Чорноморський національний університет імені Петра Могили
(повне найменування вищого навчального закладу)

факультет політичних наук
(повне найменування інституту, назва факультету)

кафедра журналістики та політології
(повна назва кафедри)

«Допущено до захисту»
В.о. завідувача кафедри журналістики та політології
_____ Тетяна СИДОРЕНКО
«___» _____ 2025 року

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття ступеня вищої освіти

магістр
(ступінь вищої освіти, спеціальність)

на тему: «Інформаційна безпека як ключовий елемент політичної стабільності держави»

Керівник: к. політ. н., доцент
Громадська Наталя Анатоліївна
(вчене звання, науковий ступінь, П.І.Б.)

Рецензент: д. політ. н, професор
Шевчук Олександр Володимирович
(вчене звання, науковий ступінь, П.І.Б.)

Виконав: студент VI курсу, групи 631М
Мизь Максим Дмитрович
(П.І.Б.)

Спеціальності: 052 «Політологія»
(шифр і назва спеціальності)

ОПП: «Політологія»

Миколаїв – 2025 рік

ЗМІСТ

ВСТУП

Актуальність дослідження. У XXI столітті інформація стала визначальним ресурсом, який формує політичні наративи, впливає на прийняття рішень і визначає рівні довіри між громадянами та інститутами влади. Швидкий розвиток цифрових технологій та інформаційних комунікацій створив нове поле політичної конкуренції — інформаційний простір, де операції з дезінформації, маніпулювання увагою громадськості та кібератаки здатні завдати істотної шкоди державній стабільності. Тому питання інформаційної безпеки набуває статусу пріоритету національної безпеки та політики.

Український досвід останніх десятиліть демонструє практичну значущість цієї проблеми. Системні кампанії з дезінформації, кібератаки на державні органи та критичну інфраструктуру, а також використання інформаційно-психологічних операцій у гібридних ворожих діях виявили слабкі місця в механізмах захисту інформаційного простору. Наслідки таких атак виходять далеко за межі технічних збоїв — вони підривають суспільну згуртованість, спричиняють енергетичні та економічні втрати і можуть змінювати поведінку громадян та легітимність політичних інституцій. Особливо після початку повномасштабної агресії 2022 року інформаційний фронт став рівнозначним військовому, й постійні потоки пропаганди та регулярні кібератаки спрямовані на дискредитацію української влади, деморалізацію населення та розкол суспільства стали ще небезпечнішими.

Таким чином, дослідження, яке розглядає інформаційну безпеку як ключовий елемент політичної стабільності, є актуальним і практично значущим. Також, необхідним є розробка та впровадження ефективної державної політики у сфері інформаційної безпеки.

Стан наукової розробки дослідження. Проблематика інформаційної безпеки в контексті забезпечення політичної стабільності держави привертає значну увагу зарубіжних та українських дослідників, які розглядають її на перетині політичної науки, права, соціології, кібернетики та комунікаційних студій.

Проблематика інформаційної безпеки та її забезпечення у різних аспектах досліджувались у наукових працях І. Бонадар, І. Грамика, В. Гурковського, О. Дзьобаня, О. Данільяна, О. Довганя, Р. Калюжного, В. Ліпкан, М. Панова, В. Шульга, Т. Мужанова, Т. Ткачука, Г. Нестеренко, Б. Кормич, М. Шевчук, Я. М. Жаркова, В. Шатуна, О. Гладуна та інших.

Проблеми політичної стабільності вивчали такі вчені, як М. Михальченко, В. Кремень, О. Кіндратець, І. Кіянка, В. Кривошеїн, Г. Ситник, М. Яворський, О. Баталов, М. Паламарчук, А. Козьміних, В. Ребкало, В. Шахов та інші.

Окремим питанням значення соціальних мереж для інформаційної безпеки займалися О. Свідерська, Г. Четверик, А. Тлуста, М. Гончар, Н. Перепелиця та інші.

Об’єкт дослідження – політична стабільність держави.

Предмет дослідження – інформаційна безпека як ключовий елемент політичної стабільності держави.

Мета дослідження – з’ясувати сутність, загрози і механізми забезпечення інформаційної безпеки як чиннику політичної стабільності держави та визначити ефективні шляхи вдосконалення системи інформаційної безпеки.

Для досягнення поставленої мети необхідно виконати ряд таких **завдань:**

- визначити поняття, сутність і правові основи інформаційної безпеки держави;

- з’ясувати суть політичної стабільності, її ключові критерії та фактори забезпечення;
- визначити роль інформаційної безпеки у нейтралізації деструктивних інформаційно-психологічних впливів на політичну стабільність держави.
- здійснити класифікацію і типологізацію загроз інформаційній безпеці держави;
- виявити вплив гібридних загроз і інформаційно-психологічних операцій на процеси політичної дестабілізації;
- охарактеризувати вплив соціальних мереж та сучасних інформаційних технологій на політичну систему і суспільно-політичні процеси держави.
- визначити інституційні, правові та політичні механізми державної політики у сфері інформаційної безпеки;
- охарактеризувати зарубіжний досвід забезпечення інформаційної безпеки та визначити можливості його адаптації в Україні;
- визначити шляхи вдосконалення української системи інформаційної безпеки з метою зміцнення політичної стабільності держави.

Методи дослідження. Досягнення визначеної мети й вирішення поставлених завдань стало можливим завдяки використанню комплексу взаємопов’язаних і взаємодоповнюючих сучасних загальнонаукових та спеціальних методів і підходів. Під час дослідження було використано такі загальнонаукові методи як аналіз та синтез (для формування загального уявлення про інформаційну безпеку, політичну стабільність, інформаційні заргози), порівняння (для визначення особливостей інформаційної безпеки різних країни), контент-аналіз (аналіз нормативно-правових документів для оцінки правового забезпечення інформаційної безпеки).

Наукова новизна дослідження. Удосконалено шляхи вдосконалення системи інформаційної безпеки України, які ґрунтуються на актуальних загрозах та досвіді зарубіжних країн.

Теоретичне та практичне значення одержаних результатів. Теоретичне значення одержаних результатів полягає у подальшому розвитку наукових підходів до розуміння інформаційної безпеки як системоутворювального елемента політичної стабільності держави. У роботі уточнено сутність і зміст категорій «інформаційна безпека» та «політична стабільність», визначено їх взаємозв'язок у контексті сучасних гібридних загроз, що дало змогу комплексно розглянути інформаційну безпеку не лише як технічний чи правовий інструмент, але й як елемент політичного управління, суспільної комунікації та національної стійкості. На теоретичному рівні результати дослідження можуть слугувати основою для подальших наукових пошуків, зокрема в галузях політології, національної безпеки, кібернетики, соціальних комунікацій та державного управління.

Практичне значення отриманих результатів проявляється у можливості застосування сформульованих висновків і рекомендацій у діяльності органів державної влади, інституцій сектору безпеки й оборони, а також у розробці стратегічних документів у сфері інформаційної безпеки. Запропоновані положення можуть бути використані для вдосконалення державної політики щодо протидії інформаційним загрозам, підвищення ефективності комунікацій між владою та суспільством, удосконалення механізмів кіберзахисту та системи стратегічних комунікацій. Крім того, результати дослідження можуть бути впроваджені у навчальний процес закладів вищої освіти при викладанні дисциплін з інформаційної безпеки, політології, медіаграмотності та державного управління.

Апробація результатів дослідження. Презентація результатів дослідження перед науковою спільнотою реалізована шляхом публікації наукових статті в науковому журналі «Політікус» у співавторстві з науковим

керівником на тему: «Інформаційна війна в контексті національної безпеки України: загрози та виклики».

Структура роботи. Структура кваліфікаційної роботи визначена заявленою метою та завданнями. Робота складається зі вступу, трьох розділів, що містять дев’ять підрозділів, висновків, списку використаної літератури. Загальний обсяг кваліфікаційної роботи становить 92 сторінки, із них 83 сторінки основного тексту. Список використаних джерел налічує 76 найменувань.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ЕЛЕМЕНТА ПОЛІТИЧНОЇ СТАБІЛЬНОСТІ ДЕРЖАВИ

1.1. Поняття, сутність та правові засади інформаційної безпеки держави

Сьогодні інформація стала одним із ключових чинників, що формують матеріальне середовище життя людини, проявляючись у вигляді новітніх технологій, програмного забезпечення та інших продуктів. Водночас вона є основою для взаємодії між людьми, безперервно створюючись і оновлюючись у процесі переходу між різними інформаційними системами. Така роль інформації в сучасному суспільстві вимагає ставитися до неї не тільки як до цінного ресурсу або товару, а й шукати та забезпечувати шляхи для контролю та захисту. Тому, розглядаючи сутність інформаційної безпеки, потрібно звернутися до поняття «інформація».

Взагалі, інформація походить від латинського «information» і перекладається: ознайомлення, роз’яснення. Для розуміння сутності інформації можна частково продемонструвати узагальнені підходи, які були складені українським дослідником В. Шульгою:

Таблиця 1.1

Узагальнені підходи до формулювання поняття «інформація»

Дослідник	Визначення
Н. Вінер	Інформація є інформація, не матерія й не енергія. Це позначення змісту, отриманого від зовнішнього світу в процесі пристосування до нього.
А.М. Яглом	Здатність знаків викликати образи
К. Шеннон	Комунікація й зв'язок, у процесі якої усувається невизначеність
А.Д. Урсул	Передача відбиття розмаїтості в процесі й об’єктах

Джерело: [74]

Таким чином, аналізуючи різні підходи, які пояснюють сутність інформації можна побачити, що цей термін не має універсального визначення та характеризується складністю та багатогранністю.

Так, українська бібліотечна енциклопедія трактує інформацію таким чином: «…у загальному тлумаченні – зафіксовані в документній формі або публічно виголошені відомості про події та явища в суспільстві, державі, довкіллі, які людина сприймає безпосередньо за допомогою власних органів чуття чи спеціальних пристроїв як віддзеркалення фактів матеріального або духовного світу в процесі використання різних каналів комунікації, включно із засобами масової інформації, текстовими, вербальними повідомленнями; джерелом інформації є також взаємодія з природою» [50]. В Законі України «Про інформацію» надається більш коротке визначення, що обмежено сферою дії закону, призначеного регулювати відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації: «будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» [21].

Окремо інформація розглядається різними науками та галузями. Є цікавим розуміння цього поняття суспільними науками, де важливим є вивчення того, як інформація існує та поширюється в суспільстві, її взаємозв’язок із документами, що слугують засобом її фіксації, а також її роль у соціальній, економічній та політичній сферах.

Також інформацію потрібно розглядати на двох рівнях: макрорівні та мікрорівні. Для цього дослідження важливий є саме макрорівень, бо на макрорівні інформація є не просто ресурсом, а стратегічним інструментом розвитку та безпеки, що визначає конкурентоздатність держави, її стійкість до зовнішніх загроз та здатність ефективно управляти суспільством.

Тому розуміння важливості та значення інформації для держави доводить необхідність забезпечення захисту або доступу інформації. Таким

чином, в сучасних умовах стає необхідність формування інформаційної безпеки держави.

Термін «інформаційна безпека» уперше з'явився наприкінці 1980-х років у роботі німецького дослідника Я. М. Жаркова, де підкреслювалася значущість інформаційної складової в системі міжнародної безпеки та робилася спроба всебічно проаналізувати проблеми, пов'язані з інформаційними загрозами [74].

Осмислення терміна «інформаційна безпека» є одним із ключових завдань наукових досліджень. Сутність цього поняття розкривається через загальніше поняття безпеки, яке в широкому сенсі розуміють як процес контролю та реагування на загрози й ризики. Відтак «інформаційна безпека» трактується як управління небезпеками та загрозами, що виникають у сфері інформаційного простору.

У наукових джерелах можна знайти значну кількість різних трактувань терміна «інформаційна безпека». Варто підкреслити, що наукова спільнота поки не виробила узгодженого підходу до визначення поняття «інформаційна безпека». Для одних дослідників воно описує певний стан, для інших — процес, вид діяльності, здатність, систему забезпечення, характеристику чи функцію.

Зокрема, О. Данільян, О. Дзьобань і М. Панов трактують інформаційну безпеку як захищеність об'єкта від інформаційних загроз або шкідливих впливів, пов'язаних з обігом інформації, а також як забезпечення нерозголошення відомостей про об'єкт, що становлять державну таємницю [62, с. 92].

В. Гурковський визначає інформаційну безпеку як систему суспільних відносин, що забезпечують захист життєво важливих інтересів особи, суспільства й держави від реальних або можливих загроз у інформаційному просторі [14, с. 74].

За думкою Р. Калюжного, інформаційна безпека є видом суспільних інформаційних правовідносин, що стосуються створення, підтримки, охорони та захисту безпечних умов життя для людини, суспільства і держави. Вона також охоплює спеціальні правовідносини, пов’язані зі створенням, зберіганням, поширенням та використанням інформації [30, с. 18].

Через властивість управління загрозами і небезпеками пропонує розглядати інформаційну безпеку В. Шульга [74].

І. Бондар пропонує розглядати інформаційну безпеку, як інтегральну цілісність чотирьох складових – персональної, суспільної, комерційної й державної безпеки [6, с. 69].

І. Громико розглядає інформаційну безпеку як стан захищеності державних інтересів, що передбачає запобігання, виявлення та нейтралізацію внутрішніх і зовнішніх інформаційних загроз, забезпечення інформаційного суверенітету країни та безпечний розвиток міжнародного інформаційного співробітництва [13, с. 134].

В. Шатун та О. Гладун визначають інформаційну безпеку як процес контролю та управління загрозами й ризиками, що походять від державних і недержавних структур, а також окремих громадян, з метою забезпечення інформаційного суверенітету України [71, с. 137].

У зарубіжних наукових джерелах систему інформаційної безпеки зазвичай розглядають як комплекс заходів щодо захисту інформації, що включає такі ключові елементи, як цілісність, доступність і конфіденційність даних [62, с. 94]:

- Цілісність інформації означає її властивість залишатися незмінною для неавторизованих користувачів або процесів, тобто зберігати стан, встановлений її творцем або законним власником; до цілісності також відноситься достовірність інформації, тобто її відповідність дійсності;

- Конфіденційність характеризує здатність інформації бути недоступною для осіб без відповідних прав і пов’язана з обмеженням доступу залежно від режиму інформації;
- Доступність полягає в тому, що уповноважений користувач може отримати та використовувати інформацію відповідно до встановлених правил без очікування понад допустимий час, тобто у потрібному форматі та в потрібному місці у момент потреби.

При розгляді сутності поняття «інформаційна безпека» варто зазначити, що в англійській мові існують два терміни, які однаково перекладаються українською, але мають різний зміст: «safety» та «security». Перший означає стан захищеності об’єкта, тоді як другий підкреслює діяльність, спрямовану на забезпечення цього стану. Відтак інформаційну безпеку можна визначати як стан, що характеризується відсутністю загроз і небезпек для об’єкта у інформаційно-комунікаційному середовищі, а також як здатність об’єкта ефективно захищатися, нейтралізувати та протидіяти різним інформаційним загрозам [43, с. 9].

Варто також зазначити, що деякі дослідники приділяють особливу увагу інформаційно-психологічним та державно-ідеологічним аспектам інформаційної безпеки, що обумовлено поділом інформаційної сфери на інформаційно-технічну та інформаційно-психологічну складові [62].

Важливим є також зіставлення національної безпеки та інформаційної. Так, чинна Стратегії інформаційної безпеки України за 2021 р., дає таке визначення поняттю інформаційної безпеки: «…складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню

шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом» [66]. А в статті 17 Конституції України згадується, що «захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави». Тому складовою національної безпеки можна визнати інформаційну безпеку [34]. Також відповідно до закону України «Про інформацію» забезпечення інформаційної безпеки є одним із основних напрямів державної інформаційної політики [21].

