомірний доступ до інформації, втручання в системи;
- Адміністративна: за порушення правил захисту інформації, зберігання даних, роботи з ЗМІ;
- Цивільно-правова: за збитки, спричинені витоком інформації чи порушенням договірних зобов'язань.

Інформаційна безпека сьогодні — це сфера, в якій перетинаються знання з політики, права, соціології, психології та комунікацій. Її забезпечення вимагає не стільки окремих рішень, скільки системного мислення: комплексної взаємодії технічних інструментів, нормативно-правової бази та здатності суспільства критично сприймати інформацію.

Ключова проблема полягає в тому, що інформаційний простір став полем боротьби за свідомість. У цьому середовищі виграє не той, хто має більше даних, а той, хто краще керує наративами, довірою та смислами.

Справжня стійкість в інформаційній сфері ґрунтується не лише на технологічному захисті, а на поєднанні стратегічної комунікації як інструмента впливу і захисту, правової чіткості у правилах гри, ідеологічної готовності громадян чинити опір маніпуляціям.

Без формування цілісної культури інформаційної безпеки — на рівні інституцій і на рівні індивіда — жодна модель захисту не буде ефективною. Це і є головний виклик XXI століття: перейти від оборони до проактивного управління інформаційним середовищем.

1.2 Стратегічні комунікації як інструмент державної політики

В умовах гібридних загроз, кібератак і поширення дезінформації стратегічні комунікації стали критичним інструментом захисту національної безпеки та стійкості демократичних інституцій. У сучасному світі стратегічні комунікації є невід'ємною складовою державної політики, що спрямована на формування довіри, консолідацію суспільства та забезпечення національної безпеки.

Згідно з визначенням НАТО, **стратегічні комунікації** (StratCom) — це скоординоване використання комунікаційних інструментів і ресурсів держави для досягнення стратегічних цілей, шляхом формування громадської думки та підтримки як всередині країни, так і на міжнародному рівні [24]. Метою стратегічних комунікацій є формування позитивного іміджу держави, забезпечення інформаційної безпеки, протидія дезінформації та зміцнення довіри до державних інституцій. Стратегічні комунікації виступають як засіб гармонізації відносин між державою, суспільством та міжнародними партнерами.

У практиці державного управління використовуються різноманітні стратегії комунікаційної діяльності, ефективність яких досягається за умов [24]:

1. Підхід до формування стратегії має бути адаптивним, це вимагає гнучкої та відкритої системи, коли інституції працюють разом з метою зосередити зусилля на необхідному.

2. Дотримання політики активного інформування громадськості, що спрямована на стимулювання її зацікавленості та ЗМІ до подій та діяльності інституцій. Цей інтерес може стимулюватися за допомогою пресрелізів, інформаційних бюлетенів, випусків новин, особистих контактів, пресконференцій та інших видів публічної презентації.

3. Розроблення стратегії має ґрунтуватися на культурному усвідомленні поточних та історичних цінностей, норм і вірувань, що

відображаються в різних соціальних структурах, зокрема в тому, як вони впливають на мотиви, наміри та поведінку реципієнтів, та враховувати наявну психологічну обстановку – емоційний стан, менталітет та інші поведінкові мотивації реципієнтів, що ґрунтуються переважно на національних, політичних, соціальних, економічних та психологічних особливостях, але при цьому на них також можуть впливати обставини та події.

4. Варто розраховувати ефективність реципієнтів – їхню можливість реалізувати бажану реакцію або поведінку свою чи інших як результат впровадження стратегії.

5. Стратегія має бути гнучкою, тобто легко адаптуватися до вимог, що змінюються. Ці вимоги можуть бути передбачуваними та непередбачуваними й впливати, наприклад, на конфігурацію, застосування, розміщення, використання певних інформаційних матеріалів.

6. Не слід боятися інноваційності. Інновація часто розглядається як загроза наявному потенціалу та інвестиціям, що були вкладені, та навколо яких розвинулися субкультури та культури. Інновації завжди піддаються сумніву, саме тому це завжди підготовка до можливих конфліктів.

Саме через дотримування стратегій комунікаційної діяльності, можна впроваджувати тактики реалізації стратегічних комунікацій, які включають:

- сегментацію цільової аудиторії [25];
- адаптацію повідомлень до потреб і цінностей різних груп населення; [26]
- використання емоційного впливу та сторітелінгу;
- моніторинг інформаційного середовища.

Серед основних інструментів стратегічних комунікацій можна виокремити:

1) Офіційні заяви органів влади — формальні повідомлення, що визначають позицію держави з ключових питань. Яскравим прикладом є реакція України на повномасштабне вторгнення РФ у 2022 році. Серед основних комунікаційних органів — Офіс Президента України, ЗСУ, Центр

стратегічних комунікацій. Стратегія комунікації у цьому випадку була мобілізаційною, спрямованою на зміцнення бойового духу, антикризове реагування та інформаційну безпеку. Ключовими елементами висутпили щоденні відеозвернення Володимира Зеленського, чіткі меседжі: “Ми тут”, “Ми не здамося”, постійна координація з міжнародною пресою, центр стратегічних комунікацій (Stratcom) оперативно спростував фейки РФ. Результатом стало формування позитивного глобального іміджу України й інформаційна протидія у перші місяці повномасштабного вторгнення.

2) Публічні виступи лідерів — звернення Президента, Прем’єр-міністра, міністрів та інших посадових осіб, які мають високий вплив на суспільну думку. Прикладом можна зазначити виступ прем’єр-міністра Великої Британії Бориса Джонсона щодо введення карантину (23 березня 2020 р.). Головною стратегією, як інструмент мобілізації, було переконання та легітимації жорстких рішень. Ключовими елементами виступали пряма мова, емоційна інтонація, апеляція до моралі та акцентуючі звернення: “Ви повинні залишатися вдома.”; чітке пояснення нових правил (1 раз на день на вулицю, тільки одна прогулянка, закриття бізнесів); риторика відповідальності: “Якщо ви не будете дотримуватись правил, поліція матиме повноваження їх забезпечити”. У результаті сформувався образ Джонсона як лідера, який здатен ухвалювати складні рішення й дотримання високого рівня карантину у перші тижні.

3) Соціальні мережі — інструмент прямої комунікації з громадськістю. Вони дозволяють оперативно реагувати на виклики та мобілізувати підримку. Популярним прикладом є кампанія #BlackLivesMatter (2020). Одним із ключовим елементом стратегії є тимчасове реагування на масові протести проти расизму й поліцейського насильства після вбивства Джорджа Флойда в США. Використовувались такі інструменти, як: соціальні мережі (Twitter, Instagram, Facebook), короткі відео у форматі “селфі”, де мер Лондона дякує протестувальникам за мирну поведінку, закликає до солідарності й недопущення насильства, реакція в реальному часі. У результаті

мер отримав підтримку більшості протестувальників і громадських організацій, його позиція стала частиною міжнародного інформаційного потоку, зміцнивши імідж столиці як відкритого, толерантного міста.

4) Медіаплатформи — виступають каналами широкого розповсюдження державної позиції поширюючись на телебаченні, радіо, онлайн-платформах. Відома австралійська кампанія “Quit Smoking” (2011 — донині) є прикладом успішної стратегії зменшення рівня куріння серед населення. Запроваджувались інформаційні вістки, стосовно підвищення обізнаності про шкоду тютюну; заборонялась реклама тютюну; впроваджувалися податкові підвищення на тютюнові вироби. Головними інструментами ставали національні телебачення, радіо, інтернет-ресурси, зовнішня реклама, онлайн-ЗМІ. Важливим фактором була інтегрована багатоканальна медіа-кампанія з єдиним візуальним стилем і тоном повідомлення й регулярне оновлення контенту. Кампаній тривала роками, змінюючи месенджі й підходи, використовуючи вплив державних ЗМІ для легітимації й посилення впливу серед реципієнтів. У результаті з 2011 до 2020 року рівень куріння серед дорослих знизився з ~16% до менш ніж 11%. Австралія стала однією з перших країн, яка ввела "plain packaging" — пакування без бренду, лише попередження. Кампанія визнана ВООЗ прикладом найефективнішої державної антисигаретної комунікації.

Міжнародні стандарти та практики формування інформаційно безпечного середовища (практика НАТО, ЄС) базуються на досвіді ISO, НАТО та ЄС. Серія стандартів **ISO/IEC 27000,** створена Міжнародною організацією за стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC) забезпечує рамку для розробки, удосконалення, підтримки та впровадження системи управління інформаційною безпекою (ISMS). Основні стандарти серії включають [28]:

- ISO/IEC 27000 — Огляд і термінологія (містить базові терміни, визначення та концепції, використовується як вступ до серії);

- ISO/IEC 27001 — Основний стандарт ISMS (описує вимоги до впровадження ISMS; єдиний стандарт у серії, який підлягає сертифікації);
- ISO/IEC 27002 — Кодекс практик (містить практичні рекомендації для реалізації заходів безпеки, згаданих у ISO/IEC 27001);
- ISO/IEC 27005 — Управління ризиками інформаційної безпеки (методика оцінювання та обробки ризиків; підтримує ISO/IEC 27001 в частині оцінки загроз, вразливостей, ймовірності та наслідків).

НАТО визнає кіберпростір п’ятим доменом ведення бойових дій (поряд із сушею, морем, повітрям та космосом). З огляду на це, захист інформаційних систем та критичної інфраструктури є одним з основних елементів стратегічної оборони Альянсу. Саме тому НАТО впровадило ключові документи та політики, серед яких NATO Cyber Defence Policy, що підкреслює необхідність захисту інформаційно-комунікаційних систем Альянсу підвищення кіберстійкості членів Альянсу; швидке реагування на кіберінциденти; інтегрування кіберзасобів у військове планування [29].

Cyber Defence Pledge є добровільним зобов’язання країн-членів НАТО інвестувати у національну кібербезпеку, яке забезпечить розвиток національних стратегій, кібеспроможностей, професійної підготовки кадрів [30]. А в оновленій Strategic Concept 2022 кіберзагрози визнані однією з ключових проблем безпеки, що потребує тісної координації з ЄС, ООН, приватним сектором та партнерами [31].

Практична діяльність кіберзахисту НАТО впроваджує навчання, співпрацю та симуляції: Locked Shields [32] (щорічні наймасштабніші у світі кібернавчання з реагування на атаки), Cyber Coalition (навчання взаємодії союзників у кібероперацiях) [33], Cyber Rapid Reaction Teams (CRRTs) (мобільні експертні групи, які можуть бути направлені до країни-члена у разі масштабного кіберінциденту) [34].

НАТО тісно співпрацює з: Європейським Союзом (ENISA, CERT-EU); Приватним сектором (технологічні компанії, оператори інфраструктури); Партнерськими державами (зокрема Україною).

Європейський Союз, у свою чергу, розглядає кібербезпеку як невід'ємну складову цифрового суверенітету, економічної стабільності та безпеки громадян. Враховуючи зростання кіберзагроз (включаючи державне та хактивістське втручання), ЄС формує системний, багаторівневий підхід до кіберзахисту, основні принципи яких складає: колективна залученість країн-членів, захист критичної інфраструктури, надійність цифрового середовища.

У цьому контексті ухвалено стратегічні документи ЄС, зокрема EU Cybersecurity Strategy for the Digital Decade, яка передбачає створення єдиного цифрового ринку безпеки, підвищення кіберстійкість ключових секторів, посилення ролі Європейського агентства з кібербезпеки (ENISA), розвиток міжнародне співробітництво (з НАТО, ООН, країнами-партнерами) [35].

Інший ключовий документ — EU Security Union Strategy — охоплює боротьбу з гібридними загрозами, зокрема кібератаками, зосереджується на інформаційній боротьбі та захисті демократичних інституцій [36].

ЄС не поступається НАТО стосовно запровадженню практичних заходів та ініціатив — EU Cybersecurity Skills Academy [37] (програми для підготовки фахівців); кампанії для громадян щодо цифрової гігієни; EU Cybersecurity Act [38] (передбачає європейську систему сертифікації безпеки продуктів, послуг та процесів); EU Cybersecurity Atlas [39] (база даних інституцій, проєктів, дослідницьких груп); Joint Cyber Unit (ініціатива для спільного реагування на серйозні кібератаки).

Таким чином, сучасна стратегічна комунікація опирається як на інструменти впливу в межах держави, так і на стандартизовані міжнародні практики, що підсилюють інформаційну стійкість у глобальному вимірі.

