Харківський національний університет імені В.Н. Каразіна
Навчально-науковий інститут «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Кафедра міжнародних відносин

КВАЛІФІКАЦІЙНА

РОБОТА МАГІСТРА

на тему: **«ІНФОРМАЦІЙНА БЕЗПЕКА ІСПАНІЇ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ»**

Виконав:
студент 2-го курсу, групи УМІБ–61
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
ОПП «Міжнародна інформаційна безпека»

Бевзюк Олег Романович
(прізвище, ім’я, по батькові)

Керівник:

д.п.н., проф. Куц Галина Михайлівна
(науковий ступінь, вчене звання, прізвище, ім’я, по батькові)

Рецензент:
к.п.н., доц Дібікова Юлія Сергіївна
(науковий ступінь, вчене звання, прізвище, ім’я, по батькові)

ХАРКІВ – 2025 р.

Харківський національний університет імені В. Н. Каразіна
Навчально-науковий інститут «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Кафедра міжнародних відносин
Спеціальність 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
Освітньо-професійна програма «Міжнародна інформаційна безпека»
Рівень вищої освіти: другий (магістерський)

ЗАТВЕРДЖУЮ
завідувачка кафедри

_____ _____ **Наталія ВІННИКОВА**
(Підпис) (ім'я, прізвище)

«_2_» червня 2025 року
(зі змінами від 10.09.2025; 06.10.2025)

ЗАВДАННЯ
на кваліфікаційну роботу магістра

Бевзюк Олег Романович
(прізвище, ім'я та по батькові)

1. Тема роботи «Інформаційна безпека Іспанії в умовах гібридних загроз» керівник роботи д.п.н., проф. Куц Галина Михайлівна
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом по університету від «02» червня 2025 року № 4001-5/1324 зі змінами від «10» вересня 2025 року № 4001-5/3049, зі змінами від «6» жовтня 2025 року № 4001-5/3656.
2. Строк подання здобувачем вищої освіти роботи 21 листопада 2025 р.
3. Перелік питань, які потрібно розробити:
– поняття та структура інформаційної безпеки держави
– гібридні загрози в системі сучасних міжнародних відносин
– забезпечення інформаційної безпеки держави в умовах гібридних загроз
– інституційна складова забезпечення системи інформаційної безпеки Іспанії
– нормативно-правове забезпечення інформаційної безпеки Іспанії
– функціонування системи інформаційної безпеки Іспанії в умовах гібридних загроз
– виклики щодо стійкості системи інформаційної безпеки Іспанії в умовах сучасних гібридних загроз
– роль міжнародного співробітництва у забезпечення інформаційної безпеки Іспанії
– використання досвіду Іспанії у зміцненні інформаційної безпеки України в умовах гібридних загроз

4. План роботи

№ з/п	Назви етапів роботи	Строк виконання етапів
1	Вибір здобувачем теми КРМ і подання заяви на кафедру; затвердження теми та призначення наукового керівника; складання та затвердження індивідуального завдання на виконання КРМ	19.05.2025-30.06.2025
2	Підготовка вступу і розділу 1 КРМ	01.09.2025-30.09.2025
3	Підготовка розділу 2 КРМ	01.10.2025-15.10.2025
4	Підготовка розділу 3 КРМ	16.10.2025-31.10.2025
5	Підготовка висновків і переліку використаних джерел	03.11.2025-14.11.2025
6	Подання студентом завершеної КРМ науковому керівнику для перевірки та оформлення відгуку, перевірка КРМ на відсутність запозичень	17.11.2025-21.11.2025
7	Попередній розгляд КРМ на комісії від кафедри	24.11.2025-28.11.2025
8	Прийняття кафедрою рішення про допуск роботи до захисту в ЕК, оформлення та зовнішнє рецензування	01.12.2025-05.12.2025
9	Захист КРМ в ЕК і присвоєння випускникам кваліфікації	08.12.2025-24.12.2025

5. Дата видачі завдання: 2 червня 2025 року (зі змінами від 10.09.2025; 06.10.2025).

Здобувач вищої освіти _____ _____ Олег БЕВЗЮК
(підпис) (ім’я, прізвище)

Керівник роботи _____ _____ Галина КУЦ
(підпис) (ім’я, прізвище)

ЗМІСТ

ВСТУП

Актуальність теми зумовлена трансформацією сучасного безпекового середовища, у якому цифровий простір став одним із ключових театрів міжнародної конкуренції. Зокрема, стрімке зростання кіберінцидентів, інформаційних операцій та технологічно вдосконалених методів дезінформації, що активно застосовуються державними й недержавними акторами, висуває перед Мадридом якісно нові вимоги до розбудови національної системи інформаційної безпеки. Більш того, як член ЄС і НАТО, Іспанія інтегрована у ширші європейські та євроатлантичні механізми протидії гібридним загрозам, а тому її спроможність ефективно реагувати на них безпосередньо впливає на колективну стійкість об'єднання.

Водночас особлива актуальність теми пов'язана з тим, що сучасні гібридні загрози спрямовані не лише на критичну інфраструктуру, а й на підрив суспільної довіри, маніпуляцію громадською думкою, дестабілізацію політичних процесів. Іспанія, маючи багатомовне та багатокультурне середовище, стає потенційно вразливою до зовнішніх інформаційних впливів, які, за певних умов, здатні загострювати внутрішні соціально-політичні лінії поділу. Тому дослідження її стратегій інформаційної безпеки дає змогу, по-перше, глибше осмислити механізми взаємодії між національними та наднаціональними інструментами протидії дезінформації, а по-друге, визначити, наскільки вони відповідають динаміці сучасних технологічних і політичних викликів. Окрім того, Іспанія є прикладом держави, яка поєднує жорсткі технологічні рішення у сфері кіберзахисту з інституційними заходами з підвищення цифрової грамотності населення, що надає її досвіду додаткової практичної значущості.

Ступінь вивченості теми можна вважати достатньою на теоретичному рівні, хоча комплексні дослідження саме іспанського виміру залишаються фрагментарними. У базовому концептуальному полі сутність інформаційної безпеки, її роль у структурі національної та міжнародної безпеки, а також

природу гібридних загроз ґрунтовно аналізують Є. Вознюк, В. Андрюхіна [1], М. Гончаров [2], Д. Дрига [3], С. Кавин [4], О. Карпенко [5], С. Мазепа [7], І. Милосердна [8], О. Прудникова [10], О. Пугачов [11]. Їхні праці створюють методологічний фундамент для дослідження специфіки іспанської моделі інформаційної безпеки. Безпосередньо національну політику Іспанії у сфері кібербезпеки та державного управління висвітлюють В. Кононенко, В. Годлевська [6], тоді як інституційну архітектуру та механізми забезпечення інформаційної безпеки Іспанії аналізує Х. Гарсія Ґутієррес [34]. Окремий, особливо активний напрям становлять дослідження дезінформації та інформаційних впливів в іспанському медіапросторі: вагомий внесок у цей дискурс роблять А. Бадільйо [17], Р. Куето Діас [22], Б. де-Фрутос-Торрес, Г. Таддео, М.-К. Альварадо [25], Д. Гарсія-Марін, Ґ. Сальват-Мартінрей [35], К. Лопес-Ріко, Ф. Мартінес-Верду [52], Ф. Мартінес-Рохет [54], Д. Мартінес-Санчес [55], Х. Муньйос [57], П. Прієто Барраль [63], Х. Рібейро [67]. У ширшому європейському контексті гібридних загроз важливими є також дослідження Х. Паломареса Лерми [61] та К. Руєда Ріко [68], які, хоча й не зосереджені виключно на Іспанії, формують підґрунтя для глибшого розуміння особливостей її інформаційної безпеки в умовах сучасних гібридних викликів.

Мета дослідження – визначити особливості функціонування системи забезпечення інформаційної безпеки Іспанії в умовах гібридних загроз.

Завдання дослідження:

– визначити поняття, структуру інформаційної безпеки держави та типологію гібридних загроз у системі сучасних міжнародних відносин;

– виявити механізми забезпечення інформаційної безпеки держави в умовах гібридних загроз;

– розкрити нормативно-правове забезпечення інформаційної безпеки Іспанії та його значення для протидії сучасним гібридним загрозам;

– встановити особливості функціонування системи інформаційної безпеки Іспанії та ключові виклики, що впливають на її стійкість у контексті сучасних гібридних загроз;

– з’ясувати роль міжнародного співробітництва у зміцненні інформаційної безпеки Іспанії та можливості використання її досвіду для посилення інформаційної безпеки України.

Об’єкт дослідження – система забезпечення інформаційної безпеки держави.

Предмет дослідження – система забезпечення інформаційної безпеки Іспанії в умовах гібридних загроз.

Теоретико-методологічна база дослідження спирається на комплекс сучасних наукових підходів, які дозволяють всебічно охопити специфіку формування, функціонування та трансформації національної системи захисту інформаційного простору. Насамперед, ключовими є положення теорії національної безпеки, що трактує інформаційну безпеку як структурний компонент загальної безпекової політики держави та інтегрує політичний, правовий, військовий, кібернетичний і соціальний виміри. Важливим є використання концепції гібридних загроз, що ґрунтується на дослідженнях Ф. Хоффмана та документів ЄС і НАТО, де акцент робиться на поєднанні традиційних і нетрадиційних форм впливу, включно з дезінформацією, кібератаками, інформаційно-психологічними операціями та втручанням у внутрішні політичні процеси. Методологічно дослідження базується на системному підході, який дозволяє розглядати інформаційну безпеку Іспанії як багаторівневу й інтегровану систему, де поєднуються державні інституції, правоохоронні структури, кіберкомандування, приватний сектор і громадянське суспільство. Використання інституціонального підходу забезпечує можливість проаналізувати механізми взаємодії між цими акторами, а також оцінити ефективність діяльності національних органів,

Інформаційна база дослідження ґрунтується на комплексі офіційних документів, аналітичних матеріалів та наукових праць, що дозволяють цілісно відтворити особливості формування та реалізації політики Іспанії у сфері інформаційної безпеки в умовах зростання гібридних загроз. Передусім використано нормативно-правові акти Королівства Іспанія, зокрема

Національну стратегію кібербезпеки, Стратегію національної безпеки, а також положення законів про захист персональних даних і цифрові права, які створюють фундаментальні рамки забезпечення безпеки інформаційного простору. Крім того, використано матеріали Національного інституту кібербезпеки, Центру криптологічної безпеки та щорічні звіти Міністерства внутрішніх справ Іспанії. Водночас, важливою складовою інформаційної бази стали аналітичні огляди Європейського Союзу та НАТО, адже Іспанія інтегрує власні підходи до інформаційної безпеки у ширший євроатлантичний контекст. Окрему увагу приділено публікаціям провідних міжнародних дослідників, які розкривають природу гібридних загроз, механізми їхнього впливу та специфіку реагування держави.

Практичне значення отриманих результатів. Запропоновані у кваліфікаційній роботі магістра теоретичні положення та висновки можуть бути використані: органами державної влади України полягає насамперед у можливості використання іспанського досвіду як дієвої моделі адаптації системи національної інформаційної безпеки до умов багатовимірних гібридних загроз. Зокрема, аналіз стратегічних документів Іспанії та її підходів до міжвідомчої координації дозволяє українським інституціям, передусім РНБО, Міністерству оборони, Службі безпеки України та Міністерству цифрової трансформації, посилити інституційні механізми реагування на інформаційні операції, кібератаки та кампанії дезінформації; у навчальному процесі Харківського національного університету імені В.Н. Каразіна та інших вищих навчальних закладів при розробці та викладанні дисциплін, за програмами підготовки магістрів міжнародних відносин, суспільних комунікацій та регіональних студій.

Апробація дослідження була здійснена у вигляді публікації тез наукової доповіді для участі у Всеукраїнському науково-практичному круглому столі «Стратегічні напрями зовнішньої політики та дипломатії країн світу» (м. Харків, 21 листопада 2025 р.), на тему: «Functioning of Spain’s information security system under hybrid threats».

Структура роботи. Кваліфікаційна робота магістра складається зі вступу, трьох розділів, висновків, списку використаних джерел, що налічує 81 найменування. Загальний обсяг роботи становить 84 сторінки, з яких основного тексту – 75 сторінок.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

1.1. Поняття та структура інформаційної безпеки держави

В умовах стрімкої трансформації міжнародної системи, зумовленої інтенсивною цифровізацією, посиленням гібридних загроз та появою нових форм протиборства, інформаційна безпека держави стала одним із ключових вимірів національної безпеки, що визначає здатність країни ефективно функціонувати в політичній, економічній, соціальній і військовій сферах [38]. Хоча не існує єдиного універсального визначення цього поняття, науковий дискурс поступово формує комплексний погляд, який охоплює не лише технічні аспекти захисту інформаційних ресурсів, а й політичні, правові, соціально-психологічні та культурні виміри інформаційної взаємодії [8]. Відтак інформаційна безпека трактується як стан захищеності інтересів особи, суспільства і держави у сфері формування, використання, поширення та зберігання інформації, що забезпечує стабільність державної системи та стійкість до внутрішніх і зовнішніх інформаційних впливів [2].

У сучасній науковій літературі існує кілька підходів до визначення сутності інформаційної безпеки. Перший, технологічний – акцентує увагу на забезпеченні конфіденційності, цілісності та доступності інформації. Цей підхід сформувався під впливом розвитку кіберінфраструктури та прагнення держав мінімізувати ризики кібератак. Другий, системно-комунікативний – розглядає інформаційну безпеку як складову інформаційної політики, що включає управління потоками інформації, протидію дезінформації, формування стійкого суспільного дискурсу та підвищення рівня медіаграмотності. Третій підхід, політико-стратегічний – трактує інформаційну безпеку як інструмент захисту державного суверенітету, відображає боротьбу за контроль над інформаційним простором та використання інформації як ресурсу геополітичного впливу [11]. Згадані

підходи взаємодоповнюють один одного, поступово формуючи сучасне комплексне уявлення про структуру та функції інформаційної безпеки.

Водночас інформаційна безпека держави передбачає наявність чіткої структурної організації, яка охоплює нормативно-правові засади, інституційні механізми, технологічні ресурси та практики стратегічних комунікацій. З одного боку, структура інформаційної безпеки включає правове регулювання, що визначає статус інформації, принципи кіберзахисту, обмеження щодо поширення шкідливого контенту та відповідальність за інформаційні правопорушення [3]. З іншого боку, вона передбачає інфраструктурні компоненти: системи кіберзахисту, мережеві протоколи, національні центри реагування на кіберінциденти, механізми міжвідомчої координації та спеціалізовані служби безпеки. Окрім цього, значною складовою інформаційної безпеки стає гуманітарно-комунікативний блок, що охоплює діяльність у сфері стратегічних комунікацій, протидії пропаганді, публічної дипломатії, цифрової освіти та медіаграмотності населення [10]. Слід зауважити, що зростання гібридних загроз істотно розширило спектр ризиків, пов’язаних із функціонуванням інформаційного простору [15]. Яскравим сучасним прикладом є системні кібератаки на критичні інфраструктури держав Європейського Союзу, які здійснювалися як державними, так і недержавними акторами [1]. Зокрема, у 2023 році Європейське агентство з кібербезпеки (ENISA) зафіксувало різке зростання атак на енергетичний сектор, що супроводжувалося інформаційними кампаніями, спрямованими на дестабілізацію суспільних настроїв у країнах Балтії [29]. Іншим показовим прикладом є масовані операції з дезінформації, що поширювалися через соціальні мережі під час виборів у США у 2020 році та під час загальнонаціональних виборів у Франції 2022 року.

Разом із тим, концепція інформаційної безпеки має важливий соціально-психологічний вимір. Інформаційні загрози не обмежуються втручанням у цифрові системи, адже вони також спрямовані на свідомість громадян, формування хибних уявлень, деморалізацію населення або підрив довіри до

державних інституцій [37]. У цьому контексті структура інформаційної безпеки держави передбачає створення систем раннього виявлення фейків, посилення інформаційної прозорості органів влади та розвиток державних платформ перевірки фактів. Не менш значущою частиною структури інформаційної безпеки є інституційний вимір. У більшості сучасних держав сформовані спеціалізовані інститути, відповідальні за кіберзахист та інформаційну політику. Наприклад, у США функціонує Агентство з кібербезпеки та інфраструктурної безпеки (CISA), яке забезпечує моніторинг критичних інфраструктур та координацію реакції на кібератаки. У країнах ЄС діють як національні агентства, так і наднаціональні структури, зокрема, згадана ENISA, а також Європейська служба зовнішніх дій, яка займається стратегічними комунікаціями та протидією іноземній дезінформації [14]. В Україні відповідні функції виконують Служба безпеки України, Національний координаційний центр кібербезпеки, Державна служ ба спеціального зв'язку та захисту інформації.

Таблиця 1.1.

Структура інформаційної безпеки держави

Компонент	Основні елементи
Нормативно-правовий	Закони та підзаконні акти; стандарти кіберзахисту; регулювання інформаційної діяльності; відповідальність за порушення інформаційної безпеки.
Інституційний	Державні органи (СБУ, ДССЗЗІ, МВС, Міноборони, МЗС); національні центри кібербезпеки; міжвідомча координація; спеціальні служби.
Технологічний	Засоби кіберзахисту; захист критичної інфраструктури; системи моніторингу; штучний інтелект та аналітика даних; криптографія; системи реагування на інциденти.
Комунікативно-гуманітарний	Стратегічні комунікації; протидія дезінформації; підтримання медіаграмотності; державна інформаційна політика; формування національного наративу.

Соціально-психологічний	Робота з громадською думкою; підтримання суспільної стійкості; формування довіри до інститутів; подолання панічних та маніпулятивних впливів.
Міжнародний	Співпраця з НАТО, ЄС, ООН, ОБСЄ; участь у програмах кіберзахисту; обмін інформацією; спільні навчання і стандарти.
Економічний	Забезпечення цифрового суверенітету; інвестиції у власні технології; контроль над критичними технологічними ресурсами; кіберстрахування.

У межах структури інформаційної безпеки важливу роль відіграє нормативно-правовий механізм, який встановлює правила поводження з інформацією, визначає категорії інформаційних загроз та окреслює повноваження державних інституцій у сфері кіберзахисту. Зауважимо, що у 2021-2023 рр. Європейський Союз значно оновив свою нормативну базу, ухваливши Директиву NIS2, яка встановлює розширені вимоги до кіберзахисту критичної інфраструктури, а також Регламент про цифрові послуги (DSA), спрямований на підвищення прозорості інформаційного простору та обмеження поширення маніпулятивного контенту [59]. Аналогічні тенденції простежуються і в Україні, де оновлення законодавства у сфері інформаційної та кібербезпеки відбувається з урахуванням умов воєнного стану та активних інформаційно-психологічних операцій проти держави [7]. Поряд із правовими та інституційними аспектами важливо розглянути також стратегічний вимір інформаційної безпеки. Сучасні держави все частіше розробляють комплексні стратегії, що інтегрують інформаційні, кібернетичні, дипломатичні та військово-політичні інструменти. У межах цього підходу інформація розглядається як стратегічний актив, що може бути використаний для посилення міжнародного впливу або, навпаки, як об’єкт атаки в рамках інформаційної війни [32]. Серед прикладів – Стратегія національної безпеки США 2022 року, яка окремо виділяє інформаційну безпеку як ключовий елемент захисту демократії.

Важливо наголосити, що структура інформаційної безпеки держави є багаторівневою. Перший рівень, внутрішній – охоплює державні органи влади, правові засоби, інститути громадянського суспільства та медіапростір. Другий, міжнародний – базується на співпраці з міжнародними організаціями (НАТО, ЄС, ОБСЄ, ООН), участі у спільних програмах кіберзахисту, обміні інформацією та формуванні коаліцій проти дезінформаційних кампаній [21]. Третій рівень, технологічний – визначає залежність держави від цифрової інфраструктури та необхідність її модернізації, захисту та адаптації до нових умов функціонування. Більш того, розвиток інформаційної безпеки неможливий без урахування еволюції засобів масової комунікації, адже саме вони стають ключовими каналами взаємодії між державою та суспільством, між різними міжнародними акторами, а також між недержавними структурами, які дедалі активніше впливають на глобальний порядок денний [8]. У XXI столітті інформаційний простір характеризується надзвичайною швидкістю поширення контенту, його фрагментованістю та неконтрольованістю. Це створює не лише нові можливості для держав, але й безпрецедентну кількість ризиків. Саме тому ефективна структура інформаційної безпеки повинна бути адаптивною, здатною швидко реагувати на зміни в медіаландшафті та використовувати інноваційні технології для прогнозування й нейтралізації загроз.