Взагалі, нормативно-правове розуміння інформаційної безпеки відображене у багатьох законах та інших правових актах України, що регулюють відносини в цій сфері. Насамперед слід зазначити, що поняття інформаційної безпеки охоплює широкий спектр складових елементів. Так, ще в Законі України «Про Концепцію Національної програми інформатизації» інформаційну безпеку вперше офіційно визначено як складову політичної, економічної, оборонної та інших сфер національної безпеки [22]. Згодом у Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» вперше на законодавчому рівні було закріплено визначення інформаційної безпеки як стану захищеності життєво важливих інтересів особи, суспільства та держави [23].

Також належність інформаційної безпеки до національної можна пояснити наявністю певних чинників [43, с. 11]:

- Національні інтереси, загрози їм та заходи щодо їхнього захисту у всіх сферах національної безпеки реалізуються та забезпечуються через інформацію та інформаційну сферу.

- Людина та її права, інформація і інформаційні системи, а також права на них є ключовими об’єктами не лише інформаційної безпеки, а й всіх інших видів безпеки.
- Виконання завдань у сфері національної безпеки сьогодні неможливе без використання інформаційно-комунікаційних засобів і технологій, які стали основними інструментами на сучасному етапі.
- Проблеми національної безпеки мають інформаційний характер.

Слід коротко окреслити й взаємозв’язок між поняттями «інформаційна безпека» та «безпека інформації». Перший термін має ширше значення і включає другий. Так, безпека інформації визначається як стан захищеності інформації, при якому гарантується її конфіденційність, доступність та цілісність. Крім самої інформації, до об’єктів безпеки інформації часто відносять також інфраструктуру, що забезпечує її обробку та передачу [43, с. 12].

Можна узагальнити, що частина дослідників інформаційну безпеку держави трактують як стан, розвиток або умови функціонування суспільства, його структур, інститутів та установ, за яких забезпечується збереження їхньої якості, автономності, природної відповідності та інноваційної здатності до функціонування.

Інші ж науковці оцінюють інформаційну безпеку з точки зору розвитку інформаційного простору держави та суспільства, розуміючи її як стан захищеності інформаційного середовища, за якого забезпечується його формування, ефективне використання та розвиток на користь особистості, суспільства і держави, незважаючи на вплив внутрішніх і зовнішніх інформаційних загроз.

Для кращого розуміння доречно використати узагальнення підходів до визначення сутності поняття інформаційної безпеки, яку розробила дослідниця В. Шульга на основі трактувань багатьох вчених [74]:

- Стан захищеності інформаційного простору;
- Процес управління загрозами та небезпеками;
- Стан захищеності національних інтересів;
- Захищеність встановлених законом правил;
- Суспільні відносини пов’язані із захистом життєво важливих інтересів людини і громадянина, суспільства та держави;
- Важливі функції держави;
- Невід’ємна частина політичної, економічної, оборонної та інших складових національної безпеки.

Окрім вищеназваних підходів, також існують більш загальні та лаконічні три основні підходи [71, с. 138]:

- Статичний — розглядає безпеку як стан захищеності інформаційного середовища чи інформації та систему гарантій;
- Діяльнісний — розглядає безпеку як процес її забезпечення та здатність держави ефективно захищати національні інтереси та цінності;
- Комплексний — поєднує обидва аспекти — стан і процес.

Інформаційну безпеку держави можна розглядати як ключову функцію державного управління та невід’ємну складову національної безпеки, що охоплює низку взаємопов’язаних аспектів. Це, зокрема, захищеність інформаційного простору та національних інтересів у ньому, процес управління інформаційними загрозами для збереження суверенітету держави, дотримання законодавчих норм, що регламентують інформаційні процеси, а також організацію суспільних відносин для захисту життєво важливих інтересів громадян, суспільства і держави від реальних і потенційних загроз у інформаційній сфері.

В центрі концепції інформаційної безпеки знаходиться принцип «інформаційного гуманізму», який гарантує захист об’єктів соціальної природи [43, с. 9].

Інститут інформаційної безпеки в системі інформаційного права реалізує правові, організаційні та технічні заходи, що забезпечують безпеку всіх компонентів інформаційно-комунікаційної системи держави: інформаційних ресурсів, інфраструктури, науково-технічного і виробничого секторів інформаційної індустрії, ринку інформаційної продукції та послуг, системи масової інформаційної освіти, просвіти та підготовки професійних кадрів для роботи в інформаційній сфері [43, с. 9].

Водночас до інформаційної безпеки доцільно відносити сукупність суспільних відносин, які формуються у процесі захисту конституційних прав і свобод від внутрішніх та зовнішніх загроз у сфері інформації.

Інформаційна безпека насправді є доволі багатогранним і складним явищем.

По-перше, вона має об’єктивний характер, оскільки зумовлена закономірностями суспільного розвитку. Також формування інформаційної безпеки відбувається в умовах інформатизації суспільства, яке й досі перебуває на етапі становлення та потребує подальшого ґрунтовного дослідження.

По-друге, складність визначення терміна «інформаційна безпека» пов’язана з тим, що він розглядається в різних наукових площинах — технічній, правовій, психологічній, соціальній тощо.

Представники різних наукових напрямів наповнюють це поняття власним змістом відповідно до специфіки своїх досліджень, що ще раз підкреслює його багатовимірність і ускладнює формування універсального визначення.

1.2. Політична стабільність: визначення, критерії та фактори забезпечення

Питання політичної стабільності належить до ключових і найактуальніших напрямів дослідження в сучасній політичній науці. У період активних суспільних трансформацій і реформ саме політична стабільність визначає, наскільки результативно вдасться реалізувати заплановані зміни в усіх сферах життя суспільства та наскільки стійкою є взагалі політична система держави.

Тому, в рамках нашого дослідження, досить важливо проаналізувати сутність політичної стабільності.

Для початку, поняття стабільності, зважаючи на швидкі темпи суспільного розвитку, має багатовимірний характер і може використовуватися в різних смислах. У сучасному науковому дискурсі під терміном «стабільність» зазвичай мають на увазі сталість розвитку певних елементів, що забезпечує їхнє повноцінне та безперешкодне функціонування протягом тривалого часу. Як характеристика, що визначає ефективність функціонування та життєдіяльності, стабільність проявляється в усіх сферах суспільного буття. Також з погляду суспільних наук, стабільність розглядається у зв'язці зі сферою суспільного життя (економічної, соціальної, політичної, військової тощо) [76, с. 62].

Одне з ранніх визначень політичної стабільності тлумачить її як систему взаємозв'язків між різними політичними суб'єктами, якій притаманні цілісність і здатність ефективно виконувати свої функції [45, с. 108]. Подібне за змістом визначення подане й у «Філософії політики: Короткому енциклопедичному словнику», де політичну стабільність розуміють як стан політичної системи суспільства, що характеризується стійкими та цілісними зв'язками між політичними акторами, а також їхньою здатністю до

результативної та конструктивної взаємодії [76, с. 62]. Але такі трактування майже не враховують динамічні аспекти політичної стабільності, що робить.

Піднімав тему політичної стабільності А. де Токвіль на прикладі Франції перед Великою революцією. Також Б. Барі вважав, що основне завдання політичної стабільності – забезпечувати стійкий політичний устрій. Дж. Роулс, аналізуючи питання політичної стабільності в демократичних державах, пропонує концепцію справедливості як інструмент ефективного вирішення проблем стабільності в умовах сучасних плюралістичних суспільств. Також одні вчені вважали, що політична стабільність виявляє стан політичного життя, а інші – виявляли хвилеподібні коливання у стабільності політичних систем і періодичності кризових ситуацій. Також деякі дослідники відмічали, що стабільність існує завдяки балансу інтересів різних соціальних груп. [45, с. 107-108].

У сучасній науковій літературі термін «політична стабільність» використовується доволі часто, однак його зміст і досі не має однозначного трактування. Дослідники погоджуються в тому, що це поняття є складним, багатовимірним і охоплює узагальнену, комплексну та функціональну характеристику якості взаємодії ключових політичних суб'єктів, ефективності роботи органів влади, а також здатності політичного керівництва й суспільства загалом адекватно реагувати на виклики часу, вирішувати актуальні завдання, зберігаючи стійкість та необхідний рівень згоди між основними політичними силами [54, с. 161].

Політичну стабільність потрібно розглядати як один з вимірів соціальної стабільності. Окрім цього, політична стабільність є якісною властивістю політичної системи.

Для систематизації ключових положень про політичну стабільність доречно розглянути її з точки зору різних підходів. Для цього доречно буде використати дослідження українських науковців О. Баталова та М. Паламарчук:

Таблиця 2.1

Основні підходи до визначення політичної стабільності

Підхід	Характеристика
Інституціональний	Оцінювання стійкості політичних інститутів та їхньої спроможності гарантувати безпеку, законність і належне функціонування політичної системи. У межах цього підходу аналізується роль і результативність ключових політичних установ — парламенту, уряду, судової влади та інших.
Соціально-економічний	Урахування рівня соціальної стабільності та стану економічного розвитку як ключових чинників політичної стабільності. Цей підхід передбачає аналіз впливу економічних і соціальних факторів на політичний порядок та загальну стабільність системи.
Психологічних	Аналіз взаємин між політичними лідерами та громадянами, дослідження психології мас і рівня громадянської довіри. Оцінюється сприйняття влади, легітимність політичних лідерів та задоволеність громадян політичними процесами.
Геополітичний	Врахування зовнішніх чинників, зокрема міжнародних відносин і геополітичного середовища. Досліджується вплив зовнішніх сил на політичну стабільність держави чи регіону, зокрема через дипломатичні відносини, міжнародні угоди та геополітичні конфлікти.
Системний	Розгляд політичної стабільності як результату взаємодії різних системних компонентів — політичних, економічних, соціальних та інших. Оцінюється їхня взаємозалежність і вплив один на одного, що дає змогу сформувати комплексне уявлення про стан політичного середовища.

*Джерело: сформовано на основі [*2, с. 16*]*

Більшість дослідників відмічають складність та багатогранність політичної стабільності, тому окрім наведених підходів, цей явище можна розглядати як:

- Впорядкованість суспільних відносин і узгоджене функціонування різних складових суспільної системи;

- Баланс різних політичних сил та інтересів;
- Вияв демократичної форми управління;
- Відсутність реальної загрози нелегітимного насильства в суспільстві або наявність у держави ресурсів для її подолання в умовах кризи.

У західній політології політична стабільність здебільшого розглядається як різновид соціальної стабільності — стан взаємозбалансованості різних соціальних груп і політичних сил, за якого жодна з них не має можливості змінити політичну систему на власну користь [54, с. 162].

Якщо брати до уваги, що політична стабільність є характеристикою функціонування політичної системи держави, то можна виявити певні особливості цього явища.

По-перше, політична стабільність має багатовимірну природу і проявляється на всіх рівнях та у всіх підсистемах політичної системи. Так, наприклад, політична стабільність в контексті інформаційної безпеки — це баланс між вільним потоком інформації, контролем її достовірності та забезпеченням безпеки, що підтримує стійке функціонування політичної системи.

По-друге, політична стабільність є динамічним явищем, що проявляється через хвилеподібні коливання політичної системи, існуючі виклики та адекватні реакції на них.

По-третє, політична стабільність — це властивість, яка проявляється в процесі функціонування політичної системи та водночас є результатом цього функціонування. Іншими словами, політична система держави повинна забезпечувати політичну стабільність.

По-четверте, суть політичної стабільності полягає у забезпеченні порядку, що проявляється через ефективність роботи органів влади, їх легітимність та сталість норм і цінностей політичної культури [32].

По-п’яте, важливим чинником впливу на політичну стабільність є масова підтримка влади з боку суспільства. Рівень такої підтримки

визначається стійкістю позитивних оцінок та думок, що відображають схвалення діяльності органів влади. Підтримка населення запобігає конфліктам, свідчить про консолідованість суспільства та є показником ефективності функціонування політичної системи [76, с. 63]

І останнє, протилежним до політичної стабільності є нестабільність. Тобто наявність або відсутність конфліктів у суспільстві, зокрема культурних, ідеологічних та соціально-економічних розколів.

Цікаво відмітити, що часто виділяють декілька типів політичної стабільності, де основними є: демократична стабільність та стабільність «не демократій». Тобто питання політичної стабільності по-різному себе проявляє в залежності від політичного режиму [33, с. 126]. Стабільність демократії проявляє себе через здатність демократичних структур ефективно та швидко реагувати на зміни суспільних настроїв і забезпечувати громадянської згоди. Стабільність «не демократій» досягається шляхом авторитарних методів.

Також потрібно відзначити, що існує безліч типологій політичної стабільності, де потребують уваги такі різновиди [76, с. 64]:

- Абсолютна політична стабільність є теоретичною категорією, оскільки в реальному житті немає механізмів для її досягнення. Її можна уявити лише в умовах повністю ізольованих політичних систем, які не мають контактів із зовнішнім середовищем. Для демократичних режимів досягнення такої стабільності на практиці неможливе;
- Статична стабільність проявляється у сталій, непорушній структурі політичних традицій і норм. Вона ґрунтується на прагненні зберегти консервативні цінності, формувати стереотипи політичної поведінки та підтримувати домінуючу ідеологію;
- Динамічна політична стабільність виступає активною та конструктивною основою для функціонування і самовідтворення демократичних режимів. Зміни в рамках демократії відбуваються через процес

політичної наступності та здатність відкритих систем ефективно реагувати на внутрішні й зовнішні впливи;

- Стагнаційна стабільність характеризується застійним станом, уповільненням або припиненням політичних змін і процесів, а також руйнуванням структур політичного життя. Подібна політична система приречена на занепад, зупинку розвитку та загальний політичний регрес;
- Консолідаційна стабільність характерна для демократичних режимів і формується на основі широкої суспільної згоди, взаємоповаги між різними соціальними групами та підтримки громадянського миру. Вона забезпечує ефективне функціонування політичних інститутів і сприяє довготривалому розвитку демократичної системи.

На основі цієї типології, для сучасної України найбільш характерною є динамічна політична стабільність з елементами консолідаційної стабільності. Система здатна адаптуватися до змін, підтримує демократичні інститути та реагує на внутрішні й зовнішні виклики, при цьому певна консолідація суспільства забезпечує стійкість у критичних ситуаціях.

Окрім характеристики політичної стабільності, важливо також розглянути дестабілізаційні аспекти політичної системи. Зазвичай їх ділять на три наступні види [33, с. 125].

Системна дестабілізація характеризується порушенням закономірностей та тенденцій цілісного й комплексного розвитку політичної системи, що негативно впливає на стійкість усіх її інститутів. Внаслідок цього порушується узгодженість між різними ланками влади, що підриває загальну координацію політичних процесів та створює ризики втрати системної рівноваги.

Когнітивна дестабілізація формується через порушення раціонального розподілу владних повноважень між суб’єктами політичної системи, коли дестабілізуючі чинники обмежують або спотворюють доступ до повної і достовірної інформації щодо подій і процесів у суспільстві. Це ускладнює механізми прийняття та узгодження рішень на різних рівнях управління,

знижує ефективність функціонування політичних інститутів і створює загрозу стабільності системи.

Функціональна дестабілізація проявляється в процесі реалізації повноважень, планів та програм політичних суб'єктів і спрямована на створення умов для негативних наслідків їхньої діяльності. Вона може виявлятися у вигляді зриву політичних ініціатив, невиконання програм або реалізації заходів, що підривають ефективність політичних процесів, що в підсумку призводить до загального політичного регресу та послаблення стабільності суспільства.

З погляду факторів, що визначають стан стабільності як важливу якісну характеристику політичної системи, яка забезпечується ефективними взаємозв'язками між усіма її складовими, можна виділити об'єктивні та суб'єктивні чинники [33, с. 125].

Таблиця 2.1

Чинники політичної стабільності

Суб'єктивні чинники	Об'єктивні чинники
Ефективність влади	Стійкість політичних інститутів
Легітимність влади	Ефективність системи поділу влади
	Політична культура суспільства

Джерело: сформовано на основі [33]

Безсумнівно, ключовим суб'єктом у забезпеченні політичної стабільності є держава та її інститути. Як вже відмічалося раніше, рівень і характер політичної стабільності в державі значною мірою залежать від типу політичного режиму, що в ній функціонує, будь то демократичний, авторитарний або інший. Відповідно до цього відрізняються й механізми, за допомогою яких забезпечується підтримання політичної стабільності.