РОЗДІЛ 2. СУЧАСНІ ВИКЛИКИ ТА ТЕНДЕНЦІЇ В СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Сучасні виклики та загрози для інформаційної безпеки держав

Сучасний розвиток цифрових технологій, глобалізація, диджиталізація, розширення глобальної інформаційної інфраструктури й зростаюче споживання інформаційного контенту створюють як нові можливості, так і серйозні ризики захисту інформації. В умовах гібридних війн, кіберзлочинності, інформаційного тероризму питання захисту інформаційного простору має ключовий характер національної безпеки держави. Даний розділ аналізує основні сучасні виклики та загрози, які постають перед державами у сфері інформаційної безпеки. Розглянуто розповсюджені форми інформаційного впливу, зокрема кібератаки, дезінформаційні кампанії, інформаційне шпигунство й інші різновиди дискредитації країн.

Кіберзлочинність, робота хакерських груп, використання шкідливих програм та поширення фішингових атак стають дедалі поширенішими. Дані проблеми пов’язані не лише зі збільшення обсягу даних в Інтернеті, а й з ускладненням атак спрямовані на державні установи та відомості, приватні компанії, критично важливу інфраструктуру. Країни стають потенційними об'єктами кібератак, спрямованих не тільки на нанесення економічного збитку, а й дестабілізації політичної ситуації [48].

Саме тому важливість ефективного захисту інформаційної безпеки значно зросла. Головна проблема захисту інформаційних ресурсів полягає у тому, що механізми захисту відстають від темпів розвитку загроз. Тому державам необхідно постійно впроваджувати нові стратегії, розвивати інноваційні технології та запобігати глобальним ризикам за допомогою міжнародного співробітництва.

Розвиток штучного інтелекту – одне з найважливіших досягнень сучасності, яке зачіпає всі сфери життя, зокрема й інформаційну безпеку. Штучний інтелект відкриває нові можливості для автоматизації процесів, обробки даних і створення передових систем кіберзахисту. У цей час, дана технологія може бути використана зловмисниками як потужний інструмент для проведення атак.

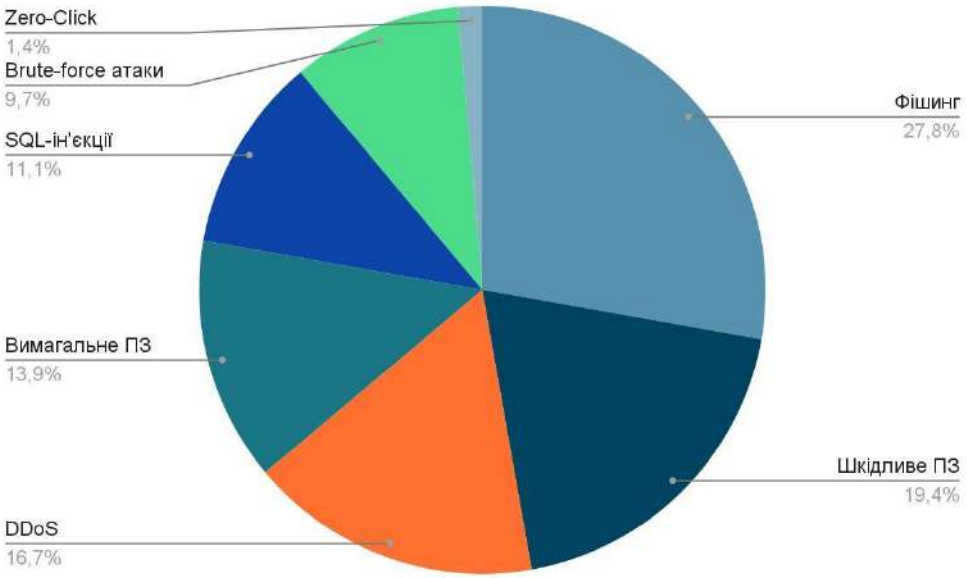

Рис. 2.1 Найпоширеніші типи кіберзагроз у цифровому середовищі
Джерело: https://www.bdo.ua/uk-ua/insights-2/information-materials/2023/top-10-cybersecurity-threats-to-businesses-in-2023 [47]

Особливу небезпеку становлять технології підроблення на основі штучного інтелекту, які використовуються для створення реалістичних підробок відео та аудіозаписів (DeepFake) з метою поширення дезінформації, маніпуляцій, управління громадською думкою та дискредитації політичних лідерів. Це підриває довіру до інформації і може мати серйозні наслідки [40, 49].

Deepfake — це технологія, що використовує методи штучного інтелекту, зокрема глибокого навчання (deep learning), для створення фальсифікованих відео-, аудіо- чи фотоматеріалів, які імітують реальних осіб з високим рівнем достовірності. Основою deepfake є генеративно-змагальні мережі (GAN), які

дозволяють синтезувати реалістичний контент шляхом навчання на великому обсязі даних.

У березні 2022 року, під час повномасштабної війни Росії проти України, у мережі з'явилося deepfake-відео із "зображенням" Володимира Зеленського, який закликає Збройні сили України скласти зброю та припинити опір. Відео було розміщено на зламаному новинному сайті та активно поширювалось через медіа. Насправді це було підроблене відео, створене за допомогою технологій глибокого навчання, і воно швидко було викрито як фейк [41].

Автоматизовані кіберзагрози на основі штучного інтелекту мають більш складний і масштабний характер. Наприклад, хакери можуть використовувати алгоритми машинного навчання для адаптації систем безпеки, виявлення їхніх вразливостей і створення шкідливого програмного забезпечення, що обминають традиційні методи захисту. Крім того, штучний інтелект може аналізувати поведінку користувачів і виявляти найбільш вразливі елементи системи, що дає змогу проводити цілеспрямовані атаки.

ШІ-модифіковане шкідливе програмне забезпечення — новий клас загроз, у якому зловмисне програмне забезпечення використовує штучний інтелект (ШІ) та алгоритми машинного навчання (ML) для підвищення своєї ефективності, адаптивності та здатності ухилятися від виявлення. Таке програмне забезпечення здатне самостійно аналізувати середовище, у якому воно функціонує, змінювати власну структуру та поведінку, ухилятися від захисних механізмів і вибирати найбільш вразливі точки атаки. Ключовий напрям застосування ШІ у шкідливому програмному забезпеченні є *еволюція поведінки*: за допомогою навчання на великій кількості спроб та помилок, такі системи здатні виявляти закономірності у діях антивірусного програмного забезпечення та обирати шляхи обходу захисту [42].

У 2020–2021 роках Японія стала однією з цілей глобальної хвилі кібератак, пов'язаних із розповсюдженням шкідливого програмного забезпечення Emotet, який активно використовував ШІ-механізми для адаптації фішингових повідомлень під певних отримувачів. За допомогою машинного навчання, вірус

аналізував вміст електронного листування та створював фальшиві повідомлення, максимально схожі на стиль спілкування реальних реципієнтів. Це значно підвищувало рівень успішності фішингу та проникнення до внутрішніх мереж. Emotet також виявляв вразливості в системах та здійснював автоматизоване розповсюдження всередині державних і корпоративних інфраструктур. Однією з цілей атаки стали урядові установи та муніципальні системи в Японії, що створило загрозу для критично важливої інфраструктури [43].

Сучасні технології дозволяють зловмисникам отримувати доступ до конфіденційних даних починаючи від фішингових атак і закінчуючи проникненням у захищені системи за допомогою складних кіберзасобів. Дана проблема особливо актуальна для державних установ, військових відомств і великих корпорацій, що працюють зі стратегічно важливою інформацією.

Частіше цифрове шпигунство здійснюється за допомогою шкідливого програмного забезпечення, яке таємно проникає в комп’ютерні системи і збирає дані (приклад Японії). Також поширені атаки на хмарні середовища, де зберігаються великі обсяги конфіденційної інформації. Уразливими залишаються і мобільні пристрої, що використовуються для передачі службових даних. Цифрове шпигунство – це не тільки проблема кібербезпеки, а й проблема національної безпеки, оскільки зловмисники часто діють за іноземного сприяння.

Викрадення конфіденційної інформації може мати катастрофічні наслідки. Це може призвести до витоку державних стратегій, зриву дипломатичних переговорів, економічних втрат або навіть ослаблення обороноздатності країни. Крім того, дані інциденти завдають непоправної шкоди репутації держави або організації, яка не забезпечила належний рівень захисту.

У 2020 році США зазнали однієї з найбільших кібершпигунських операцій в історії, коли хакери, пов’язані з Росією (група APT29 або "Cozy Bear"), зламали програмне забезпечення компанії SolarWinds. Шкідливий код був інтегрований у програму Orion, яку використовували понад 18 000 клієнтів, включно з низкою ключових американських державних установ:

Держдепартаментом, Міністерством фінансів, Міністерством енергетики та ін. Хакери отримали доступ до електронного листування, внутрішніх документів та конфіденційної інформації. Атака тривала понад 9 місяців до виявлення, і її масштаби викликали суттєве занепокоєння в уряді США щодо вразливості цифрової інфраструктури [44].

Щоб протистояти загрозі цифрового шпигунства, необхідно впроваджувати новітні технології шифрування даних, посилювати контроль доступу до інформації та регулярно проводити аудит з кібербезпеки. Також необхідно навчати співробітників, які працюють із конфіденційними даними, щоб мінімізувати людський фактор, який часто стає причиною успішних атак.

Ефективний захист конфіденційної інформації вимагає комплексного підходу, що включає як технічні рішення, так і політичні заходи на національному рівні.

Однією із серйозних загроз є DDoS-атаки, які перевантажують сервери і блокують доступ до важливих ресурсів. Такі атаки використовуються для шантажу, організаційної нестабільності та навіть соціальної паніки. DDoS-атаки особливо небезпечні для критично важливих об’єктів інфраструктури, таких як банківські системи, енергетичні мережі та урядові портали, і їхній успіх може мати далекосяжні наслідки [50].

У квітні–травні 2007 року Естонія стала об’єктом однієї з перших масштабних кібератак на рівні держави, що включала серію DDoS-атак на урядові вебсайти, банки, ЗМІ та телекомунікаційні структури, було порушено роботу цифрових каналів урядової комунікації. Атаки почалися після рішення уряду Естонії перенести пам’ятник радянському солдату з центру Таллінна, що викликало протест з боку Росії. Після цього урядові та комунікаційні системи країни зазнали цифрової атаки, що, за припущеннями, координувалася з території Росії [45].

Інформаційна війна має вплив на політичну стабільність, соціальну згуртованість і національну безпеку. Одним з основних інструментів такої війни є пропаганда, мета якої – створити фейкове уявлення про реальність,

маніпулювати суспільними настроями та формувати наратив на користь агресора. Фальшиві новини, що набули поширення в цифрову епоху, також є основою кіберзлочинності. Новинні агентства такого типу, часто видають себе за надійні джерела, але їхня мета – поширення дезінформації. Фальшиві новини можуть створюватися і поширюватися окремими особами, організованими групами або іноземними урядами. Маніпулювання громадською думкою – ще один аспект інформаційної війни, який має довгострокові наслідки. Використовуючи соціальні мережі та інші цифрові платформи, зловмисники створюють контент, спрямований на поляризацію суспільства, загострення конфліктів і підрив соціальної стабільності. Подібні маніпуляції включають у себе використання ботів, які надають видимість масової підтримки певної ідеології, і таргетовану рекламу, яка використовує емоційні тригери громадян [47, 51].

У середині XX століття уряд США здійснював системну діяльність з інформаційного впливу на масові медіа як усередині країни, так і за кордоном. Одним із найбільш відомих прикладів такої діяльності стала таємна операція

ЦРУ під кодовою назвою “Operation Mockingbird”, що тривала з кінця 1940-х до 1970-х років. Основною метою програми було використання засобів масової інформації для формування сприятливого міжнародного іміджу США та протидії радянській пропаганді в умовах Холодної війни. У межах цієї операції ЦРУ співпрацювало з американськими журналістами великих відомих видань, таких як: The New York Times, Time, Newsweek тощо, фінансуючи підконтрольні інформаційні джерела через підставні фонди. Також сприяли створенню публікацій, які відповідали зовнішньополітичним інтересам США й таким чином вплинули на редакційну політику ЗМІ як і у США, так і в інших країнах світу. Програма залишалась засекреченою до початку 1970-х років, коли її існування було розкрито під час розслідування Комісії Черча (U.S. Senate Select Committee to Study Governmental Operations, 1975). Комісія підтвердила, що десятки журналістів фактично діяли як агенти впливу, а також наголосила на

необхідності обмеження подібних форм державного контролю над інформаційним простором у демократичному суспільстві [46].