У цьому контексті важливим і водночас складним компонентом стає аналіз даних і застосування штучного інтелекту. Останніми роками ці технології активно інтегруються в системи управління безпекою, оскільки дозволяють виявляти аномалії у мережевому трафіку, прогнозувати атаки, оцінювати достовірність інформації та ідентифікувати мережі поширення дезінформації [56]. У 2024 році ЄС запустив ініціативу AI4Trust, спрямовану на використання штучного інтелекту для моніторингу онлайн-маніпуляцій у реальному часі, що стало відповіддю на зростаючий обсяг фейкових новин, глибоких підробок (deepfakes) та автоматизованих інформаційних операцій. У США подібні системи застосовуються у рамках діяльності CISA та Пентагону,

особливо перед виборами та в період кризових ситуацій. Це демонструє, що технологічний прогрес є не лише чинником ризиків, але й потужним інструментом зміцнення інформаційної безпеки держави. Водночас слід зауважити, що технологічні інструменти не можуть повністю замінити людський фактор. Експерти, аналітики, фахівці зі стратегічних комунікацій та дипломатії відіграють ключову роль у формуванні та реалізації інформаційної політики. Вони забезпечують якісний аналіз контексту, розробку інформаційних стратегій, комунікацію з громадськістю та міжнародними партнерами. Зокрема, під час активної фази російсько-української війни після лютого 2022 року саме людський фактор став основою інформаційної стійкості України: професійна робота журналістів, прозорість органів влади, ефективність комунікаційних команд Офісу Президента та Міністерства закордонних справ дозволили не лише нейтралізувати значну частину ворожих інформаційних атак, але й сформувати глобальну підтримку України [36].

Крім того, структура інформаційної безпеки охоплює економічний вимір, адже інформація стала стратегічним ресурсом, порівнянним за значенням із природними чи фінансовими активами. Держави, які не контролюють власну цифрову інфраструктуру або залежні від іноземних технологічних компаній, автоматично потрапляють у зону підвищених ризиків. Саме тому Європейський Союз активно розвиває політику цифрового суверенітету, спрямовану на зменшення залежності від зовнішніх IT-платформ та посилення контролю над передовими технологіями [10]. Подібна логіка простежується і в Азії: Китай та Південна Корея створюють власні еко-системи електронних сервісів та соціальних мереж, а Японія активно інвестує у розвиток національних центрів кібербезпеки. Вказані приклади підтверджують, що інформаційна безпека стає складовою економічної стратегії держави, визначаючи її конкурентоспроможність у глобальному середовищі.

Важливою складовою структури інформаційної безпеки є міжнародне співробітництво. Жодна держава, навіть технологічно розвинена, не здатна

самостійно протистояти транснаціональним кіберзагрозам та глобальним дезінформаційним кампаніям [15]. Тому на міжнародному рівні формуються різні платформи взаємодії: кіберцентри НАТО, програми кіберзахисту ЄС, глобальні ініціативи ООН щодо відповідального використання інформаційних технологій у міжнародній безпеці. Наприклад, НАТО Cooperative Cyber Defence Centre of Excellence у Таллінні проводить щорічні навчання Locked Shields, у яких тренуються державні інституції з понад 30 країн. Навчання включали відпрацювання реагування на складні сценарії гібридних атак, що поєднували кібернетичні операції з інформаційно-психологічними впливами [38]. Це демонструє розуміння того, що сучасні загрози є комплексними, а отже, і структура захисту повинна бути гнучкою та багатовекторною. Окремий вимір інформаційної безпеки держави пов'язаний із культурою та ідентичністю. Інформаційні атаки нерідко спрямовані на підрив національних цінностей, спотворення історичної пам'яті, нав'язування альтернативних інтерпретацій подій чи створення штучних соціальних протиріч [33]. У багатьох країнах, зокрема в Україні, Польщі та балтійських державах, формування стійкого національного наративу стало ключовим елементом протидії ворожій пропаганді. Саме тому культурна політика, освіта, національні ЗМІ та громадянські ініціативи включаються в структуру інформаційної безпеки нарівні з технологічними та юридичними механізмами.

Зміцнення інформаційної безпеки також потреб ує розбудови механізмів демократичного контролю та прозорості діяльності органів влади. У демократичних державах інформаційна політика не може ґрунтуватися виключно на жорсткому контролі та обмеженні доступу до інформації. Навпаки, саме відкритість і відповідальність влади перед громадянами створюють умови для зростання довіри, а отже, для формування стійкого інформаційного середовища [11]. Нарешті, значну увагу варто приділити людському праву на доступ до інформації, яке також є частиною структури інформаційної безпеки держави. Обмеження доступу виправдане лише тоді, коли воно відповідає принципам пропорційності, законності та необхідності.

Виклики останніх років, від пандемії до повномасштабної війни, показали, що надмірне обмеження інформаційного простору може мати протилежний ефект.

Зазначимо, що поняття та структура інформаційної безпеки держави формуються під впливом широкого спектра факторів, від розвитку технологій і трансформації глобального інформаційного середовища до політичних стратегій окремих держав та міжнародних організацій. У сучасних умовах інформаційна безпека набуває характеристик міждисциплінарної категорії, що поєднує правові, технічні, гуманітарні та стратегічні елементи [51]. Її ефективність залежить не лише від можливостей державних інститутів, а й від рівня довіри в суспільстві, якості інформаційної культури громадян, здатності держави адаптуватися до нових викликів та забезпечувати відкритий, але водночас захищений інформаційний простір.

1.2. Гібридні загрози в системі сучасних міжнародних відносин

Попри уявну структурованість і передбачуваність міжнародної системи, сучасна епоха демонструє дедалі складніші та більш багатовимірні форми протистояння, які виходять далеко за межі традиційних моделей силової взаємодії. Гібридні загрози, що поєднують інструменти військового, політичного, інформаційного, економічного та технологічного впливу, стали однією з ключових характеристик геополітичної динаміки XXI ст. Їхня поява є не випадковим явищем, а результатом трансформації міжнародних відносин, у яких зростають роль інформації, швидкість комунікацій, взаємозалежність держав і водночас вразливість політичних систем. Власне тому гібридні загрози нині розглядають як комплексний феномен, що поєднує приховану агресію, правдоподібне заперечення, роботу через посередників і вплив на критичні інфраструктури [51]. Центральною особливістю гібридних загроз є їхня здатність адаптуватися під конкретні політичні, соціальні та технологічні умови, що значно ускладнює їх ідентифікацію та протидію [9]. Наприклад, події після 2014 року, пов’язані з російською агресією проти України, стали одним із найяскравіших свідчень того, як гібридні інструменти застосовуються

державою для досягнення політичних та військових цілей без офіційного оголошення війни. У цьому контексті слід згадати використання «зелених чоловічків» у Криму, масштабні дезінформаційні кампанії, кібератаки на енергетичну інфраструктуру України, а також активне застосування економічного тиску, що разом створило ситуацію багатовимірного впливу. З огляду на це, гібридні загрози часто характеризують як інструмент «сірої зони», простору між війною та миром, де агресор формально уникає відповідальності [20].

Однак важливо зазначити, що гібридні загрози не обмежуються лише євразійським простором. У 2020-2025 рр. Європейський Союз зафіксував зростання випадків політично мотивованих кібератак, втручання у виборчі процеси та маніпулятивного поширення контенту, спрямованого на підрив довіри до демократичних інституцій [10]. Відомими стали атаки групи «Ghostwriter» проти Литви, Польщі та Німеччини, спрямовані на дискредитацію військової присутності НАТО в регіоні. Паралельно збільшилася активність прокитайських і проросійських угруповань у соціальних мережах, які через емоційно навантажені наративи намагалися впливати на громадську думку щодо війни в Україні, санкційної політики та енергетичної безпеки ЄС. У результаті держави-члени Євросоюзу були змушені переглянути підходи до інформаційної стійкості, зокрема активізувати роботу Європейського центру протидії гібридним загрозам у Гельсінкі [5]. Показовим є те, що гібридні загрози дедалі частіше пов’язані з конкуренцією за технологічне домінування. Підрив ланцюгів постачання мікрочипів, маніпулювання рідкоземельними матеріалами, інформаційні атаки на технологічні компанії, усе це стало частиною глобального стратегічного суперництва між США та Китаєм [49]. Наприклад, дискусії щодо діяльності компанії Huawei у Європі не обмежувалися лише технологічними питаннями; вони стали маркером ширшої боротьби за геополітичний вплив, де Китай, використовуючи економічні стимули, інфраструктурні інвестиції та м’яку

силу, намагався розширити свою присутність, тоді як євроатлантичні партнери застерігали щодо ризиків залежності.

Водночас гібридні загрози активно використовують внутрішню вразливість держав. Поляризація суспільств, криза довіри до традиційних медіа, поява постправди створюють сприятливе середовище для маніпуляцій [8]. Окремої уваги заслуговують гібридні енергетичні загрози. У 2021-2023 рр. Європа пережила найсерйознішу енергетичну кризу після Холодної війни. Російська Федерація, використовуючи постачання газу як інструмент шантажу, різко зменшила обсяги поставок до країн ЄС, що спричинило підвищення цін на енергоносії, інфляцію та політичну напругу всередині держав-членів Євросоюзу [60]. Водночас інформаційні атаки супроводжували енергетичну дестабілізацію, створюючи хаос та посилюючи невдоволення політикою урядів. Приклад із вибухами на газопроводі «Північний потік» у 2022 році також засвідчив, наскільки вразливими є критичні інфраструктури та як легко їх можна використати для політичного тиску в «гібридному режимі» [15].

Проте гібридні загрози проявляються й у менш очевидних формах, таких як використання міграційних потоків для створення політичних криз. Ситуація на кордоні Білорусі та Польщі у 2021 році стала прикладом того, як авторитарний режим може спрямовано маніпулювати міграцією, аби дестабілізувати Європейський Союз [39]. Разом із тим сучасні гібридні загрози активно використовують приватних акторів, що робить їх ще складнішими. Компанії, соціальні мережі, фінансові інституції, технологічні корпорації фактично стали новими «полями битви», де держави змагаються за вплив [64]. Протягом 2023-2025 рр. компанія Meta неодноразово повідомляла про видалення десятків проросійських і прокитайських мереж впливу, які використовували фейкові акаунти для просування політичних наративів у США, Європі та навіть Африці.

Варто також відзначити, що гібридні загрози активно використовують міжнародно-правові «сірі зони». Відсутність чітких міжнародних норм щодо кібервійни, інформаційних операцій чи штучного інтелекту створює

можливості для недобросовісних акторів [50]. Наприклад, кібератаки на урядові системи Естонії у 2007 році стали одними з перших, що привернули увагу до необхідності розробки міжнародно-правових рамок у сфері кібербезпеки. Проте навіть до 2024 року глобальні нормативні механізми залишаються фрагментарними, що дозволяє державам вести гібридні операції без формальних наслідків. Після початку повномасштабної війни в Україні у 2022 році гібридні загрози стали не просто елементом зовнішньополітичного інструментарію, а системним явищем глобальної безпекової архітектури [69]. Росія, намагаючись вплинути на підтримку України з боку ЄС і НАТО, одночасно здійснювала кібератаки, поширювала фейки про «втому Заходу», маніпулювала цінами на енергоносії та активізувала проксі-актори в Африці й Латинській Америці, які поширювали антизахідні наративи.

Не менш важливим є те, що гібридні загрози дедалі частіше пов’язані з розвитком штучного інтелекту. Генерація дипфейків, автоматизоване поширення дезінформації, маніпулювання громадською думкою за допомогою алгоритмів створюють новий рівень небезпеки [56]. Наприклад, у 2024 році Європейська комісія попередила про використання реалістичних відео та аудіо маніпуляцій у передвиборчих кампаніях у Словаччині та Франції. Гібридні загрози також глибоко проникають у сферу міжнародної торгівлі, фінансів та економічної безпеки. Відомими стали випадки, коли держави використовували санкції, ембарго або маніпуляції валютними ринками як частину ширших операцій впливу. До прикладу, у 2023 році США запровадили низку обмежень на експорт високотехнологічних товарів до Китаю, аргументуючи це ризиками національної безпеки, що фактично стало елементом технологічного протистояння, яке теж можна кваліфікувати як гібридне [14]. Усе це свідчить про те, що гібридні загрози стали інтегральною складовою сучасних міжнародних відносин, формуючи нове уявлення про конфліктність, владу та вплив [38]. З огляду на зростання кількості інструментів, що можуть застосовуватися у гібридному форматі, держави вимушені переглядати власні стратегії безпеки, посилювати кіберзахист, формувати системи раннього

попередження, удосконалювати механізми співпраці з міжнародними партнерами. Водночас ключовим викликом залишається пошук балансу між свободою інформації та необхідністю захисту.

Не можна оминути й екологічний вимір гібридних загроз. У 2023 році Європейська комісія задокументувала випадки навмисного поширення фейкової інформації про нібито токсичність українського зерна, яка мала на меті дестабілізувати ринки та підірвати економічну співпрацю між Україною та ЄС. Подібні атаки, з одного боку, маніпулюють екологічною чутливістю суспільств, а з іншого – створюють підґрунтя для політичного тиску. Таким чином, гібридні загрози охоплюють навіть ті сфери, що традиційно асоціювалися з гуманітарною або економічною політикою, що свідчить про їхню універсальність [47]. Варто звернути увагу й на те, що у світі формується нова архітектура міжнародної відповіді на гібридні загрози. Наприклад, у 2022-2025 рр. країни НАТО активно розвивали модель «тотальної оборони», яка передбачає мобілізацію всіх державних інститутів і суспільства для протидії гібридним викликам. Естонія, Литва та Фінляндія стали лідерами у впровадженні цієї концепції, поєднуючи кіберзахист, інформаційну протидію, стійкість критичної інфраструктури та підготовку населення до кризових ситуацій [81]. Такий підхід демонструє, що ефективна протидія гібридним загрозам можлива лише за умови поєднання заходів національної безпеки, міжнародного партнерства та суспільної стійкості [20]. З іншого боку, у країнах Західної Європи відчутно посилилася увага до питань стратегічних комунікацій. У 2024 році Франція, Німеччина та Нідерланди створили спільну платформу для виявлення й аналізу іноземних інформаційних впливів. Її завдання полягає не лише у моніторингу цифрового простору, але й у виробленні рекомендацій для політиків, медіа та освітніх установ щодо мінімізації вразливостей суспільства [21]. Таким чином, держави дедалі більше визнають важливість поєднання безпекових і когнітивних інструментів у боротьбі з гібридними загрозами.

Особливе місце у структурі сучасних гібридних загроз займає маніпулювання міжнародними інституціями. У 2023 році було зафіксовано випадки, коли окремі держави намагалися блокувати рішення в межах ООН або ОБСЄ, використовуючи юридичні механізми, що формально відповідають правилам організацій, але на практиці служили інструментом збереження стратегічного впливу. Подібні дії вважають «інституційним саботажем», який також належить до гібридних форм тиску [50]. Це явище, до слова, набирає поширення і в регіональних організаціях, що ще раз підтверджує комплексний характер сучасних викликів.

Нарешті, аналізуючи глобальний ландшафт гібридних загроз, слід акцентувати на тому, що їхня ефективність часто базується на здатності агресора використовувати слабкі місця міжнародної системи. Неврегульовані конфлікти, економічні кризи, гуманітарні катастрофи – усе це створює «вікна можливостей», у межах яких гібридні операції можуть бути особливо результативними. Саме тому країни, що стикаються з внутрішньополітичними проблемами або низьким рівнем економічного розвитку, стають значно вразливішими. Приклад Молдови у 2022-2024 рр., де проросійські політичні сили активно використовували енергетичну кризу для дестабілізації ситуації, показує, як гібридний вплив здатен впливати на демократичні процеси, навіть без прямого використання військової сили [60].

Зазначимо, що гібридні загрози не є тимчасовим явищем, притаманним окремому регіону чи конкретному конфлікту. Вони становлять основу нової моделі міжнародної конфліктності, де межі між миром і війною, державним і недержавним, відкритим і прихованим поступово зникають [51]. У цих умовах світова спільнота має перемістити фокус із реактивного на проактивний тип безпеки, розвиваючи стійкість суспільств, підвищуючи технологічну компетентність та посилюючи міжнародну координацію. Лише так можна ефективно протистояти викликам, що постають у добу гібридних загроз, які дедалі більше визначають якість і стабільність глобальної політичної системи.

Утім, навіть попри активізацію міжнародних зусиль, слід підкреслити, що гібридні загрози залишаються явищем, яке відзначається високим рівнем невизначеності та непередбачуваності. Це пояснюється тим, що їхні прояви еволюціонують паралельно зі змінами у глобальному інформаційному просторі, розвитком цифрових технологій і трансформацією політичних режимів. Значною мірою це також пов’язано з тим, що гібридні операції можуть здійснюватися навіть без значних матеріальних ресурсів, а ефект їхнього впливу часто є диспропорційно великим порівняно з витратами. Наприклад, маніпулятивний відеоролик, створений за допомогою штучного інтелекту, може стати тригером суспільних протестів або дипломатичного скандалу, що підтверджує важливість розуміння психологічних механізмів масової комунікації.

1.3. Забезпечення інформаційної безпеки держави в умовах гібридних загроз

Інформаційна безпека держави сьогодні дедалі більше визначає її здатність не лише зберігати внутрішню стабільність, а й ефективно реагувати на зовнішні виклики, які, як свідчить практика останніх років, часто мають гібридний характер. Поступово стає очевидним, що традиційні інструменти протидії загрозам виявляються недостатніми, адже сучасні конфлікти відбуваються не лише на полі бою, а й у цифровому просторі, у медіасередовищі, у соціальних мережах та навіть у сфері міжособистісної комунікації. У цьому контексті забезпечення інформаційної безпеки держави вимагає комплексного, багаторівневого підходу, який поєднує нормативно-правові інструменти, технологічні рішення, інституційну взаємодію та стратегічні комунікації. Саме така комбінація дозволяє державам успішно протистояти дедалі складнішим гібридним загрозам, що проявляються у формі кібератак, інформаційних кампаній, маніпуляцій суспільною думкою, втручань у виборчі процеси та підриву довіри до інституцій [9]. У цьому світлі особливого значення набуває здатність держави швидко ідентифікувати

джерела загроз і адаптувати механізми реагування до нових умов. Наприклад, кібератаки на енергетичні системи України у 2015 та 2016 роках стали одним із перших глобальних сигналів, що держави повинні розглядати кіберпростір як ключовий вимір національної безпеки. Згодом цей підхід лише посилився, зокрема у зв'язку зі зростанням кількості атак на критичну інфраструктуру країн ЄС, США, Канади та Великої Британії. У 2021 році масштабна атака на компанію Colonial Pipeline у США призвела до тимчасового паралічу паливних поставок на сході країни, продемонструвавши, що навіть приватний сектор може стати точкою входу для дестабілізації національних процесів [29]. Отже, інформаційна безпека давно вийшла за межі виключно державного адміністрування і потребує тісної співпраці між урядом, бізнесом, громадянським суспільством та міжнародними партнерами.

Проте гібридні загрози включають не лише кіберсферу. Вони охоплюють інформаційно-психологічні операції, спрямовані на підрив ідентичності, посилення внутрішньої поляризації та руйнування довіри до державних інститутів. Саме тому стратегічні комунікації стали частиною сучасних систем безпеки. Зокрема, після 2014 року Європейський Союз створив підрозділ East StratCom для протидії дезінформації, спрямованій проти країн Європи [36]. Його діяльність підкреслює важливість не лише оперативного спростування неправдивих наративів, а й створення альтернативних, достовірних комунікаційних платформ, що формують стійкість суспільства до інформаційних впливів. У свою чергу, країни НАТО адаптували Стратегічну концепцію 2022 року, визначивши гібридні дії одним із ключових викликів колективній безпеці [20]. Це означає, що держави-члени зобов'язуються розвивати спроможності у таких сферах, як кіберзахист, боротьба з дезінформацією, аналітика загроз та підвищення медіаграмотності населення. Більше того, Альянс у 2023 році створив Центр з питань запобігання та протидії гібридним загрозам, який координує обмін досвідом між країнами-членами та проводить моделювання сценаріїв можливих атак. Такий підхід відповідає тенденції до розширення концепту «тотальної оборони», яка

охоплює не тільки військовий, а й соціальний, економічний, інформаційний та технологічний виміри [81].

Разом з тим необхідно підкреслити, що інформаційна безпека держави ґрунтується на стійкості суспільства, яке здатне критично оцінювати інформацію, розуміти природу маніпуляцій і розпізнавати спроби інформаційного впливу. У багатьох країнах, від Фінляндії до Канади, програми підвищення медіаграмотності стали частиною державної політики. Наприклад, у Фінляндії ще з 2019 року системна інтеграція медіаосвіти у шкільну програму дозволила країні стати однією з найбільш стійких до дезінформації у Європі [46]. Досвід цієї держави свідчить, що формування інформаційної культури громадян є не менш важливим, ніж розвиток технологічних інструментів. Технологічний вимір інформаційної безпеки також відіграє ключову роль. Адже гібридні загрози постійно трансформуються разом із розвитком штучного інтелекту, соціальних мереж, алгоритмів автоматичного поширення контенту та програм здатних генерувати фальшиві зображення чи відео, так звані deepfake. Уже у 2023–2024 роках фіксувалися численні випадки використання глибинних фейків у політичних кампаніях у США, Словаччині, Індії та Аргентині [18]. Відповідно, держави мають інвестувати у створення систем автоматичного виявлення маніпулятивного контенту та технологій перевірки достовірності інформації.