Наприклад, авторитарним режимам властива особлива форма стабільності, яка дозволяє державі зберігати цілісність навіть за надзвичайно складних умов. Механізми підтримки такої стабільності спрямовані на

формування закритого, соціально однорідного суспільства, де регулювання будь-яких відносин здійснюється через насильство. Така стабільність веде до застою та політичної стагнації [54, с. 162].

На противагу стабільності авторитарної, в демократичному суспільстві наявна відкрита система, яка здатна відносно безболісно адаптуватися до змін внутрішнього та зовнішнього середовища. Для такої системи характерна динамічна стабільність, яка включає політичний плюралізм і багатопартійність, де конкуренція за владу відбувається в межах загальноприйнятих демократичних правил. Відкритість системи забезпечує швидке та ефективне реагування на виклики, що виникають у зовнішньому та внутрішньому середовищі. Ця форма стабільності є живою, конструктивною і сприяє самовідтворенню демократичних режимів, забезпечуючи оптимальні умови для нормального функціонування політичної системи.

На фоні цього порівняння в сучасному соціально-політичному середовищі більш прийнятною є саме політична стабільність демократичного типу. Тому важливо узагальнити основні фактори та умови, які дозволяють ефективно досягати політично стабільності в державі [33, с. 127]:

1. легітимність політичного режиму та його законність;
2. підтримання високого рівня довіри населення до органів влади через подолання бюрократичних перешкод і корупції;
3. здатність політичної системи ефективно функціонувати та швидко реагувати на внутрішні й зовнішні виклики;
4. наявність ефективної правової системи в державі;
5. гарантування прав і свобод громадян та підтримка прагнення населення брати участь у політичному житті країни;
6. забезпечення оптимального балансу між моральними нормами та правом у суспільстві;
7. підтримання гармонійної класової структури суспільства;
8. запобігання загостренню соціально-етнічних і релігійних конфліктів;

9. ефективна політична комунікація та взаємодія влади з населенням;

10. використання владою міжнародного досвіду в сфері державного та політичного розвитку.

Також цікавою є думка політолога Дж. Лінца, який вважає основою політичної стабільності три елемента: легітимність, дієвість та ефективність. Легітимність виступає як підтримка влади, дієвість як здатність вирішення проблем, а ефективність як здатність впровадження рішень з бажаними результатами [76, с. 63].

Аналізуючи чинники, фактори та умови політичної стабільності, варто звернути й на стан України в цьому полі досліджень.

Для української політичної системи характерна чітка зміна фаз стабілізації та дестабілізації. Також слід відзначити позитивну динаміку темпів і масштабів політичних перетворень та реформ у різних сферах. В Україні послідовно здійснюється реформування численних сфер політичного, економічного та суспільного життя.

Окрім цього, для України характерна слабка ефективність процесів формування демократичних інститутів політичної системи. Це пояснюється, зокрема, інертністю та реакційністю політичної еліти, що знижує рівень довіри населення до інституцій влади та їхніх представників.

Серед позитивних змін, варто відмітити помітне зростання рівня політичної свідомості населення, а також активності організацій громадянського суспільства у політичному житті України.

Також здатність забезпечувати політичну стабільність в Україні обмежується через низьку ефективність державного управління, пронизаного корупцією та браком професійних кадрів. Додатково цьому сприяє нестійка судова система та відсутність надійних гарантій права приватної власності [54, с. 167].

Політична стабільність української політичної системи значною мірою визначається різницею інтересів окремих осіб, соціальних груп та політичних

акторів. Це об’єктивно створює суперечності всередині системи, породжує різноманітні конфлікти та чинники їх виникнення, що, у свою чергу, підвищує ймовірність порушення стабільності в суспільстві.

Таким чином, в сучасному світі політична стабільність виступає ключовим чинником ефективного функціонування політичних систем та запобігання конфліктам.

1.3. Інформаційна безпека як засіб протидії деструктивним інформаційно-психологічним впливам на політичну стабільність

Інформаційна безпека є невід’ємною частиною національної безпеки та виступає одним із ключових пріоритетів державної політики. Вона охоплює два взаємопов’язані напрями: з одного боку — забезпечення громадянам повного, достовірного та вільного доступу до різноманітних інформаційних джерел; з іншого — запобігання поширенню дезінформації, захист цілісності суспільства, збереження інформаційного суверенітету та протидія негативним інформаційно-психологічним впливам, включно з маніпуляціями, інформаційними війнами та операціями. Вирішення цих комплексних завдань дозволяє водночас захищати державні та суспільні інтереси й гарантувати громадянам право на отримання об’єктивної, всебічної та якісної інформації.

Для питання інформаційної безпеки в контексті політичної стабільності потрібно звернути увагу на об’єкти, інтереси та види інформаційної безпеки.

Взагалі, об’єктами й суб’єктами інформаційної безпеки можуть бути як окремі індивіди, так і суспільство або держава, бо й інформаційно-психологічні впливи відбувається над цими самими об’єктами.

В рамках впливу на політичну стабільність варто та важливо звертати увагу не тільки на інтереси держави в інформаційній сфері, а й на інтереси особи та суспільства.

Так, наприклад основними інтересами індивіда в інформаційній сфері є [28, с. 12]:

- забезпечення реалізації гарантованих прав людини й громадянина на отримання інформації та користування нею для здійснення дозволеної законом діяльності, а також для власного фізичного, духовного й інтелектуального розвитку;
- охорона такої інформації, яка є необхідною для гарантування особистої безпеки.

Інтересами суспільства в інформаційній сфері можна виділити такі [28, с. 12]:

- захист та просування інтересів кожної людини в інформаційній сфері;
- посилення демократичних засад державного устрою;
- формування правової та соціально орієнтованої держави;
- забезпечення й збереження стабільності та громадського спокою;
- сприяння духовному оновленню та моральному зміцненню держави.

На останок, інтереси держави в інформаційній сфері, зазвичай виділяють такі [28, с. 12]:

- збалансований й цілісний розвиток національної інформаційної інфраструктури;
- повна реалізації прав і свобод громадян щодо отримання та використання інформації, що сприяє збереженню устрою, суверенітету й територіальної цілісності держави, підтримці політичної, економічної та

соціальної стабільності, дотриманню законності й правопорядку, а також розвитку рівноправного та взаємовигідного міжнародного партнерства.

Дивлячись на інтереси кожного об’єкта інформаційної безпеки, можна однозначно визначити, що багато в чому ці інтереси збігаються тому в рамках розгляду політичної стабільності потрібно звертати увагу не тільки на інформаційну безпеку держави, а й включати сюди інформаційну безпеку особи та суспільства.

На основі цього твердження науковці також виділяють й три рівні або види інформаційної безпеки відповідно до об’єкта.

Так, інформаційною безпекою особи можна визначити як стан захищеності індивіда, за якого її психічний стан і здоров’я не зазнають шкідливого інформаційного впливу, що міг би спотворити сприйняття реальності або негативно позначитися на фізичному самопочутті [28, с. 13].

Інформаційна безпека суспільства визначається як здатність суспільства й кожного його члена без обмежень користуватися своїми конституційними правами на вільне отримання, створення та поширення інформації, а також рівень їхньої захищеності від шкідливих інформаційних впливів [28, с. 13].

Відповідно до визначень цих двох видів інформаційної безпеки, можна виявити, що інформаційна безпека особи та суспільства багато в чому між собою тісно пов’язані.

В контексті політичної стабільності важливо також представити й такий варіант характеристики інформаційної безпеки: інформаційна безпека держави — це такий рівень її захищеності, за якого зовнішні інформаційні атаки, спеціальні інформаційні операції, акти інформаційного тероризму, незаконне перехоплення даних технічними засобами, кіберзлочинність та інші руйнівні інформаційні впливи не здатні завдати істотної шкоди національним інтересам.

Забезпечення ж високого рівня для всіх видів інформаційної безпеки залежить від сукупного комплексу політичних, економічних та організаційних

дій, спрямованих на запобігання, виявлення й усунення умов, чинників і загроз, що можуть завдати шкоди або перешкодити реалізації інформаційних прав, потреб і інтересів держави та її громадян.

З огляду на вищесказане, можна сформувати проблему інформаційно-психологічної безпеки особи і суспільства як складової інформаційної безпеки держави.

Сучасні інформаційні технології та нові методи інформаційно-психологічного впливу на людину й суспільство дедалі активніше застосовуються не лише під час підготовки чи ведення воєнних операцій, а й поступово стають звичним елементом повсякденного життя. Маніпулятивні технології та інструменти впливу на масову свідомість нині можна побачити під час виборчих кампаній, у сфері реклами, а також у діяльності різноманітних мас-медіа [29, с. 43].

Деструктивні інформаційно-психологічні операції мають глибокі соціальні й політичні наслідки. Дослідження показують, що дезінформація і маніпуляція громадською думкою «стають потужними інструментами, здатними дестабілізувати політичний ландшафт, підривати довіру до державних інститутів і формувати поляризоване середовище» [3]. Такі атаки підривають єдність суспільства, посилюють розбрат за етнічними, релігійними чи ідеологічними лініями та підривають легітимність влади.

Іншими словами, інформаційний вплив прямо пов’язаний з політичною стабільністю. Формування неправдивих наративів може спричиняти соціальну напругу, протестні настрої і невдоволення владою, що, у свою чергу, послаблює спроможність держави ефективно діяти в кризових ситуаціях.

Як відповідь на інформаційно-психологічних впливів, можна коротко перерахувати ключові інструменти та засоби інформаційної безпеки для підтримування високого рівня політичної стабільності [28, с. 27-30]:

- Законодавче та нормативне регулювання: прийняття національних стратегій і законів (наприклад, «Стратегія інформаційної безпеки України»)

забезпечує правові основи протидії інформаційно-психологічним впливам та регулює джерела поширення цих впливів.

- Спеціалізовані органи і центри: ці органи повинні координувати, виявляти та спростування дезінформаційних кампаній, моніторити інформаційний простір і розробляти контрзаходи.
- Стратегічні комунікації: створення ефективної системи стратегічних комунікацій. Це передбачає використання інформаційних кампаній на підтримку власних політичних цілей і спростування ворожих наративів.
- Освіта та медіаграмотність: Підвищення рівня критичного мислення й інформаційної грамотності суспільства
- Технічні та кіберзахисні заходи: Забезпечення інформаційної безпеки через надійний захист інформаційної інфраструктури.
- Громадсько-експертна участь: окрім державних інструментів, важливо залучення громадських організацій, медіаекспертів та аналітичних центрів. Саме завдяки громадському моніторингу зростає швидкість реагування на реальні та потенційні негативні інформаційно-психологічні впливи.

Таким чином, важливо також звертати увагу на всі рівні інформаційної безпеки: особи, суспільства та держави. Інформаційна безпека повинна приділяти увагу усім об’єктам інформаційно-психологічного впливу. Мати ефективні засоби протидії деструктивним впливам важливо для підтримання високого рівня політичної стабільності.

Отже, у першому розділі розкрито поняття, сутність і правові засади інформаційної безпеки, поняття «політичної стабільності» та проаналізовано значення інформаційної безпеки для політичної стабільності.

Аналіз різних підходів до визначення поняття «інформаційна безпека» демонструє відсутність усталеного трактування, однак дає змогу окреслити низку спільних характеристик. Інформаційна безпека може розглядатися як:

стан захищеності інформаційного простору, національних інтересів та життєво важливих прав громадян; процес управління загрозами, спрямований на нейтралізацію внутрішніх та зовнішніх впливів; система суспільних відносин, що забезпечує дотримання встановлених законом норм та функціонування інформаційної інфраструктури; невід'ємна складова національної безпеки.

Також вітчизняні та зарубіжні дослідники акцентують увагу на тому, що інформаційна безпека охоплює як технічну сферу, так і інформаційно-психологічну, пов'язану з впливами на суспільну свідомість, цінності та політичну поведінку.

Окремо розкрито поняття політичної стабільності, що постає як складне, багаторівневе явище, визначає ефективність функціонування політичної системи та здатність держави протистояти внутрішнім і зовнішнім викликам. Її сутність пов'язують зі стійкістю політичних інститутів, ефективною взаємодією політичних акторів, легітимністю влади, соціально-економічною стабільністю та здатністю держави забезпечити прогнозований розвиток.

Було звернуто увагу на ключову роль інформаційної безпеки як засобу захисту політичної стабільності держави від деструктивних інформаційно-психологічних впливів. Проаналізовано, що сучасні інформаційні загрози мають психологічний та соціальний характер, й спрямовані на маніпулювання свідомістю громадян, дискредитацію політичних інститутів та дестабілізацію суспільства.

Встановлено, що ефективна інформаційна безпека має включати комплекс превентивних, захисних та контрзаходів, які дозволять виявляти, оцінювати та нейтралізувати загрози в інформаційному середовищі.

РОЗДІЛ 2
АНАЛІЗ СУЧАСНИХ ІНФОРМАЦІЙНИХ ЗАГРОЗ ПОЛІТИЧНІЙ СТАБІЛЬНОСТІ ДЕРЖАВИ

2.1. Класифікація та типологія загроз інформаційній безпеці держави

Для розгляду класифікацій та типологій загроз інформаційній безпеці, потрібно спочатку дати визначення загроз інформаційній безпеці та окреслити суть.

Взагалі, під загрозою зазвичай розуміють потенційно можливу подію, дію, процес або явище, які здатні завдати шкоди певним інтересам. Також, у науковій літературі загрозу трактують як вищий ступінь небезпеки або безпосередню загрозу; будь-який потенційно негативний вплив, етап максимального загострення протиріч, а також стан, що передує конфлікту [69, с. 191].

За визначенням експертів у галузі національної безпеки, загроза — це етап максимального загострення протиріч, що передує конфлікту, коли один із політичних суб'єктів готовий застосувати силу проти конкретного об'єкта для досягнення своїх політичних чи інших цілей [43, с. 40].

Також можна виділити наступні особливості загрози [43, с. 41]:

- динамічність та змінність, що охоплює події, процеси або дії;
- завдання шкоди або порушення нормального функціонування об'єкта (держави), що призводить до збитків і втрат;
- виникнення під впливом різних факторів (зовнішніх і внутрішніх), що вимагає комплексних заходів державного реагування для їхнього усунення та нейтралізації.

Таким чином, можна перейти до визначення «інформаційної загрози» та загрози інформаційній безпеці.

Так, наприклад, в Стратегії інформаційної безпеки України встановлено, що «інформаційна загроза - потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні» [66].

А в науковій літературі поняття «загрози інформаційній безпеці» подано у двох формулюваннях [44, с. 22; 69, с. 192]:

- комплекс обставин і чинників, які становлять загрозу життєво важливим інтересам людини, суспільства та держави в інформаційній сфері;
- явище, дії негативних факторів або процес, унаслідок яких соціальні суб'єкти інформаційної безпеки частково або повністю втрачають здатність реалізовувати свої інтереси в інформаційній сфері, а також порушується нормальне функціонування, відбувається руйнування або сповільнюється розвиток технічних об'єктів інформаційної безпеки.

Отже, аналізуючи ці два терміни, можна прийти висновку, що вони достатньо схожі по суті та сенсу.

Взагалі, виявлення та аналіз загроз інформаційної безпеки є ключовим елементом забезпечення її ефективності. У значній мірі структура розроблюваної системи захисту та склад механізмів її впровадження залежать від характеру потенційних загроз.

Загроза зазвичай виникає через існування слабких або вразливих точок у системі захисту інформаційних ресурсів. Історичний розвиток інформаційного середовища свідчить, що нові вразливості виникають постійно. Засоби захисту з'являються приблизно з такою ж регулярністю, хоча трохи пізніше, здебільшого як реакція на вже існуючі загрози. Тим не менш, у

цьому контексті більш ефективним є превентивний підхід до захисту, який передбачає створення механізмів для запобігання можливим, прогнозованим і потенційним загрозам.

Щодо саме типологізації загроз інформаційній безпеці держави, то фахівці пропонують велику різноманітність різних класифікацій.