У сучасному цифровому середовищі інформаційна безпека стала критично важливою складовою національної безпеки. Швидкий розвиток технологій, поширення штучного інтелекту, зростання кіберзлочинності та інформаційних маніпуляцій формують нові типи загроз, на які держави повинні оперативно реагувати. До основних викликів належать кібератаки, фішингові кампанії, цифрове шпигунство, deepfake-технології та дезінформація, що використовуються як у міждержавній конкуренції, так і в умовах гібридної війни. Ці явища загрожують критичній інфраструктурі, підривають довіру до інформації, впливають на політичну стабільність і формують нову реальність інформаційного протистояння.

2.2 Тенденції у державних комунікаційних стратегіях

Комунікаційні стратегії державної влади розглядаються у контексті двох підходів: *практичного* (медіа- та PR-технологічного) і *теоретико-прикладного* (концептуального), які взаємодоповнюють один одного й акцентують увагу на різні аспекти даного поняття. Спираючись на перший підхід, комунікаційна стратегія розглядається як план соціальної діяльності представників державної влади (високопосадовці, топ-менеджери, співробітники відповідних підрозділів, найманих фахівців, інших спеціалістів органу державної влади), який спрямований на відносини і мотивацію до дії цільової аудиторії за допомогою визначених практик і етапів інформаційно-комунікаційної роботи. Дана робота представлена двома напрямками: *стратегічним*, що відповідає за планування комунікацій і реалізується структурними підрозділами зі зв'язків з громадськістю, комунікації, інформаційної політики тощо, незалежно від назви, і *тактичним*, що відповідає за щоденну систематичну роботу за двома

напрямками: 1) відстеження і аналізування громадської думки; 2) планова робота інформаційно-аналітичного й організаційного характеру [52].

Практичний підхід пов’язаний із медіа, які вживаються значною групою громадськості, що опосередковує зв’язок влади із максимально широкою аудиторією, відповідно вимагають регулярної та цілеспрямованої роботи. Саме тому державам важливо забезпечувати достатньо надійний рівень

інформаційної безпеки. Світові країни постійно розробляють та вдосконалюють комплексні стратегії інформаційної безпеки, у центрі яких - оперативні державні комунікації, кіберзахист, партнерство із приватними секторами та підвищення інформаційної обізнаності населення.

Досвід провідних країн таких як США, Тайвань, Естонія, ЄС, а також інші демократичні держави — демонструє найефективніші моделі реагування на інформаційні загрози. Порівняльний аналіз даних моделей дозволяє виявляти універсальні механізми, які мають бути адаптовані в українському контексті.

Цей досвід може бути релевантним для адаптації в національних стратегіях України з урахуванням локального контексту та інформаційної вразливості.

Для систематизації досвіду обрано чотири показові країни — США, Європейський Союз, Тайвань і Естонія, які мають інноваційний підхід до захисту інформаційного середовища. Їхній досвід порівнюється за такими критеріями:

– наявні інституції;
– ключові механізми протидії;
– інструменти, що застосовуються в комунікаційних стратегіях;
– законодавче забезпечення;
– освітній вектор;
– практичні приклади реалізації.

Наведені приклади ілюструють, як окремі держави трансформують свої стратегії, інституційні моделі та інструменти протидії дезінформації у практичні рішення. Ці кейси демонструють ефективність різних підходів, а також адаптивність держав до нових викликів у сфері інформаційної безпеки.

Таблиця 2.1

Порівняльний аналіз інституційних та практичних підходів до захисту інформаційного простору в США, ЄС, Тайвані та Естонії

	США	Тайвань	Естонія	ЄС
Інституції	Global Engagement Center (GEC); CISA (Cybersecurity and Infrastructure Security Agency)	Cofacts; Міністерство цифрових справ g0v-рух	NATO CCDCOE (Таллінн); Центр стратегічних комунікацій; RIKS; e-Estonia	East StratCom Task Force; Rapid Alert System; EDMO;
Основні механізми	Співпраця з BigTech; Підтримка фактчекінгу; Контрінформаці йні кампанії	Краудсорсинг фейків; Гумор як контрнаратив; Прозорість уряду	Протидія фейкам в режимі реального часу; Кіберзахист критичної інфраструктури; Розвинуті цифрові сервіси	EUvsDisinfo база фейків; Міждержавне попередження; Аналітика кампаній
Законодавчі ініціативи	Foreign Influence Transparency Act; Executive Order 13848	Рекомендації для платформ; Підтримка цифрових ініціатив	Cybersecurity Act; Державна стратегія кібербезпеки 2022–2027	Digital Services Act (2022); Audiovisual Media Services Directive
Освітній вектор	Тренінги з кібербезпеки; Програми цифрової грамотності	Інфобезпека в школах; Фактчекінг для молоді	Програми цифрової грамотності для школярів; Кіберосвіта для держслужбовців	Media Literacy for All; Освітні програми в школах і ВНЗ
Практики	PolitiFact; FactCheck.org; Централізоване реагування на фейки	Humor over; Rumor; Cofacts; Відкриті дані уряду	e-Estonia Showroom; Тренувальні симуляції атак; Кампанії з довіри до цифрового урядування	EUvsDisinfo.org; Співпраця з НГО та медіа
Інструменти	PolitiFact, FactCheck.org; Аналітичні панелі CISA	Платформи фактчекінгу; Системи оцінки достовірності	e-ID (електронна ідентифікація); KSI Blockchain; Система цифрових підписів	Rapid Alert Platform; Бази EDMO; Моніторинг EUvsDisinfo

Тайвань. Кейс "Humor over Rumor"

Одним із найуспішніших підходів до боротьби з дезінформацією в Тайвані стала кампанія Humor over Rumor. Її суть полягає у використанні гумористичних мемів як засобу знецінення та нейтралізації фейків [53]. Такий підхід дозволив ефективно протидіяти пропаганді, не вдаючись до прямих заборон чи цензури.

Серед основних інструментів цього підходу варто виділити платформу Cofacts, яка дозволяє будь-кому надіслати потенційний фейк і отримати перевірку. Ще одним дієвим механізмом є урядова політика оперативного спростування дезінформації: у режимі "24 години — 3 спростування" публікуються перевірені й чітко сформульовані розвінчання фейкових новин

Завдяки поєднанню швидкої реакції, прозорості та залучення громадян, Тайваню вдалося не лише знизити ефективність ворожих інформаційних впливів, а й досягти високого рівня довіри громадськості до фактчекінгових ініціатив.

США. Вибори 2020 року

Під час президентських виборі 2020 року [54], Сполучені Штати активізували боротьбу з дезінформацією шляхом співпрацею зі технологічними гігантами.

Центр GEC (Global Engagement Center) виявляв зовнішні впливи, тоді як CISA проводила кампанію "Rumor Control", спрямовану на розкриття фейків. Незважаючи на масштабну інформаційну кампанію з боку Росії та інших учасників, США успішно зменшили вплив штучно створених наративів і зберегли довіру до виборчого процесу.

ЄС. Кейс "EUvsDisinfo"

У межах боротьби з дезінформацією в Європейському Союзі особливу роль відігравала ініціатива East StratCom Task Force [55], яка створювала найбільшу європейську базу кремлівських фейків. Серед основних інструментів

— Rapid Alert System, що забезпечує оперативне інформування країн-членів ЄС, а також платформа EUvsDisinfo.org, яка містить аналітичні матеріали, приклади дезінформаційних кампаній і глибокий аналіз їх впливу.

Результатом діяльності програми стало підвищення рівня медіаграмотності серед громадян, посилення міжурядової координації та зниження ефективності російських інформаційних атак.

Естонія. Кейс "Протидія проросійській пропаганді"

У відповідь на гібридні загрози з боку Росії Естонія вжила рішучі заходи для захисту інформаційного простору. Зокрема, було закрито десятки проросійських медіа-ресурсів і обмежено їхнє мовлення. Ключову роль у зміцненні внутрішньої цифрової безпеки відіграла система e-Estonia, яка базується на високому рівні довіри до електронного врядування. Важливим елементом також стала постійна співпраця з Центром передового досвіду НАТО з питань кібероборони (CCDCOE). Завдяки цим крокам Естонії вдалося забезпечити високий рівень кіберзахисту, підвищити стійкість суспільства до дезінформації та суттєво зменшити вплив кремлівських інформаційних кампаній.

Також слід розглянути та детальніше проаналізувати саме законодавчі ініціативи, які мають провідну дію у сфері кібербезпеки та протидії дезінформації.

У цьому контексті приклади **США** демонструють цілісний підхід, що поєднує вимоги до прозорості інформаційного простору з санкційними механізмами у випадку втручання у виборчі процеси.

У Сполучених Штатах одним із ключових законодавчих інструментів, спрямованих на протидію інформаційним загрозам, є *Foreign Influence Transparency Act (FITA).* Ця ініціатива має на меті посилити прозорість зовнішнього впливу на політичні процеси в США та виявляти й оприлюднювати спроби іноземних держав впливати на американське суспільство через ЗМІ, цифрові платформи та лобістів. FITA сприяє позначенню джерел пропаганди в

соціальних мережах; зменшує анонімність ворожих інформаційних операцій; підвищує рівень прозорості політичної реклами та контенту в інтернеті.

Законопроєкт передбачає обов'язкову реєстрацію іноземних агентів, зокрема цифрових медіа, які фінансуються іноземними урядами (переважно РФ, КНР тощо). Крім того, він розширює дію Закону про реєстрацію іноземних агентів (FARA) на цифрові платформи; забезпечує громадський доступ до інформації про джерела іноземного впливу.

Доповненням цього закону є *Executive Order 13848: "Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election" (2018)* — указ Президента США Дональда Трамп, підписаний 12 вересня 2018 р. Документ створює правову базу для санкційного реагування на втручання з боку іноземних держав у виборчий процес.

Значення цього указу в сфері кібербезпеки полягає у створенні стримувального механізму: держави-зловмисники знають, що втручання тягне юридичні наслідки. Він узаконює швидке реагування на кампанії дезінформації (особливо у виборчий період), а також підвищує роль розвідки у виявленні інформаційних атак.

Таблиця 2.2

Порівняльна характеристика законодавчих ініціатив США — FITA та Executive Order 13848

	FITA	Executive Order 13848
Фокус	Прозорість зовнішнього впливу на суспільство	Санкції за втручання у вибори
Правовий статус	Законопроєкт	Указ президента
Механізми	Реєстрація, оприлюднення, публічні бази	Розвіддані, оцінка втручання, санкції
Цільові актори	Іноземні медіа та агенти	Іноземні уряди, приватні компанії, фізособи
Цінність для боротьби з дезінформацією	Зменшення прихованого впливу	Стримування та покарання втручання

Указ забезпечує обов'язкову оцінку спецслужбами будь-якого втручання в федеральні вибори; дає президенту право запроваджувати санкції проти осіб, компаній або урядів, залучених до дезінформаційних кампаній або кібератак; включає внутрішній механізм моніторингу (через ODNI, DHS, DoJ та інші).

У **Тайвані** ключову роль у протидії дезінформації та зовнішньому впливу відіграє модель добровільного саморегулювання цифрових платформ, відома як Taiwan Platform Governance Model. Її суть полягає у формування партнерських відносин між державою та технологічними компаніями — такими як Meta, LINE, YouTube — без запровадження примусового регулювання або обмеження свободи слова. Мета моделі полягає у протидії зовнішньому впливу (зокрема — Китаю) через координацію дій із соціальними мережами; створення структури «спільного управління платформами», яка не обмежує свободу слова, але зменшує ефективність дезінформаційних атак.

Уряд не видає наказів, а натомість співпрацює з платформами (Meta, LINE, YouTube) шляхом "спільного узгодження правил"; розробка єдиних стандартів швидкого реагування на кризову дезінформацію; прозорі комунікаційні протоколи між урядом та платформами. Одним із яскравих прикладів ефективності цієї моделі стала практика під час пандемії COVID-19, коли неправдиві повідомлення спростовувалися упродовж двох годин. У цьому процесі активно використовувався ресурс Taiwan FactCheck Center, що забезпечував платформам достовірний верифікований контент для маркування повідомлень. Таким чином, було реалізовано модель швидкої, прозорої та ефективної реакції без втручання в свободу слова.

Доповненням до платформи саморегулювання стала масштабна підтримка цифрових громадських ініціатив у рамках підходу *підтримки цифрових ініціатив (Civil Tech та громадське залучення).* Цей напрям передбачає залучення громадян до процесу цифрової демократії та інформаційної безпеки. Одним із найвідоміших прикладів є рух g0v (gov-zero) — громадська платформа хактивістів, яка створює альтернативні урядові сервіси з відкритим кодом. Cofacts — чат-бот на платформі LINE, який дозволяє користувачам надсилати

повідомлення для перевірки. Команда волонтерів надає фактчек-аналіз. Taiwan FactCheck Center — незалежна ініціатива, яка співпрацює з урядом і отримує підтримку на розвиток цифрових інструментів верифікації.