Нормативно-правове забезпечення інформаційної безпеки є наступним критично важливим елементом. У багатьох країнах після 2020 року було оновлено законодавство у сфері кіберзахисту, захисту персональних даних, регулювання цифрових платформ та протидії дезінформації. Наприклад, у 2022 році ЄС ухвалив Акт про цифрові послуги (Digital Services Act), який зобов’язує великі онлайн-платформи контролювати поширення незаконного та маніпулятивного контенту і запров аджує відповідальність у разі його нерегулювання [50]. Завдяки цьому держави отримали можливість накладати санкції на транснаціональні корпорації, які не виконують вимоги щодо прозорості алгоритмів та захисту користувачів.

Інституційний аспект забезпечення інформаційної безпеки передбачає чітке розмежування повноважень та відповідальності різних органів влади. Успішні моделі, як правило, включають координаційні центри, що об’єднують роботу спецслужб, органів внутрішніх справ, дипломатичних структур, кіберполіції, регуляторів цифрових платформ та наукових установ. Наприклад, у Франції функціонує національне агентство ANSSI, яке координує кіберзахист державного та приватного секторів. У США – CISA, створена у 2018 році, стала центральною установою для запобігання кіберзагрозам і взаємодії з ключовими інфраструктурними операторами [14]. Такі інституційні моделі демонструють, що ефективне забезпечення інформаційної безпеки можливе лише за умов системної взаємодії та безперервного аналізу загроз. Однак у світлі сучасних гібридних загроз особливої уваги потребує міжнародний вимір. Оскільки інформаційні атаки та кіберзагрози не визнають кордонів, окремі держави часто не здатні самостійно забезпечити власну безпеку. Тому зростає значення міжнародних форматів, від співпраці в межах НАТО та ЄС до участі у глобальних ініціативах, таких як Паризький заклик до довіри та безпеки у кіберпросторі, чи Женевські процеси з міжнародного регулювання кіберконфліктів [39]. У 2024 році, під час серії скоординованих атак на телекомунікаційні компанії Європи, саме міжнародна співпраця реагувальних центрів дозволила оперативно локалізувати загрози.

Говорячи про забезпечення інформаційної безпеки держави, необхідно наголосити на взаємодії між державою та приватними компаніями. Великі IT-корпорації, такі як Microsoft, Google, Meta чи Amazon, володіють унікальними даними про аномальну активність у мережі та про потенційні кібератаки. В останні роки їхні аналітичні звіти стали важливим джерелом виявлення інформаційно-кібернетичних загроз, що впливають на національну безпеку [60]. Водночас забезпечення інформаційної безпеки неможливе без врахування соціально-психологічного виміру. Гібридні загрози часто базуються на використанні слабких місць суспільства: політичної поляризації, економічної нестабільності, недовіри до владних інституцій, історичних травм чи

міжетнічних напружень [33]. Отже, стійкість суспільства до таких впливів повинна включати розвиток критичного мислення, а також ефективну взаємодію між державою та громадянами.

Водночас варто зазначити, що гібридні загрози стають дедалі складнішими та багатошаровими, що потребує від держави постійного оновлення підходів і гнучкості у прийнятті рішень [38]. Нові форми інформаційно-психологічного впливу, такі як маніпуляція алгоритмами соціальних мереж, застосування штучного інтелекту для мікротаргетингу політичної реклами або створення фальшивих онлайн-спільнот формують абсолютно інший вимір безпекових ризиків [51]. Наприклад, у 2024 році в ЄС були зафіксовані випадки створення мережі фейкових акаунтів, що позиціонували себе як локальні громадські ініціативи й поширювали антиєвропейські та антиукраїнські меседжі [26]. Така діяльність була складним інструментом впливу, адже поєднувала технологічні методи (боти, автоматизоване поширення постів), психологічні (експлуатація страхів населення) та політичні (підрив довіри до офіційних структур) механізми.

Крім того, слід звернути увагу на стратегічну взаємодію між інформаційними та енергетичними аспектами гібридної агресії [50]. Кібератаки на енергосистеми, супроводжувані кампаніями дезінформації, мають подвійний ефект: вони не лише завдають технічної шкоди, але й формують атмосферу невизначеності та паніки. Яскравим прикладом є масовані атаки на енергетичну інфраструктуру України у зимовий період 2022-2025 рр., коли одночасно з фізичними обстрілами та кібервтручаннями поширювалися меседжі про нібито повний колапс системи, безпорадність держави та нездатність міжнародних партнерів реагувати [36]. Така комбінація показує, наскільки важливою є координація між інституціями різних секторів для захисту критичної інфраструктури.

Розглядаючи перспективу посилення інформаційної безпеки, важливо підкреслити роль наукового аналізу й аналітичної діяльності [8, с. 179-185]. У ряді країн створюються спеціальні аналітичні центри, що займаються

дослідженням трендів у сфері гібридних загроз, прогнозуванням сценаріїв, розробкою рекомендацій для органів влади. У 2023 році у Великій Британії розширено функціонал Центру урядових комунікацій, який аналізує іноземні інформаційні впливи та координує методики протидії дезінформації [15]. В Україні також посилюється інституційне середовище для дослідження гібридних загроз, зокрема на базі Центру стратегічних комунікацій та інформаційної безпеки, який проводить моніторинг інформаційного простору та здійснює оперативне спростування фейків [5, с. 70-76]. Таким чином, аналітична складова є необхідним елементом усього циклу управління інформаційною безпекою, від виявлення загроз до формування стратегій реагування. Не менш вагомим є підсилення кадрового потенціалу держави [81, с. 1-30]. Для ефективного функціонування системи інформаційної безпеки потрібні фахівці з кіберзахисту, комунікацій, психології, соціології, політичних наук, програмної інженерії, міжнародних відносин. У провідних країнах світу активно розвиваються програми підготовки таких спеціалістів. Наприклад, у Канаді діють міждисциплінарні курси з кіберполітики, що поєднують технічні аспекти з політичними й юридичними [14, с. 1-25]. В Україні також зростає потреба у фахівцях подібного профілю, адже гібридні загрози стали частиною повсякденної реальності держави, що перебуває у стані тривалої оборони від зовнішньої агресії. Систематична підготовка кадрів дозволяє не тільки зміцнити національну безпеку, а й посилити міжнародну співпрацю у сфері протидії гібридним впливам.

При цьому особливого значення набуває формування національних стандартів реагування на інформаційні інциденти [59]. У багатьох країнах створено протоколи дій у разі здійснення кібератак, масованих інформаційних кампаній або поширення панічних наративів. У Німеччині після подій 2015-2017 років, коли фіксувалися масштабні кампанії зовнішнього впливу на політичні процеси, було ухвалено оновлену стратегію інформаційної безпеки, що містить чіткі алгоритми взаємодії між федеральними органами, спецслужбами та медіа [11]. У свою чергу, Литва у 2022 році запровадила

національний протокол реагування на інформаційні кризи, який визначає процедури оперативної комунікації та залучення експертного середовища [69, с. 1-15]. Подібні моделі демонструють, як важливою є інституціоналізація практик протидії гібридним загрозам для забезпечення стійкості держави. Досліджуючи проблему забезпечення інформаційної безпеки, необхідно окреслити й економічний вимір цього процесу [29]. Інформаційні атаки здійснюють значний негативний вплив на бізнес-середовище, призводять до витоку даних, фінансових збитків і втрати довіри клієнтів. За даними спеціалізованих компаній, середній економічний збиток від великої кібератаки у 2023-2025 рр. сягав понад 4 млн доларів [73]. У випадку держави наслідки можуть бути ще масштабнішими: порушення функціонування систем електронного врядування, атаки на банківський сектор або дестабілізація біржової системи можуть мати довгострокові макроекономічні наслідки. Саме тому інвестиції у кіберзахист та інформаційну безпеку розглядаються сьогодні як інвестиції у на ціональну стійкість і конкурентоспроможність.

На завершення зазначимо, що забезпечення інформаційної безпеки держави в умовах гібридних загроз є безперервним процесом, а не одноразовим заходом. Ворог постійно адаптує свої інструменти, тестує нові методи впливу, використовує технологічні прориви та соціальні зміни для розширення можливостей маніпуляції. Тому держава повинна діяти на випередження, формуючи багаторівневу систему безпеки, що включає нормативно-правові, інституційні, технологічні, освітні, комунікаційні та міжнародні складові. Успішна протидія гібридним загрозам передбачає синергію між урядом, бізнесом, науковцями, експертами та громадянами, адже лише комплексні підходи забезпечують реальну стійкість нації у XXI столітті. Ця стійкість допомагає не лише протистояти зовнішнім впливам, а й зміцнює внутрішню єдність, формує довіру до державних інституцій та створює підґрунтя для сталого розвитку навіть в умовах глобальної турбулентності.

Висновки до розділу 1

Зазначимо, що поняття та структура інформаційної безпеки держави формуються як комплексна система, що охоплює технологічний, правовий, організаційний, інституційний та, безумовно, соціально-комунікаційний виміри. Інформаційна безпека, у найширшому значенні, відображає здатність держави забезпечувати захист національного інформаційного простору від зовнішніх і внутрішніх загроз, водночас зберігаючи умови для вільного розвитку демократичних інститутів і інформаційного середовища. При цьому важливо наголосити, що сучасні міжнародні відносини стають дедалі складнішими, а інформаційні процеси – швидшими, що, відповідно, зумовлює необхідність постійного оновлення підходів до розуміння сутності інформаційної безпеки.

В умовах ескалації гібридних загроз, які поєднують військові, політичні, економічні, інформаційні та кібернетичні інструменти впливу, інформаційна сфера перетворюється на ключовий театр протиборства між державами й недержавними акторами. Більше того, гібридні операції, що спрямовані на маніпулювання свідомістю, дезінформацію, руйнування цифрової інфраструктури та підрив довіри до інститутів влади, стають інструментом досягнення стратегічних переваг без прямого застосування сили. Саме тому виявлення, класифікація та аналіз гібридних загроз є необхідною умовою формування ефективної моделі інформаційної безпеки сучасної держави.

Забезпечення інформаційної безпеки в умовах гібридних загроз потребує системного підходу, що включає розбудову нормативно-правової бази, зміцнення національних кіберзахисних спроможностей, розвиток стратегічних комунікацій, підвищення медіаграмотності населення та активізацію міжнародного співробітництва. Крім того, важливим є створення механізмів раннього попередження та ефективного реагування, що дозволить державі мінімізувати наслідки інформаційних атак і водночас підвищити стійкість своїх інституцій. У підсумку можна зробити висновок, що інформаційна безпека стає не лише складовою національної безпеки, а й фундаментальною

умовою стабільності держави у світовому середовищі, де гібридні виклики дедалі більше визначають логіку міжнародних відносин.

РОЗДІЛ 2. СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІСПАНІЇ

2.1. Інституційна складова забезпечення системи інформаційної безпеки Іспанії

Розуміння інституційної складової забезпечення системи інформаційної безпеки Іспанії потребує, передусім, комплексного аналізу взаємодії державних структур, нормативно-правових механізмів та оперативних інструментів, які дозволяють країні ефективно реагувати на гібридні виклики XXI століття [38]. У сучасних міжнародних відносинах, де інформаційний простір стає ключовим полем конкуренції між державами, Іспанія вибудовує багаторівневу систему, що органічно поєднує національні інституції, європейські механізми та співпрацю в межах НАТО. Важливо, що ця система не є статичною: вона постійно адаптується до нових ризиків, адже, скажімо, зростання кібератак у 2022-2025 рр. змусило уряд суттєво оновити стратегічні документи та розширити повноваження ключових органів, зокрема Національного центру кібербезпеки (INCIBE) та Національного криптологічного центру (CCN-CERT) [34]. Разом із тим, інституційна архітектура Іспанії вирізняється значною координаційною складністю, оскільки вона включає як загальнодержавні структури, так і регіональні інституції. Центральним елементом цієї системи є Рада національної безпеки, що діє під керівництвом прем’єр-міністра та координує діяльність спеціалізованих комітетів, серед яких найбільш значущим для інформаційної сфери виступає Комітет з кібербезпеки [6]. Саме він, починаючи з 2019 року, розробляє механізми реагування на кризові ситуації, зокрема на масові спроби дестабілізації політичних процесів через цифрові платформи. Наприклад, під час парламентських виборів 2023 року було зафіксовано численні спроби зовнішнього втручання через поширення дезінформаційних наративів у соціальних мережах; у відповідь комітет активізував міжвідомчу взаємодію між Міністерством внутрішніх справ, Міністерством оборони та

Національною поліцією, забезпечивши оперативне спростування неправдивої інформації та блокування фейкових акаунтів [13] (Таблиця 2.2.).

Таблиця 2.2.

Інституційна складова забезпечення системи інформаційної безпеки Іспанії

Інституція	Основні функції у сфері інформаційної безпеки
Національний центр кібербезпеки (INCIBE)	Координація кіберзахисту, реагування на інциденти, підтримка приватного сектору та громадян, освітні програми з кібергігієни.
Національний центр криптології (CCN-CERT)	Захист урядових інформаційних систем, криптографічні стандарти, реагування на атаки на державні установи.
Міністерство внутрішніх справ Іспанії	Забезпечення безпеки інфраструктур, протидія терористичним та гібридним загрозам, координація дій поліції та цивільної гвардії.
Міністерство оборони Іспанії	Військовий кіберзахист, захист оборонних інформаційних систем, участь у кібероперaціях НАТО.
Іспанська національна поліція та Цивільна гвардія	Розслідування кібератак, боротьба з кіберзлочинністю, протидія дезінформації та онлайн-екстремізму.
Комісія з національної безпеки (DSN)	Стратегічний аналіз загроз, координація міжвідомчих рішень, моніторинг гібридних загроз, включно з дезінформаційними кампаніями.
Національна рада з кібербезпеки	Розробка державної кіберполітики, узгодження стратегій між різними міністерствами та органами.
Європейські інституції (ENISA, платформи ЄС щодо дезінформації)	Підтримка Іспанії на рівні ЄС, участь у спільних операціях, доступ до

	аналітики та попереджень, захист виборчих процесів.

Зі свого боку, Міністерство внутрішніх справ Іспанії відіграє надзвичайно важливу роль у структуруванні інституційної моделі інформаційної безпеки. Його підрозділи відповідають не лише за кіберзахист критичної інфраструктури, а й за моніторинг екстремістського контенту, що може становити загрозу національній безпеці. У цьому контексті, варто згадати діяльність Гвардії Сівіль — однієї з найстаріших іспанських силових структур, що має спеціалізовані відділи з протидії кіберзлочинності. Протягом 2021–2024 років вони реалізували низку гучних операцій, серед яких операція GOLEM, спрямована на ліквідацію масштабної мережі, що поширювала шкідливе програмне забезпечення та здійснювала атаки на державні вебресурси [43]. Окремо слід відзначити діяльність Національного інституту кібербезпеки (INCIBE), який виконує ключову функцію у взаємодії держави з приватним сектором. Адже сучасні гібридні загрози, зокрема атаки на фінансові установи, енергетичні компанії чи операторів мобільного зв’язку, вимагають постійної готовності до реагування на інциденти та обміну технічною інформацією. INCIBE, починаючи з 2020 року, активно реалізовує Програму розвитку цифрової стійкості бізнесу, в межах якої щороку понад 50 тисяч компаній отримують консультації з безпеки [30]. Крім того, інститут координує єдину державну лінію реагування на кіберінциденти, що дозволяє бізнесу й громадянам оперативно повідомляти про загрози та отримувати експертну підтримку.

У сфері національної оборони ключову роль відіграють структури, що входять до складу Міністерства оборони, а саме: Командування кібероперацій, створене для забезпечення кіберзахисту військових систем та реагування на можливі зовнішні атаки. Показовим є те, що з 2022 року командування проводить щорічні навчання CyberGuardian, які моделюють сценарії гібридних атак на критичні елементи військової інфраструктури. До цих навчань

долучаються не лише національні підрозділи, а й партнери по НАТО, адже Альянс визначає Іспанію як одного з активних учасників формування спільної політики кіберстійкості [20].

Водночас інституційна система інформаційної безпеки Іспанії має й цивільно-технічний вимір, який реалізується передусім через Національний криптологічний центр (CCN-CERT). Він забезпечує криптографічний захист державних інформаційних ресурсів та аналіз складних кіберінцидентів. Наприклад, у 2021–2023 роках CCN-CERT виявив і нейтралізував понад 70 атак, спрямованих на урядові системи, що здійснювалися з використанням шкідливого ПЗ сімей SunBurst і BianLian [42]. До інституційної системи також належить Верховна рада з аудіовізуальної політики та цифрових медіа, яка відіграє важливу роль у сфері протидії дезінформації. З огляду на зростаючий вплив соціальних мереж на політичні процеси, ця рада регулює діяльність медіаплатформ, контролює дотримання стандартів прозорості та відповідальності, а також взаємодіє з Європейською комісією у межах виконання Кодексу практик щодо протидії дезінформації (2022) [17]. Особливо варто підкреслити участь Іспанії у створенні європейської Системи швидкого попередження (Rapid Alert System), яка дозволяє державам-членам оперативно обмінюватися даними щодо інформаційних атак [21].

У свою чергу, важливим елементом інституційної архітектури є активна участь Іспанії у формуванні спільної політики інформаційної безпеки Європейського Союзу. Зокрема, країна активно підтримала прийняття Директиви NIS2 (2022), яка посилила вимоги до кіберзахисту операторів критичної інфраструктури та поклала на національні органи обов’язок контролювати виконання цих вимог [59]. Інституції Іспанії, передусім INCIBE і CCN-CERT, стали ключовими виконавцями імплементації директиви.

Не можна оминути увагою і роль приватного сектору, адже компанії Telefónica, Santander, Indra, BBVA та інші беруть участь у національних програмах підвищення кіберстійкості та розробляють інноваційні технологічні рішення у сфері безпеки [40]. Характерною рисою іспанської моделі є також

глибока залученість освітніх і наукових інституцій. Університети Мадрида, Барселони, Валенсії та Саламанки мають спеціалізовані центри дослідження інформаційної безпеки, які беруть участь у міжнародних наукових проєктах, таких як Horizon Europe (2021–2027) [56].

У цьому контексті дедалі очевидніше простежується тенденція до інтеграції інституційних механізмів Іспанії з ширшими європейськими та євроатлантичними структурами [6]. Адже інформаційні загрози, як показали події останніх років, не визнають державних кордонів [38]. Наприклад, у 2024 році зафіксовано масштабну хвилю атак на логістичні компанії в Іспанії, Португалії та Франції, що була здійснена угрупованням, пов’язеним із російськими хакерами [19]. Відповідь на інцидент вимагала координації між агентствами трьох держав, а також консультацій із CERT-EU. Цей випадок переконливо продемонстрував, що навіть найефективніша національна система інформаційної безпеки потребує розбудови стійких механізмів міжнародного обміну інформацією та швидких спільних реакцій. Унаслідок цього Іспанія посилила участь у колективних кібернавчаннях НАТО, зокрема Locked Shields 2024, де її команда вперше увійшла до п’ятірки найсильніших, а також ініціювала спільні тренінги з Францією та Італією щодо виявлення дезінформаційних кампаній [20]. Утім, інституційна система Іспанії стикається і з низкою внутрішніх викликів, серед яких, зокрема, потреба в узгодженні повноважень центральних і регіональних органів управління [34]. Каталонія, Країна Басків та інші автономні спільноти мають власні підрозділи з цифрової безпеки та кіберзахисту, які діють паралельно з національними структурами. Хоча така децентралізація дозволяє враховувати локальні потреби й швидше реагувати на специфічні загрози, вона водночас створює ризик дублювання функцій або недостатньої координації у критичних ситуаціях. З цієї причини у 2023 році уряд ухвалив рішення про створення Єдиної координаційної платформи для обміну технічною інформацією між регіонами та центральними органами, що має забезпечити більш узгоджене управління інцидентами.

Варто підкреслити, що важливим інституційним елементом є також сфера правового регулювання, адже без чітких законодавчих рамок неможливо забезпечити ефективне функціонування всієї системи. Оновлений Закон про національну безпеку 2021 року визначив інформаційну безпеку одним із ключових пріоритетів держави та закріпив повноваження урядових структур у сфері кризового реагування [65]. Крім того, Іспанія активно адаптує своє законодавство до європейських вимог у межах Регламенту про цифрові послуги (DSA) та Регламенту про цифрові ринки (DMA), що були введені в дію у 2023 році [3]. Ці нормативні акти посилюють відповідальність цифрових платформ, передбачають обов'язок прозорості алгоритмів та зобов'язують провайдерів оперативно реагувати на поширення незаконного контенту.