Так, на думку деяких дослідників, загрози інформаційній безпеці можна поділити на три основні групи [28, с. 19]:

- загрози, пов’язані з впливом недостовірної, фальшивої або маніпулятивної інформації на особу, суспільство та державу;
- загрози несанкціонованого чи незаконного втручання сторонніх осіб у інформаційні ресурси та процеси їх створення, обробки і використання;
- загрози порушенню інформаційних прав і свобод людини, включно з правом на створення, поширення, пошук, отримання, передавання та використання інформації, правом інтелектуальної власності на інформацію та матеріальної власності на документовані дані, а також правом на захист честі та гідності.

Також загрози інформаційній безпеці можна поділити на два види: соціальні та технічні. Соціальні загрози обмежують чи роблять неспроможним особою та суспільством загалом реалізувати ключові інтереси в інформаційній сфері. Технічні загрози — порушують функціонування та виводять з ладу інформаційну інфраструктуру та інформаційні ресурси [43, с. 41].

Досить розгорнуту типологізацію надає В. Ліпкан:

Таблиця 2.1

Типологізація загроз інформаційній безпеці за В. Ліпканом

Критерій класифікації	Типи
За джерелами походження:	природного походження, техногенного походження, антропогенного походження
За ступенем гіпотетичної шкоди:	загроза та небезпека
За повторюваністю вчинення:	повторювані та продовжувані

За сферами походження:	екзогенні та ендогенні
За ймовірністю реалізації:	вірогідні, неможливі, випадкові
За рівнем детермінізму:	закономірні та випадкові
За значенням:	допустимі та неприпустимі
За структурою впливу:	системні, структурні та елементні
За характером реалізації:	реальні, потенційні, здійснені, уявні
За ставленням до них:	об’єктивні та суб’єктивні
За об’єктом впливу:	особа; суспільство; держава

Джерело: сформовано на основі [26, с. 109]

Цікавим є підхід, що передбачає класифікацію загроз інформаційній безпеці за напрямами діяльності держави [43, с. 44-46]:

1. Зовнішньополітична сфера: поширення недостовірної або упередженої інформації; комп’ютерні злочини та тероризм; зовнішній негативний інформаційний вплив через ЗМІ та інтернет.

2. Сфера державної безпеки: інформаційні впливи, спрямовані на підрив конституційного ладу, суверенітету та територіальної цілісності; несанкціонований доступ до інформаційних ресурсів органів влади.

3. Воєнна сфера: інформаційно-психологічний вплив на населення та військових для зниження обороноздатності і погіршення іміджу служби; несанкціонований доступ і незаконне використання інформації з питань оборони.

4. Внутрішньополітична сфера: слабка розвиненість інститутів громадянського суспільства, недосконаліть партійно-політичної системи та непрозорість політичної діяльності; негативний інформаційний вплив на свідомість окремих осіб та суспільства; неефективна державна інформаційна політика; недосконале законодавство.

5. Економічна сфера: відставання вітчизняних високотехнологічних і наукоємних виробництв; низький рівень інформатизації економіки; недостатній розвиток національної інформаційної інфраструктури.

6. Соціальна сфера: відставання у інформатизації соціальної та гуманітарної сфер, зокрема освіти, охорони здоров'я, соцзабезпечення та культури; порушення права громадян на інформацію; витіснення з інформаційного простору національного ЗМІ, мистецтва, кінематографу тощо.

7. Науково-технологічна сфера: зниження наукового потенціалу у сфері інформатизації та зв'язку; низька конкурентоспроможність інформаційної продукції на світовому ринку; відтік наукових кадрів; недостатній захист інформації через використання іноземних технологій

8. Екологічна сфера: приховування, несвоєчасне або недостовірне інформування населення про надзвичайні ситуації природного чи техногенного характеру; ненадійність інформаційно-телекомунікаційних систем збору, обробки та передачі даних в умовах надзвичайних ситуацій.

Окремо хочеться виділити інші розробки українських науковців. Так, класифікація одних дослідників ґрунтується на визначенні властивостей інформації, де визначаються такі типи: загрози порушення конфіденційності інформації; загрози порушення цілісності інформації; загрози порушення доступності інформації. Ряд інших науковців представляють таку типологію загроз: загрози впливу неякісної інформації; загрози незаконного або несанкціонованого втручання сторонніх осіб в інформаційні ресурси та дані; загрози інформаційним правам і свободам особистості [26, с. 109].

Також важливо звернутися й до нормативно-правових документів, які надають свій підхід та погляд на типи загроз.

Так у Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007 − 2015 роки» загрозами інформаційній безпеці визначено: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [23].

Також в Постанові Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» говориться, що система захисту призначається для захисту інформації від [49]:

- витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій;
- несанкціонованих дій з інформацією, у тому числі з використанням комп'ютерних вірусів;
- спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування.

В Державному стандарті України «Захист інформації. Технічний захист інформації. Терміни та визначення» – ДСТУ 3396.2-97 виділяються три типи загроз: загрози витоку інформації; загрози порушення цілісності інформації; загрози блокування інформації [24].

Необхідною частиною дослідження загроз інформаційній безпеці держави становлять їх джерела. Джерелами загроз можуть бути як суб'єкти (особа, група, організація, держава), так і об'єктивні фактори. Вони можуть походити як зсередини країни (внутрішні джерела), так і ззовні (зовнішні джерела) Всі джерела загроз поділяють на: антропогенні, де джерелом є суб'єкт; техногенні, де джерело – технічні засоби; стихійні джерел, де джерело – природні явища [43, с. 46].

Важливо також виділяти об'єкти або суб'єкти, на які впливають джерела загроз інформаційній безпеці.

Так, для особистості або індивіда небезпечним джерелом загроз є значне розширення можливостей маніпулювання свідомістю людини через створення

для неї індивідуального «віртуального інформаційного простору» та застосування технологій впливу на психіку. Ще одним небезпечним джерелом загроз інтересам особи є використання її персональних даних на шкоду, що накопичуються різними структурами, включно з органами влади, а також можливість прихованого збору інформації про особисте та сімейне життя, яка становить приватну таємницю [44, с. 24-25].

Для суспільства одне з джерел загроз інтересам суспільства в інформаційній сфері — це постійне ускладнення інформаційних систем і комунікаційних мереж критично важливих інфраструктур. Небезпеку також становить концентрація ЗМІ у руках обмеженої групи власників. Ще одним небезпечним джерелом загроз інформаційної безпеки є розширення масштабів комп'ютерної злочинності [28, с. 24].

Важливо також визначити джерела загроз для держави. Так, найперше загрози інтересам держави можуть проявлятися через незаконний доступ до інформації, що становить державну таємницю. Але найбільшу небезпеку для державних інтересів в інформаційному суспільстві становить неконтрольоване поширення інформаційної зброї, розвиток гонки озброєнь у цій сфері та спроби проведення інформаційних війн [44, с. 27].

Класифікації та типології загроз інформаційній безпеці держави є надзвичайно важливими, оскільки дозволяють систематизувати потенційні ризики, визначити їх пріоритетність та розробити ефективні заходи протистояння.

Класифікація загроз інформаційній безпеці має важливе теоретико-прикладне значення, оскільки забезпечує внутрішню впорядкованість системи інформаційної безпеки та виконує дві ключові функції: евристичну і аналітичну. Евристична функція дозволяє ідентифікувати існуючі загрози, досліджувати їхню природу та групувати за об'єктами, суб'єктами, часом і простором. Аналітична функція спрямована на розробку методів оцінки та

нейтралізації цих загроз, що підвищує ефективність захисту держави та підтримання її політичної стабільності.

2.2. Гібридні загрози та інформаційно-психологічні операції як фактор дестабілізації

Для ознайомлення з загрозами інформаційній безпеці особи, суспільства та держави, які у різних форма та методах впливають на політичну стабільність, потрібно дослідити та розкрити питання «гібридних загроз» та більш вузьких явищ, таких як: «гібридна війна», «інформаційна війна» та «інформаційно-психологічні операції».

Найбільш широким поняттям, яке розкриває зміст цієї теми, є «гібридні загрози». Детально проаналізовані підходи до визначення цього поняття, зробив міжнародний проект «WARN», де визначено декілька характеристик [9].

По-перше, гібридні загрози описуються як скоординовані й синхронізовані дії, спрямовані на використання системних вразливостей демократичних держав і їхніх інституцій. Вони охоплюють широкий спектр інструментів – від політичних і економічних до інформаційних чи військових.

По-друге, підкреслюється, що такі дії мають на меті вплив на процес ухвалення рішень, підрив стабільності або завдання шкоди об’єкту атаки. Гібридний вплив може реалізовуватися у політичній, економічній, військовій, цивільній та інформаційній сферах, часто одночасно.

По-третє, гібридні загрози характеризують як дії супротивника, який поєднує традиційні та нетрадиційні засоби боротьби, адаптуючи їх до конкретних умов. Серед таких інструментів можуть бути як звичайні військові

спроможності, так і засоби кібервпливу, інформаційні операції, підтримка терористичних груп чи кримінальних мереж.

По-четверте, стратегічна логіка гібридних дій спрямована на досягнення політичних або стратегічних результатів без відкритої війни. Об'єктом впливу стає не стільки армія противника, скільки саме суспільство: його свідомість, довіра до влади, соціальна стійкість. У межах такої моделі стирається різниця між цивільними та комбатантами, адже інформаційні, психологічні, економічні та інші інструменти застосовуються комплексно й одночасно.

По-п'яте, у теоретичній площині гібридні загрози визначають як наслідок поєднання різнорідних елементів, які у поєднанні формують багаторівневу та складну небезпеку. На відміну від гібридного конфлікту чи гібридної війни, це поняття охоплює ширший набір інструментів впливу та не обмежується військовими компонентами [9].

По-шосте, гібридні загрози часто постають як соціально небезпечні процеси, що формуються в умовах трансформації глобального безпекового середовища. Їх виникнення зумовлене синергією дій агресора, який поєднує [8, с. 11]:

- використання традиційних військових можливостей;
- застосування нетрадиційних методів боротьби – тероризму, диверсій, кримінальних схем, провокування внутрішніх конфліктів;
- невійськові засоби впливу, перетворені на інструмент тиску – дипломатичні, інформаційні, фінансові, торговельні, соціальні та інші.

Взагалі, головною метою гібридних загроз, судячи з характеристики, полягає у примушенні об'єкта агресії до вимог, що суперечать його національним інтересам, незалежно від оголошення війни [8, с. 11].

Однією з відповідей на численні виклики, які зумовлені впливом гібридних загроз, є розробка «Концептуальної моделі гібридних загроз» створена спільними зусиллями Об'єднаного дослідницького центру Європейської комісії (JRC) та Європейського центру передового досвіду з

протидії гібридним загрозам (Hybrid CoE). В цій моделі визначено чотири базові компоненти, вивчення яких є необхідним для повного розуміння структури та особливостей гібридних загроз [8, с. 18]:

- ворожі актори (та їхні стратегічні цілі);
- інструменти, які використовує ворожій актор;
- цільові сфери;
- фази (включаючи види діяльності, що спостерігаються в кожній фазі).

З цих компонентів важливо виділити вплив гібридних загроз на інформаційну сферу. Так, інформація в умовах гібридних загроз перетворюється на інструмент впливу, за допомогою якого підривають відчуття безпеки та штучно посилюють протистояння між різними політичними, соціальними й культурними спільнотами. Головною метою таких інформаційних дій є маніпуляція ідентичностями та лояльностями, щоб розколоти ключові групи інтересів і послабити існуючі політичні союзи.

Інформаційні гібридні загрози часто використовують для впливу на політичні дискурси, формування чи поширення потрібних наративів, а також для управління громадськими настроями та сприйняттям подій. У деяких випадках такі інструменти здатні обмежувати свободу висловлювань і вільне формування поглядів.

Також інформаційний вимір тісно переплітається з культурним і соціальним, адже дезінформаційні операції та інші інструменти в цій сфері спрямовані на послаблення культурної цілісності та суспільної єдності об’єкта впливу. Крім того, оскільки одним із завдань інформаційного впливу є руйнування політичного дискурсу й підрив політичних процесів, інформаційна сфера безпосередньо перетинається і з політичною сферою.

Більш вужчим є поняття «гібридних війн». Можна сказати, що почав користуватися цим терміном американський дослідник М. Маклюен, який розглядав комунікаційні технології як новий стратегічний ресурс держави та

наголошував, що сучасні конфлікти розгортаються передусім у площині інформаційного простору [68, с. 67].

Також можна виділити декілька варіантів визначення сутності гібридної війни [68, с. 67-68]:

- Підхід до ведення бойових дій, що поєднує класичні воєнні операції, тактику малої війни та кібератаки;
- Форма атаки, яка включає застосування ядерних, біологічних, хімічних засобів, імпровізованої зброї для терору та інтенсивного інформаційного впливу;
- Сучасна модифікація партизанської боротьби, що використовує новітні технології;
- Ключовий інструмент асиметричної війни, яка розгортається одночасно на трьох «фронтах»: серед місцевого населення, у тилових регіонах та у міжнародному просторі.

Дивлячись на визначення, можна побачити, що гібридна війна включає сучасні методи інформаційно-психологічного впливу та використання сучасних технологій. Тому до елементів гібридної війни варто зарахувати застосування традиційних воєнних методів, інформаційних та інформаційно-психологічних впливів, партизанських тактик, кібератак, окремих проявів тероризму й диверсій, а також інструментів економічного та дипломатичного тиску.

Таким чином, гібридна війна становить особливу загрозу тим, що розмиває самі межі воєнного протистояння: її старт і завершення важко ідентифікувати, реального противника нерідко неможливо одразу визначити, а формальний перехід від війни до миру не гарантує припинення конфлікту — навпаки, подальша ескалація може лише посилитися.

На сьогодні поняття «гібридної війни» та «гібридних загроз» введено в документи західної військової політики. Наприклад, на саміті НАТО в 2014

році, було широко розглянуто небезпечність гібридних війн, сформовані методи та інструменти ведення таких конфліктів [68, с. 68].

Важливо розкрити також сутність «інформаційної війни», що, очевидно, є провідною складовою гібридних війн.

Наразі термін «інформаційна війна» має переважно публіцистичне забарвлення і ще не набув сталого визначення. Це підтверджують постійні дискусії стосовно справжнього змісту цього поняття, а також дебати щодо його коректності та практичної корисності.

Вперше поняття «інформаційна війна» застосував Т. Рон у доповіді «Системи озброєння та інформаційна війна», яку він підготував у 1976 році. У документі було наголошено, що інформаційна інфраструктура становить основний елемент американської економіки, водночас перетворюючись на потенційно вразливу ціль як у період війни, так і в мирний час [51, с. 77].

Серед поглядів дослідників, які займаються питаннями інформаційних війн, можна виділити декілька підходів до цього визначення, деякі з яких можна представити наступним чином [51, с. 78-81]:

Перший – психологічний підхід, який розглядає інформаційну війну як прихований вплив інформації на свідомість окремих людей, груп і мас у цілому за допомогою пропаганди, дезінформації та маніпуляцій, спрямований на формування нових уявлень про соціально-політичний устрій суспільства через зміну ціннісних орієнтацій та базових переконань особистості;

Другий – геополітичний підхід, що трактує інформаційну війну як міждержавне протиборство, спрямоване на досягнення зовнішньополітичних цілей не через фізичну силу, військову техніку або зброю, а за допомогою витончених технологій примусового контролю, що зовні проявляються у дипломатичних формах;

Третій – соціально-комунікативний підхід, який розуміє інформаційну війну як комунікаційну технологією, що спрямована на здобуття

інформаційної переваги в рамках національної стратегії, де ключову роль відіграє інформація, яка впливає на когнітивні орієнтації.

Четвертий – системний підхід, де інформаційну війну розглядають як динамічний процес, що протікає в складній самоорганізованій системі з великою кількістю елементів, взаємозв'язки між якими мають імовірнісний, а не детермінований характер.

Крім того, привертає увагу дослідження П. Шпиги та Р. Рудника, в якому виділяються чотири підходи до тлумачення цього поняття.