Інституційним центром підтримки таких ініціатив стало створене у 2022 році Міністерство цифрових справ (MODA), відповідальне за стратегічну підтримку civic tech, кіберзахист та цифрову інклюзію.

У сукупності ці інструменти створюють стійку, адаптивну модель цифрової демократії, де боротьба з дезінформацією базується не лише на державному втручанні, а й на активній участі суспільства та високому рівні цифрової культури. Такий підхід суттєво знижує ефективність інформаційних атак і зміцнює довіру громадськості до джерел інформації.

Таблиця 2.3

Порівняльна характеристика законодавчих ініціатив Тайваню — Taiwan Platform Governance Model та Civil Tech

	Рекомендації для платформ	Підтримка цифрових платформ
Тип ініціативи	Добровільне саморегулювання через співпрацю	Інституційна підтримка civic tech та фактчекінгу
Механізми	Швидка комунікація з платформами, узгоджені протоколи	Гранти, партнерства, волонтерські сервіси
Інституції	Facebook, LINE, YouTube, Google	g0v, Cofacts, FactCheck Center
Роль держави	Посередник і координатор, не цензор	Каталізатор громадських цифрових рішень
Цінність для боротьби з кіберзагрозами	Прозоре управління платформами	Високий рівень залучення громадян, цифрова грамотність

Естонія, одна з провідних країн у сфері цифрового врядування, демонструє системний підхід до побудови національної кібербезпеки, який базується на поєднанні європейського законодавства, технологічної інфраструктури та стратегічного планування. Центральним елементом законодавчого регулювання в цій сфері став *Cybersecurity Act*, що слугує

правовою рамкою для захисту критичних інформаційних систем як державного, так і приватного секторів.

Закон є адаптацією європейської Директиви NIS (Network and Information Security) до естонського контексту і запроваджує чіткі стандарти безпеки IT-систем для органів влади, телекомунікаційних операторів, банків і медичних установ. Значну роль у реалізації закону відіграє Естонське інформаційне агентство (RIA), якому надано повноваження моніторингу та контролю дотримання вимог; визначення "основних постачальників послуг" (оператори зв'язку, банки, охорона здоров'я).

Іншим важливим елементом національної цифрової політики Естонії стала *Державна стратегія кібербезпеки 2022–2027*. Вона спрямована на адаптацію до нових типів гібридних загроз, зокрема з боку Росії; забезпечення стійкості кіберпростору та захисту демократичних процесів. В Стратегії визнано роль інформаційної безпеки як елементу нацбезпеки, а крім того вона враховує гібридний характер загроз: технічний, інформаційний, когнітивний.

Ключовими векторами реалізації стратегії є міжнародна співпраця — насамперед — з НАТО, ЄС, CCDCOE (Cooperative Cyber Defence Centre of Excellence), який базується в Таллінні — а також розвиток національної спроможності до виявлення та нейтралізації кіберінцидентів.

Таблиця 2.4

Порівняльна характеристика законодавчих ініціатив Естонії — Cybersecurity Act та Стратегія кібербезпеки 2022–2027

	Cybersecurity Act	Стратегія кібербезпеки 2022–2027
Фокус	Технічна безпека та обов'язки провайдерів	Широкий спектр — від технічної до інформаційної безпеки
Міжнародна співпраця	У межах NIS, ЄС	НАТО, CCDCOE, країни Балтії
Механізми	Регулювання, обов'язкове повідомлення про інциденти	Навчання, стратегічна комунікація, кібернавчання
Ключові інституції	RIA (Information System Authority)	RIA, STRATCOM, CERT-EE, Міністерство оборони

Цінність для боротьби з дезінформацією	Опосередкована: створює надійну інфраструктуру для захисту каналів комунікації	Пряма: передбачає стратегічну комунікацію, протидію фейкам

Європейський Союз у своїй нормативній політиці приділяє особливу увагу регулюванню цифрового середовища, формуючи системні механізми відповідальності онлайн-платформ за поширення дезінформації, мови ворожнечі та шкідливого контенту. Ключовим інструментом у цій сфері є Регламент про цифрові послуги *Digital Services Act* (2022). Він створює юридичний механізм відповідальності платформ за поширення фейків; сприяє координації зусиль між державами-членами; посилює довіру до цифрового простору та медіаграмотність користувачів. Серед його ключових положень —встановлення зобов'язань для Very Large Online Platforms (VLOPs) (>45 млн користувачів у ЄС): Google, Facebook, X, TikTok тощо; алгоритмічна прозорість: звітність про системи рекомендацій; заборона таргетингу реклами для неповнолітніх; запровадження незалежного аудиту платформ.

Ще одним важливим нормативним документом у сфері медіа є Директива про аудіовізуальні медіапослуги Audiovisual Media Services Directive, що забезпечує уніфікацію стандартів для всіх аудіовізуальних медіа у ЄС: ТБ, VoD, стримінг-сервіси, YouTube, соцмережі. Ця директива визнає відеоплатформи повноцінними медіапровайдерами, покладаючи на них обов'язки зі збалансованого інформування, прозорості власності, захисту неповнолітніх та протидії дезінформації.

Таблиця 2.5

Порівняльна характеристика законодавчих ініціатив ЄС — Digital Services Act та Audiovisual Media Services Directive

	Digital Services Act (2022)	Audiovisual Media Services Directive
Ціль	Безпечний цифровий простір, протидія дезінформації	Прозорість медіа, захист глядачів, відповідальність контенту
Фокус	Онлайн-платформи, соцмережі, маркетплейси	Аудіовізуальні медіа, стримінг, онлайн-відеоплатформи

Механізми	Зобов'язання VLOPs, аудит, прозорість алгоритмів	Контроль над відеоплатформами, вимоги до контенту
Національні регулятори	Взаємодія з Digital Services Coordinators	Підпорядковані незалежним органам медіарегулювання
Цінність для боротьби з дезінформацією	Висока — систематизує контроль за онлайн-дезінформацією	Середня — зосереджена переважно на контенті та мовленні у відео

Зокрема, директива зобов'язує платформи забезпечувати наявність принаймні 30% європейського контенту на платформах; захист неповнолітніх від шкідливого контенту; обов'язок запобігати поширенню мови ворожнечі, тероризму, дезінформації.

У сукупності ці два документи формують правову основу для боротьби з інформаційними загрозами в ЄС, зміцнюючи довіру до цифрового простору та підтримуючи демократичну інформаційну екосистему.

Виходячи із порівняльних характеристик маємо загальну порівняльну таблицю комунікаційних стратегій (реагування та превенція) (Табл. 2.6)

Порівняння державних комунікаційних стратегій провідних країн і регіонів — США, Тайваню, Естонії та Європейського Союзу — дозволяє виявити відмінності у підходах до реагування на дезінформаційні кампанії та запобігання гібридним загрозам.

Таблиця 2.6

Загальне порівняння комунікаційних стратегій країн США, ЄС, Естонії та Тайваню

Країна / регіон	Механізми реагування	Превентивні заходи
США	Центр стратегічних комунікацій (GEC) при Держдепі; "Executive Order 13848" — санкції за іноземне втручання;	Освітні кампанії з цифрової грамотності; Партнерства з платформами (Facebook, Google); Ініціатива Foreign Influence Transparency Act

	Робочі групи в DHS і NSA з виявлення фейків у режимі реального часу	
Тайвань	Тайванський Центр фактчекінгу; Платформа MyGoPen та співпраця з LINE; Стратегічні онлайн-кампанії у кризові періоди (наприклад, вибори, пандемія)	Медіаграмотність у школах; Публічна база дезінформації (реєстр фейків); ІТ-волонтерські мережі для протидії фейкам
Естонія	STRATCOM — підрозділ з протидії інформаційним операціям; CERT-EE реагує на кіберзагрози з інформаційною складовою; Міжвідомча координація через RIA	Нац. стратегія кібербезпеки включає комунікаційну безпеку; Підготовка державних спікерів; Інтеграція медіаграмотності у формальну освіту
ЄС	Система Rapid Alert System (RAS) для обміну між країнами; Центр з дезінформації при EEAS (East StratCom Task Force); Зобов’язання платформ у межах DSA	Кодекс практик проти дезінформації; Digital Services Act (2022) — зобов'язання VLOPs; Інвестиції в дослідження та фактчекінг (EDMO)

США застосовують централізовану, безпекову модель, у якій ключову роль відіграють державні інституції — Державний департамент, Міністерство внутрішньої безпеки, розвідка та спеціальні уповноважені органи. Особливу увагу приділено іноземному втручанню у вибори, а також санкційним механізмам як інструменту стримування. У цьому контексті США демонструють модель, де зовнішньополітична комунікація перетинається з питаннями національної безпеки, а співпраця з цифровими платформами є важливою, але все ще переважно добровільною.

Тайвань, навпаки, виступає прикладом інноваційного, гнучкого та високотехнологічного підходу, орієнтованого на широку участь громадськості. Тут дезінформація розглядається не лише як загроза безпеці, а як проблема

суспільної довіри та комунікативної гігієни. Тайвань активно залучає ІТ-волонтерів, фактчекерські платформи, цифрові інструменти на базі месенджерів, а також інтегрує медіаграмотність у формальну освіту. Цей приклад свідчить про ефективність децентралізованих горизонтальних моделей, в яких громадяни — не лише об’єкти, а й суб’єкти комунікаційної безпеки.

Естонія — держава з провідним досвідом цифрової трансформації — інтегрувала комунікаційний компонент у загальну систему кібербезпеки. Механізми реагування спираються на спеціалізовані підрозділи (наприклад, STRATCOM та CERT-EE), а превенція включає стратегічну підготовку державних комунікаторів, підвищення цифрової обізнаності громадян і міжвідомчу взаємодію. Таким чином, Естонія пропонує гібридну модель, що поєднує жорстку інституційну дисципліну з довірою до цифрової освіти населення.

Європейський Союз репрезентує нормативно-координований підхід, де основний акцент робиться на регулюванні поведінки платформ, встановленні спільних стандартів (через Digital Services Act, AVMSD), а також підтримці національних і транскордонних ініціатив через програми EDMO та Rapid Alert System. Унікальність ЄС полягає в його мультиакторній природі — комунікаційна безпека розглядається не як виняткова компетенція держав, а як кооперація між урядами, платформами, громадськими організаціями та незалежними медіа.

РОЗДІЛ 3 ВИКОРИСТАННЯ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

3.1 Приклади державних комунікаційних кампаній щодо протидії дезінформації

Сучасні комунікаційні стратегії нерозривно пов'язані із цифровими технологіями. Що пояснює активне користування ШІ для аналізу даних, автоматизації задач та перехід на інтерактивні платформи, як то соціальні медіа, які стали вагомим та впливовим інструментом у комунікаційних стратегіях.

Виходячи із Розділу 2, такого типу ініціативи постійно піддаються масованим кібератакам задля дисфункції країн, підриву довіри до організацій / політичних лідерів / урядових програм і так далі. Саме тому країни ЄС почали активно формувати механізми для протидії викликам з боку кібертерористів.

Провідну роль у цьому напрямі стали спеціалізовані структури, які здатні реагувати на інформаційні загрози й посилювати стійкість до маніпуляцій у публічному просторі. Такі ініціативи повинні не лише реагувати на кібератаки, спрямовані на дезінформацію, але й активно працювати над формуванням стратегічних комунікаційних підходів, що є важливим для зміцнення довіри до урядових органів та політичних лідерів.

У цьому контексті важливу роль відіграє *East StartCom Task Force* — ініціатива Європейської служби зовнішніх справ, яка спрямована на боротьбу з дезінформацією та посилення стратегічних комунікацій у східних регіонах (Рис.

Мета дослідження East StartCom Task Force — виявити особливості функціонування ЄС в епоху постправди та проаналізувати діяльність ініціативи.