До інституційної структури захисту інформаційного простору входять також підрозділи судової та прокурорської системи, що спеціалізуються на злочинах у сфері кібербезпеки. Національна аудієнсія Іспанії, зокрема, розглядає найскладніші справи, пов'язані з міжнародним кібертероризмом, фінансуванням незаконних цифрових структур та зламами урядових ресурсів [43]. Так, у 2022 році суд розглядав резонансну справу проти групи хакерів, які здійснювали атаки на системи Міністерства охорони здоров'я Іспанії під час пандемії COVID-19. Судова система відіграє надзвичайно важливу роль у зміцненні інституційної стійкості, оскільки формує правозастосовну практику та демонструє невідворотність покарання за злочини у цифровому середовищі.

Разом із тим, інституційна модель Іспанії значною мірою спирається на системний розвиток стратегічного планування. Національна стратегія кібербезпеки 2019 року, оновлена у 2023 році, визначає сім ключових напрямів, серед яких: захист критичної інфраструктури, протидія дезінформації, гарантування цифрових прав громадян, розвиток наукових інновацій, удосконалення міжнародного співробітництва та забезпечення кіберстійкості оборонного сектору [58]. Документ став результатом роботи міжвідомчої групи за участю Міністерства оборони, Міністерства внутрішніх справ, Ради з

національної безпеки та низки експертних центрів, що дозволило врахувати різні точки зору та забезпечити комплексність політики.

Насамкінець важливо підкреслити, що інституційна система Іспанії не обмежується лише технічними й координаційними елементами, вона включає й важливий соціально-комунікаційний вимір. Оскільки однією з найгостріших загроз є поширення дезінформації, уряд створив у 2021 році спеціальний Механізм систематичного моніторингу інформаційного середовища, який працює в тісній взаємодії з медіа, університетами та громадськими організаціями [23]. Цей механізм не лише фіксує інформаційні атаки, а й визначає їхню природу, канали поширення та потенційний вплив на громадську думку. Наприклад, у 2024 році він виявив скоординовану кампанію, спрямовану на дискредитацію Іспанії як енергетичного хабу ЄС у контексті розвитку водневих коридорів H2Med [17]. Завдяки швидкій реакції інституцій інформацію було спростовано, а медіаплатформи отримали рекомендації щодо маркування сумнівного контенту.

У підсумку можна зазначити, інституційна складова системи інформаційної безпеки Іспанії є складною та багатогранною, адже вона включає політичний, безпековий, правовий, науковий та громадський рівні. Вона не лише підтримує стійкість держави перед зовнішнім інформаційним тиском, а й формує засади для довгострокового розвитку цифрової демократії, захисту прав громадян та модернізації ключових секторів економіки. Можна стверджувати, що іспанська інституційна модель інформаційної безпеки є прикладом успішної трансформації державного управління у відповідь на гібридні загрози сучасності, і, що особливо важливо, вона демонструє високий потенціал для подальшого розвитку у контексті поглиблення інтеграції з ЄС та зміцнення колективної цифрової безпеки Європи.

2.2. Нормативно-правове забезпечення інформаційної безпеки Іспанії

Необхідність формування сучасної та комплексної системи нормативно-правового забезпечення інформаційної безпеки в Іспанії зумовлена кардинальною трансформацією міжнародного безпекового середовища, що спостерігається протягом останнього десятиліття. Зокрема, інтенсивне поширення цифрових технологій, зростання ролі соціальних мереж, а також активізація гібридних впливів з боку державних і недержавних акторів стимулювали уряд країни до переосмислення підходів до захисту інформаційного простору [38]. Саме тому іспанська правова система, спираючись на стандарти Європейського Союзу та НАТО, поступово вибудовує багаторівневу структуру нормативних механізмів, спрямованих на зміцнення державної, суспільної та індивідуальної безпеки у цифрову епоху. Водночас важливо наголосити, що сучасне регулювання інформаційної сфери в Іспанії не є статичним: воно постійно оновлюється, реагуючи на нові виклики, серед яких: кібератаки на критичну інфраструктуру, кампанії дезінформації, втручання у виборчі процеси та загальний ріст інформаційних маніпуляцій [17]. У цьому контексті одним із ключових документів, що визначив стратегічну рамку розвитку інформаційної безпеки, стала Стратегія національної безпеки Іспанії 2021 року, яка, серед іншого, виокремлює кібербезпеку та інформаційну стійкість як пріоритетні напрями [65]. Вона підкреслює необхідність захисту демократичних інституцій від зовнішнього втручання, а також створення умов для стійкості суспільства до інформаційних впливів [32]. Саме цей документ вперше на національному рівні відобразив розуміння інформаційної безпеки як міжсекторальної сфери, що охоплює не лише технічні, але й гуманітарні, правові, політичні та психологічні виміри. Більше того, стратегія визначає партнерство з ЄС як один із ключових інструментів забезпечення інформаційного суверенітету. Як приклад, після активізації російських дезінформаційних кампаній у 2022-2023 роках Іспанія

посилила співпрацю з Європейською службою зовнішніх дій (EEAS) у межах робочих груп StratCom East та Hybrid CoE [46].

Особливе місце у нормативно-правовій архітектурі Іспанії посідає Органічний закон «Про захист персональних даних і гарантію цифрових прав» (2018), який гармонізує національне законодавство з вимогами Загального регламенту ЄС про захист даних (GDPR) [34]. Він установлює суворі правила обробки, зберігання та використання персональних даних, а також передбачає відповідальність за їх неправомірне поширення чи маніпулятивне застосування. Не менш важливо, що закон закріпив нову категорію цифрових прав громадян, зокрема, право на цифрову освіту, цифрову безпеку, а також право на захист від дезінформації.

Важливо також відзначити Королівський декрет 43/2021 року, який імплементує директиву ЄС NIS та запроваджує жорсткі вимоги до кіберзахисту операторів критичної інфраструктури [59]. Цей документ створив чіткі стандарти для роботи державних установ, енергетичних компаній, фінансових операторaів, телекомунікаційних структур та інших суб’єктів критичної інфраструктури [6]. Наприклад, після серії кібератак на медичні установи Каталонії у 2022 році саме цей норматив став підставою для оперативного реагування та введення обов’язкових планів кіберстійкості. Не можна оминути увагою й Закон про Національний центр криптографії та інформаційної безпеки (CCN), який визначає повноваження цього органу у сфері захисту державних інформаційних систем [42]. CCN, діючи у межах Національного криміналістичного центру Іспанії, опікується криптографічними стандартами, надає методологічні рекомендації державним інституціям та контролює відповідність інформаційних систем державних структур вимогам безпеки. У 2024 році центр розширив свою діяльність, створивши новий департамент з моніторингу дезін-інформаційних кампаній [41].

Одним із найважливіших напрямів державної політики є також регулювання діяльності медіа в умовах поширення маніпулятивного контенту.

У 2022 році Іспанія приєдналася до Європейського кодексу практики щодо дезінформації, оновленого відповідно до ініціатив ЄС у сфері інформаційної безпеки [27]. Іспанський уряд, своєю чергою, ухвалив низку підзаконних актів, що передбачають адміністративну відповідальність за порушення платформами цих вимог. У структурі нормативного забезпечення важливе місце займає Закон про національну безпеку (2015), який, незважаючи на дату ухвалення, залишається фундаментальним документом для формування політики в інформаційній сфері [58]. Саме на підставі цього закону щороку формується план національної безпеки, що традиційно включає пріоритети у сфері кіберзахисту та протидії дезінформації. Крім національних актів, важливу роль відіграє імплементація загальноєвропейських документів. Зокрема, Акт ЄС про цифрові послуги (DSA), який набув чинності у 2023 році, суттєво вплинув на регулювання інформаційної безпеки в Іспанії [50]. Іспанія стала однією з перших країн, які почали активну перевірку виконання норм DSA. Важливим елементом нормативно-правового забезпечення є також регулювання діяльності політичної рекл ами у цифровому середовищі. У 2022 році Іспанія ухвалила спеціальні поправки до виборчого законодавства, спрямовані на запобігання іноземному втручанню у виборчі процеси [26].

Не менш важливою складовою нормативного забезпечення є державні програми цифрової грамотності, що мають опосередкований, але надзвичайно впливовий ефект на інформаційну безпеку. Уряд Іспанії системно впроваджує програми «Іспанія цифрова 2026» та «План цифрових компетентностей» [30]. Розглядаючи нормативно-правове забезпечення інформаційної безпеки Іспанії у ширшому контексті, варто зазначити, що воно формується під впливом європейських стандартів та інтеграційних процесів [14]. Водночас Іспанія не лише імплементує відповідні норми, але й активно долучається до їх розроблення. Варто також наголосити, що нормативно-правові акти Іспанії почали поступово враховувати появу нових технологічних викликів, пов’язаних із штучним інтелектом, автоматизованою генерацією контенту та дедалі складнішими формами онлайн-маніпуляцій. У 2024 році країна

приєдналася до Акту ЄС про штучний інтелект (AI Act), який запроваджує ризик-орієнтований підхід до регулювання алгоритмічних систем [56]. Це має важливе значення, оскільки саме алгоритми дедалі частіше визначають, який контент отримує користувач, які новини поширюються швидше, а які, навпаки, залишаються непоміченими. Іспанія однією з перших держав Європи розробила національні керівні принципи етичного застосування ШІ у сфері безпеки, які передбачають прозорість автоматизованих рішень, обмеження можливостей для маніпулятивного впливу та запобігання дискримінаційним практикам [44]. Після скандалу 2024 року, коли низка великих медіаплатформ була звинувачена в маніпулятивному ранжуванні політичного контенту перед виборами до Європарламенту, іспанський уряд посилив вимоги до моніторингу таких алгоритмічних систем, зобов'язавши компанії регулярно надавати звіти про вплив ШІ на формування інформаційного середовища [13].

Суттєвим аспектом є інтеграція інформаційної безпеки у сектор оборони. У 2022 році Іспанія ухвалила нову Стратегічну концепцію національної оборони, у якій гібридні загрози визначені як пріоритетний напрям уваги [32]. Документ передбачає розроблення військових протоколів реагування на інформаційні операції, у тому числі на такі, що спрямовані на дискредитацію національних збройних сил, підрив боєздатності чи дестабілізацію оборонних програм. Під час спільних навчань НАТО у 2023 та 2024 роках іспанські підрозділи з кібер- та інформаційної оборони вперше відпрацьовували сценарії комплексних атак, де кібервтручання поєднувалося із ворожими інформаційними наративами у соціальних мережах, що поширювалися через мережі ботів [20]. Така практика сприяла симетричному розвитку правового регулювання, яке враховує не лише традиційні загрози, але й специфічні психологічні та інформаційно-комунікаційні механізми впливу на суспільство. На окрему увагу заслуговують нормативні інструменти співпраці між державою та приватним сектором. Іспанія, за прикладом США та країн Північної Європи, активно розвиває модель публічно-приватного партнерства у сфері кібербезпеки [81]. У 2024 році були ухвалені нові регуляції, що

стимулюють обмін інформацією про загрози між телекомунікаційними компаніями, банківськими структурами та державними органами. Примітним є випадок співпраці між Banco Santander та INCIBE у 2023 році, коли завдяки обміну аналітикою вдалося запобігти масштабній фішинговій атаці, що могла зачепити понад 600 тисяч користувачів [42]. Подібні інциденти не лише демонструють важливість правової бази, але й підтверджують, що саме нормативне врегулювання стає основою успішної безпекової політики.

У сфері медіарегулювання спостерігається тенденція до посилення контролю за діяльністю іноземних інформаційних агентств і платформ, які підозрюються у поширенні ворожих наративів. У 2023 році Іспанія підтримала спільне рішення ЄС щодо обмеження мовлення російських державних медіа, що системно порушували принципи журналістської етики та поширювали антидемократичні меседжі [78]. Водночас країна ухвалила нові внутрішні норми, за якими іноземні медійні агенції зобов'язані розкривати джерела фінансування, структуру власності та механізми редакційної політики [17]. Метою цих вимог стало запобігання прихованому впливу, а також забезпечення гласності діяльності зовнішніх акторів у внутрішньому інформаційному полі. Особливе значення має нормативне забезпечення протидії дезінформації в освітньому просторі. Починаючи з 2021 року в Іспанії впроваджуються освітні стандарти інформаційної грамотності, які включають обов'язкові модулі з критичного мислення, цифрової безпеки та аналізу медіаконтенту для учнів середніх шкіл [23]. У 2024 році уряд затвердив нову рамкову програму, яка зобов'язує шко ли навчати учнів способам розпізнавання маніпуляцій у соціальних мережах, зокрема deepfakes, емоційно забарвлених заголовків та штучно створених новин. Університети, у свою чергу, отримали фінансування для розробки дослідницьких центрів інформаційної стійкості. Очевидно, що така система нормативного супроводу сприяє створенню довгострокової стратегії формування стійкого суспільства, здатного протистояти зовнішнім впливам.

Варто згадати й про механізми парламентського контролю, які відіграють значну роль у забезпеченні прозорості інформаційної політики держави. Комісія з питань національної безпеки парламенту Іспанії регулярно проводить слухання за участю представників уряду, експертів та громадськості, де оцінюється ефективність чинних нормативних актів і визначаються напрями їх оновлення. Наприклад, після масштабної атаки програмного забезпечення Pegasus у 2022 році парламент ініціював всебічну перевірку правових норм, що регулюють діяльність спецслужб у сфері цифрового стеження [41]. Нормативно-правове забезпечення інформаційної безпеки Іспанії також активно взаємодіє із зовнішньополітичними механізмами. Країна бере участь у розробці спільних європейських санкційних режимів проти держав і суб'єктів, які здійснюють інформаційні атаки проти країн-членів ЄС. Так, у 2023-2025 рр. Іспанія підтримала запровадження санкцій проти кількох російських хакерських угруповань, що були причетні до атак на урядові мережі країн Європи [60]. Крім того, Іспанія посилила співпрацю з НАТО у межах Координаційного центру з протидії гібридним загрозам у Гельсінкі, де активно розробляються рекомендації щодо правового регулювання інформаційної оборони [39].

Узагальнюючи викладене, можна стверджувати, що нормативно-правове забезпечення інформаційної безпеки Іспанії є багатовимірним, динамічним та інтегрованим до ширшої європейської системи цифрової стійкості. Іспанія продемонструвала здатність швидко адаптуватися до сучасних викликів, водночас активно впливаючи на формування міжнародних норм. Саме тому її досвід є важливим прикладом для країн, які прагнуть вибудувати ефективну та комплексну систему захисту інформаційного простору в умовах глобальної гібридизації загроз. Водночас постає питання ефективності взаємодії між ключовими інституціями, відповідальними за виконання нормативно-правових актів у сфері інформаційної безпеки. Хоча Іспанія й створила розгалужену мережу структур, таких як Національний центр кібербезпеки (INCIBE), Національний центр криптографії та інформаційної безпеки (CCN),

Державний секретаріат цифрового розвитку, а також спеціалізовані підрозділи в Міністерстві оборони й Міністерстві внутрішніх справ, координація між ними потребує постійного вдосконалення. Саме тому у 2023 році уряд запровадив новий механізм міжвідомчої взаємодії – Платформу оперативного реагування на гібридні загрози, яка об'єднує представників силових структур, експертів з кіберзахисту, аналітиків інформаційних потоків та фахівців зі стратегічних комунікацій. Платформа працює у форматі постійного моніторингу ризиків і, що ключове, дозволяє оперативно реагувати на багатовекторні атаки, у яких кіберінциденти поєднуються з масштабними кампаніями дезінформації.

2.3. Функціонування системи інформаційної безпеки Іспанії в умовах гібридних загроз

У сучасних умовах стрімкої цифровізації, зростання впливу соціальних мереж і безпрецедентної швидкості циркуляції даних іспанська модель забезпечення інформаційної безпеки демонструє дедалі більшу складність та багатовимірність. З одного боку, Іспанія є однією з найбільш цифрово розвинутих країн Європейського Союзу; з іншого – вона стикається з широким спектром гібридних загроз, що поєднують у собі кібернапади, інформаційні операції, маніпулятивні кампанії та технологічні ризики. Внаслідок цього функціонування її системи інформаційної безпеки перетворюється на динамічний процес, який потребує постійного оновлення інструментів, адаптації інституційних рамок і всебічної взаємодії з партнерами ЄС і НАТО. Особливо важливо підкреслити, що після 2022 року, коли зовнішньополітична та безпекова ситуація в Європі різко погіршилася, Іспанія істотно модернізувала підходи до захисту критичної інформаційної інфраструктури [41].

Передусім необхідно зазначити, що ключовим інституційним елементом є Національний центр кібербезпеки (INCIBE), який функціонує як головний координатор державних, приватних і громадських структур, залучених до

боротьби з кіберзлочинністю та інформаційними ризиками [34]. Однак INCIBE не єдине ядро національної системи: важливу роль відіграє також Командування кібероперацій Збройних сил Іспанії, створене відповідно до Стратегічного плану оборони. Воно забезпечує як захист військових мереж, так і активну участь у колективних операціях НАТО, зокрема у спільних навчаннях «Locked Shields 2024», де іспанські команди продемонстрували високі результати у протидії складним моделюванням атак [58]. Примітно, що участь у подібних навчаннях сприяє не лише відпрацюванню технічних навичок, а й координації між різними відомствами, що в умовах гібридних загроз має вирішальне значення. Попри суттєві інституційні успіхи, критично важливо враховувати, що система інформаційної безпеки Іспанії функціонує в постійній напрузі через численні кібератаки, які останніми роками набули більш цілеспрямованого і політично мотивованого характеру. Наприклад, протягом 2023 року було зафіксовано різке зростання атак типу ransomware на об’єкти охорони здоров’я, що змусило уряд активізувати механізми реагування відповідно до Національного протоколу кіберінцидентів [42]. Більше того, у 2024 році стало відомо про спроби проникнення у цифрову інфраструктуру декількох великих іспанських університетів, що свідчило про не лише кримінальний, а й потенційно розвідувальний характер таких операцій [19]. Таким чином, ця ситуація чітко демонструє, що інформаційні загрози стають багатовимірними, а їх мета – не тільки завдати економічної шкоди, а й підірвати довіру суспільства до державних інституцій.

Ще одним визначальним напрямом функціонування системи інформаційної безпеки є протидія дезінформації, що у контексті Іспанії має свої особливості. Оскільки країна характеризується високим рівнем політичної поляризації, поширення маніпулятивних наративів у соціальних мережах здатне істотно впливати на громадську думку [48]. Під час парламентських виборів 2023 року уряд був змушений активізувати створені раніше механізми виявлення фейкових новин, у тому числі співпрацю зі спеціальною платформою FactCheckEU та з Центром аналізу та протидії дезінформації, що

функціонує при Міністерстві внутрішніх справ [17]. Йдеться не лише про технічні засоби моніторингу, а й про стратегічні комунікації, спрямовані на підвищення стійкості суспільства. До цього додається ще один важливий аспект – захист критичної інформаційної інфраструктури, що охоплює енергетичні мережі, транспортні системи, порти, аеропорти й телекомунікаційні платформи. Не випадково в оновленій Стратегії національної безпеки Іспанії 2023 року було наголошено на необхідності створення більш гнучких механізмів управління ризиками, зокрема на рівні автономних співтовариств [41]. Наприклад, Каталонія та Столичний регіон Мадрида вже впровадили власні центри кіберзахисту, які інтегруються в національну систему через спільні протоколи та платформу обміну даними. Результати таких ініціатив стали очевидними, коли у другій половині 2024 року Іспанія успішно нейтралізувала кілька серйозних атак на енергетичний сектор, що були пов’язані з діяльністю іноземних хакерських груп [79].

Крім того, значну увагу приділено регулюванню інформаційного простору. Іспанія активно впроваджує норми Європейського Союзу, зокрема Digital Services Act і Cybersecurity Act [59]. На практиці це означає, що державні органи можуть ефективніше контролювати діяльність великих технологічних платформ, вимагати від них більш прозорих алгоритмів модерації контенту й оперативніше реагувати на поширення шкідливої інформації. У 2024 році уряд оштрафував один з великих цифрових сервісів за невиконання вимог DSA щодо видалення контенту, що містив елементи підбурювання до насильства [27]. Водночас слід підкреслити, що ефективне функціонування системи інформаційної безпеки Іспанії значною мірою залежить від рівня цифрової грамотності населен ня. Уряд реалізує масштабний проєкт Plan Nacional de Competencias Digitales, спрямований на розвиток навичок безпечної поведінки в інтернеті, критичного мислення та здатності розпізнавати фейки [23]. Зрештою, інформаційна безпека в сучасних умовах, це не лише про кіберзахист, а й про формування культури відповідального використання цифрових технологій. Окремої уваги потребує

питання взаємодії держави та приватного сектору. Іспанія є однією з тих країн ЄС, де телекомунікаційні та енергетичні компанії відіграють ключову роль у забезпеченні кіберстійкості [30]. Наприклад, у 2024 році оператор мобільного зв'язку Telefónica спільно з INCIBE запустив інтегровану платформу для раннього виявлення потенційних кіберзагроз у мережах 5G.