Таблиця 2.2

Підходи до «інформаційної війни» П. Шпиги та Р. Рудника

Підхід	Опис
Перший	Інформаційна війна як комплекс політико-правових, соціально-економічних і психологічних дій, спрямованих на контроль інформаційного простору, усунення противника, руйнування його комунікацій та обмеження доступу до засобів передачі повідомлень.
Другий	Найгостріша форма протистояння в інформаційному просторі, де ключовими є безкомпромісність, висока інтенсивність суперечки та короткі періоди активного конфлікту.
Третій	Інформаційна війна як спосіб підтримки військових дій через сучасні електронні засоби, такі як цифрові випромінювачі, супутникові передавачі та інші технології.
Четвертий	Інформаційна війна ототожнюється з кібернетичною війною, тобто протистоянням між технічними системами.

*Джерело: сформовано автором на основі [*73, с. 328*]*

Інформаційна війна може включати такі дії: збір тактичної інформації, перевірку її достовірності, поширення пропаганди та дезінформації з метою деморалізації або маніпулювання опонентом і громадськістю, підрив якості інформації опонента та обмеження його здатності збирати дані. Можна побачити, що інформаційна війна ведеться як на ворожий суб'єкт (державу, групу тощо), так і населення [40, с. 239].

Окремо потрібно відмітити, що у дослідженнях, присвячених сутності гібридної війни та гібридних загроз, часто використовується поняття «психологічна війна». Цей термін уперше був запроваджений британським істориком Дж. Фуллером під час аналізу подій Першої світової війни. Сучасні американські фахівці частіше використовують близькі за змістом поняття «психологічна операція» або «інформаційна операція».

Подібно зв'язку гібридної війни та інформаційно, низка західних експертів визначають психологічну війну як ключовий елемент інформаційного протиборства. Основне її призначення полягає у цілеспрямованому впливі на масову та індивідуальну свідомість, що передбачає [68, с. 71]:

- нав'язування суспільству та окремим групам деструктивних ідей і поглядів;
- дезорієнтацію населення та поширення дезінформації;
- підрив базових переконань, норм і цінностей;
- формування образу ворога з метою залякування власного населення;
- психологічний тиск на противника шляхом демонстрації сили чи переваги.

Таким чином, психологічна війна виступає одним із центральних інструментів гібридних конфліктів, забезпечуючи вплив на поведінку, емоції та рішення цілих соціальних груп.

Найменшим, за масштабністю, інструментом гібридних загроз можна назвати інформаційно-психологічні операції. Загалом, Інформаційно-психологічні операції (часто в інформаційному просторі можна почути абревіатуру ІПСО) є різновидом інформаційних операцій, що передбачає практичне застосування складної системи узгоджених, скоординованих і взаємопов'язаних форм, методів і прийомів психологічного впливу. Вони включають політичні, військові, економічні, дипломатичні та власне

інформаційно-психологічні заходи, спрямовані на окрему людину або групи людей з метою впровадження в їхнє середовище чужих ідеологічних і соціальних установок, формування хибних стереотипів поведінки та спрямованої трансформації їхніх настроїв, почуттів і волі [16].

Зрозумівши, що з себе представляють гібридні загрози, можна продемонструвати реальні приклади. Для України є актуальним більшість гібридних загроз і, фактично, вона перебуває в стані гібридної війни, що достатньо сильно впливає на політичну стабільність держави.

Так, наглядними для розуміння є окреслені національні загрози та виклики в Стратегії інформаційної безпеки України, які безпосередньо стосуються небезпеки гібридних війн для держави та суспільства [66]:

- Інформаційне домінування держави-агресора на тимчасово окупованих територіях України;
- Обмежені можливості реагувати на дезінформаційні кампанії;
- Несформованість системи стратегічних комунікацій;
- Недосконалість регулювання відносин у сфері інформаційної діяльності та захисту професійної діяльності журналістів;
- Спроби маніпуляції свідомістю громадян України щодо європейської та євроатлантичної інтеграції України;
- Недостатній рівень інформаційної культури та медіаграмотності в суспільстві для протидії маніпулятивним та інформаційним впливам.

Вищезгадані загрози вказують на те, що для України явище гібридної та, особливо, інформаційної війни є актуальним та критичним. Тому важливо розглянути прояви інформаційної війни в контексті агресії з боку Росії.

Певні прояви інформаційних операцій по відношенню до України можна побачити ще під час президентських виборів 2004 року, де російські медіа та політичні діячі відкрито протистояли одному кандидату (В. Ющенко) та підтримували іншого (В. Януковича). Також російські інформаційні кампанії намагалися знизити міжнародний імідж України під час «газових війн» 2005

року. Крім цього, в різні часи змінювався перелік провідних тем, таких як проблеми Чорноморського флоту, проблематика паливно-енергетичного комплексу, проблеми Криму і кримських татар, а також діяльність екстремістських політичних організацій [57, с. 19].

Окремо також потрібно виділити висвітлення російськими ЗМІ подій Євромайдану в агресивно-пропагандистському світлі, де подальші події показали вразливість українського населення до інформаційно-пропагандистських атак [61, с. 239].

Науковці виділяють п’ять основних методів інформаційної агресії Росії проти України до початку широкомасштабного вторгнення: дезінформацію та маніпуляції, пропаганду, перекручування громадської думки, психологічний і психотропний тиск, а також поширення чуток [61, с 239].

Також інші дослідники виділяли (до широкомасштабного вторгнення), що Росія діяла в таких напрямках ведення інформаційної війни [57, с. 21]:

- Зниження міжнародного авторитету України для послаблення її геополітичного значення;
- Спотворення та фрагментування інформації з метою дестабілізації країни та впровадження «керованого хаосу»;
- Створення стереотипу меншовартості українців і руйнування національної самосвідомості;
- Поширення російської мови та культури для утвердження російської ідентичності при витісненні української.

Серед інструментів інформаційної війни, які використовуються донині, на нашу думку, можна відзначити такі:

- Широке використання підконтрольних ЗМІ (телебачення, радіо, інтернет) для пропаганди та здійснення спрямованого інформаційно-психологічного впливу на українців з метою дезінформації, нагнітання, виправдання агресії та деморалізації патріотично налаштованих верств суспільства;

- Використання методів контрінформаційної боротьби, включно з блокуванням загальнодержавних українських телеканалів і радіостанцій на окупованих територіях, а також контролем регіональних та місцевих ЗМІ;
- Застосування пропагандистських підрозділів та «лідерів думок» у соціальних мережах та онлайн-платформах.

Вразливість України до інформаційних атак відмічається, з однієї сторони – несформованістю і недостатньою визначеністю системи цінностей та інтересів суспільства, а також наявністю численних протиріч між інтересами різних соціальних спільнот і професійних груп, що, з однієї сторони, спричиняє політичну та соціальну нестабільність, а з іншої – недосконаліть системи національної інформаційної безпеки [61].

Продовжуючи тему ведення гібридної війни РФ, варто відзначити, що об'єктом впливу ставали також і країни ЄС. Так, основними видами загроз, які можна виділити є [4, с. 121]:

- загрози, пов'язані з дезорієнтацією та дезорганізацією європейського суспільства, зокрема стимулюванням сепаратистських рухів через кібератаки на політичні партії та державні органи;
- загрози активізації дій ворожих збройних формувань, спричинені російськими дезінформаційними кампаніями, пропагандою та маніпуляціями.

Так, наприклад, наприклад, у 2007 році через дипломатичну суперечку з Москвою щодо радянського військового меморіалу Естонія зазнала серії масштабних кібератак, у результаті яких DDoS-атаки вивели з ладу веб-сайти урядових, медіа та фінансових установ. На початку 2019 року в Польщі була викрита трирічна кампанія дезінформації, яка діяла через соціальні мережі, зокрема «Facebook»; потік фейкових новин на користь трьох проросійських польських політиків охопив до 4,5 млн осіб [4, с. 121].

Отже, досліджуючи питання гібридних загроз та інформаційно-психологічних впливів, можна дійти думки, що такі небезпеки впливають на

політичну стабільність держави та підвищують значення, необхідність покращувати та зміцнювати інформаційну безпеку.

2.3 Вплив інформаційних технологій та соціальних мереж на політичну стабільність держави

Сучасні інформаційно-комунікаційні технології дозволяють у Інтернеті створювати як постійні, так і тимчасові соціальні спільноти, об’єднані спільними нормами, інтересами та можливостями комунікації. На відміну від традиційних ЗМІ, мережеві спільноти мають соціальний характер, ґрунтуються на емпатії та забезпечують ряд переваг: доступність, відкритість, оперативний обмін інформацією, зворотний зв’язок, можливість встановлення нових контактів, неформальне спілкування та спрощений пошук потрібних користувачів.

У широкому розумінні соціальна мережа — це спільнота людей, об’єднана спільними інтересами або діяльністю для прямого спілкування. Соціальні мережі є авторитетним джерелом інформації та завдяки своїй популярності охоплюють найбільшу кількість користувачів в глобальному Інтернеті. Потік інформації в них двосторонній, тому учасники можуть одночасно виступати і як комунікатори, і як реципієнти. Соціальні мережі часто виконують роль неформальних ЗМІ, де будь-який користувач може опублікувати новинне повідомлення, що формує у відвідувачів відчуття власної участі та впливу.

Сучасні соціальні мережі входять до числа найбільш відвідуваних онлайн-ресурсів. Вони дозволяють одночасно передавати інформацію великій глобальній аудиторії у реальному часі, незалежно від відстані.

Втім, ця можливість може бути використана і для здійснення цілеспрямованих деструктивних впливів на національний інформаційний

простір. Це створює ризики соціального характеру, пов’язані із застосуванням технологій штучного коригування поведінки людини та втручання в її свободу вибору. Виникають нові форми загроз, що включають непомітні інформаційні впливи, формування штучної психологічної залежності та маніпулювання масовою свідомістю. Такий психологічний тиск, уміло реалізований через соціальні мережі, може непомітно спонукати людину до дій і рішень, які не відповідають її справжнім бажанням.

Можна виділити, що основними проблемами соціальних мереж для інформаційної безпеки особистості, суспільства та держави є:

- захист особисті та суспільства, в цілому, від впливів інформації, яка несе певну шкоду;
- захисту інформації громадян та держави.

За для повного розуміння шкоди інформаційно-психологічного впливу, можна виокремити декілька ознак такого впливу на особистість в соціальних мережах [72, с. 37]:

- прихований характер впливу;
- ефективне використання інформаційних ресурсів;
- прихований примус до певного вибору;
- акцент на широкі маси населення;
- стимулювання потрібної поведінки;
- застосовування маніпулятивних технологій;
- формування потрібних думок, намірів, емоцій, переконань та моделей поведінки;
- підтримання ілюзії автономності того, на кого здійснюється вплив.

Якщо ж брати до уваги суспільство, то тут потрібно говорити про масштабні заплановані інформаційно-психологічні операції. Ефективність інформаційно-психологічних операцій саме в соціальних мережах супроводжується наступними факторами [56, с. 302]:

- широке охоплення аудиторії;
- миттєве розповсюдження інформації;
- можливість таргетування контенту;
- труднощі з перевіркою справжності джерел;
- емоційна форма сприйняття матеріалів користувачами;
- невисокі витрати на проведення інформаційно-психологічних операцій.

Найочевидніше використання можливостей соціальних мереж — під час виборчих кампаній. Так, соціальні мережі можуть виступати потужним інструментом піару та формування іміджу. Так, прикладом може стати передвиборча кампанія Б. Обами. Під час виборчої кампанії 2008 року він забезпечив активну присутність у всіх провідних соціальних мережах. Б. Обама став одним із перших політичних лідерів, які широко застосовували інтернет-платформи для формування та зміцнення власного публічного іміджу. Також соціальні мережі дали можливість політику бути присутнім усюди та завжди [63, с. 196].

З іншої сторони, соціальна мережі дають можливість формуванню «лідерів думок», які використовуючи довіру аудиторію, можуть поширювати небезпечні для суспільства та держави повідомлення та маніпулювати думками та цінностями.

В контексті гібридної війни Росії проти України, інформаційні загрози у соціальних мережах набувають особливої актуальності. Дезінформація виступає ключовим елементом інформаційно-психологічних операцій в умовах російсько-української війни. Серед основних типів таких загроз можна виділити [56, с. 302]:

- поширення неправдивої або спотвореної інформації;
- маніпулювання громадською думкою;
- підрив довіри до державних органів;
- провокування паніки та тривожності;

- стимулювання міжнаціональної ворожнечі.

Також дослідники виділяють специфічні інформаційні загрози для України. Зазвичай інформаційно-психологічні операції концентруються на: підриві відчуття національної ідентичності та послабленні суспільної згуртованості; спробах очорнити Збройні сили України та вищі органи влади; поширені міфів про «братні народи» та вигаданої «громадянської війни»; спотворені або навмисному перекручуванні історичної пам'яті; ініціюванні внутрішніх протистоянь на основі релігійних чи мовних розбіжностей [75, с. 270-271].

Цікавими є спостереження українських дослідників щодо проведення типових інформаційно-психологічних операцій з боку противника: «…інформаційно-психологічні операції в умовах війни зазвичай впроваджують через неформальні канали комунікації, неправдиві інформаційні повідомлення у вайбер-групах або меседжерах … комунікаційним полем для реалізації ІПСО слугують ті канали, які намагаються охопити якомога більшу кількість людей … для цього формують певну авдиторію, яку спонукають мислити в потрібних цілях ... На наступному етапі авдиторії вказують, що потрібно робити … ІПСО часто виникає на константному вживанні патріотичних закликів і якоїсь фальшивої тези зі шкідливим вмістом, як наслідок – шкідлива теза починає поширюватися під прикриттям правильних гасел» [75, с. 270]. З цього аналізу видно, що соціальні мережі дають можливість проводити ефективні, швидкі та достатньо дешеві в фінансах й технічних засобах операції.

Також типовими ознаками інформаційно-психологічних операцій є синхронність публікацій повідомлень, наявність мовних помилок, а також специфічні ім'я авторів, які поширюють такі публікації.

Також, як відмічають автори дослідження, яке стосується інформаційно-психологічних операцій в України, автори маніпулятивного контенту часто приховуються національною символікою та гаслами (наприклад, прапори,

герби та гасла: «Слава Україні»): «У соціальних мережах вони нагадують віртуальних диверсантів, адже як і в тилу, часто окупанти вдягають український піксель і під виглядом бійців Збройних сил України проникають у тил» [75, с. 270].

Цікавим також є підняті теми в подібних російських інформаційно-психологічних операціях. Часто використовуються наративи, які нагнітають конфлікт між громадянами західної та східної України. Також повідомлення створювали ефект надзвичайної сили ворога. Дає розуміння проблематики й те як в українських спільнота поширювали емоційний заклик до покари «російських загарбників» в особливо антигуманній формі, що шкодило іміджу не тільки українських військових, а й державі в міжнародному просторі. Часто повідомлення подібного характеру мали вказівку на ігнорування офіційних джерел та повного їх знецінення [75, с. 271].

Основною методою подібних проявів гібридної війни є введення українського суспільства в стан паніки й зневіри, дискредитування держави в очах суспільства й міжнародної спільноти.

Загалом, можна продемонструвати такі аспекти використання соціальних мереж у гібридній війні України та Росії:

Таблиця 2.3

Ключові аспекти гібридної війни проти України

Мета використання	Організаційні аспекти
Формування альтернативної реальності	Створення мереж ботів і фейкових акаунтів
Поляризація суспільства	Використання лідерів думок та псевдоекспертів
Мобілізація прихильників агресора	Координація дій через закриті групи та канали
Дезорієнтація та деморалізація населення	Застосування технологій глибинних фейків
Збір розвідувальної інформації	Використання алгоритмів соціальних мереж для посилення ефекту

Джерело: сформовано автором на основі [56, с. 303]

Таким чином, особливість інформаційних загроз в українських умовах полягає в їх комплексності, поєднуючи дезінформацію, маніпулювання громадською думкою та психологічний тиск. Вони націлені на послаблення національної ідентичності, дискредитацію державних інституцій та провокування внутрішніх конфліктів.