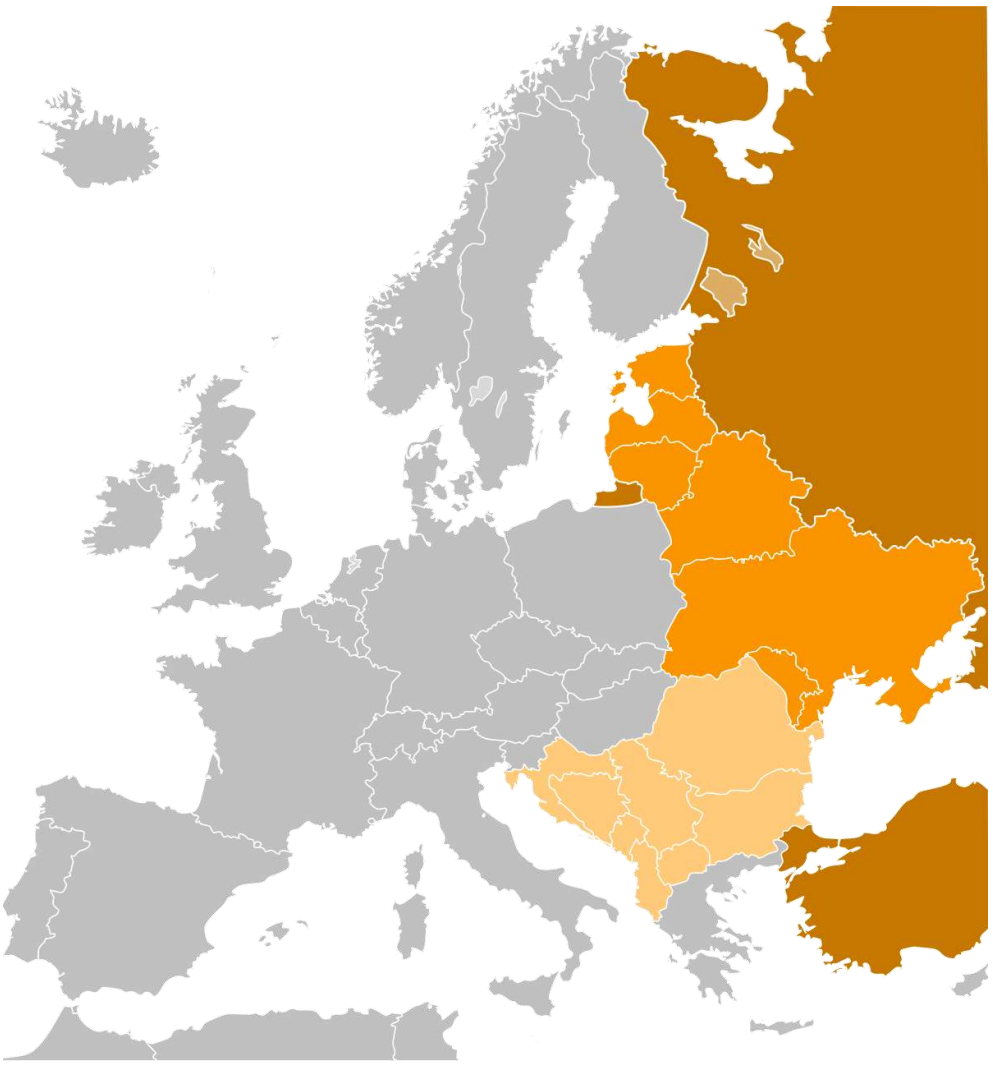

Рис. 3.1 Східні країни Європи, на які поширюється дія ініціативи East StartCom Task Force

East StratCom Task Force була створена у 2015 році за рішенням Європейської служби зовнішніх дій (European External Action Service, EEAS) [56] у відповідь на зростання інформаційних загроз з боку зовнішніх акторів, насамперед Російської Федерації. Її створення стало реакцією на анексію Криму та події на сході України, коли стало очевидним, що інформаційна війна стала невід'ємною складовою гібридної агресії. Й тому постало питання дослідження феномену постправди та пошуку методів боротьби з дезінформацією.

Згідно зі сайтом East StratCom Task Force, її завдання має на меті роз'яснення ключових аспектів політики ЄС, протидія дезінформації.

Організація відповідальна за збір та поширення прикладів дезінформаційних атак Росії на їхньому вебсайті, редагування офіційного російськомовного сайту Європейської служби зовнішньополітичної діяльності ЄС. Група розробляє комунікаційні продукти та кампанії, орієнтовані на краще пояснення політики ЄС у країнах Східного партнерства. Ця організація тісно співпрацює з інституціями ЄС та делегаціями ЄС у країнах Східного партнерства.

За допомогою аналізу даних і моніторингу медіа 15-ма різними мовами EUvsDisinfo виявляє, аналізує та викриває випадки дезінформації, що походять із прокремлівських медіа, які поширюються в ЄС і країнах Східного партнерства.

Станом на 2019 рік моніторингові можливості дали змогу виявляти дезінформацію, поширену на Західних Балканах і в країнах, що межують із ЄС на півдні. Усі випадки зібрані в базі даних EUvsDisinfo — єдиному відкритому сховищі з можливістю пошуку, яке наразі містить понад 17 000 прикладів прокремлівської дезінформації.

Крім того, ведення бази даних, регулярно публікуються статті й аналітичні матеріали про новітні тенденції в методах і практиці дезінформації, а також узагальнюються міжнародні дослідження, які роблять інноваційний внесок у цю галузь.

East StratCom Task Force також активну працює з громадськістю й урядами. Проводяться брифінги й тренінги для інституцій ЄС, урядів країн-членів, журналістів та організацій громадянського суспільства, а також регулярно виступаємо на міжнародних конференціях. Як запевняє East StratCom Task Force — результати роботи є важливим ресурсом для політичних лідерів, державних установ, дослідників, аналітичних центрів і журналістів у всьому світі [57].

Мета створення даної ініціативи:

- протидія дезінформації, спрямованій проти ЄС, політик, цінностей та держав-членів;
- посилення стійкості до інформаційних загроз як в межах ЄС, так і за його межами;

- підтримка країн Східного партнерства (Грузія, Україна, Вірменія, Азербайджан, Молдова, Білорусь).

Основними інституціями East StratCom Task Force, які пов'язані із протидією дезінформації (у більшості в онлайн-просторі), є Єврокомісія (зокрема, Експертна група високого рівня, HLEG; Експертна група з медіаграмотності, EU Expert Group on Media Literacy); Європарламент (зокрема, політико-адміністративний орган The Panel for the Future of Science and Technology (STOA), European Ideas Network); Оперативна робоча група зі стратегічних комунікацій (East StratCom Task Force) [58].

East StratCom активно співпрацює з журналістами, редакціями ЗМІ, фактчекерами, громадянськими організаціями та урядами країн ЄС і Східного партнерства. Формати взаємодії включають: проведення спеціалізованих тренінгів з медіаграмотності; надання експертних коментарів для ЗМІ; участь у міжнародних конференціях та форумах; публічне роз'яснення політики ЄС через інтерв'ю, статті, онлайн-дискусії.

Таблиця 3.1

Загальний опис ініціативи East StratCom Task Force

East StratCom Task Force	
Мета	Протидія дезінформації проти ЄС, його політик, цінностей, держав-членів; Посилення стійкості до інформаційних загроз в ЄС і за його межами; Підтримка країн Східного партнерства (Грузія, Україна, Вірменія, Азербайджан, Молдова, Білорусь).
Завдання	Виявлення, моніторинг і викриття дезінформаційних кампаній (особливо прокремлівських); Розробка комунікаційних продуктів, роз'яснювальних матеріалів. Підготовка публікацій, оглядів, баз даних EUvsDisinfo; Проведення тренінгів, брифінгів для урядів, медіа, громадянського суспільства; Сприяння розумінню політики ЄС.
Ключові напрямки	Моніторинг медіа 15 мовами та виявлення дезінформації; Ведення відкритої бази даних EUvsDisinfo (17 000+ кейсів); Публікація аналітики, статей, оглядів трендів дезінформації;

	Освітня робота: тренінги для журналістів, урядів, громадян; Співпраця з країнами Східного партнерства.
Інституції	Європейська Комісія: • Експертна група високого рівня (HLEG); • Експертна група з медіаграмотності (EU Expert Group on Media Literacy); Європейський парламент: • The Panel for the Future of Science and Technology (STOA); • European Ideas Network.
Взаємодія з медіа	Поширення контенту через сайт EUvsDisinfo.eu; Інформаційні бюлетені (Disinfo Review), аналітичні матеріали, пресрелізи; Брифінги, тренінги, міжнародні конференції для журналістів; Співпраця з редакціями, ЗМІ, фактчекерами; Публічне роз'яснення політики ЄС у регіоні.

East StratCom Task Force успішно використовують рушійні формати комунікації, які використовуються в інформаційних бюлетенях, на онлайн-платформах й також у інформаційних прес-релізах.

Інформаційні бюлетені (Disinfo Review)

Щотижневі аналітичні огляди, що узагальнюють виявлені приклади дезінформації та основні тенденції поширення. Вони містять короткі анотації приклади дезінформації та посилання на повні кейси у базі.

Прикладом використання є щотижневі випуски Disinfo Review [59], розсилки для урядів, медіа, експертів. Одним із випусків є "Кремль переписує історію об'єднання Німеччини" [61] від 15 листопада 2024 року, який є зразком аналітичного дослідження дезінформаційних наративів, спрямованих на маніпуляцію історичними подіями з метою впливу на сучасну політичну свідомість. Дану статтю можна прослухати також в аудіо форматі.

Стаття демонструє використання різних ключових дезінформаційних тактик. Одна із яких є *зміна історичних подій* — порівняння об'єднання Німеччини з анексією Австрії створює хибні уявлення, що викривляють історичну правду. *Дискредитація демократичних інституцій* — критика політики мультикультуралізму та партії "зелених" спрямована на підрив довіри до демократичних процесів у Німеччині, як ще приклад дезінформаційної

стратегії. *Політична інструменталізація пам'яті* — використання пам'яті про Kristallnacht для критики сучасної політики Німеччини щодо Ізраїлю є прикладом маніпуляції історії з політичними цілями.

Основні тези статті:

- *Маніпуляція історичними датами*: у статті аналізується, як прокремлівські медіа, зокрема RT Deutsch, використовують символічні дати, такі як 3 жовтня (День об'єднання Німеччини) та 9 листопада (річниця падіння Берлінського муру та Kristallnacht), для створення альтернативних історичних наративів.
- *Інтерпретація Kristallnacht*: RT Deutsch стверджує, що сучасна Німеччина використовує пам'ять про Kristallnacht як виправдання для підтримки Ізраїлю, зокрема після нападу ХАМАС у жовтні 2023 року.
- *Переосмислення об'єднання Німеччини*: RT Deutsch називає об'єднання Німеччини «аншлюсом» (Anschluss), що є терміном, який зазвичай використовується для опису анексії Австрії нацистською Німеччиною у

1938 році, тим самим намагаючись делегітимізувати процес об'єднання.

- *Критика політики мультикультуралізму*: у статті RT Deutsch підкреслюється, нібито, зміна позиції партії «Зелених» щодо імміграції та ісламу, що, за словами авторів, свідчить про кризу мультикультуралізму в Німеччині.

Онлайн-платформи

Інтерактивні ресурси для пошуку інформації та матеріалів, тобто застосовуються сайт EUvsDisinfo.eu, база даних дезінформації із 19000 кейсів (EUvsDisinfo) [62], статті, аналітика.

EUvsDisinfo — флагмантська онлайн-платформа, створена

Європейською службою зовнішніх дій (EEAS), яка є головним інструментом ЄС для моніторингу, збору, аналізу й публічного оприлюднення дезінформації, що виходять, переважно, із прокремлівських медіа. Платформа поєднує у собі декілька функціоналів, що робить її універсальним ресурсом для урядів, медіа, громадянського суспільства. Кожен кейс у базі містить деталізований аналіз: джерела походження інформації, країною поширення,

датою публікацією, коротким описом кейсу та пояснення, чому цей матеріал є дезінформацією.

Завдяки інтегрованим фільтрам користувачі можуть здійснювати пошук через ключові слова, країни, теми, дати, що робить EUvsDisinfo зручною для користуванням журналістами, науковцями, громадянами та урядовими структурами.

EUvsDisinfo надає корисні ресурси журналістам, дослідникам, студентам і так далі, щодо пошуку та виявлення дезінформації. Також надається мультимедійний контент: відео, інфографіки та візуальні пояснення стосовно механізмів функціонування дезінформаційних кампаній. Через це, її матеріали регулярно цитуються у звітах міжнародних організацій, використовуються під час підготовки до публічних виступів, тренінгів та курсів з медіаграмотності.

Наприклад, у звіті Європейської Ради зазначено, що “East StratCom Task Force — покладається на волонтерів, які спеціалізуються на зборі дезінформаційних повідомлень, але людських ресурсів суттєво не вистачає. У звіті Атлантичної ради, підготованому в березні 2018 року, рекомендовано, щоб ЄС вимагав від усіх держав-членів відряджати національного експерта для посилення роботи цієї оперативної групи”.