Разом з тим, критики часто зазначають, що система інформаційної безпеки Іспанії стикається з низкою труднощів, зокрема браком висококваліфікованих фахівців у галузі кіберзахисту [34]. Як наслідок, у 2025 році розпочато програму стимулювання навчання фахівців з кібербезпеки, пропонуючи стипендії та гранти для студентів технічних закладів. Функціонування системи інформаційної безпеки Іспанії було б неповним без урахування міжнародного виміру її діяльності. Іспанія активно взаємодіє з іншими державами ЄС, з НАТО і з низкою міжнародних організацій. Наприклад, у рамках Європейського центру протидії гібридним загрозам у Гельсінкі вона бере участь у створенні аналітичних моделей для оцінки впливу інформаційних операцій на демократичні процеси [38]. Однак, у контексті гібридних загроз, що постійно еволюціонують, інформаційна безпека Іспанії потребує подальшого удосконалення. Виклики, пов'язані з використанням штучного інтелекту для створення глибоких фейків (deepfakes), а також загрози для виборчих процесів, зумовлюють необхідність формування нових нормативних механізмів [47]. Уже у 2025 році у парламенті почали обговорювати законодавчі ініціативи щодо регулювання алгоритмічних ризиків, зокрема обов'язковість маркування контенту, створеного за допомогою генеративних моделей.

У цьому контексті важливо підкреслити, що однією з найхарактерніших рис функціонування системи інформаційної безпеки Іспанії є її орієнтація на комплексність та багаторівневість реагування [38]. Адже гібридні загрози, на відміну від традиційних військових викликів, не мають чітко визначеного джерела й можуть виходити як від державних, так і від недержавних суб'єктів: хакерських угруповань, екстремістських спільнот, кримінальних мереж чи

навіть окремих осіб, які володіють достатніми технічними ресурсами [9]. У зв'язку з цим Іспанія формує механізми, здатні протидіяти одночасно кільком категоріям ризиків. Зокрема, у 2024 році уряд активізував діяльність Робочої групи з протидії іноземному втручанню, яка діє на основі міжвідомчої координації та включає представників МЗС, Міністерства оборони, Міністерства внутрішніх справ та експертів з цифрової аналітики [41].

Важливою складовою цієї діяльності є аналіз інформаційних потоків, за допомогою якого державні структури намагаються виявити «аномальну активність» у медіапросторі. Такий моніторинг дозволив ідентифікувати кілька кампаній впливу, що мали ознаки зовнішнього походження та були спрямовані на розпалювання соціальних суперечностей всередині країни. Одним із показових випадків стала інформаційна операція навколо масових протестів у Барселоні, коли у 2023 році в соціальних мережах було зафіксовано раптове зростання кількості нових облікових записів, що поширювали радикальні повідомлення. За висновками аналітичних центрів, значна частина цих акаунтів була створена автоматизовано, а їхня діяльність координувалася з-за кордону [17]. Іспанські служби безпеки змогли оперативно локалізувати проблему, що запобігло подальшій дестабілізації регіону.

Окрім того, сучасна система інформаційної безпеки Іспанії активно інтегрує інноваційні технології. У 2025 році було оголошено про запуск державної платформи на основі штучного інтелекту, здатної аналізувати великі масиви даних про кіберінциденти та прогнозувати потенційні загрози [40]. Ця платформа використовує алгоритми машинного навчання для виявлення аномалій у мережевій активності та автоматично повідомляє відповідні відомства про ризики. Такий підхід дозволяє реагувати на загрози ще до того, як вони реалізуються, і, більш того, підвищує швидкість та ефективність роботи оперативних центрів. Подібні технології вже застосовуються в інфраструктурі кількох великих іспанських банків, що значно зменшило кількість успішних атак типу phishing та спроб несанкціонованого доступу до фінансових систем [42]. Показовим є також те, що Іспанія активно впроваджує

моделі публічно-приватного партнерства у сфері інформаційної безпеки [34]. Оскільки значна частина критично важливої інфраструктури належить саме приватним компаніям, держава прагне забезпечити ефективний обмін інформацією про кіберзагрози між усіма зацікавленими сторонами. Для цього у 2024 році було створено спеціальний механізм Crisis Information Exchange, який передбачає регулярні консультації між представниками уряду, телекомунікаційних компаній, банківського сектору та промислових підприємств. Така взаємодія виявилася надзвичайно результативною під час масштабного кіберінциденту у травні 2024 року, коли завдяки спільним діям вдалося оперативно локалізувати потенційно небезпечну атаку на транспортну систему Мадрида [41]. Отже, механізми партнерської взаємодії стають ключовим інструментом підвищення загальнонаціональної стійкості.

Однак, незважаючи на ефективність багатьох інституційних та технологічних рішень, система інформаційної безпеки Іспанії стикається з певними обмеженнями. Насамперед ідеться про складність взаємодії між центральним урядом і автономними співтовариствами, які мають різні рівні цифрової інфраструктури та різні підходи до організації безпеки. У деяких регіонах, наприклад у Валенсії та Андалусії, бракує власних центрів кіберкомунікації, що ускладнює оперативність реагування [58]. У зв’язку з цим у 2025 році уряд започаткував програму гармонізації регіональних стратегій, що передбачає створення єдиного технічного стандарту для обміну даними та координації дій між усіма рівнями влади. Не менш значущим є міжнародний аспект функціонування іспанської системи інформаційної безпеки. З одного боку, Іспанія активно долучається до проєктів ЄС у межах Європейської програми кіберстійкості, Digital Europe та Horizon Europe [31]. З іншого, вона поглиблює співпрацю з НАТО, беручи участь у формуванні стратегічних підходів до реагування на гібридні загрози. Саміт НАТО у Вільнюсі 2023 року став визначальним щодо посилення ролі кіберзахисту у структурі колективної оборони, і Іспанія була однією з країн, що підтримали створення Об’єднаного центру з кібероперацій [20]. Більше того, іспанські фахівці здійснюють аналіз

ризиків, пов’язаних з використанням штучного інтелекту державами-конкурентами, а також беруть участь у спільних тренінгах зі США та Канадою щодо виявлення інформаційних операцій [45].

Суттєвим компонентом міжнародної діяльності є включення Іспанії до глобальної дискусії щодо етичного та відповідального використання штучного інтелекту. У 2024 році країна підтримала Європейський акт про штучний інтелект (AI Act), який запроваджує класифікацію ризиків для цифрових систем та встановлює обмеження на застосування алгоритмів, що можуть створювати серйозні загрози для безпеки [56].

Попри очевидний прогрес, Іспанія усвідомлює, що гібридні загрози змінюються швидше, ніж нормативні системи встигають адаптуватися. Особливо це стосується феномену глибоких фейків, використання яких уже зафіксовано під час місцевих виборів 2024 року [13]. Такі технології здатні суттєво підірвати довіру громадян до політичних процесів, а також створити штучні приводи для соціальних конфліктів. Саме тому уряд розглядає можливість запровадження обов’язкової цифрової ідентифікації для політичної реклами, а також створення державної системи відстеження ШІ-згенерованих матеріалів. Узагальнюючи, можна відзначити, що система інформаційної безпеки Іспанії функціонує як багаторівнева, інтегрована та адаптивна структура, що відбиває сучасні реалії гібридних загроз [6]. Практика останніх років демонструє, що Іспанія поступово переходить від реактивної моделі кіберзахисту до превентивної, що спирається на прогнозування ризиків, підвищення цифрової грамотності та міжнародне співробітництво. Попри всі виклики, країна має стратегічний потенціал для зміцнення власної стійкості: як технологічної, так і суспільної.

Висновки до розділу 2

Слід наголосити, що система інформаційної безпеки Іспанії являє собою багаторівневу та інституційно збалансовану модель, яка поєднує державні структури, спеціалізовані агентства та механізми міжвідомчої координації.

Зокрема, інституційна складова охоплює діяльність Національного центру кібербезпеки (INCIBE), Національного криптологічного центру (CCN-CERT), а також міжміністерських підрозділів, що забезпечують оперативне реагування на кіберінциденти, моніторинг медіапростору та підтримку стратегічних комунікацій. Саме така розгалуженість дозволяє Іспанії ефективно розподіляти повноваження, зберігаючи, водночас, високий рівень узгодженості дій у сфері захисту критичної інформаційної інфраструктури.

Водночас, нормативно-правове забезпечення інформаційної безпеки Іспанії є проактивним і динамічним. Прийняття Закону про кібербезпеку, оновлення національної Стратегії безпеки 2021 року та впровадження директив ЄС, зокрема NIS2, створюють комплексне правове підґрунтя для регулювання цифрового середовища. Крім того, правові акти встановлюють чіткі вимоги до роботи приватного сектору, що є надзвичайно важливим у контексті швидкого технологічного розвитку. Отже, нормативна система формує стабільний каркас для подальшого вдосконалення інституційних механізмів.

Функціонування системи інформаційної безпеки Іспанії в умовах гібридних загроз демонструє високу адаптивність та здатність держави формувати превентивні стратегії. З одного боку, зростання кількості кібератак, кампаній дезінформації та спроб втручання у виборчі процеси вимагає постійного оновлення механізмів реагування. З іншого, Іспанія активно інтегрує власні можливості у загальноєвропейські структури, зміцнюючи співпрацю в межах НАТО та ЄС. У підсумку, можна стверджувати, що іспанська модель інформаційної безпеки є ефективною, оскільки поєднує юридичну чіткість, інституційну гнучкість і стратегічну орієнтацію на ризики гібридного характеру. Саме така синергія забезпечує її стійкість та перспективність у сучасній міжнародній безпековій архітектурі.

РОЗДІЛ 3. НАПРЯМКИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІСПАНІЇ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

3.1. Виклики щодо стійкості системи інформаційної безпеки Іспанії в умовах сучасних гібридних загроз

Попри значні інституційні здобутки та наявність розгалуженої нормативної бази, іспанська система інформаційної безпеки дедалі частіше стикається з багатовимірними викликами, що зумовлені стрімкою еволюцією гібридних загроз. Вони поєднують у собі кібернетичні атаки, кампанії дезінформації, маніпулятивне використання соціальних мереж, економічний тиск і технологічну вразливість інфраструктури. Насамперед варто зазначити, що Іспанія, будучи одночасно членом ЄС і НАТО, перебуває у зоні перетину різних геополітичних інтересів, що підвищує частоту та складність загроз. Зокрема, починаючи з 2022 року, після масштабної ескалації російсько-української війни, активність проросійських кампаній у цифровому просторі Європи, включно з Іспанією, істотно зросла [60]. Це зумовлено прагненням зовнішніх акторів послабити єдність ЄС, вплинути на громадську думку та дискредитувати підтримку України. Саме тому, як зазначають у звітах іспанської Національної криптографічної центри (Centro Criptológico Nacional, CCN), протягом 2023-2025 рр. кількість виявлених спроб проникнення у державні мережі зросла більш ніж на 20%, що свідчить про постійне нарощування атакувального потенціалу недружніх держав і неурядових кібергруп [42].

Кіберзагрози стають особливо небезпечними у контексті захисту критичної інфраструктури. Іспанія входить до п’ятірки європейських лідерів за використанням відновлюваних джерел енергії, що робить її енергетичний сектор водночас інноваційним і вразливим [79]. Енергетичні компанії, включно з Iberdrola та Endesa, регулярно повідомляють про численні спроби втручання у їхні цифрові системи. У 2023 році було публічно підтверджено спробу масштабної атаки на регіональні мережі управління об’єктами

відновлюваної енергії, що могла спричинити локальні перебої у постачанні. Хоча інцидент вдалося вчасно нейтралізувати, він засвідчив, наскільки критично важливим для Іспанії є посилення кіберзахисту інфраструктурних комплексів, які функціонують у тісному зв'язку з цифровими системами [16].

Окремий вимір гібридних загроз – це дезінформація та маніпулятивні інформаційні операції. Іспанія протягом останнього десятиліття неодноразово ставала ціллю зовнішніх кампаній, спрямованих на загострення внутрішніх соціально-політичних розбіжностей. Найвідомішим прикладом залишаються події 2017–2018 років, коли у цифровому середовищі було зафіксовано активне втручання іноземних акторів у перебіг каталонської кризи [17]. Аналітичні звіти ЄС зазначали, що значна кількість онлайн-контенту, поширеного з акаунтів, пов'язаних із Росією та Венесуелою, мала на меті радикалізацію суспільних настроїв і посилення внутрішнього протистояння. Хоча з того часу була суттєво модернізована система унеможливлення зовнішнього втручання, нові технології, зокрема використання штучного інтелекту для створення діпфейків, роблять дезінформаційні кампанії іще складнішими для ідентифікації [27]. Іспанські дослідницькі центри у 2024 році фіксували значне зростання виявлених відеоматеріалів, створених за допомогою генеративного ШІ, які дискредитують політичних лідерів або поширюють неправдиві відомості про міжнародну політику країни [47].

Проблемою, що посилює негативні наслідки гібридних загроз, є нерівномірний рівень цифрової компетентності населення. Хоча Іспанія входить до числа країн ЄС із високими показниками цифровізації та значними державними інвестиціями в розбудову електронного уряду, суспільство все ще залишається недостатньо захищеним від маніпулятивних впливів [25]. Так, за даними Eurobarometer 2023 року, понад 40% іспанських громадян не завжди можуть ідентифікувати неправдивий контент у соціальних мережах, а приблизно третина не перевіряє джерело інформації перед її поширенням. У цьому контексті освітній компонент інформаційної безпеки стає не менш важливим, ніж технологічний. Водночас ускладнюється ситуація у сфері

захисту персональних даних, які дедалі частіше стають об’єктом незаконного збору та продажу. У 2022–2024 роках кількість зафіксованих інцидентів витоку даних зросла, що було пов’язано не лише зі зламами корпоративних мереж, а й із недотриманням правила кібергігієни з боку користувачів [43]. Проблема ускладнюється тим, що сучасні гібридні операції покладаються на масовий аналіз «метаданих», від геолокації до цифрових слідів у мобільних додатках, які дозволяють створювати таргетовані інформаційні впливи.

Особливої уваги заслуговує питання безпеки виборчих процесів. Вибори до Європарламенту 2024 року стали черговою перевіркою для усіх країн ЄС у сфері протидії зовнішньому втручанню. Іспанія у цьому контексті демонструє значну стійкість, але при цьому визнає наявні слабкі місця: відкритість публічної дискусії у соціальних мережах, висока поляризація та, фактично, необмежений потенціал для маніпулятивного контенту [13]. Національний центр кібербезпеки (INCIBE) фіксував підвищену активність бот-мереж під час передвиборчих кампаній, включно з контентом, що мав на меті підірвати довіру до європейських інституцій і внутрішніх політични х сил [26].

Сучасні гібридні загрози включають також економічні аспекти, зокрема залежність від зовнішніх технологічних платформ і постачальників обладнання. Іспанія, попри розвиток власного технологічного сектору, все ще значною мірою покладається на іноземні продукти у сферах телекомунікацій, хмарних сервісів та апаратного забезпечення. Розгортання 5G інфраструктури стало предметом активних розслідувань і дискусій про потенційні ризики, пов’язані зі співпрацею з окремими китайськими компаніями [49]. Уряд у 2023 році ухвалив нові правила сертифікації обладнання для критичних секторів, однак повна технічна автономія залишається віддаленою перспективою. Варто також врахувати, що гібридні загрози мають не лише зовнішнє, а й внутрішнє походження. Поширення радикальних і популістських меседжів, зростання політичної поляризації, використання маніпулятивної риторики в медіа підвищують вразливість суспільства [48]. Такі процеси, зокрема у контексті дебатів щодо міграції, економічної політики або реформ автономних регіонів,

активно підхоплюються зовнішніми акторами, що створює мультиплікативний ефект інформаційної дестабілізації.

Нарешті, важливим залишається фактор технологічного розвитку, який одночасно розширює можливості захисту та збільшує ризики. Штучний інтелект, великі дані, автоматизовані системи аналізу загроз є ключовими інструментами кібероборони Іспанії [40]. Проте ті самі технології активно використовують і противники. У 2024 році INCIBE повідомляв про зростання атак з використанням алгоритмів машинного навчання, які дозволяють значно обійти стандартні механізми захисту [42]. Поряд із цим важливим викликом, про який часто згадують науковці, є необхідність формування цілісної системи стратегічної комунікації [17]. Іспанія, як і багато країн ЄС, все ще рухається шляхом інституційного узгодження між різними відомствами, що відповідають за інформаційну політику, цифрове врядування та національну безпеку. У межах боротьби з дезінформацією активно діє структура «Equipo de Respuesta ante Incidentes» (CERT), однак її діяльність інколи ускладнюється браком координації з іншими міністерствами, зокрема Міністерством оборони, Міністерством внутрішніх справ та Міністерством у справах цифрової трансформації. Саме через це механізми швидкого оприлюднення достовірної інформації або спростування фейкових повідомлень не завжди працюють належним чином. У періоди криз, наприклад під час масштабних лісових пожеж 2023 року чи хвиль міграційної напруги, в інформаційному просторі поширювалися фейкові наративи, які доводилося спростовувати постфактум [55]. Це свідчить про необхідність створення інтегрованої системи комунікації держави з громадянами, що унеможливило б маніпулятивний вплив у критичні моменти.

Не менш важливою залишається потреба постійного оновлення національної нормативно-правової бази, яка має відповідати інноваційним технологічним викликам. Іспанія вже адаптувала низку директив ЄС у сфері кібербезпеки, включно з NIS2, упровадженою у 2023–2024 роках, що суттєво підвищила вимоги до приватних компаній і секторів критичної інфраструктури

[59]. Проте експерти зазначають, що нормативні акти часто не встигають за темпами розвитку цифрових технологій, а отже, необхідне більш системне використання механізмів прогнозування технологічних ризиків та регулярних аудитів кіберстійкості. У цьому контексті важливо згадати про дискусії навколо правового регулювання генеративного ШІ, які тривають в Іспанії з початку 2024 року [44]. Питання створення стандартів відповідальності за контент, згенерований ШІ, один із найскладніших викликів для законодавців, адже він напряму пов'язаний із ризиками для інформаційної безпеки та демократичних процесів. Крім того, глобальна конкуренція у сфері цифрових технологій створює додаткове навантаження на іспанську модель інформаційної безпеки, адже країна мусить одночасно забезпечувати свою технологічну незалежність та інтегрованість у європейські й трансатлантичні структури. Залежність від іноземних технологічних рішень, у сфері телекомунікацій, хмарних сервісів, оборонних систем, ставить Іспанію в умовно вразливе становище, оскільки будь-які політичні коливання між постачальниками можуть трансформуватися у стратегічні ризики [34]. Саме тому Іспанія активно долучається до європейських проєктів на кшталт EU Cyber Solidarity Act чи ініціативи щодо створення єдиної системи кіберзахисту ЄС, яка передбачає формування мережі центрів оперативного реагування та аналітичних платформ обміну даними між державами-членами [31].

Поряд із міжнародною співпрацею, велику роль відіграє внутрішня здатність держави забезпечувати інформаційну стійкість суспільства. Тут особливу увагу привертає проблема медіаграмотності, яка у XXI столітті стала ключовим елементом національної безпеки [23]. У відповідь на гібридні загрози Іспанія реалізує численні освітні ініціативи, спрямовані на підвищення здатності громадян критично оцінювати інформацію. Зокрема, у 2024 році були запущені програми спільно з Європейською Комісією та платформами Meta, YouTube і X щодо маркування потенційно маніпулятивного контенту [27]. Проте, як зазначають експерти, формування критично мислячого

суспільства, процес тривалий і потребує постійної взаємодії між освітніми установами, державою та приватними компаніями.

На додачу, одним із фундаментальних викликів є швидке зростання кіберзлочинності, яка дедалі частіше набуває характеристик гібридності [38]. Організовані злочинні угруповання та кібератори, пов’язані з іноземними спецслужбами, нерідко діють у взаємодії, поєднуючи фінансові злочини, викрадення даних і інформаційні операції. У 2023-2025 рр. Іспанія фіксувала різке збільшення кількості атак типу ransomware проти муніципалітетів, лікарень та освітніх установ [74]. Наприклад, у лютому 2024 року масштабна атака на лікарню в Барселоні тимчасово паралізувала її цифрову інфраструктуру, що призвело до відтермінування медичних процедур та ускладнило роботу персоналу [19]. Парадоксальним чином такі інциденти демонструють, наскільки тісно переплетені інформаційна безпека, життєдіяльність суспільства і функціонування держави у сучасному середовищі.

Ураховуючи зазначені виклики, можна стверджувати, що забезпечення стійкості інформаційної безпеки Іспанії в умовах гібридних загроз потребує багаторівневого підходу. По-перше, необхідне подальше вдосконалення технологічної інфраструктури, створення систем раннього виявлення аномалій та автоматизованих платформ аналізу загроз. По-друге, потрібне зміцнення координаційних механізмів між державними структурами, що дозволить швидко реагувати на кризові ситуації та запобігати інформаційним атакам ще на початковому етапі. По-третє, актуальною залишається потреба у формуванні високого рівня медіаграмотності населення, адже саме вона визначає ступінь вразливості суспільства до дезінформації. По-четверте, Іспанія має активніше інтегруватися у спільні європейські ініціативи з кіберзахисту та інформаційної стійкості, адже гібридні загрози не знають державних кордонів [39].