Можна стверджувати, що поряд з позитивними досягненнями соціальними мереж (об'єднання людей, створення спільнот, обмін думками, можливість проявляти політичну активність) можливе використання маніпулятивних технологій і негативного впливу на користувачів соціальних мереж, особливо в контексті інформаційно-психологічного впливу.

Отже, у другому розділі було здійснено аналіз сучасних інформаційних загроз, які безпосередньо впливають на стан політичної системи, громадську думку та рівень довіри до влади.

Узагальнюючи результати аналізу класифікацій і типологій загроз інформаційній безпеці держави, можна стверджувати, що сучасний інформаційний простір формує широку та багатовимірну систему ризиків, які охоплюють особу, суспільство та державу. Загрози проявляються у вигляді маніпулятивного інформаційного впливу, несанкціонованого доступу до інформації, порушення її конфіденційності, цілісності та доступності, а також у формі технічних та соціальних ризиків. Їх систематизація за різними критеріями — від джерел походження та масштабів потенційної шкоди до сфери прояву — дозволяє глибше розуміти природу небезпек і особливості їхнього впливу. Класифікація загроз відіграє ключову теоретико-прикладну роль, забезпечує впорядкованість системи інформаційної безпеки, сприяє виявленню вразливостей та формує базу для ефективного державного реагування, що є визначальним для підтримання політичної стабільності.

Розгляд гібридних загроз, гібридних війн, інформаційної війни та інформаційно-психологічних операцій показує, що сучасні конфлікти виходять за межі традиційної війни та спрямовані передусім на свідомість,

цінності й політичну стійкість суспільства. Гібридний вплив поєднує військові, інформаційні, кібератаки, пропаганду, маніпуляції та економічний тиск, що робить державу вразливою у політичній, соціальній та інформаційній сферах.

Україна вже тривалий час перебуває під таким комплексним тиском, особливо з боку Росії, що проявляється у дезінформаційних кампаніях, пропаганді, кібератаках, спотворенні національного дискурсу та маніпуляції громадською думкою. Це підриває довіру до влади, послаблює суспільну єдність і створює умови для політичної нестабільності. Досвід інших країн ЄС підтверджує, що гібридні впливи є глобальним явищем.

Окремо розглянуто вплив інформаційних технологій та соціальних мереж на політичну стабільність. Соціальні мережі значно впливають на політичну стабільність держави: вони полегшують комунікацію та активізують громадян, але водночас створюють умови для дезінформації, маніпуляцій і психологічного тиску. В українських умовах їхній вплив посилюється гібридною війною, де соціальні платформи використовуються для підриву довіри до влади, розпалювання конфліктів та послаблення національної єдності. Таким чином, соцмережі поєднують значний потенціал розвитку і високі ризики для інформаційної безпеки.

Підсумовуючи результати аналізу, можна зробити висновок, що інформаційні загрози сучасності є одними з головних факторів дестабілізації політичних систем, а їхня ефективна нейтралізація вимагає комплексного підходу.

РОЗДІЛ 3
МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ЧИННИКА ПОЛІТИЧНОЇ СТАБІЛЬНОСТІ ДЕРЖАВИ

3.1. Державна політика у сфері інформаційної безпеки: інституційні та правові механізми

Як вже зазначалося, однією з головних завдань інформаційною безпеки держави є контроль над наявними й можливими загрозами, для забезпечення умов для повноцінного задоволення інформаційних потреб населення та гарантувати захист і реалізацію національних інтересів.

Часто, при розгляді державної політики у сфері інформаційною безпеки, використовуються словосполучення «державна інформаційна політика» та «інформаційна безпека держави». Потрібно відзначити, що ці визначення дуже тісно пов’язані між собою. Тим не менш, державна інформаційна політика має ширше значення. Так її розглядають наступним чином [31, с. 47]:

- У вузькому значенні: як сукупність напрямів і способів діяльності держави з одержання, використання, поширення та зберігання інформації;
- У широку значенні: як сукупність напрямів діяльності держави в інформаційній сфері, зміст якої конкретизується у відповідних концепціях, стратегіях і програмах державної інформаційної політики.

Зважаючи на це, ці поняття, при розгляді нашої теми, можна тісно використовувати і представляти, що: державна інформаційна політика включає забезпечення інформаційної безпеки держави.

Так під терміном «забезпечення інформаційної безпеки» слід розуміти: комплекс дій, заходів та інституційних механізмів, спрямованих на

забезпечення такого рівня захищеності, який відповідає потребам держави й суспільства та гарантує їхню стабільність і безпеку [43, с. 10].

На думку дослідників в області інформаційної безпеки, її забезпечення повинно мати три складові: діяльність, засоби та суб'єкти.

Таблиця 3.1

Структура забезпечення інформаційної безпеки

Забезпечення інформаційної безпеки		
Діяльність	Засоби	Суб'єкти
надання допомоги суб'єктам для досягнення поставлених цілей	сукупність матеріальних, духовних, фінансових, правових, організаційних і технічних засобів здійснення діяльності щодо забезпечення	індивіди, організації, органи держави, які здійснюють діяльність щодо забезпечення

Джерело: створено на основі [43, с. 10]

Також науковці зазначають, що потрібно виділяти ряд положень державної політики забезпечення інформаційної безпеки [46, с. 31-32]:

- обмеження доступу до інформації допускається лише як виняток із загального принципу відкритості та виключно на підставі закону;
- відповідальність за зберігання, засекречення чи розсекречення інформації має бути персоніфікованою;
- надання або обмеження доступу до інформаційних ресурсів здійснюється відповідно до законодавчо визначеного права власності на відповідну інформацію;
- держава формує нормативно-правову базу, яка регламентує права, обов'язки та відповідальність усіх суб'єктів інформаційного простору;
- юридичні та фізичні особи, що збирають, накопичують чи обробляють персональні дані та конфіденційну інформацію, несуть правову відповідальність за їхнє збереження та використання;

- держава в законний спосіб захищає суспільство від неправдивих, викривлених або недостовірних повідомлень, що поширюються через ЗМІ;
- органи влади контролюють розроблення та застосування будь-яких засобів інформаційного захисту, обов'язково сертифікуючи та ліцензуючи діяльність у сфері інформаційної безпеки;
- держава проводить протекціоністську політику, підтримуючи національних виробників засобів інформатизації та інформаційного захисту та захищаючи внутрішній ринок від неякісної інформаційної продукції;
- державна політика спрямована на те, щоб зробити світові інформаційні ресурси та глобальні мережі більш доступними для громадян;
- країна прагне мінімізувати використання іноземних інформаційних технологій у державних органах управління, віддаючи перевагу конкурентоспроможним вітчизняним рішенням;
- формується державна програма інформаційної безпеки, у межах якої державні установи та комерційні структури об'єднують свої зусилля для побудови єдиної системи захисту інформації;
- держава активно протидіє інформаційній агресії з боку інших держав і підтримує процес інтернаціоналізації глобальних інформаційних мереж та систем.

Крім того, державна політика у сфері інформаційної безпеки спрямована на три ключові напрями: гарантування інформаційних прав і свобод громадян; забезпечення державної безпеки в інформаційному просторі; охорону національного інформаційного ринку, економічних інтересів держави та підтримку вітчизняних виробників інформаційних продуктів [37, с. 19].

Правову основу забезпечення інформаційної безпеки становить комплекс норм різної юридичної сили, які належать до різних галузей права. Сукупно вони відображають характер процесів у сфері інформаційної безпеки та формують цілісну, узгоджену систему.

Так, найвищим рівнем нормативно-правового забезпечення інформаційної безпеки є міжнародні документи, серед яких документи Організації Об'єднаних Націй, її профільних установ, фондів, програм, зокрема, ООН з питань освіти, науки і культури (ЮНЕСКО), Програми розвитку ООН (ПРООН), Міжнародного Союзу Електрозв'язку (МСЕ, International Telecommunication Union, ITU), Всесвітньої організації інтелектуальної власності (ВОІВ) та інших [44, с. 34].

Аналізуючи нормативну базу, сформовану в межах ООН, передусім слід згадати такі фундаментальні міжнародні акти, як Загальна декларація прав людини 1948 року, яка закріпила свободу висловлення поглядів як одну з ключових демократичних цінностей, а також Міжнародний пакт про громадянські та політичні права 1966 року. У подальшому Генеральна Асамблея ООН ухвалила значну кількість резолюцій, присвячених розвитку інформаційного суспільства та питанням інформаційної безпеки. Серед них — «Необхідність формування нового, більш справедливого й ефективного міжнародного інформаційного та комунікаційного порядку» (1978 р.), регулярні з 1998 року резолюції «Досягнення в галузі інформатизації та телекомунікацій у контексті міжнародної безпеки», документи «Застосування інформаційно-комунікаційних технологій з метою розвитку» (2002 р.), «Формування глобальної культури кібербезпеки та захист критично важливих інформаційних структур» (2002, 2003, 2009 рр.), «Протидія злочинному використанню інформаційних технологій» (2002 р.) та багато інших [43, с. 56].

Вагомий внесок у формування світових підходів до розвитку інформаційного суспільства та забезпечення інформаційної безпеки робить ЮНЕСКО, яка в межах своєї компетенції ухвалила низку важливих документів. Серед них — Декларація про основні принципи щодо ролі засобів масової інформації у зміцненні миру, міжнародного порозуміння, розвитку прав людини та протидії расизму, апартеїду й пропаганді війни (1978 р.); програма «Інформаційне суспільство для всіх» (1996 р.); Загальна декларація

ЮНЕСКО про культурне різноманіття (2001 р.); Рекомендація про розвиток і використання багатомовності та забезпечення відкритого доступу до кіберпростору (2003 р.); а також Хартія про збереження цифрової спадщини (2003 р.) та інші документи [43, с. 57].

Важливу роль у міжнародному нормотворенні в сфері інформаційних технологій і безпеки відіграє також Міжнародний союз електрозв'язку. Організація бере участь у створенні міжнародних стандартів у сфері ІКТ, формує стратегічні документи та рекомендації. У 2007 році Союз презентував Глобальну програму кібербезпеки, що визначила ключові цілі, принципи та підходи до формування моделей законодавства у сфері протидії кіберзлочинності. Крім того, ним було ухвалено низку резолюцій, спрямованих на підвищення рівня довіри, безпеки та ефективності використання інформаційно-комунікаційних технологій, а також на боротьбу з кіберзлочинами [44, с. 35].

На європейському рівні також ведеться інтенсивна нормотворча діяльність у сфері інформаційної безпеки. Зокрема, Рада Європи ухвалила Конвенцію про кіберзлочинність (2001 р.), яка набула глобального значення. Крім того, було прийнято Конвенцію про захист осіб у зв'язку з автоматизованою обробкою персональних даних (1981 р.), а також ряд резолюцій і рекомендацій Комітету міністрів щодо ключових аспектів розвитку інформаційного суспільства [44, с. 37].

На погляд багатьох фахівців, нормативно-правова основа інформаційної безпеки повинна насамперед виконувати три ключові завдання [43, с. 58]:

– упорядковувати взаємовідносини між усіма суб'єктами у сфері інформаційної безпеки, визначаючи їхні права, обов'язки та міру відповідальності;

– забезпечувати правове підґрунтя для діяльності суб'єктів інформаційної безпеки на всіх рівнях — особистісному, суспільному та державному;

– визначати правила й процедури використання різних механізмів, ресурсів і інструментів, спрямованих на забезпечення інформаційної безпеки.

На цьому тлі, варто також розглянути й нормативно-правову базу України у сфері інформаційної безпеки.

Як вже відмічалося раніше, Конституція України визначає забезпечення інформаційної безпеки як одну з ключових функцій держави та гарантує громадянам комплекс прав у сфері інформації. До них належать свобода слова і думки, право на вільне висловлення власних поглядів, можливість безперешкодно збирати, зберігати, використовувати й поширювати відомості, а також захист інтелектуальної власності й авторських прав [34].

Також у Законі України «Про інформацію» основними напрямами державної інформаційної політики України визнається: «забезпечення доступу кожного до інформації; забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації; створення умов для формування в Україні інформаційного суспільства; забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень; створення інформаційних систем і мереж інформації, розвиток електронного урядування; постійне оновлення, збагачення та зберігання національних інформаційних ресурсів; забезпечення інформаційної безпеки України; сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору» [21].

Окремо, в Стратегії інформаційної безпеки визначається, що забезпечення інформаційної безпеки України є однією з найважливіших функцій держави [66].

Законодавчі акти Верховної Ради України та розпорядчі документи Президента та Кабінету Міністрів України з питань інформаційної безпеки України розподіляють за сферою регулювання. Так, всього виділяють 6 груп [44, с. 37].

Таблиця 3.2

Нормативно-правова основа України за сферою регулювання

Сфера регулювання	Нормативно-правові документи
Концептуальні засади інформаційної безпеки як складової національної безпеки	• Закон України «Про національну безпеку України»; • Указ Президента України «Про рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України»; • Указ Президента України «Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України»; • Указ Президента «Про рішення Ради національної безпеки і оборони України «Про Стратегію інформаційної безпеки»
Використання, розповсюдження інформації	• Закон України «Про інформацію»; • Закон України «Про медіа»; • Закон України «Про доступ до публічної інформації»; • Закон України «Про Суспільне телебачення і радіомовлення України».
Використання інформації з обмеженим доступом	• Закон України «Про державну таємницю»; • Постанова Кабінету Міністрів України «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію»; • Закон України «Про Національну систему конфіденційного зв’язку»; • Закон України «Про захист персональних даних».
Розвиток інформаційного суспільства, інформатизація	• Закон України «Про Національну програму інформатизації»; • Закон України «Про Концепцію Національної програми інформатизації»; • Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки»; • Розпорядження Кабінету Міністрів України «Про схвалення Стратегії розвитку інформаційного суспільства в Україні»;

	• Розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку електронної демократії в Україні та плану заходів щодо її реалізації».
Зв'язок, інформаційно-комунікаційні системи, технічний захист інформації	• Закон України «Про захист інформації в інформаційно-комунікаційних системах»; • Закон України «Про державну підтримку розвитку індустрії програмної продукції»; • Закон України «Про електронні комунікації».
Електронні системи інформації	• Закон України «Про електронні документи та електронний документообіг»; • Закон України «Про електронну ідентифікацію та електронні довірчі послуги»; • Постанова Кабінету Міністрів України від «Про заходи щодо створення електронної інформаційної системи «Електронний Уряд»; • Розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку системи електронних послуг в Україні»; • Розпорядження Кабінету Міністрів України від «Про схвалення Концепції розвитку електронного урядування в Україні»

Джерело: складено на основі [44, с. 37-40]

Як визначають українські дослідники, суб'єктами державної інформаційної політики виступають органи, організації та особи, наділені законом правом здійснювати інформаційну діяльність. Тому реалізація державної інформаційної політики забезпечується насамперед державними органами, відповідальними за регулювання соціально-політичних відносин у інформаційній сфері, а також залученням недержавних суб'єктів інформаційної діяльності для підтримки завдань державного управління [31, с. 49].

Тому важливо розібрати й інституційне забезпечення державної політики у сфері інформаційної безпеки. Як не дивно, в Україні вже створена

та функціонує досить розгалужена система державних органів, які реалізують завдання з забезпечення інформаційної безпеки в різних сферах.

Органами державної влади, на які покладено функції формування, реалізації та контролю державної політики у сфері інформаційної безпеки є [5, с. 39]:

1. У сфері формування державної політики – Президент України, Верховна Рада України, Кабінет Міністрів України, Міністерство оборони України, Міністерство культури та інформаційної політики України, Міністерство цифрової трансформації, Рада національної безпеки і оборони України;

2. У сфері реалізації державної політики – Президент України, Верховна Рада України, Кабінет Міністрів України, Міністерство оборони України, Міністерство культури України, Міністерство цифрової трансформації, Державна служба спеціального зв'язку та захисту інформації, Державний комітет телебачення і радіомовлення України, Департамент кіберполіції Національної поліції України, інші центральні органи виконавчої влади та органи сектору безпеки і оборони України, місцеві органи виконавчої влади та органи місцевого самоврядування;

3. У сфері контролю за реалізацією політики – Рада національної безпеки і оборони України.