Офіційні пресрелізи

Оперативна реакція на актуальні події, формування позиції ЄС. Пресрелізи EEAS [60] висвітлюють конкретні інформаційні атаки або міжнародні кризи й є важливим інструментом комунікації ЄС у сфері зовнішньої політики. Вони публікуються на офіційному сайті EEAS, як протидія ключовим загрозам міжнародного кіберпростору: військові конфлікти, кібератаки, інформаційні кампанії, що спрямовані проти ЄС та його партнерів або важливі політичні рішення ЄС. Мета та функції пресрелізів:

- насамперед публічна демонстрація стійкості та єдності ЄС;
- формування єдиної позиції ЄС у відповідь на інформаційні загрози;
- інформаційне забезпечення партнерських країн, зокрема, країн Східного регіону (рис. 3.1);

- сприяння прозорості діяльності ЄС для громадськості та медіа.

Стиль письма пресрелізів офіційно-діловий, без емоційного забарвлення, усі месенджі чітко спрямовані на передачу головних тем. Також часто використовуються донесення такі, як: “ЄС закликає”, “засуджує”, “вимагає”, “підтримує”, що підкреслює нормативно-політичний характер комунікації.

Головна аудиторія — це представники урядів, журналісти, експерти та дослідники, медіа, що висвітлюють ЄС й громадяни країн-членів ЄС та партнерських держав.

Головна тематика пресрелізів — засудження дезінформації, яка поширюється Кремлем, у контексті вторгнення в Україну, рекомендації щодо посилення стійкості до кібератак, підтримка України у боротьбі із гібридною агресією.

Ці формати комунікації дозволяють East StratCom Task Force ефективно виявляти, аналізувати та протидіяти дезінформаційним кампаніям, забезпечуючи прозорість та інформування громадськості та зацікавлених сторін.

Одна із найрезонансніша історія успішної роботи ініціативи East StratCom Task Force став аналіз масштабної кампанії під назвою “Doppelganger” [64]. Дана кампанія почалася у 2022 році, була організована російською IT компанією Social Design Agency й мала на меті підрив підтримки України в Європі та світі шляхом поширення фейкових новин. Особливість цієї кампанії полягала в тому, що зловмисники створювали професійно виконані копії сайтів відомих медіа таких, як Der Spiegel, Fox News, The Washington Post, The Guardian, Bild та інших. Візуальні сторінки сайтів нічим не відрізнялись від оригіналів: мали той самий логотип, кольори оформлення, шрифти, стиль письма, стиль верстки та доменні імена, що співпадають зі справжніми (наприклад, використовувались кириличні літери, які заміняли латинські).

Фейкові сайти публікували статті, які виглядали як справжні журналістські розслідування або новинні матеріали, але містили дезінформаційну сфальсифіковану інформацію, спрямовану на дескридитацію України, США, ЄС, НАТО та іншої східної спільноти. Основні наративи “стверджували”, що Україна

є “невдячною” державою, європейці “втомились” від підтримки України, санкції проти Росії завдаються шкоди усьому світу, українські військові “здійснюють” воєнні злочини проти громадського населення.

Дана кампанія була детально спланована: для поширення фейкових статей активно використовувались соціальні мережі, боти, а також розсилки спаму. Більшість матеріалів набирали тисячі переглядів, створюючи ілюзію підтримки кремлівських наративів.

East StratCom Task Force разом із EU DisinfoLab, Bellingcat, BBC Verify, а також національними урядами країн-членів ЄС, почали масштабне розслідування, що дозволило ідентифікувати мережу пов’язаних сайтів та акаунтів у соцмережах, зібрати технічні докази (метадані сторінок, IP-адреси, сервери) та простежити зв’язок із російськими угрупуванням.

У звіті EUvsDisinfo детально описали механізми роботи «Doppelganger», особливості створення фейкових сайтів, а також способи виявлення таких маніпуляцій. Цей кейс став прикладом того, як скоординовані зусилля міжурядових структур, медіа та громадських організацій можуть ефективно протидіяти дезінформаційним атакам.

Викриття «Doppelganger» отримало резонанс у міжнародних медіа. Про нього писали The Guardian, BBC, Politico, Le Monde, Deutsche Welle. Офіційні представники ЄС неодноразово згадували цей кейс у своїх пресрелізах як приклад результативної роботи системи стратегічних комунікацій. Наприклад, у заяві речника EEAS [65] зазначалося:

«Doppelganger — це яскравий приклад того, як Кремль намагається маніпулювати громадською думкою в Європі, і як важливо вчасно викривати та нейтралізувати такі загрози».

США часто стає об'єктом вразливості кібератакам через чисельну кількість інформаційних систем й значення у світовій економіці. Число кібератак може коливатись від невеликих інцидентів до значних інформаційних нападів. Атаки є постійною загрозою через важливість кібербезпеки у всіх сферах, включаючи урядові структури, приватні компанії, критичну інфраструктуру.

Відповіддю США на ці виклики стало створення Global Engagement Center (GEC) — структурного підрозділу Державного департаменту, який з 2016 року виконував функції координації та реалізації стратегічних комунікацій для протидії іноземній дезінформації та пропаганді [66].

Важливим ключовим напрямком діяльності GEC є проведення інформаційних кампаній, спрямованих на розвінчання пропагандистських наративів й формування загартованості суспільства до інформаційних впливів.

Ці кампанії охоплюють створення сайтів-вітрин, які містять аналітичні матеріали, що розкривають механізми та інструменти іноземної пропаганди. Наприклад, на таких платформах публікують тематичні дослідження щодо діяльності російських, китайських або іранських пропагандистських мереж, надаючи аудиторії вичерпну інформацію про їхні методи впливу.

Крім того, GEC активно розробляє брошури, інформаційні матеріали та підручники, які допомагають журналістам, освітянам та громадським активістам ідентифікувати ознаки дезінформації. Важлива складова роботи Центру є проведення соціальної реклами — кампаній у соціальних мережах, на телебаченні й в Інтернеті, що спрямовані на підвищення медіаграмотності населення та формування критичного мислення у споживачів інформації. Такі кампанії часто орієнтовані на молоду аудиторію.

Окрему увагу GEC приділяє підтримці незалежних медіа, зокрема в країнах, де свобода слова та незалежна журналістика перебувають під загрозою втручання держслужбовців. Через програми грантової підтримки та навчальні ініціативи Центр надає фінансування, експертну допомогу та ресурси для розвитку медіа, що дотримуються принципів об'єктивності та неупередженості у висвітленні подій.

Важливим аспектом діяльності GEC є співпраця з приватними технологічними компаніями, включаючи такі медіа-гіганти як Meta (Facebook), Google, Twitter (X) та інші. Ця взаємодія дозволяє виявляти та нейтралізувати бот-мережі, які системно поширюють дезінформацію через соціальні платформи. Зокрема, спільні аналітичні центри та робочі групи аналізують

активність підозрілих акаунтів, виявляють координовані кампанії впливу та блокують облікові записи, що порушують правила платформ. Така співпраця забезпечує комплексний підхід до інформаційної безпеки, поєднуючи можливості державних структур та приватного сектору.

Основними джерелами роботи Global Engagement Center були:

- Фінансування — GEC функціонував із щорічним бюджетом $61 мільйона та мав штат приблизно 120 осіб. Фінансування надавали оборонні бюджети США, зокрема через Закон про національну оборону (NDAA).

Однак у 2024 році Конгрес, підконтрольний Республіканській партії, відмовився продовжити фінансування [67].

- Грантові програми — Центр надавав гранти на дослідження та ініціативи, спрямовані на виявлення та протидію дезінформаційним кампаніям, особливо в таких країнах, як Україна, Білорусь та інші регіони Євразії.
- Партнерства — GEC активно співпрацював із неурядовими організаціями, громадянським суспільством, міжнародними мовниками (такими як Voice of America та Radio Free Europe/Radio Liberty) та аналітичними центрами. Ці партнерства були критично важливими для поширення достовірної інформації та протидії іноземній пропаганді [68].

Місія та структура GEC були засновані відповідно до Указу Президента США №13721 від 14 березня 2016 року, який перетворив попередній Центр стратегічних комунікацій протидії тероризму (CSCC) на нову структуру з розширеним мандатом. Основною місією GEC було «керувати, координувати та інтегрувати зусилля федерального уряду США щодо виявлення, розуміння, викриття та протидії іноземній державній та недержавній пропаганді та дезінформації, спрямованим на підрив політики, безпеки або стабільності США, їхніх союзників та партнерів» [69].

Основними напрямами діяльності Центру були аналітичні дослідження, міжнародне партнерство, викриття інформаційних операцій, інформаційні кампанії та соціальна реклама.

Таблиця 3.2

Основні напрями діяльності Global Engagement Center

Напрям діяльності	Суть діяльності	Приклади реалізації
Аналітика та дослідження	Збір і аналіз даних про іноземні інформаційні операції, підготовка звітів та досліджень	Звіти: «Стовпи дезінформації РФ», «Роль RT та Sputnik», «Гендерна дезінформація»
Інформаційна кампанії та соціальна реклама	Проведення просвітницьких кампаній, спрямованих на підвищення медіаграмотності та стійкості суспільства	Відеоролики, публікації в соцмережах, брошури, навчальні матеріали
Підтримка незалежних медіа	Фінансування, гранти, навчальні програми для розвитку незалежної журналістики	Гранти для журналістів у регіонах, тренінги з виявлення дезінформації
Міжнародна співпраця	Взаємодія з урядами, міжнародними організаціями та партнерами для боротьби з дезінформацією	Ukraine Communications Group, співпраця з країнами НАТО та ЄС
Виявлення та викриття інформаційних операцій	Моніторинг та публічне викриття кампаній іноземної дезінформації	Розслідування щодо Pressenza, спростування російської та китайської пропаганди
Співпраця з технологічними кампаніями	Партнерство для моніторингу бот-мереж, виявлення та блокування шкідливих акаунтів	Спільні проекти з Meta, Google, Twitter для виявлення бот-мереж
Розробка технологічних рішень	Впровадження інноваційних інструментів для аналізу та протидії дезінформації	Демонстрації аналітичних платформ, тестування нових технологій

17 квітня 2025 року, Держсекретар США — Марко Рубіо, оголосив про закриття Global Engagement Center. У своїй заяві Рубіо зазначив, що відділ Держдепу, раніше відомий як Global Engagement Center, витратив мільйони доларів на те, щоб активно цензурувати голоси американців [70].

У 2023 році GEC зазнав значної критики з боку громадських діячів та політиків. Зокрема, Ілон Маск назвав GEC «найгіршим порушником цензури та маніпуляцій у медіа» та «загрозою для демократії». Крім того, деякі консервативні політики звинувачували центр у цензуруванні правих голосів та витрачанні коштів платників податків на придушення американських голосів.

У 2024 році Конгрес США, контрольований Республіканською партією, відмовився продовжити фінансування GEC, що призвело до його закриття 23 грудня 2024 року. Це рішення було частиною ширшої тенденції до скорочення фінансування програм, пов'язаних з боротьбою проти дезінформації, які, на думку деяких законодавців, обмежували свободу слова.

Закриття GEC викликало занепокоєння серед експертів з інформаційної безпеки. Деякі вважають, що це послаблює здатність США протидіяти іноземній дезінформації, особливо з боку таких країн, як Росія та Китай . Інші підтримують рішення про закриття, вважаючи, що уряд не повинен втручатися у модерацію контенту в Інтернеті.

3.2 Комунікаційні механізми та формати державної взаємодії з аудиторіями

Сучасні політичні системи активно використовують механізми публічної дипломатії та інструменти «м’якої сили» для формування позитивного іміджу, просування власної позиції у міжнародному дискурсі та протидії дезінформаційним кампаніям супротивників. Публічна дипломатія включає комплекс заходів, спрямованих на встановлення комунікаційного зв’язку між державними інституціями та зарубіжною аудиторією, зміцнення довіри до офіційних джерел та просування цінностей демократії, прав людини, безпеки й міжнародної стабільності.

Одним із ключових інструментів такої взаємодії є публічна дипломатія, що передбачає систематичну діяльність державних структур, спрямовану на формування позитивного образу країни, просування власних цінностей та протидію негативним інформаційним впливам. Концепція “м'якої сили” (soft power), запропонована Джозефом Найєм [8], підкреслює важливість не лише економічної або військової потужності, а й культурного впливу, освітніх програм, цінностей, що сприяють залученню симпатій міжнародної спільноти.