Отже, сучасний стан інформаційної безпеки Іспанії перебуває у фазі активного розвитку, проте він супроводжується складними викликами, що

виникають унаслідок поєднання політичних, технологічних, соціальних і глобальних факторів. Гібридні загрози змінюються настільки швидко, що традиційні моделі безпеки вже не здатні повністю забезпечити захист. Саме тому Іспанія має продовжувати модернізацію всіх складових своєї інформаційної стратегії, від інституційної архітектури до технологічних платформ і механізмів взаємодії з громадянами. Лише за умови системного та інтегрованого підходу держава зможе сформувати справді стійку модель інформаційної безпеки, яка відповідатиме викликам сучасного гібридного середовища та забезпечить стабільність політичної системи, економіки й демократичних процесів.

3.2. Роль міжнародного співробітництва у забезпечення інформаційної безпеки Іспанії

Іспанія, опинившись у центрі зростаючих гібридних загроз, дедалі активніше інтегрує міжнародне співробітництво у власну систему забезпечення інформаційної безпеки, оскільки саме транснаціональний вимір таких загроз робить національні ресурси недостатніми для їх ефективного стримування. Зрештою, навіть найпотужніші держави, стикаючись із кібератаками, дезінформаційними кампаніями або технологічним шантажем, приходять до висновку, що колективні механізми реагування, а також узгоджені міжнародні стандарти стають критично необхідними [15]. Зокрема, Іспанія в останні роки демонструє зважений і водночас стратегічно вивірений курс на зміцнення міжнародних партнерств у сфері кібербезпеки, цифрового врядування та протидії дезінформації. Причому не лише в межах ЄС і НАТО, а й у співпраці з ООН, OECD, ENISA, групою держав Latin Cybersecurity Initiative і навіть з окремими технологічними корпораціями, що формують глобальний цифровий простір [58].

Передусім, необхідно наголосити, що Іспанія традиційно виступає одним із прихильників зміцнення європейської архітектури інформаційної та кібербезпеки. У цьому контексті важливим кроком стало активне залучення

країни до реалізації Європейської стратегії кібербезпеки 2020 року, спрямованої на формування стійкого та безпечного цифрового ринку [1]. Цей документ, як відомо, зосереджений на трьох ключових напрямках: стійкість критичної інфраструктури, оперативне реагування на інциденти і посилення колективної кібероборони. З огляду на це Іспанія значно розширила функціонал Національного інституту кібербезпеки (INCIBE), який взаємодіє з ENISA для створення європейських центрів компетенцій [30]. Наприклад, у 2023 році Іспанія долучилася до роботи Європейського центру з протидії кіберзлочинності Europol, що дозволило запровадити спільні тренінги та обмін оперативними даними щодо нових типів кібератак, зокрема атак на інфраструктуру дронів і системи штучного інтелекту. Водночас, не менш важливою складовою міжнародної взаємодії Іспанії є співпраця в рамках НАТО, оскільки Альянс ще з 2016 року визнав кіберапростір окремим операційним доменом, що зробило питання колективної кібероборони елементом статті 5 [20]. Як наслідок, Іспанія активно підтримує оновлення кіберстратегії НАТО 2021 року та бере участь у навчаннях типу Cyber Coalition, у яких задіяні понад 30 держав. У 2024 році Іспанія направила власну групу експертів до НАТО Cooperative Cyber Defence Centre of Excellence (Таллінн), де вони долучилися до відпрацювання сценаріїв захисту енергетичних систем від атак типу ransomware.

Крім того, міжнародні формати дають змогу Іспанії ефективно протидіяти дезінформаційним кампаніям, що, між іншим, стали особливо інтенсивними після 2022 року. Зростання кількості російських і китайських інформаційних впливів, спрямованих на поляризацію іспанського суспільства, спонукало країну активізувати роботу в межах ЄС щодо імплементації Європейського плану дій проти дезінформації (2018) та створення мережі EU vs Disinfo [27]. У 2023–2024 роках Іспанія була серед основних учасників розробки спільних стандартів прозорості політичної реклами в мережі, а також ініціатив зі встановлення відповідальності платформ за швидке видалення ворожих інформаційних операцій [17]. Більш того, у співпраці з Францією та

Німеччиною МЗС Іспанії долучилося до створення європейської системи раннього попередження про інформаційні атаки, яка вже у 2025 році продемонструвала ефективність під час відстеження координованих кампаній щодо дискредитації саміту ЄС-CELAC у Мадриді. Не можна оминути увагою й співпрацю Іспанії у межах Ради Європи, особливо у контексті виконання Будапештської конвенції про кіберзлочинність та її Протоколу 2022 року щодо посиленої транскордонної співпраці [59]. Іспанські кіберполіційні підрозділи, зокрема Brigada de Investigación Tecnológica, активно взаємодіють з іноземними партнерами у сфері обміну цифровими доказами, що дозволяє прискорити розслідування складних кіберзлочинів.

У ширшому міжнародному контексті важливим є те, що Іспанія активно підтримує діяльність ООН щодо формування глобальних правил поведінки держав у кіберпросторі. Зокрема, Мадрид бере участь у дискусіях Групи урядових експертів ООН щодо недопущення застосування ІКТ для підриву міжнародної стабільності [41]. Показово, що країна також підтримує впровадження Digital Geneva Convention, запропонованої Microsoft, яка передбачає відповідальність держав за створення кіберзброї. У цьому контексті варто виокремити й трансрегіональні ініціативи. Іспанія активно співпрацює з країнами Латинської Америки, просуваючи спільні програми INCIBE з кіберосвіти та обміну інформацією про загрози [6]. У 2023 році було запущено платформу Ciberseguridad LATAM–España, яка поєднує аналітичні центри Аргентини, Чилі та Колумбії.

Окремої уваги потребує співпраця Іспанії з приватним сектором, яка стала невід’ємною частиною міжнародних механізмів кіберзахисту. Перш за все, Іспанія входить до Microsoft Government Security Program, що дає можливість Іспанському цен тру реагування на кіберінциденти (CERTSI) отримувати інформацію про вразливості програмного забезпечення до їх публікації [34]. У 2024 році Мадрид підписав додаткову угоду з Google щодо захисту хмарних сервісів органів державної влади, а також впровадив політику Zero Trust у співпраці з Cisco та Deloitte. Більш того, міжнародна взаємодія

сприяє формуванню стратегічної культури безпеки, яка спрямована на попередження загроз, а не лише на реагування на них [38]. Це проявляється у формуванні спільних навчань, семінарів і міжурядових зустрічей, де Іспанія бере активну участь. У 2024 році Мадрид став місцем проведення глобальної конференції CyberSec@EU, під час якої країни ЄС узгодили рамкові підходи до захисту систем штучного інтелекту від маніпулятивного використання. Іспанія виступила ініціатором створення нового механізму аудиту безпеки алгоритмів, який уже тестується у співпраці з Європейською комісією [56]. Це свідчить не лише про високий авторитет Іспанії, але й про її амбіцію впливати на вироблення європейських та міжнародних стандартів у сфері цифрової безпеки.

Важливо й те, що Іспанія активно підтримує розвиток кіберспроможностей партнерів, особливо тих держав, які стикаються з масштабними інформаційними загрозами. Через проєкти з кіберосвіти, консультацій та технічної допомоги Іспанія сприяє підвищенню цифрової стійкості країн Східного партнерства, Латинської Америки та Північної Африки [30]. Така політика не лише створює мережу союзників, здатних спільно протидіяти загрозам, але й підвищує геополітичний вплив самої Іспанії. У цьому сенсі міжнародне співробітництво стає не лише інструментом захисту, але й інструментом проєкції м’якої сили та зміцнення стратегічних позицій держави у світі. Разом із тим, ефективність міжнародних партнерств значною мірою залежить від здатності Іспанії інтегрувати отримані напрацювання у внутрішні механізми безпеки. Це стосується як модернізації правових норм, так і посилення інституційної взаємодії між державними структурами та приватним сектором. Наприклад, імплементація Директиви NIS2 стала каталізатором реформ у сфері контролю за кіберризиками у критичних секторах, зокрема в енергетиці, транспорті та фінансовій системі [59]. Міжнародні консультації відіграли ключову роль у розробці механізмів сертифікації кібербезпеки для операторів критичної інфраструктури, які Іспанія адаптувала відповідно до власних стандартизованих вимог [34].

Зрештою, міжнародне співробітництво Іспанії у сфері інформаційної безпеки поступово формує таку модель, де зовнішня та внутрішня безпека взаємопов'язані та взаємозалежні. Іспанія не просто отримує доступ до досвіду партнерів, але й сама вносить суттєвий внесок у спільну безпекову екосистему. Цей взаємообмін знаннями і технологіями дозволяє державі не тільки зменшувати власну вразливість, але й робити внесок у формування стійкого та передбачуваного міжнародного цифрового середовища. Через активну участь у глобальних і регіональних коаліціях Іспанія фактично створює багатошарову систему безпеки, що поєднує превентивні, оперативні та стратегічні складові. Міжнародне співробітництво для Іспанії перестає бути факультативним компонентом державної політики у сфері інформаційної безпеки. Воно перетворюється на системний фундамент, без якого неможливо гарантувати належний рівень стійкості критичної інфраструктури, ефективність механізмів кіберзахисту та здатність держави протистояти динамічним гібридним впливам. Завдяки міжнародним партнерствам Іспанія отримує доступ до найновіших технологічних рішень та спеціалізованих наукових розробок, що відіграє особливу роль в епоху штучного інтелекту, машинного навчання та швидкоплинних кіберзагроз. Таким чином, Іспанія не тільки адаптується до нових викликів, але й долучається до їх передбачення, що робить її одним із провідних європейських центрів з інновацій у галузі кібербезпеки.

3.3. Використання досвіду Іспанії у зміцненні інформаційної безпеки України в умовах гібридних загроз

Україна, стикаючись із затяжною гібридною агресією з боку Російської Федерації, потребує оновлених, системно інтегрованих і водночас практично орієнтованих підходів до зміцнення власної інформаційної безпеки. У цьому контексті, як свідчить порівняльний аналіз, надзвичайно цінним є досвід Іспанії, яка за останні десятиліття сформувала багаторівневу, технологічно розвинену та нормативно врегульовану інфраструктуру захисту національного

інформаційного простору [6]. Передусім варто звернути увагу на те, що іспанська модель стала результатом послідовного розвитку у рамках ширших європейських безпекових процесів, зокрема стратегій ЄС із протидії дезінформації, кіберзагрозам та інформаційним впливам третіх держав [58]. Отже, українська держава, адаптуючи ключові інструменти, здатна значно посилити власну стійкість у середовищі гібридних загроз, які з кожним роком набувають дедалі складніших форм.

Першим важливим аспектом досвіду Іспанії є розбудова інституційної архітектури, що забезпечує координацію між державними органами, приватним сектором і громадянським суспільством. Зокрема, створення Національного центру кібербезпеки (INCIBE), діяльність якого охоплює моніторинг кіберінцидентів, реагування на атаки, проведення навчань і підготовку фахівців, стало фундаментальним кроком у зміцненні інформаційного захисту країни [34]. Україна, безумовно, уже має низку подібних інститутів, таких як Державна служба спеціального зв'язку та захисту інформації, але, беручи до уваги іспанський досвід, можна поглибити міжвідомчу взаємодію, стандартизувати обмін даними й удосконалити систему раннього попередження про загрози. Наприклад, у 2023 році INCIBE впровадив новий механізм спільного реагування на масові фішингові кампанії, що дозволило зменшити наслідки атак на національні компанії [42]. Україні було б доцільно адаптувати аналогічні механізми у відповідь на постійні російські кібератаки, спрямовані на енергетичні та телекомунікаційні об'єкти.

У цьому ж контексті особливо актуальним є розвиток державного управління ризиками, який в Іспанії здійснюється шляхом регулярного оновлення національних стратегій і планів кіберстійкості. Так, стратегія 2023 року акцентує увагу на протидії іноземним інформаційним операціям, які спрямовані на внутрішньополітичну дестабілізацію [16]. Україна, яка пережила низку масштабних інформаційних спецоперацій, повинна інтегрувати подібні підходи, зокрема розширюючи мережу моніторингу інформаційних потоків, що циркулюють у соціальних мережах. Адже саме там

розгортається значна частина російських кампаній, спрямованих на підрив довіри до державних інституцій, дискредитацію оборонних зусиль чи маніпулювання суспільними настроями.

З іншого боку, досвід Іспанії переконує, що ефективність інформаційної безпеки визначається не лише технічними ресурсами, а й нормативно-правовою базою. Іспанія однією з перших у ЄС запровадила комплексне законодавство щодо цифрових прав, що дозволяє регулювати питання збору даних, їхнього захисту, а також відповідальності держави й приватних структур за інформаційні порушення [59]. Україна, вже зробивши значний крок у напрямку євроінтегрованих стандартів, зокрема ухваливши закон «Про захист персональних даних» у новій редакції, могла б надалі переймати іспанські підходи до цифрових прав як інструменту формування довіри між державою та громадянами. До прикладу, Іспанія активно розвиває етичні принципи використання штучного інтелекту в державному управлінні, що стає актуальним і для України, де цифрові сервіси активно інтегруються у повсякденне життя громадян [44].

Не менш важливим компонентом іспанського досвіду є стратегічна комунікація, яка ґрунтується на відкритості, швидкості реагування та прозорості. Іспанський уряд має окремі підрозділи, відповідальні за боротьбу з дезінформацією, які працюють у партнерстві з Європейською службою зовнішніх дій та міжнародними аналітичними центрами [27]. Вони щоденно аналізують інформаційні тенденції, виявляють ворожі наративи та оперативно їх нейтралізують. Україні, якій доводиться протистояти системним дезінформаційним кампаніям, варто зміцнити власні спроможності у сфері стратегічних комунікацій, створивши єдину міжвідомчу платформу для аналізу та оперативного реагування, подібну до іспанської моделі. Окрему увагу слід звернути на іспанські програми підготовки кадрів, адже саме кваліфікований людський ресурс забезпечує стійкість інформаційної системи. В Іспанії діють спеціалізовані академії та навчальні курси для держслужбовців, журналістів і фахівців приватного сектору, у межах яких формуються навички

реагування на гібридні загрози [30]. В Україні також відбувається активний розвиток освітніх програм з кібербезпеки, однак, використовуючи іспанський підхід, можна посилити міждисциплінарність таких програм, поєднавши технічну, правову та комунікаційну підготовку.

Окремо варто наголосити на взаємодії Іспанії з Європейським Союзом та НАТО. Іспанія активно бере участь у розробці європейських механізмів протидії дезінформації, а також у проєктах Альянсу, таких як платформа Cooperative Cyber Defence Centre of Excellence [20]. Україна, яка вже є учасником цілого спектра програм ЄС і НАТО, може значно посилити свої позиції, інтегрувавши іспанський досвід участі у міжнародних кіберінціативах.тСеред інших важливих напрямів іспанського досвіду – взаємодія держави з медіасектором. Іспанія активно інвестує в медіаграмотність і підвищення критичного мислення населення, що охоплює шкільні програми, громадські ініціативи й навіть спеціальні курси для людей старшого віку [23]. Подібна практика могла б суттєво підвищити інформаційну стійкість України.

Значним у контексті іспанського досвіду є й питання захисту критичної інфраструктури. У країні створено спеціальні протоколи співпраці між державою і приватними компаніями, які зобов’язані звітувати про кіберінциденти протягом короткого часу [41]. Для України, що неодноразово переживала атаки на енергетичну систему, адаптація цього досвіду є вкрай важливою. Важливим прикладом для України є іспанський підхід до оцінювання ефективності політик інформаційної безпеки. В Іспанії щорічно публікують аналітичні звіти про інформаційні загрози, у яких визначають динаміку атак, ефективність реагування й ключові тенденції [41].

Водночас важливо підкреслити, що ефективне використання іспанського досвіду вимагає врахування специфічних особливостей українського безпекового середовища, яке характеризується прямою воєнною агресією, інтенсивним інформаційним тиском і постійними спробами зовнішніх акторів вплинути на політичні та соціальні процеси в країні. Проте саме ці виклики

роблять адаптацію іспанських підходів не просто корисною, а необхідною. Адже Іспанія, попри відсутність прямої воєнної загрози, також тривалий час стикалася з екстремістськими рухами, терористичними організаціями та інформаційними кампаніями з боку третіх держав, що стимулювало її до створення високоефективної системи стратегічної комунікації та інформаційної протидії [6]. Україна може перейняти практики, які в Іспанії використовуються для забезпечення прозорої комунікації між державними структурами та громадянами під час загострень, адже такі механізми сприяють зниженню рівня паніки, попередженню маніпуляцій і підвищенню довіри до інституцій влади.

На особливу увагу заслуговує також іспанський досвід інтеграції інформаційної безпеки у систему національної освіти. Шкільні програми з медіаграмотності, що були оновлені у 2021-2022 рр., містять модулі щодо аналізу джерел інформації, розпізнавання дезінформації та фейкових новин, а також основ цифрової безпеки [23]. Для України, де питання критичного мислення стає фактором національної безпеки, масштабування подібних освітніх програм є стратегічним завданням. Це особливо актуально під час тривалих інформаційних атак, які супроводжують активні фази війни. Крім того, варто застосовувати іспанську модель партнерства між державою і технологічними компаніями, спрямовану на розробку освітніх платформ і проведення інноваційних тренінгів. Наприклад, у 2023 році Іспанія спільно з провідними IT-компаніями запустила програму «Digital Security for All», що охоплює як молодь, так і осіб старшого віку [30]. Для України такі програми можуть стати важливою частиною інформаційної оборони, особливо враховуючи потребу в підготовці великої кількості фахівців. Не менш важливою є організація системи кібергігієни, один із пріоритетів іспанської державної політики, що охоплює регулярне проведення інформаційних кампаній, тренінгів і тестувань цифрових навичок серед населення [34]. Україна, попри значні успіхи в цифровізації, потребує ширшого впровадження таких практик, насамперед у державному секторі, де людський фактор

залишається одним із найвразливіших елементів інформаційної безпеки. Іспанський досвід свідчить, що систематичні тестування персоналу, моделювання кібератак і впровадження процедур перевірки доступу можуть істотно підвищити загальну стійкість системи. Окрім цього, в Іспанії широко застосовується практика «червоних команд», груп фахівців, які імітують атаки для перевірки готовності інституцій [42].

Окрім того, одним із ключових напрямів адаптації іспанського досвіду є формування ефективного механізму взаємодії між державою та медіасектором. Іспанія вибудувала систему партнерств із журналістськими організаціями, редакціями, громадськими інститутами та незалежними фактчекінговими платформами [17]. Вони виконують важливу роль у попередженні дезінформації, оперативному спростуванні неправдивих повідомлень і виробленні стандартів відповідальної журналістики. В українському контексті такі практики можуть бути адаптовані шляхом створення міжсекторних аналітичних платформ, які, подібно до іспанських ініціатив, забезпечуватимуть швидку перевірку інформації та спільне реагування на інформаційні інциденти. Ще одним корисним елементом іспанського досвіду є розвиток регіональних центрів інформаційної безпеки. Іспанія має розгалужену мережу центрів, які здійснюють аналіз інформаційних загроз на місцевому рівні, що дозволяє підвищувати ефективність реагування на регіональні інциденти [41]. Україна, враховуючи свої територіальні особливості та масштабність гібридних атак, могла б застосувати цей досвід, створивши центри інформаційної стійкості в кожному регіоні.

У сфері законодавчого регулювання варто згадати, що Іспанія активно впроваджує європейські стандарти захисту даних, зокрема положення Загального регламенту про захист даних (GDPR) [7]. Україна, рухаючись шляхом європейської інтеграції, має можливість не лише гармонізувати власні норми із законодавством ЄС, а й адаптувати іспанські механізми регуляції у сфері цифрових прав громадян. Досвід Іспанії свідчить, що надійна система захисту даних підвищує рівень довіри громадян до державних цифрових

сервісів і створює передумови для розбудови ефективної моделі електронного врядування [58]. У міжнародному вимірі іспанська модель може бути корисною Україні через активну участь Іспанії у формуванні європейської п олітики з протидії дезінформації. Зокрема, Іспанія має розвинену систему співпраці з Європейською Службою зовнішніх дій та платформою EUvsDisinfo [78]. Україна могла б суттєво посилити власну міжнародну інформаційну присутність, розширивши участь у подібних ініціативах і формуючи спільні механізми реагування на інформаційні загрози.

Переваги іспанського підходу полягають також у його довгостроковій стратегічності. Іспанія розглядає інформаційну безпеку не як реакцію на кризи, а як безперервний структурний процес, що пронизує всі рівні державного управління [65]. Україні варто взяти до уваги цю модель, формуючи довгострокові плани, спрямовані на модернізацію кіберінфраструктури, посилення кадрового потенціалу, розвиток інформаційної культури та інтеграцію новітніх технологій.