Також можна визначити напрями за якими проводиться державне регулювання та управління інформаційною сферою.

Так, законодавча гілка влади визначає державну політику у сфері інформації та інформаційної безпеки, забезпечує свободу слова, права громадян на інформацію, регламентує діяльність засобів масової інформації та Інтернету, рекламної діяльності. Також визначає державну політику у сфері розвитку інформаційного суспільства, інформатизації, електронного урядування, документообігу та цифрового підпису, електронних інформаційних ресурсів тощо.

Можна виділити й певні органи державної влади, які реалізують та контролюють державну політику інформаційної безпеки.

Міністерство культури України забезпечує інформаційний суверенітет України, поширює суспільно важливої інформації, забезпечує функціонування державних інформаційних ресурсів.

Основними завданнями Державної служби спеціального зв'язку та захисту інформації як центрального органу виконавчої влади зі спеціальним статусом, згідно з чинним законодавством, є реалізація державної політики у сфері захисту державних інформаційних ресурсів у мережах передачі даних, забезпечення функціонування Державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, криптографічного та технічного захисту інформації [5, с. 38].

Рада національної безпеки і оборони України як координаційний орган при Президентові України уповноважена приймати рішення щодо визначення концептуальних підходів та напрямів забезпечення національної безпеки в цілому та, в тому числі, в інформаційній сфері з урахуванням масштабу потенційних та реальних загроз національним інтересам України [47, с. 71].

Реалізацію державної політики в сфері протидії кіберзлочинності як невід'ємної складової державної політики у сфері інформаційної безпеки здійснює Департамент кіберполіції Національної поліції України [5, с. 40].

Таким чином, інституційно-правове та організаційне забезпечення інформаційної безпеки, що враховує взаємодію між суб'єктами (державними та недержавними інституціями, а також громадянами), формує інституційне середовище інформаційної безпеки. Від ефективності його функціонування залежить рівень захисту інтересів громадян, суспільства та держави як соціальних об'єктів інформаційної безпеки загалом.

3.2. Досвід зарубіжних країн у забезпеченні інформаційної безпеки та уроки для України

Провідні країни світу орієнтують свою політику на розвиток, впровадження та контроль цифрових технологій, що спричиняє формування сфер технологічного впливу та глобального цифрового порядку — сукупності технічних, економічних, політичних і нормативних заходів, які регулюють міжнародні інформаційні потоки. В складних реаліях України доцільно дослідити основні механізми формування та забезпечення інформаційної безпеки як складової національної безпеки.

Європейський Союз, як один із ключових центрів розробки правових стандартів у сфері інформаційної безпеки, сформував комплексну систему регулювання, що слугує зразком для численних країн світу.

У 2001 році Європейська Комісія представила документ «Мережева та інформаційна безпека: європейський політичний підхід», який став ключовим кроком у формуванні загальноєвропейської стратегії інформаційної безпеки. У ньому були окреслені основні проблеми в цій сфері та запропоновано політичний підхід до їх вирішення на рівні ЄС. Документ став фундаментом для подальших ініціатив і розробок, слугуючи орієнтиром для держав-членів ЄС у створенні національних стратегій. Ідеї та підходи, викладені в ньому, лягли в основу наступних політик і нормативних актів, зокрема вплинули на прийняття у 2016 році Директиви про безпеку мережевих та інформаційних систем, що зобов’язує країни ЄС впроваджувати мінімальні стандарти кібербезпеки на національному рівні [53].

Окрім цього, Європейський Союз є лідером у розробці комплексного правового регулювання кібербезпеки, яке реалізовано через численні директиви та регламенти.

Так, загальний регламент про захист даних встановлює уніфіковані правила обробки персональних даних фізичних осіб у межах ЄС. Він закріплює принципи мінімізації даних, прозорості їх обробки. Впровадження цього регламенту суттєво змінило підходи до інформаційної безпеки, вимагаючи від організацій проведення оцінки впливу на захист даних і призначення відповідальних осіб у випадках високого ризику [39, с. 292].

Також директива NIS 2 (EU) 2022/2555 посилює вимоги щодо управління кіберризиками, встановлює жорсткіші санкції за порушення та зобов'язує держави-члени розробляти національні стратегії кібербезпеки. Документ також акцентує на підвищенні стійкості критичної інфраструктури до кіберінцидентів та забезпеченні оперативного відновлення після атак. Директива про стійкість критичних суб'єктів встановлює вимоги щодо високого рівня стійкості таких об'єктів. Вона зобов'язує держави-члени ідентифікувати критичні суб'єкти, оцінювати ризики та впроваджувати відповідні заходи стійкості. Важливим регламент про кібербезпеку, який встановлює постійний мандат для Агентства Європейського Союзу з кібербезпеки та вводить європейську схему сертифікації кібербезпеки. Він передбачає розробку загальних стандартів сертифікації і сприяє підвищенню довіри до цифрових технологій та забезпеченню сумісності систем кібербезпеки на єдиному цифровому ринку [39, с. 292].

Окремо, посилення інформаційної безпеки в ЄС проявляється у створенні загальноєвропейських оперативних центрів безпеки, а також впровадженні механізму реагування на надзвичайні ситуації у кіберпросторі та механізму обробки великих інцидентів кібербезпеки. На практиці ці центри представляють собою великі національні або транскордонні платформи для збору інформації про загрози, метою яких є підвищення ефективності виявлення, запобігання та реагування на кібератаки [41, с. 182].

Загальна робота ЄС в напрямку удосконалення інформаційної безпеки ґрунтується на таких процесах [53]:

- Впорядкування нормативної бази для забезпечення цілісності державної політики в сфері інформаційної безпеки;
- Формування європейських керівних принципів у сфері інформаційної безпеки;
- Розширення чисельності підрозділів, що відповідають за інформаційну безпеку;
- Посилення контролю над національним інформаційним простором;
- Зміцнення захисних механізмів критичної інформаційної інфраструктури.

На фоні постійного оновлення та покращення інформаційної безпеки в ЄС, Україна під час імплементації європейських норм у вітчизняне законодавство має суттєві труднощі, про які буде сказано у наступному підрозділі.

Важливим документом для розгляду також є «Концепція комплексної безпеки» Фінляндії. Ця концепція передбачає спільну відповідальність влади, бізнесу, неурядових організацій та громадян за захист життєдіяльності суспільства. Вона спрямована на те, щоб у разі кризи все фінське суспільство могло швидко мобілізувати ресурси, ефективно відновлюватися та адаптувати свої функції на основі отриманого досвіду. Коріння цієї концепції лежить у доктрині «Тотальної оборони» після Другої світової війни, коли мобілізація всього суспільства стала частиною військових оборонних зусиль [8, с. 55].

Фінська модель має ключові наступні особливості:

- Забезпечення функціонування керівництва в будь-яких ситуаціях;
- Міжнародна діяльність та співпраця;
- Регулярні курси оборони та безпеки, що покращує розуміння загроз та співпрацю між усіма секторами суспільства та держави;

- Залучення приватного сектору до забезпечення критично важливих функцій;
- Постійний обмін інформацією між державним сектором, бізнес-сектором та громадськістю;
- Інформаційна та психологічна стійкість суспільства до кризових ситуацій [8, с. 55].

Варто звернути увагу й на забезпечення інформаційної безпеки в Швеції. Так, в Швеції діють спеціальні органи Шведське агентство психологічного захисту та Агентство з питань надзвичайних ситуацій, які займаються питаннями інформаційної безпеки. Шведська доктрина інформаційної безпеки враховує нові загрози, пов'язані з кіберпростором та високим рівнем цифровізації суспільного життя. Згідно з доктриною, одним із основних методів потенційного противника є використання сучасних медіа та соціальних мереж для психологічного впливу. В доктрино звертається увага на те , що важливо працювати зі свідомістю населення та готувати його до протидії дезінформації ще до настання будь-яких криз. Тому шведська влада проводить навчання для формування психологічного захисту громадян від фейкових новин, дезінформації та пропаганди [11, с. 57].

Інформаційна політика США в рамках інформаційної безпеки має свої особливості. Так, США мають такі пріоритети в інформаційній сфері [10, с. 96]:

- Підтримка наукових досліджень і розробок у сфері інформаційних та комунікаційних технологій;
- Сприяння обміну технологіями між лабораторіями та компаніями та впровадження інновацій на ринках;
- Розвиток та вдосконалення інформаційної інфраструктури з контролем її діяльності;
- Створення глобальних комунікаційних систем і дослідження їхнього впливу на міжнародні, національні та приватні пріоритети;

- Встановлення нових засобів контролю для сучасних інформаційних відносин;
- Захист приватного життя та забезпечення конфіденційності особистої інформації на різних рівнях державного управління та у приватному секторі;
- Формування урядової політики у сфері інформації та комунікацій;
- Забезпечення підготовки спеціалістів у сфері комп'ютерної безпеки.

З цього списку видно, що державна політика США зосереджена на розвитку інформаційно-комунікаційних технологій, навчанні спеціалістів та контролі інформаційного середовища в міжнародних масштабах.

З країн-членів Європейського Союзу можна виділити Німеччину. Уряд Німеччини підтримує зусилля щодо гармонізації методів застосування міжнародного права при національному регулюванні використання інформаційно-комунікаційних технологій. Це включає розробку технічних норм, що застосовуються на добровільній основі, а також принципів відповідальної поведінки держав, спрямованих на забезпечення відкритого, безпечного, стабільного, доступного та мирного інформаційно-комунікаційного середовища. Особливу роль у цьому процесі відіграє діяльність урядових експертних груп, які займаються розвитком галузі створення та використання інформації і телекомунікацій [19, с. 50].

А в Польщі для протидії інформаційним загрозам активно залучають громадянське суспільство. Так, у 2017 році було створено неурядову організацію – Центр аналізу пропаганди і дезінформації. Це перша в країні інституція такого типу, яка зосереджує свою діяльність на аналізі та розробці системного підходу до виявлення та протидії російській дезінформації в польському інформаційному просторі [59, с. 515].

Для представлення загального стану інформаційної та кібербезпек, можна використати індекс національної кібербезпеки (National Cyber Security Index), в якому Україна посідає дуже високе місце – 13 [1].

Таблиця 3.3

Індекс національної кібербезпеки

Місце	Країна	Індекс кібербезпеки	Рівень цифрового розвитку
1.	Чехія	98,33	72,93
2.	Канада	96,67	78,14
3.	Естонія	96,67	82,56
12.	Данія	89,17	85,59
13.	Україна	88,33	71,87
14.	Італія	88,33	73,58

Джерело: створено на основі [1]

Таким чином, довід розвинутих держав та європейських сусідів може допомогти України покращити рівень інформаційної безпеки та підвищити ефективність протидії гібридним загрозам та інформаційно-психологічним впливам, що позитивно відбивається на політичній стабільності.

3.3. Шляхи вдосконалення системи інформаційної безпеки України для зміцнення політичної стабільності

Для рекомендацій по покращенню системи інформаційної безпеки України, варто розглянути які напрями забезпечення інформаційної безпеки містяться в нормативно-правових документах.

Найголовніший документ, який, в рамках нашого дослідження, нас цікавить, є Стратегія інформаційної безпеки України.

З огляду цього документу, ми можемо виділити сім стратегічних цілей, які намітила держава до 2025 року [66]:

- «Протидія дезінформації та інформаційним операціям, насамперед держави-агресора…»;
- «Забезпечення всебічного розвитку української культури та утвердження української громадянської ідентичності»;
- «Підвищення рівня медіакультури та медіаграмотності суспільства…»;
- «Забезпечення дотримання прав особи на збирання, зберігання, використання та поширення інформації, свободу вираження своїх поглядів і переконань, захист приватного життя, доступ до об'єктивної та достовірної інформації, а також забезпечення захисту прав журналістів…»;
- «Інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих територіях та на прилеглих до них територіях України, до загальноукраїнського інформаційного простору…»;
- « Розвиток інформаційного суспільства та підвищення рівня культури діалогу».

В рамках цих напрямків, також складений план заходів план заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року. Усього можна нарахувати 52 завдання [55]. Про стан виконання завдань можна дізнатися зі звітів різних органів влади, зокрема, Міністерства культури України або Державної служби спеціального зв’язку та захисту інформації України. [25]. Тобто, можна відстежити й результати впровадження Стратегії інформаційної безпеки.

Тим не менш, система інформаційної безпеки України має свої проблеми та недоліки.

Варто звернути увагу на питання євроінтеграційних процесів. Так, імплементація європейських стандартів у національне законодавство відбувається поступово, шляхом ухвалення необхідних підзаконних

нормативів і технічних регламентів. ЄС та України співпрацюють в рамках системи реагування на кіберінцеденти, захисту персональних даних, сертифікацій та кіберзлочинства.

Слід наголосити, що впровадження європейських стандартів має ряд проблем та викликів:

- Брак кваліфікованих спеціалістів;
- Низька обізнаність громадян;
- Брак фінансування;
- Відсутність певний норм в державний документах.

Також, деякі дослідники наголошують на викликах, які зумовлені як внутрішніми, так і зовнішніми чинниками [60, с. 38]:

- Внутрішні – переважно пов’язані з відставанням інформаційних технологій в Україні від провідних держав світу, недостатнім рівнем інформатизації, а також із розпорошенням повноважень органів державної влади та нормативно-правової бази у сфері інформаційної діяльності;
- Зовнішні – визначаються глобальними тенденціями розвитку й використання інформаційних технологій, прагненням іноземних акторів впливати на світовий та український інформаційний простір для просування власних інтересів, а також залежністю від зарубіжного програмного забезпечення.

Окрім вищесказаного, можна додати про зарубіжний досвід, який був проаналізований в попередньому підрозділі. Втім, втілюючи зміни, не варто механічно запозичувати іноземні підходи. Гармонізація можлива лише тоді, коли нові елементи органічно інтегруються в уже сформовану систему.

Таким чином, можна сформувати ряд рекомендацій, які мають вдосконалити систему інформаційної безпеки:

- Підвищити ефективність і забезпечити комплексний підхід до формування державної політики у сфері інформаційної безпеки шляхом тісної співпраці з приватним сектором та інститутами громадянського суспільства;

- Покращити структуру та ієрархію відповідальних державних органів і посадових осіб, із чітким розподілом функцій і завдань та усуненням дублювання повноважень;
- Проводити систематичний аналіз та оцінювання виконання законодавства у сферах інформаційної та кібербезпеки, свободи слова і поширення інформації. У разі виявлення недоліків, що перешкоджають повноцінній реалізації правових норм і досягненню поставлених цілей, необхідно вживати заходів для їх усунення;
- Проводити безперервний моніторинг українських і зарубіжних засобів масової інформації та інтернет-простору з метою своєчасного виявлення загроз інформаційній безпеці України та оперативного напрацювання і реалізації заходів для протидії таким загрозам;
- Впровадження та удосконалення щорічного звітування щодо забезпечення інформаційної безпеки України відповідними органами державної влади, які займаються питаннями інформаційної політики України. Особливо покращити підхід щодо звітування перед громадянами для підвищення обізнаності суспільства та кращої прозорості роботи органів;
- Створити і розвивати структури, що відповідають за інформаційно-психологічну безпеку суспільства та створити програму дій щодо підвищення інформаційно-психологічного стану населення;
- Забезпечити фінансову, наукову та матеріально-технічну підтримку юридичних і фізичних осіб, залучених до створення та розвитку системи інформаційної безпеки, а також покращити умови праці, професійного зростання й мотивації фахівців у цій сфері;
- Впровадити національну систему сертифікації згідно з програмою євроінтеграції для ефективної сертифікації та стандартизації засобів інформаційної та кібербезпек;
- Розробити державну політику в галузі регіонального інформаційного захисту, створюючи для її реалізації відповідні організаційні структури та

правову базу, а також посилити взаємодію регіональних структур із органами виконавчої влади для ефективного вирішення питань інформаційної безпеки;

- Сприяти розвитку вітчизняних виробників засобів інформатизації та інформаційного захисту, створюючи умови для підвищення їхньої конкурентоспроможності на національному та міжнародному ринках, тим самим знижуючи залежність від закордонних технологій;
- Підвищити ефективність заходів щодо покращенні медіаграмотності населення, тим самим формуючи культуру «цифрової стійкості» до інформаційно-психологічного впливу;
- Продовжувати та поглиблювати міждержавні співробітництва з державами-партнерами у сфері забезпечення інформаційної безпеки.