Серед основних форматів взаємодії держави з міжнародною аудиторією можна виокремити:

- проведення форумів і конференцій (наприклад, Munich Security Conference, Davos World Economic Forum), які стають майданчиками для презентації національних ініціатив і позицій щодо глобальних проблем;
- організація відкритих лекцій, культурних заходів, днів культури, національних фестивалів за кордоном, що дозволяють зміцнювати імідж країни через популяризацію мови, мистецтва, традицій;
- запуск освітніх програм обміну (наприклад, Fulbright, Erasmus+, Український інститут) для залучення студентів, науковців, митців до співпраці;
- офіційні акаунти державних органів у соцмережах (X (Twitter), Facebook, Instagram, YouTube), які виконують роль каналів прямої комунікації з іноземною аудиторією. Наприклад, акаунти МЗС України, Офісу Президента та Міноборони активно публікують оперативну інформацію, коментарі щодо міжнародної політики, спростування фейків, заклики до партнерів і демонструють відкритість держави.

Реальні приклади ефективних інформаційних кампаній включають:

- інформаційний супровід українських військових операцій під час війни з Росією, коли українські державні акаунти оперативно публікували офіційну інформацію, розвіювали дезінформацію та координували міжнародну підтримку (наприклад, кампанія #StandWithUkraine);
- кампанії МЗС України, спрямовані на привернення уваги до ситуації на тимчасово окупованих територіях, як-от кампанія “Crimea is Ukraine” або інформаційні проекти щодо депортації українських дітей;
- приклади з інших країн, наприклад, кампанія #ThinkCanada, яка демонструє відкритість Канади для інвестицій і талантів, або проєкти BrandUSA, що популяризують туристичний потенціал США.

Важливою складовою сучасної комунікаційної політики держав є національні інформаційні платформи. Вони слугують джерелом достовірної та

перевіреної інформації для громадян і міжнародної спільноти. В Україні прикладом є сайти **“**Спростуй**”** (spravdi.gov.ua) [71] та Center for Strategic

Communications and Information Security (Stratcom Ukraine) [72], які надають дані про дезінформацію, роз’яснюють складні теми безпеки зрозумілою мовою, публікують інфографіку, відео, аналітичні матеріали.

Механізми оперативної комунікації також включають створення спеціалізованих сайтів і порталів для спростування фейків (наприклад, EUvsDisinfo від Європейської служби зовнішньої дії), що дозволяють реагувати на інформаційні загрози в режимі реального часу. Держави залучають експертів, журналістів, лідерів думок для створення якісного контенту та підвищення рівня довіри аудиторії. Наприклад, в Україні діють ініціативи, як-от співпраця Stratcom Ukraine з незалежними медіа та фактчек-організаціями [73].

Сучасна державна комунікація активно інтегрує мультимедійні формати — відеоролики, інфографіку, подкасти, анімаційні пояснення, щоб складні теми безпеки, дипломатії чи міжнародного права були доступними для широкої аудиторії. Такі формати дозволяють охоплювати різні цільові групи: від молоді до професійної спільноти, залучати увагу через сучасні цифрові платформи (YouTube, TikTok, Instagram Reels).

Ефективна державна комунікація в кризових ситуаціях ґрунтується на швидкості, достовірності інформації та використанні різних форматів і каналів для охоплення широкої аудиторії.

Одним із яскравих прикладів є інформаційне супроводження військових операцій України під час повномасштабної агресії Росії у 2022–2024 роках. Українські державні органи, зокрема Міністерство оборони, Міністерство закордонних справ, Офіс Президента, активно використовували офіційні акаунти в Twitter, Facebook, Instagram, Telegram для оперативного інформування про хід бойових дій, ситуацію на фронті, втрати ворога, а також для спростування фейків, які поширювалися російською пропагандою. Наприклад, Twitter-акаунт Міноборони України став ключовим джерелом для іноземних журналістів та

аудиторії, регулярно публікуючи дані про знищену техніку ворога та інші оперативні зведення. Кампанії на кшталт #StandWithUkraine,

#ArmUkraineNow, #StopRussia були спрямовані на мобілізацію міжнародної підтримки, а візуальні матеріали (відео, інфографіка) підкреслювали масштаб агресії та необхідність допомоги Україні.

Ще один приклад — кампанія “Crimea is Ukraine”, яку реалізовували МЗС України та Український інститут у партнерстві з закордонними медіа і культурними інституціями. Її мета — нагадати міжнародній спільноті про незаконну окупацію Криму та необхідність деокупації. У межах цієї кампанії організовувалися публічні заходи, виставки, інформаційні кампанії в соцмережах, поширювалися відео- та текстові матеріали англійською мовою.

Кампанія “Bring Kids Back UA”, започаткована за ініціативи Офісу Президента України у 2023 році, стала прикладом інформаційного супроводу гуманітарної кризи — примусової депортації українських дітей до Росії. Завдяки мультимедійним форматам — відеороликам, публікаціям у соціальних мережах, офіційним заявам на міжнародних платформах — вдалося привернути увагу міжнародних організацій, правозахисників та урядів інших країн до проблеми депортації та закликати до конкретних дій для повернення дітей.

Таким чином, комунікаційні механізми та формати державної взаємодії з аудиторіями складають складну, але надзвичайно важливу систему, що дозволяє державам ефективно доносити свої позиції, боротися з дезінформацією, формувати імідж відкритої та демократичної країни, готової до діалогу та співпраці у глобальному середовищі.

ВИСНОВКИ

Дослідження теми «Інформаційна безпека в стратегіях комунікації держав: виклики і тенденції» дало змогу комплексно розглянути сучасні ризики й підходи до захисту інформаційного простору як одного з ключових елементів національної безпеки. У результаті аналізу було встановлено, що:

1) Інформаційна безпека у сучасному світі є критичним елементом національної безпеки, стабільного розвитку й ефективного функціонування держави в умовах зростаючої кількості гібридних війн. Сучасний інформаційний простір характеризується високою динамікою змін, що створює як і нові можливості, так і численні ризики, пов'язані із кібератаками, інформаційним тероризмом, пропагандою, дезінформацією та іншими формами негативного впливу на свідомість громадян, іміджу країни та стабільного розвитку економіки.

2) Аналіз теоретичних основ інформаційної безпеки продемонстрував, що захист державної інформаційної сфери потребує комплексного підходу, який включає технічні, правові й ідеологічні заходи. Було виявлено, що ефективні заходи інформаційної безпеки держави ґрунтується на трьох основних парадигмах:

- технічній, яка впроваджує інструменти кіберзахисту, шифрування, аутентифікації та моніторингу інформаційних потоків;
- ідеологічній, яка акцентує увагу на важливості розвитку медіаграмотності, навичок критичного мислення, стійкості до маніпуляцій як і серед співробітників інформаційних структур, так і серед цивільного населення країни;
- правовій, яка визначає нормативно-правове регулювання сфери інформаційної безпеки, включаючи міжнародне співробітництво та захист цифрових прав громадян.

3) Ключовим інструментом протидії інформаційним загрозам виступають стратегічні комунікації. Вони є багатокомпонентним механізмом, який поєднує

інформаційну діяльність, публічну дипломатію, PR, психологічні операції та культурну взаємодію. Ефективність таких комунікацій забезпечується завдяки чітко визначеним цілям; адаптації повідомлень до культурних особливостей та психологічного стану аудиторії; використанню багатоканальних платформ, включаючи соціальні мережі, медіа, офіційні видання, офіційні звернення політичних лідерів; механізмам швидкого реагування на кризи та дезінформаційні атаки.

4) Дослідження досвіду держав, таких як США, Тайвань, Естонія та ЄС, доводить важливість інтегрованого підходу до забезпечення інформаційної безпеки, починаючи впровадженням ініціатив і утворенням спеціалізованих центрів, закінчуючи розробки освітніх програм для населення та тісної праці із технологічними компаніями. Аналіз практик зазначених країн дозволив виявити універсальні моделі та інструменти захисту інформаційного простору, які інші країні можуть впроваджувати у роботу, серед них: прозорість інформаційного середовища, механізми фактчекінгу, розвиток цифрової грамотності в галузі інформаційної безпеки, створювати міжнародну координацію в боротьбі з кіберзагрозами та дезінформацією.

5) Для України, яка перебуває в умовах затяжної інформаційної та гібридної війни, необхідно адаптуватися до кращих практик захисту інформації, враховуючи специфіку гібридних війн, впливу дезінформації та загроз з боку країн-агресорів. Це передбачає посилення інституційного потенціалу в сфері інформаційної безпеки, удосконалення нормативно-правової бази, активне впровадження стратегічних комунікацій, формування інформаційної культури суспільства та забезпечити медіаграмотність у громадян. Українська стратегія інформаційної безпеки держави повинна будуватися на синергії технічних засобів захисту, правового регулювання, освітніх ініціатив і стратегічних комунікацій, що дозволяє забезпечити стійкість держави до сучасних загроз та гарантувати інформаційний суверенітет.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Інформаційна безпеки: підручник. К.: Ліра-К, 2021. 412 с. URL: https://jurkniga.ua/contents/informatsiyna-bezpeka.pdf?srsltid=AfmBOoqOwbi8TFuK3zu6w9F06HB-UZLQaNcVaEV7FMcsSm5371FhEGJ6 (дата звернення: 14.04.2025).

2. Дубов Д. В. Стратегічні комунікації: проблеми концептуалізації та практичної реалізації. Стратегічні пріоритети. Серія: Політика. 2016. № 4. 9-23. URL: http://nbuv.gov.ua/UJRN/sppol_2016_4_4 (дата звернення: 14.04.2025).

3. Хорішко Л. С. Досвід реалізації стратегічних комунікацій у діяльності НАТО та ЄС: інституційний аспект. Регіональні студії. 2021. № 26. 54-58. URL: http://nbuv.gov.ua/UJRN/regst_2021_26_13 (дата звернення: 04.04.2025).

4. Мартинов А. "М'яка сила" як політичний інструмент Європейського Союзу (1990-ті — 2020-ті рр.). Міжнародні зв'язки України: наукові пошуки і знахідки. 2020. Вип. 29. 113. URL: http://resource.history.org.ua/publ/Mzu_2020_29_8 (дата звернення: 04.04.2025).

5. Вальорска М. А. Діпфейк та дезінформація: практ. посіб.; пер. з нім. В. Олійника. К.: Академія української преси ; Центр Вільної Преси, 2020. 36 с.

6. Vogel D., Besenyo J. Like War – The Weaponization of Social Media, by P. W. Singer and Emerson T. Brooking. 2018. 98-101. URL: https://www.researchgate.net/publication/335149861_Like_War_-_The_Weaponization_of_Social_Media_by_P_W_Singer_and_Emerson_T_Brooking/ (дата зверненнння: 14.04.2025).

7. Меленко О. С. Стратегічні комунікації: до визначення поняття. Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція. 2023 No 64. 42-51. URL: https://vestnik-pravo.mgu.od.ua/archive/juspradenc64/9.pdf (дата звернення: 15.04.2025).

8. Гладкий І. Я. Концепція soft power: основні положення Дж. Ная. Регіональні студії. 2024. № 38. 167-171. URL: доступу: http://nbuv.gov.ua/UJRN/regst_2024_38_29 (дата звернення: 15.04.2025).

9. Проноза І. І. Інформаційна війна: сутність та особливості прояву. *Актуальні проблеми політики*. 61-ше вид. 2018.

10. Олефір І.В. Моделі побудови інформаційного суспільства. *Теорія та історія політичної науки*. 5-те вид. 2017.

11. Тихомиров О. О. Інформаційна безпека: соціотехнічна парадигма. Інформаційна безпека людини, суспільства, держави. 2014. № 1. 13-20. URL: http://nbuv.gov.ua/UJRN/iblsd_2014_1_4 (дата звернення: 18.04.2025).

12. Хешування. *Solix*. URL: https://www.solix.com/uk/kb/hashing/ (дата звернення: 18.04.2025).

13. TLS vs. SSH: When To Use Which. *WolfSSL*. URL: https://www.wolfssl.com/tls-vs-ssh-when-to-use-which/ (дата звернення: 18.04.2025).

14. Контроль доступу на основі ролей. *Solix*. URL: https://www.solix.com/uk/kb/role-based-access-control/ (дата звернення: 18.04.2025).

15. Оцінка вразливості і patch management. *Softico*. URL: https://softico.ua/uk/news/otsinka-vrazlivosti-i-patch-management/ (дата звернення: 18.04.2025).

16. Логування: поняття, вимоги, рівні. *QATestLab*. URL: https://training.qatestlab.com/blog/technical-articles/logging-in-concepts-requirements-levels/ (дата звернення: 18.04.2025).

17. Чому UEBA необхідна для сучасного бізнесу. *ESKA*. URL: https://eska.global/solutions/ueba (дата звернення: 19.04.2025).