Зазначимо, що досвід Іспанії є надзвичайно корисним для України з огляду на комплексність, інституційну структурованість і стратегічну цілісність підходів [14]. Застосування іспанських практик у національній моделі інформаційної безпеки України не передбачає механічного копіювання, натомість вимагає глибокої адаптації до умов війни, обмежених ресурсів та постійних інформаційних атак. Проте ключові елементи: ефективна координація, законодавче регулювання, стратегічні комунікації, освіта, міжнародне співробітництво та захист критичної інфраструктури, можуть істотно підвищити спроможність України протистояти гібридним загрозам. Зрештою, Іспанія демонструє, що інформаційна безпека – це насамперед здатність держави й суспільства діяти злагоджено, швидко та на основі довіри. Саме цього нині потребує Україна, вибудовуючи свій шлях до перемоги й довгострокового зміцнення демократичних інститутів.

Висновки до розділу 3

Слід підкреслити, що система інформаційної безпеки Іспанії зазнає зростаючого тиску сучасних гібридних загроз, які, своєю чергою, змінюють характер національної та європейської безпеки. Зокрема, дедалі більшої ваги набувають такі виклики, як кібератаки на критичну інфраструктуру, дезінформаційні кампанії та маніпуляції у цифровому середовищі, що спрямовані на підрив суспільної довіри й дестабілізацію державного управління. Водночас Іспанія, реагуючи на нові ризики, поступово зміцнює інституційні механізми стійкості, модернізує законодавчу базу та розвиває цифрову грамотність населення. Усе це, безумовно, сприяє формуванню більш адаптивної та прогнозованої архітектури інформаційної безпеки.

Поряд із цим важливо наголосити, що міжнародне співробітництво посідає ключове місце у забезпеченні інформаційної стійкості Іспанії. Через спільні ініціативи в межах ЄС, НАТО та Європейської ради з питань кібербезпеки держава отримує доступ до передових технологій, експертних ресурсів і механізмів швидкого реагування. Більш того, координація зусиль дозволяє ефективніше нейтралізувати транснаціональні загрози, які не визнають державних кордонів. Таким чином, як показує практика, Іспанія значною мірою покладається на багаторівневі партнерства, що підсилюють її власні можливості та забезпечують колективну безпеку.

Нарешті, використання іспанського досвіду має суттєве значення для України, адже саме Іспанія демонструє ефективні підходи до побудови цілісної, гнучкої та інклюзивної системи інформаційної безпеки. Україна, враховуючи власні реалії гібридної війни, може імплементувати найкращі практики у сфері протидії дезінформації, кіберзахисту, міжвідомчої координації та розвитку стратегічних комунікацій. До того ж, з огляду на перспективи європейської інтеграції, адаптація іспанських моделей посилить сумісність українських інституцій із європейськими стандартами та сприятиме формуванню стійкого національного інформаційного простору.

ВИСНОВКИ

У результаті дослідження особливостей функціонування інформаційної безпеки Іспанії в умовах гібридних загроз, зроблено наступні висновки:

1. З’ясовано, що інформаційна безпека держави являє собою багатовимірну категорію, яка охоплює як захист інформаційного простору від зовнішніх і внутрішніх впливів, так і забезпечення належного функціонування ключових інституцій, здатних протидіяти деструктивним інформаційним потокам. Її структура, як показано у дослідженні, включає нормативно-правовий, організаційно-інституційний, технологічний та соціально-комунікаційний компоненти, що разом формують стійкість держави до широкого спектра загроз. Водночас типологія гібридних загроз свідчить про їх прихований, багатокомпонентний і довготривалий характер: інформаційно-психологічний вплив, підрив довіри до державних інституцій, поширення дезінформації, втручання у виборчі процеси, маніпуляції у кіберпросторі.

2. Дослідження механізмів забезпечення інформаційної безпеки продемонструвало, що Іспанія виробила багаторівневу систему реагування на гібридні загрози, яка, однак, продовжує адаптуватися до нових умов. Центральна роль у ній належить інституціям, що координують дії у сфері кібербезпеки, стратегічних комунікацій та боротьби з дезінформацією, зокрема Національному центру кібербезпеки, Департаменту національної безпеки при уряді, а також спеціалізованим підрозділам у складі збройних сил та правоохоронних органів. Як показало дослідження, ключові інституційні механізми в Іспанії спрямовані не лише на реагування, але й на раннє виявлення інформаційних загроз, що дозволяє мінімізувати потенційну шкоду. Водночас, слід наголосити, що ефективність таких механізмів значною мірою залежить від координації між секторами безпеки, місцевими органами влади, медіа та громадянським суспільством, яке активно залучене до протидії маніпуляціям та фейковим наративам.

3. Розкрито нормативно-правове забезпечення інформаційної безпеки Іспанії, без якого жодна інституційна система не може функціонувати

ефективно. Аналіз законодавчих актів, від Національної стратегії безпеки до спеціалізованих актів у сфері кіберзахисту та захисту критичної інфраструктури, дозволив зрозуміти, що Іспанія дотримується системного підходу та постійно оновлює нормативну базу відповідно до змін міжнародного безпекового середовища. Законодавство визначає чіткі рамки діяльності органів влади, механізми взаємодії між ними, а також юридичні інструменти для нейтралізації дезінформації та зовнішнього втручання. Саме завдяки такій гнучкій нормативній базі, як з'ясовано, Іспанія здатна адаптивно реагувати на нові форми гібридної агресії, що, відповідно, підвищує рівень національної стійкості.

4. У ході визначення особливостей функціонування системи інформаційної безпеки Іспанії виявлено, що її ефективність формується на перетині кількох ключових чинників: технологічної спроможності держави, наявності розвинених інститутів стратегічних комунікацій, стабільної нормативної бази та активної участі у міжнародних ініціативах. Втім, існують і суттєві виклики. Серед них: швидкі темпи технологічних змін, ускладнення кіберзагроз, використання штучного інтелекту у дезінформаційних операціях, залежність інформаційної безпеки від приватних технологічних компаній, а також фрагментація медіапростору. Більше того, сучасні гібридні загрози посилюються загальноєвропейськими викликами, зокрема війною РФ проти України, що, як показує практика, спричиняє значне зростання інтенсивності інформаційних атак на країни ЄС, включно з Іспанією. Отже, стійкість системи інформаційної безпеки залежить від здатності держави не лише модернізувати технічні можливості, але й гармонізувати політику, комунікацію та взаємодію між секторами.

5. З'ясовано, що співпраця в межах ЄС, НАТО та спеціалізованих кіберцентрів дозволяє Іспанії отримувати доступ до сучасних технологій, обмінюватися даними про загрози, брати участь у спільних тренуваннях та випрацьовувати єдині підходи до протидії дезінформації. Міжнародні партнерства підвищують не лише національну, але й колективну стійкість.

Важливо, що Іспанія активно ділиться власним досвідом, який, може бути корисним для України. Зокрема, це стосується створення національної мережі стратегічних комунікацій, вдосконалення законодавства у сфері кіберзахисту, зміцнення взаємодії між державою та медіасектором, а також розвитку освітніх програм з медіаграмотності. Україна, зважаючи на тривалий досвід протидії масштабним інформаційним операціям, може адаптувати іспанські інституційні практики з урахуванням власних умов.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Вознюк Є., Андрюхіна В. Порівняльний аналіз кібербезпеки Європейського Союзу. *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2025. Вип. 2. URL: https://relint.vnu.edu.ua/index.php/relint/article/download/454/417 (дата звернення: 5.10.2025).

2. Гончаров М.В. Дослідження поняття «інформаційна безпека». *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. Вип. 82. ч. 1. С. 34-37. URL: https://doi.org/10.24144/2307-3322.2024.82.1.4 (дата звернення: 5.10.2025).

3. Дрига Д. Аналіз правових механізмів забезпечення інформаційної безпеки інформаційної інфраструктури Європейського Союзу. *Herald of Khmelnytskyi National University. Economic Sciences*. 2024. № 334(5). С. 46–51. DOI: https://doi.org/10.31891/2307-5740-2024-334-7 (дата звернення: 5.10.2025).

4. Кавин С.Я. Правові засади забезпечення кібербезпеки в державах – членах Європейського Союзу. *Актуальні проблеми держави і права*. 2020. Вип. 51. С. 51-58. URL: https://doi.org/10.32837/apdp.v0i87.2797 (дата звернення: 5.10.2025).

5. Карпенко О. Європейський досвід протидії гібридним загрозам: уроки для України. *Інвестиції: практика та досвід*. 2024. № 41. 70–76. URL: https://iepjournal.com/journals/41/2024_41_12_Karpenko.pdf (дата звернення: 5.10.2025).

6. Кононенко В., Годлевська В. Кібербезпека: державне управління у сфері національної безпеки Іспанії. *Дніпровський науковий часопис публічного управління, психології, права*. 2021. № 6. DOI: https://doi.org/10.51547/PPP.DP.UA/2021.6.9 (дата звернення: 5.10.2025).

7. Мазепа С. Міжнародний досвід захисту інформаційної безпеки: імплементація європейських правових норм в законодавство України. *Вісник юридичного факультету УжНУ*. 2025. Вип. 44. С. 47–53. URL: https://visnyk-

juris-uzhnu.com/wp-content/uploads/2025/09/44-2.pdf (дата звернення: 5.10.2025).

8. Милосердна І.М. Інформаційна безпека як елемент національної безпеки: теоретичний вимір та особливості впровадження. *Політичні проблеми міжнародних систем та глобального розвитку*. 2024. №4. С. 179–185. DOI: https://doi.org/10.24195/2414-9616.2024-4.26 (дата звернення: 5.10.2025).

9. Міщук А.Р. Технології і методи гібридних конфліктів у світі. Електронний архів КПІ, 2021. URL: https://ela.kpi.ua/bitstreams/a54c0eaa-4077-4381-bf15-99a549740638/завантажити (дата звернення: 5.10.2025).

10. Прудникова О. Інформаційна безпека Європейського Союзу: виклики та тенденції. *Вісник НЮУ імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія*. 2025. №3(66). URL: https://doi.org/10.21564/2663-5704.66.337888 (дата звернення: 5.10.2025).

11. Пугачов О. І. Зарубіжний досвід забезпечення інформаційної безпеки держави. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. 2024. №13. URL: https://doi.org/10.54929/2786-5746-2024-13-02-07 (дата звернення: 5.10.2025).

12. Романюк І. О. Антитерористична політика ЄС: аналіз законодавчих ініціатив та їх вплив на безпекову ситуацію. *Український політико-правовий дискурс.* 2024. №1. С. 60–66. URL: https://ppdnz.com.ua/index.php/home/article/download/20/18 (дата звернення: 5.10.2025).

13. 2024 Elections: Cybersecurity Challenges in Spain and Beyond. *SOCRadar. 2024.* URL: https://socradar.io/2024-elections-cybersecurity-challenges-in-spain-and-beyond/ (Last accessed: 5.10.2025).

14. Alcaraz C. A Comparative Study of National Cyber Security Strategies of ten nations. *ResearchGate.* 2023. P. 1–25. URL: https://www.researchgate.net/publication/369540767_A_Comparative_Study_of_National_Cyber_Security_Strategies_of_ten_nations (Last accessed: 5.10.2025).

15. Alone we stand: How Europe can counter hybrid threats in a post-transatlantic era. *European Council on Foreign Relations*. 2025. URL: https://ecfr.eu/article/alone-we-stand-how-europe-can-counter-hybrid-threats-in-a-post-transatlantic-era/ (Last accessed: 5.10.2025).

16. Amenazas, riesgos y desafíos a la Seguridad Nacional. Documento de Investigación DIEEEM 03/2025. *Instituto Español de Estudios Estratégicos*. Madrid: IEEE, 2025. URL: https://www.defensa.gob.es/documents/2073105/2383976/amenazas_riesgos_y%2Bdesafios_a_la_seguridad_nacional_2025_dieeem03.pdf (Last accessed: 5.10.2025).

17. Badillo Á. El impacto estratégico de la desinformación en España. *Informe Iberifier*. Madrid: Real Instituto Elcano, 2024. URL: https://media.realinstitutoelcano.org/wp-content/uploads/2024/04/informe-iberifier-el-impacto-estratagico-de-la-desinformacion-en-espana.pdf (Last accessed: 5.10.2025).

18. Bayerl P.S., et al. Navigating the complex nexus: cybersecurity in political landscapes. *arXiv*. 2023. URL: https://arxiv.org/abs/2308.08005 (Last accessed: 5.10.2025).

19. Beek C. Spain and Portugal Face Cybersecurity Crisis. *Cybersec*. 2025. URL: https://www.cybersec-365.com/articles/darkness-and-digital-danger-spain-and-portugal-face-cybersecurity-crisis (Last accessed: 5.10.2025).

20. Colom Piella G. Las estrategias de la OTAN en respuesta a los conflictos híbridos. *Amenazas híbridas, orden vulnerable. Nuevas lógicas de seguridad en el espacio euroatlántico*. CIDOB Report № 8. Barcelona: CIDOB, 2022. P. 29–40. URL: https://www.cidob.org/es/publicaciones/serie_de_publicacion/cidob_report/cidob_report_n_8/las_estrategias_de_la_otan_en_respuesta_a_los_conflictos_hibridos (Last accessed: 5.10.2025).

21. Council conclusions on a framework for a coordinated EU response to hybrid campaigns. *Council of the European Union*. 2022. URL:

https://www.consilium.europa.eu/en/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/ (Last accessed: 5.10.2025).

22. Cueto Díaz R. Desinformación en España un año después de la COVID-19. Análisis de las verificaciones de Newtral y Maldita. *Revista Latina de Comunicación Social.* 2022. № 80. P. 1–27. URL: https://nuevaepoca.revistalatinacs.org/index.php/revista/article/view/1612 (Last accessed: 5.10.2025).

23. Cultura de Seguridad Nacional y lucha contra la desinformación. *Departamento de Seguridad Nacional.* Madrid: DSN, 2023. URL: https://www.dsn.gob.es/es/cultura-de-seguridad-nacional (Last accessed: 5.10.2025).

24. Darkness and Digital Danger: Spain and Portugal Face Cybersecurity Crisis. *Cybersec 365.* 2025. URL: https://www.cybersec-365.com/articles/darkness-and-digital-danger-spain-and-portugal-face-cybersecurity-crisis (Last accessed: 5.10.2025).

25. De-Frutos-Torres B., Taddeo G., Alvarado M.-C. Creators and spectators facing online information disorder. Effects of digital content production on information skills. *Comunicar.* 2022. № 72. P. 9–20. DOI: 10.3916/C72-2022-01. URL: https://www.revistacomunicar.com/index.php?articulo=72-2022-01 (Last accessed: 5.10.2025).

26. Democratic resilience: Council approves conclusions on safeguarding electoral processes from foreign interference. *Council of the European Union.* 2024. URL: https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/democratic-resilience-council-approves-conclusions-on-safeguarding-electoral-processes-from-foreign-interference/ (Last accessed: 5.10.2025).

27. Disinformation in the Digital Age (English report). *Oficina C (Spanish Government).* 14.12.2023. URL:

https://www.oficinac.es/sites/default/files/informes/OFICINAC_desinformaci%C3%B3n_20231214_web_english_0.pdf (Last accessed: 5.10.2025).

28. Ellis C. HyperWar: The Evolution of Conflict in the Digital Age. *ResearchGate.* 2024. URL: https://www.researchgate.net/publication/382997935_HyperWar_The_Evolution_of_Conflict_in_the_Digital_Age (Last accessed: 5.10.2025).

29. ENISA Threat Landscape 2022. *European Union Agency for Cybersecurity (ENISA).* Luxemburg: ENISA, 2022. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (Last accessed: 5.10.2025).

30. España, hub de ciberseguridad europeo: oportunidades y propuestas. *Departamento de Seguridad Nacional; ISMS Forum.* Madrid: DSN / ISMS Forum, 2025. URL: https://foronacionalciberseguridad.es/publicaciones (Last accessed: 5.10.2025).

31. Fortifying Europe's digital defences: EU Cybersecurity month and protectEU strategy. *European Commission Home Affairs.* 2025. URL: https://home-affairs.ec.europa.eu/news/fortifying-europes-digital-defences-eu-cybersecurity-month-and-protecteu-strategy-2025-10-20_en (Last accessed: 5.10.2025).

32. García Gutiérrez I. La Estrategia de Seguridad Nacional 2021 y la National Defense Strategy 2022 de Estados Unidos: convergencias y divergencias. *Documento de Opinión IEEE 25/2023.* Madrid: IEEE, 2023. 13 p. URL: https://www.ieee.es/Galerias/fichero/docs_opinion/2023/DIEEEO25_2023_IGNGAR_Estrategia.pdf (Last accessed: 5.10.2025).

33. García Gutiérrez J., Hoogensen Gjørv G., Tahinjanahary Razakamaharavo V. Identidad, estabilidad, amenazas híbridas y desinformación. ICONO 14. *Revista científica de Comunicación y Tecnologías Emergentes*. 2021. Vol. 19. № 1. P. 38–69. URL: https://icono14.net/ojs/index.php/icono14/article/view/1618 (Last accessed: 5.10.2025).

34. García J. J. Understanding the plural landscape of cybersecurity governance in Spain: a matter of capital exchange. *International Cybersecurity Law Review.* 2022. Vol. 3. P. 1–20. https://link.springer.com/article/10.1365/s43439-022-00069-4 (Last accessed: 5.10.2025).

35. García-Marín D., Salvat-Martinrey G. Tendencias en la producción científica sobre desinformación en España. Revisión sistematizada de la literatura (2016–2021). adComunica. Revista Científica de Estrategias, *Tendencias e Innovación en Comunicación.* 2022. № 23. P. 23–50. DOI: 10.6035/adcomunica.6045. URL: https://www.e-revistes.uji.es/index.php/adcomunica/article/view/6045 (Last accessed: 5.10.2025).

36. Hanley M. Salvaguardar el espacio informativo: las políticas de la UE y Ucrania ante la desinformación. Barcelona: CIDOB, 2024. URL: https://www.cidob.org/publicaciones/salvaguardar-el-espacio-informativo-las-politicas-de-la-ue-y-ucrania-ante-la (Last accessed: 5.10.2025).

37. Hedling E. The Intersection of Cyberwarfare, Social Media, and Adolescent Self-Esteem: A Forensic Cyberpsychology Analysis. *ResearchGate.* 2025. P. 1–15. URL: https://www.researchgate.net/publication/390163862_The_Intersection_of_Cyberwarfare_Social_Media_and_Adolescent_Self-Esteem_A_Forensic_Cyberpsychology_Analysis (Last accessed: 5.10.2025).

38. Hybrid threats: a background analysis. *European Centre of Excellence for Countering Hybrid Threats.* Helsinki: Hybrid CoE, 2021. URL: https://www.hybridcoe.fi/publications/hybrid-threats-a-background-analysis/ (Last accessed: 5.10.2025).

39. Hybrid threats: Council paves the way for deploying Hybrid Rapid Response Teams. *Council of the European Union*. 2024. URL: https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/hybrid-threats-council-paves-the-way-for-deploying-hybrid-rapid-response-teams/ (Last accessed: 5.10.2025).

40. Indra launches IndraMind: Spain's first sovereign AI platform to tackle hybrid warfare and threats. *Defence Industry EU.* 2025. URL: https://defence-industry.eu/indra-launches-indramind-spains-first-sovereign-ai-platform-to-tackle-hybrid-warfare-and-threats/ (Last accessed: 5.10.2025).

41. Informe Anual de Seguridad Nacional 2024. *Departamento de Seguridad Nacional.* Madrid: DSN, 2025. URL: https://www.dsn.gob.es/es/publicaciones/informes-anuales-IASN2024 (Last accessed: 5.10.2025).

42. Informe de Ciberamenazas y Tendencias. *CCN-CERT (Centro Criptológico Nacional).* Edición 2024. Madrid, 2024. URL: https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/7274-ccn-cert-ia-04-24-ciberamenazas-y-tendencias-edicion-2024/file.html (Last accessed: 5.10.2025).

43. Informe sobre la cibercriminalidad en España 2021. *Ministerio del Interior.* Madrid: Ministerio del Interior, 2022. URL: https://www.interior.gob.es/opencms/es/datos-y-estadisticas/estadisticas/estudios-e-informes-de-la-secretaria-de-estado-de-seguridad/informe-sobre-cibercriminalidad-en-espana-2021/ (Last accessed: 5.10.2025).

44. Jimenez J. Waking Up Slowly: Defense AI in Spain. *SpringerLink.* 2024. URL: https://www.researchgate.net/publication/382373689_Waking_Up_Slowly_Defense_AI_in_Spain/fulltext/669a763ecb7fbf12a45cc8bb/Waking-Up-Slowly-Defense-AI-in-Spain.pdf (Last accessed: 5.10.2025).

45. Joint Statement on the Second U.S.-Spain Cyber and Digital Dialogue. *U.S. Department of State*. 2024. URL: https://2021-2025.state.gov/joint-statement-on-the-second-u-s-spain-cyber-and-digital-dialogue/ (Last accessed: 5.10.2025).