18. Yesimov S., Borovikova V. Methodological foundations of information security research. Social & Legal Studios. 2023. Vol. 6. No. 1. 49-55. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/5861 (дата звернення: 22.04.2025)

19. Оксана Дарморіз. Особливості розвитку інформаційної культури в добу глобалізації. *Вісник Львівського університету. Серія філософські науки*. 15-те вид. Львів, 2012.

20. Халамендик В.Б. Інформаційна гігієна як фактор збереження психічного здоров'я людини. *Інформаційна гігієна як фактор збереження психічного здоров'я людини*. Київ, 2008.

21. Биков О. М. Інформаційна безпека: правовий та культурологічний виміри. Аналітично-порівняльне правознавство. 2024. № 2. 396-402. URL: http://nbuv.gov.ua/UJRN/anpopr_2024_2_69. (дата звернення: 22.04.2025).

22. Синій хакер. VPN Unlimited. URL: https://www.vpnunlimited.com/ua/help/cybersecurity/blue-hat-hacker (дата звернення: 22.04.2025).

23. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с. URL: https://elibrary.kubg.edu.ua/id/eprint/18860/1/A_Nashinets-Naumova_monografia_1_FPMV.pdf (дата звернення: 22.04.2025).

24. Компанцева Л., Заруба О., Череватий С., Акульшин О. Стратегічні комунікації для безпекових і державних інституцій: практичний посібник. К.: ТОВ «ВІСТКА», 2022. 278 с.

25. Дмитро Кошкарьов. Аналіз цільової аудиторії. *Seven mountsins*. URL: https://up7mountains.com.ua/blog/analiz-tsilovoyi-audytoriyi (дата звернення: 22.04.2025).

26. Лікарчук Л.І. Локалізація у перекладі: адаптація для нових аудиторій. Вчені записки ТНУ імені В. І. Вернадського. Серія: Філологія. Журналістика. 2025. Том 36(75). № 1. Ч. 1. 310-315. URL: https://www.philol.vernadskyjournals.in.ua/journals/2025/1_2025/part_1/52.pdf (дата звернення: 22.04.2025).

27. ISO/IEC 27000 (серія). *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/ISO/IEC_27000_(серія) (дата звернення: 25.04.2025).

28. Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів. *Будстандарт*.

29. Cyber defence. *NATO*. URL: https://www.nato.int/cps/en/natohq/topics_78170.htm (дата звернення: 26.04.2025).

30. Cyber Defence Pledge. *NATO*. URL: https://www.nato.int/cps/em/natohq/official_texts_133177.htm (дата звернення: 26.04.2025).

31. NATO 2022. Strategic concept. *Access Denied*. URL: https://www.nato.int/strategic-concept/ (дата звернення: 26.04.2025).

32. Locked Shields. *CCDCOE*. URL: https://ccdcoe.org/locked-shields/ (дата звернення: 26.04.2025).

33. Cyber Coalition: NATO's Flagship Cyber Exercise. *act.nato.int*. URL: https://www.act.nato.int/activities/cyber-coalition/ (дата звернення: 29.04.2025).

34. NATO Rapid Reaction Team to fight cyber attack. *nato.int*. URL: https://www.nato.int/cps/en/natolive/news_85161.htm (дата звернення: 29.04.2025).

35. The EU's Cybersecurity Strategy for the Digital Decade. Shaping Europe's digital future. URL: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (дата звернення: 07.05.2025).

36. European Security Union. *European Commission*. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en (дата звернення: 07.05.2025).

37. Cybersecurity Skills Academy. Digital Skills and Jobs Platform. URL: https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy (дата звернення: 07.05.2025).

38. The EU Cybersecurity Act. Shaping Europe's digital future. URL: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act (дата звернення: 09.05.2025).

39. European Cybersecurity Atlas - CyberSec4Europe | Cyber Security for Europe. CyberSec4Europe Cyber Security for Europe. URL:

https://cybersec4europe.eu/events/concertation/convergence_2020/cybersecurity-atlas/ (дата звернення: 09.05.2025).

40. Contributors to Wikimedia projects. Deepfake. Wikipedia. *Wikipedia, the free encyclopedia*. URL: https://en.wikipedia.org/wiki/Deepfake (дата звернення: 12.05.2025).

41. Wakefield J. Deepfake presidents used in Russia-Ukraine war. BBC. URL: https://www.bbc.com/news/technology-60780142 (дата звернення: 12.05.2025).

42. Що таке шкідливе програмне забезпечення? Визначення й типи | Захисний комплекс Microsoft. Microsoft – AI, Cloud, Produktivität, Computing, Gaming und Apps. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-malware (дата звернення: 12.05.2025).

43. Alert Regarding Vulnerability in SonicWall SMA 100 Series (CVE-2021-20016). *JPCERT/CC*. URL: https://www.jpcert.or.jp/english/at/2021/at210006.html (дата звернення: 12.05.2025).

44. It’s not just technology. IT is community. SolarWinds. https://www.solarwinds.com/company (дата звернення: 14.05.2025).

45. Горгуленко В.А. Кіберборотьба у воєнних конфліктах сучасності: передовий досвід, тенденції та закономірності розвитку. Протибортсво у кіберпросторі. Сучасні інформаційні технології у сфері безпеки та оборони. 2024. No 2(50). 11-28. URL: https://sit.nuou.org.ua/article/download/301405/302376/719334 (дата звернення: 15.05.2025).

46. U.S Government Printing Office. Foreign And Military Intelligence. Washington, 1976. 651 p.

47. Шевчук М. О. Сучасні виклики і загрози в сфері інформаційної безпеки держави. *Актуальні проблеми вітчизняної юриспруденції № 6. 2024*. 2024.

48. Панченко О. Інформаційна безпека держави як елемент соціокультури. *Аспекти публічного управління*. 2020. *8*(1). 58-67. https://doi.org/10.15421/152006

49. Виздрик В., Мельник О. Інформаційна безпека в Україні: сучасний стан. Міжнародний науковий журнал «Грааль науки». 2023. № 24. 196-202. DOI 10.36074/grail-of-science.17.02.2023.034 *https://archive.journal-grail.science/index.php/2710-3056/article/download/867/883/896* (дата звернення: 17.05.2025).

50. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. Humanitarian vision. 2016. Vol. 2, Num. 1. 27-32. URL: http://nbuv.gov.ua/UJRN/hv_2016_2_1_7 (дата звернення: 17.05.2025).

51. Уханова Н. С. Правова культура молоді в Україні. Інформація і право. 2019. № 2. 156-166. URL: http://nbuv.gov.ua/UJRN/Infpr_2019_2_19. (дата звернення: 17.07.2025).

52. Башук А.І. Комунікаційні стратегії державної влади в умовах інформаційного суспільства: монографія. Кам'янець-Подільський: ТОВ «Друкарня "Рута"», 2019. 584 с.

53. Kaufmann B., Glatthard J. 'Humour over rumour': lessons from Taiwan in digital democracy. *SWI swissinfo.ch*. URL: https://www.swissinfo.ch/eng/politics/freedom-of-expression-humour-over-rumour-lessons-from-taiwan-in-digital-democracy/46592080 (date of access: 19.05.2025).

54. Президентські вибори у США 2020 – Вікіпедія. *Вікіпедія*. URL: https://uk.wikipedia.org/ (дата звернення: 20.05.2025).

55. Учасники проектів Вікімедіа. East StratCom Task Force – Вікіпедія. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/East_StratCom_Task_Force (дата звернення: 21.05.2025).

56. EEAS. Action Plan On Strategic Communication. EU. URL: https://www.eeas.europa.eu/sites/default/files/action_plan_on_strategic_communication.docx_eeas_web.pdf (дата звернення: 21.05.2025)

57. Про нас. *Euvsdisinfo.eu*. URL: https://euvsdisinfo.eu/ua/about-ua/ (дата звернення: 21.05.2025).

58. Хакімова В. Т. Європейський Союз в епоху постправди: діяльність East Stratcom Task Force. *Актуальні проблеми політики*. 2021. № 5.

59. East Stratcom Task Force. Disinformation Review. URL: https://euvsdisinfo.eu/disinformation-review/ (дата звернення: 22.05.2025).

60. Disinformation – Media coverage on alleged influence. *EEAS*. URL: https://www.eeas.europa.eu/eeas/disinformation-—media-coverage-alleged-influence_und_en (дата звернення: 22.05.2025).

61. EUvsDisinfo. Кремль переписує історію об'єднання Німеччини. *euvsdisinfo.eu*. URL: https://euvsdisinfo.eu/ua/кремль-переписує-історію-обєднання/ (дата звернення: 22.05.2025).

62. East Stratcom Task Force. Database. *euvsdisinfo.eu*. URL: https://euvsdisinfo.eu/disinformation-cases/ (дата звернення: 22.05.2025).

63. Дубле І.-М. Дезінформація та виборчі кампанії. Страсбург, Франція: Рада Європи, 2019. 33 с.

64. Фурсай О. Російська дезінформаційна кампанія «Doppelgänger» як новітній виклик інформаційній безпеці держав Заходу. Філософія та політологія в контексті сучасної культури. 2024. №16(Спецвипуск). 84-92. https://doi.org/10.15421/352411

65. Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI). *EEAS*. URL: https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en (дата звернення: 27.05.2025).

66. Ruppe A.E., Walker V. S. The Global Engagement Center: A Historical Overview 2001-2021. A Special Report by the U.S. Advisory Commission on Public

Diplomacy. 2024. URL: https://www.state.gov/wp-content/uploads/2024/04/2024GEC-ACPD_DIGITAL-508_FINAL.pdf (дата звернення: 27.05.2025).

67. State Department's disinformation office to close after funding nixed in NDAA. *CyberScoop*. URL: https://cyberscoop.com/state-departments-disinformation-office-to-close-after-funding-nixed-in-ndaa/ (дата звернення: 27.05.2025).

68. House Foreign Affairs. THE GLOBAL ENGAGEMENT CENTER: HELPING OR HURTING U.S. FOREIGN POLICY. *www.congress.gov*. URL: https://www.congress.gov/event/118th-congress/house-event/LC72827/text?utm_source=chatgpt.com (дата звернення: 28.05.2025).

69. Technical Difficulties. *2021-2025.state.gov*. URL: https://2021-2025.state.gov/about-us-global-engagement-center-2/ (дата звернення: 28.05.2025).

70. Кінша Д. У США закрили Центр протидії іноземній дезінформації при Держдепі – Рубіо. *Суспільне Новини*. URL: https://suspilne.media/996553-u-ssa-zakrili-centr-protidii-inozemnij-dezinformacii-pri-derzdepi-rubio/ (дата звернення: 31.05.2025).

71. Центр стратегічних комунікацій. Протидія дезінформації та гібридним операціям Росії. *Центр стратегічних комунікацій*. URL: https://spravdi.gov.ua/ (дата звернення: 31.05.2025).

72. StratCom Ukraine. Центр стратегічних комунікацій. URL: https://stratcomua.org/ua (дата звернення: 02.06.2025).

73. Семенюта А. П. І. «Стійка Україна важлива для стійкої Європи». У Києві розпочався Kyiv StratCom Forum 2025. *Detector.media*. URL: https://detector.media/infospace/article/240284/2025-04-24-stiyka-ukraina-vazhlyva-dlya-stiykoi-ievropy-u-kyievi-rozpochavsya-kyiv-stratcom-forum-2025/ (дата звернення: 02.06.2025).

ЗГОДА
здобувача(чки) освіти Державного університету економіки і технологій про перевірку кваліфікаційної роботи на прояви академічного плагіату та розміщення в Репозитарії ДУЕТ

Я, **Малько Катерина Сергіївна**, підтримую політику Державного університету економіки і технологій з академічної доброчесності і відкритого доступу. Стверджую, що кваліфікаційна бакалаврська робота «Інформаційна безпека в стратегіях комунікації держав: виклики і тенденції» виконана самостійно та не містить академічного плагіату. Я не надавав(ла) і не одержував(ла) недозволену допомогу під час підготовки цієї роботи. Використання ідей, результатів і текстів інших авторів мають покликання на відповідне джерело.

Із чинним Положенням про запобігання та виявлення академічного плагіату в роботах здобувачів вищої освіти Державного університету економіки і технологій ознайомлений(а). Чітко усвідомлюю, що в разі виявлення у кваліфікаційній роботі порушення норм академічної доброчесності робота не допускається до захисту або оцінюється незадовільно.

Також я поінформований(на), що відповідно до пункту 5.8 «Положення про Репозитарій (електронну базу даних) Державного університету економіки і технологій» згадана робота буде розміщена в Електронному архіві Університету (Репозитарії ДУЕТ) та ознайомлений(на) з умовами такого розміщення.

16.06.2025