46. Kalenský J. Countering disinformation in the Euro-Atlantic: Strengths and gaps. *Hybrid CoE.* 2025. P. 1–20. https://www.hybridcoe.fi/publications/countering-disinformation-in-the-euro-atlantic-strengths-and-gaps/ (Last accessed: 5.10.2025).

47. La desinformación como arma de guerra. Documento de Opinión IEEE 26/2024. *Instituto Español de Estudios Estratégicos.* Madrid: IEEE, 2024. URL: https://www.ieee.es/Galerias/fichero/docs_opinion/2024/DIEEEO26_2024_VVAA_Desinformacion.pdf (Last accessed: 5.10.2025).

48. La polarización política debilita a España ante las injerencias y la desinformación. *Agenda Pública. Agenda Pública – El País.* 2025. URL: https://agendapublica.es/noticia/19950/espana-injerencias-desinformacion-seguridad-nacional-rusia agendapublica.es (Last accessed: 5.10.2025).

49. Lebret M. Cross-cutting technologies in Chinese space activities: Raising the risk of hybrid threats. *Hybrid CoE.* 2024. https://www.hybridcoe.fi/publications/hybrid-coe-paper-22-cross-cutting-technologies-in-chinese-space-activities-raising-the-risk-of-hybrid-threats/ (Last accessed: 5.10.2025).

50. Lonardo L. EU Law Against Hybrid Threats: A First Assessment. *European Papers.* 2021. № 2. P. 1076-1096. URL: https://www.europeanpapers.eu/system/files/pdf_version/EP_eJ_2021_2_19_Articles_SS2_6_Luigi_Lonardo_00514.pdf (Last accessed: 5.10.2025).

51. Lonardo L. The concepts and laws applicable to hybrid threats, with a special focus on Europe. *Humanities and Social Sciences Communications*. 2023. Vol. 10. Art. 18. URL: https://www.nature.com/articles/s41599-023-01864-y (Last accessed: 5.10.2025).

52. López-Rico C., Martínez-Verdú F. Fact-checking y desinformación climática en España. *Tendencias y retos. Doxa Comunicación*. 2024. № 38. P. 1–27. URL: https://revistascientificas.uspceu.com/doxacomunicacion/article/view/2861 revistascientificas.uspceu.com (Last accessed: 5.10.2025).

53. Maasland D. Darkness and Digital Danger: Spain and Portugal Face Cybersecurity Crisis. *Cybersec 365.* 2025. URL: https://www.cybersec-365.com/articles/darkness-and-digital-danger-spain-and-portugal-face-cybersecurity-crisis (Last accessed: 5.10.2025).

54. Martínez-Roget F. Investigación sobre desinformación en España. Análisis de tendencias temáticas. *Journal of Communication*. 2021. Vol. 13, № 1. P. 199–225. URL: https://revistas.usal.es/index.php/2172-9077/article/view/fjc202123199225 revistas.usal.es (Last accessed: 5.10.2025).

55. Martínez-Sánchez D. Desinformación en situaciones de emergencia: estudio del caso de la DANA de Valencia. *Revista Mediterránea de Comunicación.* 2025. Vol. 16, № 2. URL: https://www.mediterranea-comunicacion.org/article/view/29275 (Last accessed: 5.10.2025).

56. Mihaela T. Artificial Intelligence & Cybersecurity: European Union panorama. *ResearchGate.* 2024. P. 1–50. URL: https://www.researchgate.net/publication/354343066_Artificial_Intelligence_Cybersecurity_European_Union_panorama (Last accessed: 5.10.2025).

57. Muñoz J. A. Desinformación: aproximación conceptual, riesgos y respuestas. *UNISCI Journal.* 2024. № 56. P. 1–27. URL: https://revistas.ucm.es/index.php/UNIS/article/view/91059 (Last accessed: 5.10.2025).

58. National Cybersecurity Strategies – Interactive Map (Spain NCSS and updates). *ENISA.* 2024-2025. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies (Last accessed: 5.10.2025).

59. NIS2 Directive – Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union. *ENISA.* OJ L 333, 27.12.2022. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng (Last accessed: 5.10.2025).

60. Northwave Cybersecurity. Russia's Hybrid Threats to Europe's Businesses. *Northwave Cybersecurity.* 2025. URL: https://northwave-cybersecurity.com/article/russias-hybrid-threats-to-europes-businesses (Last accessed: 5.10.2025).

61. Palomares Lerma J. La guerra híbrida: una amenaza actual a la seguridad. *Human Security – Revista Seguridad Humana.* 2024. № 18. P. 35–52.

URL: https://www.seguridadhumana.es/wp-content/uploads/2024/03/La-guerra-hibrida-una-amenaza-actual-a-la-seguridad.pdf (Last accessed: 5.10.2025).

62. Petrovic P. Information Warfare - New Security Challenge for Europe. *ResearchGate.* 2024. P. 1–20. URL: https://www.researchgate.net/publication/322695565_Information_Warfare_-_New_Security_Challenge_for_Europe (Last accessed: 5.10.2025).

63. Prieto Barral P. B. Desinformación en tiempos de polarización política: el debate público en redes sociales. Disertaciones. *Anuario Electrónico de Estudios en Comunicación Social.* 2025. Vol. 18, № 1. P. 1–22. URL: https://revistas.urosario.edu.co/index.php/disertaciones/article/view/14785 (Last accessed: 5.10.2025).

64. Rauta V. The Cyber Proxy War: Non-State Actors Role in Global Geopolitical Competition. *ResearchGate.* 2025. P. 815-826. URL: https://www.researchgate.net/publication/388324123_The_Cyber_Proxy_War_Non-State_Actors_Role_in_Global_Geopolitical_Competition (Last accessed: 5.10.2025).

65. Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021. *Boletín Oficial del Estado*. 2021. № 312. URL: https://www.boe.es/buscar/doc.php?id=BOE-A-2021-20727 (Last accessed: 5.10.2025).

66. Renedo Farpón C., García-Ull F. J. Prólogo. Análisis de la desinformación: estrategias (en) de los desórdenes informativos. Miguel Hernández *Communication Journal.* 2023. Vol. 14. URL: https://revistas.innovacionumh.es/index.php/mhcj/article/view/1292 (Last accessed: 5.10.2025).

67. Ribeiro J. C. Desinformación y polarización en la publicidad política de la extrema derecha en España y Portugal. *Estudos em Comunicação*. 2025. № 36. P. 115–132. URL: https://dialnet.unirioja.es/descarga/articulo/10286984.pdf (Last accessed: 5.10.2025).

68. Rueda Rico C. Ciberseguridad y guerra híbrida: la ampliación del espectro. *Global Affairs – Universidad de Navarra*. 2023. URL: https://globalaffairs.unav.edu/es/web/global-affairs/detalle/-/blogs/ciberseguridad-y-guerra-hibrida-la-ampliacion-del-espectro (Last accessed: 5.10.2025).

69. Rusinaitė V. Turning strategy into praxis: Lessons in hybrid threat deterrence. Hybrid CoE. 2025. P. 1–15. https://www.hybridcoe.fi/publications/turning-strategy-into-praxis-lessons-in-hybrid-threat-deterrence/ (Last accessed: 5.10.2025).

70. Sari A. The Development of Digital Technologies and Cyber Security Threats. *ResearchGate.* 2025. P. 1–18. URL: https://www.researchgate.net/publication/368928763_The_Development_of_Digital_Technologies_and_Cyber_Security_Threats (Last accessed: 5.10.2025).

71. Savitz S. The logical architecture of the cybersecurity situation awareness network for the hybrid warfare. *ResearchGate.* 2025. P. 1–10. URL: https://www.researchgate.net/figure/The-logical-architecture-of-the-cybersecurity-situation-awareness-network-for-the_fig1_333510767 (Last accessed: 5.10.2025).

72. Schuman R. Hybrid threats: the new horizons for a «Europe of internal security»? *Robert Schuman Foundation*. 2025. URL: https://www.robert-schuman.eu/en/european-issues/787-hybrid-threats-the-new-horizons-for-a-europe-of-internal-security (Last accessed: 5.10.2025).

73. Spain Cyber Security and Spanish Cyber Crime Statistics. Comparitech. *Comparitech.* 2022. URL: https://www.comparitech.com/blog/information-security/spain-cyber-security-statistics/ (Last accessed: 5.10.2025).

74. Spain is the fifth country with the most ransomware threats in 2024. *Thales Cyber Solutions.* 2024. URL: https://cds.thalesgroup.com/en/hot-topics/spain-fifth-country-most-ransomware-threats-2024 (Last accessed: 5.10.2025).

75. The Challenge of Cybersecurity in Spain: A Vulnerable Country. *Telefónica.* 2022. https://www.telefonica.com/en/communication-room/blog/the-

challenge-of-cybersecurity-in-spain-a-vulnerable-country/ (Last accessed: 5.10.2025).

76. The Global Geopolitical Situation Triggers a Surge in Cyberattacks in Spain. Barcelona Cybersecurity Congress. *Barcelona Cybersecurity Congres*. 2025. URL: https://www.barcelonacybersecuritycongress.com/the-global-geopolitical-situation-triggers-a-surge-in-cyberattacks-in-spain/ (Last accessed: 5.10.2025).

77. Threats, risks and challenges to national security. *Ministerio de Defensa de Espana.* 2025. URL: https://www.defensa.gob.es/documents/2073105/2383976/amenazas_riesgos_y%2Bdesafios_a_la_seguridad_nacional_2025_dieeem03_eng.pdf/10468d78-7b52-6c8f-1d51-27aa1bae1234?t=1759217806364 (Last accessed: 5.10.2025).

78. Unión Europea y Cooperación. La lucha contra la desinformación. *Ministerio de Asuntos Exteriores,* Madrid: MAEC, 2023. URL: https://www.exteriores.gob.es/es/PoliticaExterior/Paginas/LaLuchaContraLaDesinformacion.aspx (Last accessed: 5.10.2025).

79. Vidal R. Ciberataques a infraestructuras críticas: cuando el país se apaga. Observatorio Nacional de Ciberseguridad (blog). 2025. URL: https://observatoriociber.org/ciberataques-infraestructuras-criticas-guerra-hibrida/ (Last accessed: 5.10.2025).

80. What is the cybersecurity challenge facing Spanish companies? *Velatia.* 2023. URL: https://www.velatia.com/en/blog/what-is-the-cybersecurity-challenge-facing-spanish-companies/ (Last accessed: 5.10.2025).

81. Wigell M. Best Practices in the whole-of-society approach in countering hybrid threats. *ResearchGate.* 2021. P. 1–30. URL: https://www.researchgate.net/profile/Mikael-Wigell/publication/351836523_Best_Practices_in_the_whole-of-society_approach_in_countering_hybrid_threats/links/6357970f6e0d367d91c4d9b8/Best-Practices-in-the-whole-of-society-approach-in-countering-hybrid-threats.pdf (Last accessed: 5.10.2025).

АНОТАЦІЯ

Бевзюк О.Р. Інформаційна безпека Іспанії в умовах гібридних загроз (магістерська робота). Харків: ХНУ імені В. Н. Каразіна, 2025. 84 с. (рукопис).

Кваліфікаційна робота магістра присвячена визначенню особливості функціонування системи забезпечення інформаційної безпеки Іспанії в умовах гібридних загроз. Об'єкт дослідження – система забезпечення інформаційної безпеки держави. Предмет дослідження – система забезпечення інформаційної безпеки Іспанії в умовах гібридних загроз.

У першому розділі визначено поняття, структуру інформаційної безпеки держави та типологію гібридних загроз у системі сучасних міжнародних відносин; виявлено механізми забезпечення інформаційної безпеки держави в умовах гібридних загроз.

У другому розділі розкрито нормативно-правове забезпечення інформаційної безпеки Іспанії та його значення для протидії сучасним гібридним загрозам; встановлено особливості функціонування системи інформаційної безпеки Іспанії та ключові виклики, що впливають на її стійкість у контексті сучасних гібридних загроз.

У третьому розділі з'ясовано роль міжнародного співробітництва у зміцненні інформаційної безпеки Іспанії та можливості використання її досвіду для посилення інформаційної безпеки України.

Ключові слова: інформаційна безпека Іспанії, гібридні загрози, кібербезпека, цифровий суверенітет, дезінформація, кібертероризм.

ANNOTATION

Bevzuk O. R. Information security of Spain in the context of hybrid threats (master's work). Kharkiv: V. N. Karazin Kharkiv National University, 2025. 84 p. (manuscript).

The master's qualification work is devoted to determining the peculiarities of the functioning of the information security system of Spain in the context of hybrid threats. The object of the research is the information security system of the state. The subject of the research is the information security system of Spain in the context of hybrid threats.

The first section defines the concept, structure of information security of the state

and the typology of hybrid threats in the system of modern international relations; mechanisms for ensuring information security of the state in the context of hybrid threats are identified.

The second section reveals the regulatory and legal support for information security of Spain and its significance for countering modern hybrid threats; the peculiarities of the functioning of the information security system of Spain and the key challenges that affect its stability in the context of modern hybrid threats are established.

The third section clarifies the role of international cooperation in strengthening information security of Spain and the possibility of using its experience to strengthen information security of Ukraine.

Keywords: information security of Spain, hybrid threats, cybersecurity, digital sovereignty, disinformation, cyberterrorism.

ВІДГУК

на кваліфікаційну роботу магістра
студента 2-го курсу групи УМІБ-61 денної форми навчання
спеціальності 291 «Міжнародні відносини,
суспільні комунікації та регіональні студії»
освітньо-професійної програми
«Міжнародна інформаційна безпека»
Навчально-наукового інституту «Каразінський інститут
міжнародних відносин та туристичного бізнесу»
Харківського національного університету імені В.Н. Каразіна
Бевзюка Олега Романовича
на тему «Інформаційна безпека Іспанії в умовах гібридних загроз»

1.Актуальність теми зумовлена стрімким ускладненням міжнародного безпекового середовища, у якому інформаційний простір перетворився на один із ключових театрів геополітичної конкуренції. Іспанія, будучи членом ЄС і НАТО, дедалі частіше стикається з багатовимірними гібридними впливами, що поєднують кібератаки, дезінформаційні кампанії, маніпуляції суспільною думкою та втручання у виборчі процеси. Такі загрози, зокрема з боку недружніх державних і недержавних акторів, спрямовані на підрив демократичних інститутів, дестабілізацію внутрішньополітичної ситуації та послаблення стратегічної стійкості держави. Крім того, інформаційна безпека Іспанії тісно пов'язана з безпековими процесами на європейському рівні, адже країна активно бере участь у формуванні спільної політики кіберзахисту, протидії дезінформації та захисту критичної інфраструктури. Саме тому дослідження іспанського досвіду є важливим не лише для аналізу внутрішніх механізмів забезпечення стійкості, а й для розуміння можливостей його адаптації іншими державами, зокрема Україною. Отже, тема має значний науковий і практичний інтерес, оскільки дозволяє оцінити ефективність сучасних підходів до протидії гібридним загрозам і визначити перспективи подальшого удосконалення інформаційної політики.

2. Позитивні аспекти в роботі. Зміст роботи повністю відповідає обраній темі. Робота складається зі вступу, трьох розділів, висновків та списку використаних джерел. Позитивними рисами кваліфікаційної роботи магістра є системність та послідовність викладення матеріалу.

3. Недоліки роботи. В той же час, автору слід було б приділити більше уваги ілюстративній частині роботи, однак це не впливає на роботу вцілому.

4. Практична цінність висновків і рекомендацій. Запропоновані у кваліфікаційній роботі магістра теоретичні положення та висновки можуть бути використані: органами державної влади України полягає насамперед у

можливості використання іспанського досвіду як дієвої моделі адаптації системи національної інформаційної безпеки до умов багатовимірних гібридних загроз. Зокрема, аналіз стратегічних документів Іспанії та її підходів до міжвідомчої координації дозволяє українським інституціям, передусім РНБО, Міністерству оборони, Службі безпеки України та Міністерству цифрової трансформації, посилити інституційні механізми реагування на інформаційні операції, кібератаки та кампанії дезінформації;

5. Загальна оцінка дипломної роботи та її допуск/не допуск до захисту перед ЕК. Кваліфікаційна робота магістра Бевзюка Олега Романовича на тему «Інформаційна безпека Іспанії в умовах гібридних загроз» заслуговує на позитивну оцінку, а її автор гідний присвоєння кваліфікації магістра міжнародних відносин, суспільних комунікацій та регіональних студій.

Керівник кваліфікаційної роботи,
доктор політичних наук, професор,
професор кафедри міжнародних відносин,
міжнародної інформації та безпеки
Харківського національного

університету імені В.Н. Каразіна Куц Г.М.

РЕЦЕНЗІЯ

на кваліфікаційну роботу магістра
студента 2-го курсу групи УМІБ-61 денної форми навчання
спеціальності 291 «Міжнародні відносини,
суспільні комунікації та регіональні студії»
освітньо-професійної програми
«Міжнародна інформаційна безпека»
Навчально-наукового інституту «Каразінський інститут
міжнародних відносин та туристичного бізнесу»
Харківського національного університету імені В.Н. Каразіна
Бевзюка Олега Романовича
на тему «Інформаційна безпека Іспанії в умовах гібридних загроз»

1. Актуальність теми зумовлена суттєвим ускладненням безпекового середовища Європи, у якому Хорватія, попри свій порівняно невеликий розмір, відіграє дедалі помітнішу роль. Сучасні геополітичні виклики, зокрема російсько-українська війна, зростання гібридних загроз, енергетична нестабільність і трансформація безпекових пріоритетів Європейського Союзу та НАТО, актуалізують питання адаптації хорватської стратегії безпеки до нових реалій. Водночас вступ Хорватії до Шенгенської зони та єврозони у 2023 році суттєво посилив її відповідальність за охорону зовнішніх кордонів ЄС, що, відповідно, впливає на архітектуру регіональної стабільності. Разом із тим, Хорватія має унікальний досвід постконфліктної відбудови, інтеграції ветеранів, зміцнення інституцій оборони та переходу до сучасних стандартів НАТО, що робить її важливим джерелом практичних рішень для інших держав, зокрема України. Крім того, країна активно долучається до місій ЄС і НАТО на Західних Балканах, сприяючи зміцненню безпеки в регіоні, який традиційно вважається одним із найуразливіших до зовнішнього впливу. Усе це дозволяє стверджувати, що дослідження місця Хорватії у системі європейської безпеки є надзвичайно важливим для розуміння трансформації сучасного безпекового порядку та вироблення нових підходів до підтримання стабільності на континенті.

2. Характеристика якості виконання кожного розділу роботи. У першому розділі «ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ» визначено поняття, структуру інформаційної безпеки держави та типологію гібридних загроз у системі сучасних міжнародних відносин; виявлено механізми забезпечення інформаційної безпеки держави в умовах гібридних загроз.

У другому розділі «СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІСПАНІЇ» розкрито нормативно-правове забезпечення інформаційної безпеки Іспанії та його значення для протидії сучасним гібридним загрозам; встановлено особливості функціонування системи інформаційної безпеки Іспанії та ключові виклики, що впливають на її стійкість у контексті сучасних гібридних загроз.

У третьому розділі «НАПРЯМКИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІСПАНІЇ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ» з'ясовано роль міжнародного співробітництва у зміцненні інформаційної безпеки Іспанії та можливості використання її досвіду для посилення інформаційної безпеки України.

3. Ступінь обґрунтованості висновків роботи. Висновки достатньо обґрунтовані та відповідають поставленим завданням у кваліфікаційній роботі.

4. Використання в дипломній роботі останніх досліджень. Варто відзначити, що автором проаналізовано значний обсяг фактологічного матеріалу. Був здійснений детальний аналіз обраної проблематики, наукові методи використані коректно. Проаналізовано великий спектр вітчизняної та зарубіжної наукової літератури.

5. Позитивні сторони роботи. Зміст роботи повністю відповідає обраній темі. Робота складається зі вступу, трьох розділів, висновків і списку використаних джерел. В дипломній роботі присутня системність та послідовність викладення матеріалу.

6. Недоліки роботи. Доцільно було б більше уваги приділити теоретичній частині дослідження, однак це не впливає негативно на дипломну роботу в цілому.

7. Практичне значення. Теоретичні положення та висновки можуть бути використані: органами державної влади України полягає насамперед у можливості використання іспанського досвіду як дієвої моделі адаптації системи національної інформаційної безпеки до умов багатовимірних гібридних загроз.

8. Загальна оцінка кваліфікаційної роботи. Кваліфікаційна робота магістра Бевзюка Олега Романовича на тему «Інформаційна безпека Іспанії в умовах гібридних загроз» заслуговує на позитивну оцінку, а її автор гідний присвоєння кваліфікації магістра міжнародних відносин, суспільних комунікацій та регіональних студій.

Рецензент:
кандидат політичних наук, доцент,
доцент кафедри політології,
соціології і культурології
Харківського національного педагогічного
університету імені Г. С. Сковороди ДІБІКОВА Юлія Сергіївна

Підпис Дібікової Ю. С.
засвідчується зав. загальним відділом