Окремо також потрібно приділити увагу гібридним загрозам. Так, існує «Модель комплексної екосистеми стійкості», яка передбачає «аналіз і, зрештою, протидію гібридним загрозам, які прагнуть підірвати і завдати шкоди цілісності та функціонуванню демократій, змінити процеси прийняття рішень і створити каскадні ефекти». Цю модель можна представити в такому вигляді [8, с. 63]:

Таблиця 3.4

Схематизація «Моделі комплексної екосистеми стійкості»

Просто-ри	**Засади демокра-тичних систем**	**Сфери**	**Рівні**		
			Лока-льний	**Націона-льний**	**Міжнарод-ний**
Громад-ський простір	1. відчуття справедли-вості та рівного ставлення, 2. громадян-ські права і свободи,	культурна, соціальна сфера, політична сфера, інформаційна сфера	Грома-ди	Нації	Групи та мережі

	3. політична відповідальність та підзвітність,				
Простір управління	4. верховенство права, 5. стабільність,	військова сфера, сфера державного управління, правова сфера, розвідувальна сфера, дипломатична сфера, політична сфера	Місцевий рівень управління	Управління на державному рівні	Багатосторонній рівень управління
Простір послуг	6.доступність, 7. здатність до передбачення.	Інфраструктурна сфера, кібернетична сфера, космічна сфера, економічна сфера, інформаційна сфера	Кластерний рівень у сфері послуг	З'єднання	Глобальний рівень у сфері послуг

Джерело: сформовано на основі [8, с. 64]

Модель демонструє, що всі елементи є взаємопов'язаними: заходи з підвищення стійкості одного елемента можуть мати вплив на інші.

Таким чином, це допомагає органам влади, які приймають рішення, визначати, які ресурси, інструменти та заходи залучати на рівні держави, регіонів та на локальному рівні.

Як видно з цієї моделі, стійкість є ключовим чинником протидії гібридним загрозам і повинна розвиватися системно. Розбудова стійкості у вузьких сферах окремо неефективна, оскільки гібридні загрози створюють

багаторівнені ефекти. Потрібен комплексний підхід із врахуванням існуючих залежностей та взаємозалежностей у суспільстві.

Таким чином, для вдосконалення системи інформаційної безпеки України, що важливо для політичної стабільності держави, варто звернути на ряд напрямків, які або слабо розвинені, або ще не впроваджені. Також, формування та розвиток державної політики у сфері інформаційної безпеки сприятиме зменшенню ризику виникнення інформаційних загроз.

Отже, у третьому розділі дослідження розглянуто систему механізмів, за допомогою яких держава може ефективно забезпечувати захист свого інформаційного простору, протидіяти зовнішнім і внутрішнім загрозам та зміцнювати політичну стабільність.

Державна політика у сфері інформаційної безпеки спрямована на контроль над інформаційними загрозами та створення умов для задоволення інформаційних потреб населення, забезпечення національних інтересів і стабільності держави. Вона охоплює широкий спектр заходів, включаючи нормативно-правове регулювання, організаційні та технічні механізми. Ефективне функціонування цієї політики забезпечується чіткою структурою органів державної влади, їхніми функціями та відповідальністю. Правова база державної політики спирається на міжнародні документи та національне законодавство, що гарантує права громадян у сфері інформації, регулює доступ до даних, захист персональних даних, інформаційних ресурсів та кіберпростору, а також визначає напрями забезпечення інформаційної безпеки.

Зарубіжні країни формують інформаційну безпеку через комплексне правове регулювання, розвиток технологій та інтегровані системи кіберзахисту. ЄС розробив європейські стандарти та директиви для захисту персональних даних, критичної інфраструктури та забезпечення сумісності систем. Фінляндія та Швеція демонструють моделі комплексної безпеки та психологічного захисту населення. США зосереджені на розвитку

інформаційних технологій, контролі інформаційного середовища та підготовці фахівців. Польща активно залучає громадянське суспільство для протидії дезінформації. Аналіз досвіду інших держав показує необхідність інтегрованого підходу до інформаційної безпеки, врахування національних особливостей і послідовну імплементацію європейських стандартів в Україні.

Система інформаційної безпеки України потребує удосконалення через комплексний підхід до формування політики, оптимізацію структури державних органів та підвищення ефективності контролю й моніторингу. Основні проблеми недостатнього забезпечення інформаційної безпеки включають нестачу кваліфікованих кадрів, недостатнє фінансування, низький рівень обізнаності громадян та відставання технологій. Рекомендації для вдосконалення включають зміцнення співпраці держави з приватним сектором, підвищення інформаційно-психологічної стійкості населення, розвиток національних технологій та стандартів, а також поглиблення міжнародного співробітництва. Впровадження «Моделі комплексної екосистеми стійкості» дозволяє системно протидіяти гібридним загрозам, що позитивно впливає на політичну стабільність держави.

Підсумовуючи, можна стверджувати, що ефективна система інформаційної безпеки є одним із головних чинників політичної стабільності держави.

ВИСНОВКИ

У сучасному світі інформація стала одним із головних ресурсів, від якого залежить не лише розвиток суспільства, а й стійкість держави перед зовнішніми та внутрішніми загрозами. Україна особливо гостро відчуває це через виникаючі інформаційні загрози. Саме тому було важливо зрозуміти, як функціонує інформаційна безпека, чому вона напряму пов’язана з політичною стабільністю та які фактори здатні послабити або, навпаки, зміцнити державу в інформаційній сфері.

Мета наукового дослідження, яка полягає у з’ясуванні сутності, загроз і механізмів забезпечення інформаційної безпеки як чиннику політичної стабільності держави та визначенні ефективних шляхів вдосконалення системи інформаційної безпеки, була досягнута, поставленні завдання виконані.

Поняття «інформаційної безпеки» є достатньо складне та багатозначне. В залежності від підходу, інформаційну безпеку можуть трактувати як: певний стан, процес, система чи функція. Одні дослідники визначають, що інформаційна безпека — це система суспільних відносин, що забезпечує захист важливих інтересів усіх об’єктів, другі — трактують як стан захищеності від інформаційних загроз, а треті — як складову національно безпеки. Для нашої роботи було важливо пов’язати інформаційну безпеку з політичною стабільністю. Тому інформаційну безпеку ми будем визначати як стан захищеності життєво важливих інтересів особистості, суспільства й, в нашому випадку, держави від негативних інформаційних впливів в усіх сферах життя суспільства та діяльності держави, й який базується на діяльності людей, суспільства, держави, світового співтовариства з виявлення, попередження, послаблення, ліквідації і відбиття небезпек і загроз, які здатні, в тому числі порушувати політичну стабільність. В цілому, інформаційна

безпека в епоху інформатизації та змін перебуває на етапі постійного становлення.

Поняття політичної стабільності багатогранне, тому й існують різні підходи для її розуміння: інституціональний, соціально-економічний, психологічний, геополітичний та системний. Політична стабільність – це стійкість політичної системи, тобто відсутність різких змін та конфліктів. Тобто це такий стан політичної системи, коли відсутні різкі політичні зміни, функціонують політичні інститути, а влада легітимізована. Також під політичною стабільністю розуміють характеристику, систему зв'язків між різними політичними суб'єктами. Розумінню сутності політичної стабільності допомагає представлення її особливостей: впорядкованість суспільних відносин і складових політичної системи; баланс політичних сил та інтересів; відсутність загрози легітимності влади. Існують безліч видів політичної стабільності. Так, наприклад, Україні притаманна динамічна політична стабільність з елементами консолідаційної стабільності (консолідація у критичних ситуаціях). Основою політичної стабільності можна охарактеризувати трьома елементами: легітимністю (підтримка влади, здатність), дієвістю (здатність вирішення проблем) та ефективністю (здатність впровадження рішень). Таким чином, політична стабільність виступає чинником функціонування політичної системи.

Деструктивні інформаційно-психологічні впливи мають глибокі соціальні й політичні наслідки. Інформаційна безпека повинна бути засобом протидії таким впливам. Інформаційна безпека включає як захист інтересів об'єктів, так й гарантування права на доступ до різної інформації. Тому для ефективного забезпечення інформаційної безпеки потрібно звертати увагу на суб'єкти, об'єкти та їх інтереси. Суб'єктами та об'єктами інформаційної безпеки, зазвичай, виступають індивід, суспільство та держави. Також часто інтереси в інформаційній сфері, між цими об'єктами, збігаються. Тому для аналізу інформаційної безпеки держави потрібно звертати увагу й на

інформаційну безпеку особистості та суспільства. Існує ряд інструментів та засобів, які забезпечують високий рівень політичної стабільності в інформаційній сфері, зокрема: законодавче регулювання, інституційне забезпечення, захист інфраструктури та залучення громадян до політичних процесів.

Політичній стабільності держави, очевидно, погрожують різни види та типи інформаційних загроз. Класифікація та типологізація цих загроз допомагає й інформаційній безпеці, бо забезпечує впорядкованість та ідентифікацію наявних та можливих загроз в інформаційній сфері. Існує достатньо велика кількість класифікацій в залежності від критерію або концепції. Важливо також визначати й джерела загроз для кожного з об'єктів інформаційної безпеки. В рамках нашого дослідження, можна визначити подібні джерела загроз для держави: незаконний доступ до державної інформації; неконтрольоване поширення інформаційної зброї та її використання, та спроби проведення інформаційно-психологічних впливів. Класифікація інформаційних загроз та їх джерел, важливе для систематизації та пріоритизації потенційних та реальних ризиків.

Гібридні загрози та інформаційно-психологічні впливи — дуже небезпечні для політичної стабільності. В наш час існує достатня кількість форма та методів подібного впливу. Так, існують гібридні війни, інформаційні війни та інформаційно-психологічні операції. Ці явища можуть включати один одного. Гібридні загрози характеризуються скоординованістю, поєднанням традиційних та не традиційних засобів впливу та спрямованістю на досягнення політичних або стратегічних результатів, за часту, без активної фази силових дій. На наш, погляд, потрібно торкнутися й питання інформаційних війн, які подаються як комплекс дій різного напряму для контролю інформаційного простору, усунення супротивника та руйнування його комунікації. Взагалі, сучасні війни часто супроводжуються саме інформаційними війнами або інформаційно-психологічними операціями. В цьому ключі варто звернути

увагу на Стратегію інформаційної безпеки України, яка включає ряд викликів та загроз, а також стратегічні задачі.

Окремо, в сучасну добу інформаційно-комунікаційних технологій, важко переоцінити вплив соціальних мереж на політичну стабільність. Соціальні мережі часто використовують для цілеспрямованих деструктивних впливів на об'єкти інформаційної безпеки (індивіда, суспільство, державу). Соціальні мережи характеризуються рядом факторів, які впливають на її ефективність дестабілізаційних заходів: широке охоплення аудиторії, миттєве розповсюдження інформації, емоційна форма сприйняття та невисокі витрати. Найочевиднішим прикладом об'єкту інформаційної безпеки на який постійно нависають інформаційно-психологічні загрози є Україна. Дослідження показують велику кількість методів та форм реалізації інформаційної війни та інформаційно-психологічних операцій.

Аналіз державної політики у сфері інформаційної безпеки допомагає зрозуміти механізми забезпечення інформаційної безпеки держави. Правову основу забезпечення інформаційної безпеки становлять велика кількість норм різної юридичної сили та різного рівня. Найвищим рівням нормативно-правової бази є міжнародні документи, видані ООН, ЮНЕСКО, МСЕ, ВОІВ та іншими міжнародними організаціями, які намагаються нормувати відносини в інформаційному просторі. В України ж діють достатня кількість законів та документів подібного характеру: починаючи з Конституції України, яка визнає інформаційну безпеку як одну з ключових функцій держави, і продовжуючи Стратегією інформаційної безпеки та Законом України «Про інформацію». Інституційне забезпечення інформаційної безпеки держави реалізується суб'єктами державної інформаційної політики. В Україні діє достатня кількість як формуючих органів держави політики у сфері інформаційної безпеки, так і органів, які займаються реалізацією цієї політики. Окремо стоїть РНБО як контролюючий орган.

Досвід зарубіжних країн, особливо сильніше розвинених у сфері інформаційної безпеки, може допомогти покращенню інформаційної безпеки в Україні. Велику роботу по впорядкуванню нормативної бази та цілісності інформаційної політики зробив Європейських Союз. Також варто згади «Концепцію комплексної безпеки» Фінляндії та діяльність шведського уряду по захисту громадян від інформаційно-психологічних впливів. США також зробила свої акценти в державній політиці в сфері інформаційної сфери: сприяння розвитку національних інформаційно-комунікаційних технологій, підготовка фахівців та розвиток інформаційної інфраструктури.

Стан системи інформаційної безпеки України має достатньо високий рівень, але при цьому характеризується своїми проблеми та недоліками. Виділяються такі ризики: брак кваліфікованих спеціалістів, низька обізнаність громадян, відсутність фінансування, залежність від закордонних технологій тощо.

Для удосконалення системи інформаційної безпеки України було запропоновано ряд напрямків, на які потрібно звернути увагу: співпраця держави, приватного сектору та громадян; систематичні звіти органів, які відповідають за інформаційну безпеку; підвищення медіаграмотності та інформаційно-психологічного захисту громадян; забезпечення підтримкою фахівців у сфері інформаційної безпеки; розроблення політики регіонального інформаційного захисту; сприяння розвитку вітчизняних виробників засобів інформатизації та інформаційного захисту; поглиблення міжнародної співпраці.

Отже, інформаційна безпека представляє собою важливий елемент загальної національної безпеки держави. Забезпечення інформаційної безпеки – напряму впливає на політичну стабільність. Також дослідження інформаційної безпеки є важливою областю дослідження, яке потребує подальшого вивчення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. National cyber security index. URL: https://ncsi.ega.ee/ncsi-index/?order=rank (дата звернення: 23.09.2025).

2. Баталов О., Паламарчук М. (2023). Поняття політичної стабільності та політичних конфліктів. *Вісник Харківського національного університету імені В.Н. Каразіна. Серія "Питання політології; 44*, С. 15–18.

3. Бебко Є. Ю. Соціальні наслідки інформаційного тероризму: дезінформація та маніпуляція суспільною думкою. Науковий блог. Національний університет «Острозька академія». 2025. URL: https://naub.oa.edu.ua/sotsialni-naslidky-informatsijnoho-teroryzmu-dezinformatsiya-ta-manipulyatsiya-suspilnoyu-dumkoyu/ (дата звернення 18.08.2025).

4. Білоусов М.В., Алейник В.Г. Російська гібридна війна: загроза і кібервиклики для європейської інформаційної безпеки // Регіональні студії. 2023. № 33. С. 119-125.

5. Білько С. Інституційне забезпечення інформаційної безпеки України. Економіка і регіон. – 2021. – №3 (82). С. 43–45.

6. Боднар І. Інформаційна безпека як основа національної безпеки. Механізм регулювання економіки. 2014. № 1. С. 68–75.

7. Босак І. Інформаційна безпека України: загрози та методи протидії. Київський економічний науко-вий журнал. 2025. No 9. С. 33–38.

8. Гібридні загрози та комплексна безпека: навчальний посібник. Укл. Карпенко О.О., Осипова Є.Л. Київ : ТОВ «ТРОПЕА», 2024. 76 с.

9. Гібридні загрози. WARN. URL: https://warn-erasmus.eu/ua/glossary/gibridni-zagrozi/ (дата звернення: 18.08.2025).

10. Голод К. Інформаційна безпека США: Сучасний стан та уроки для України. Збірник наукових праць. Геополітика України: історія і сучасність. 2017. Вип. 2 (19). С. 91–107.

11. Гончар, М. (2023). Вплив соціальних мереж на політичну стабільність та національну безпеку: досвід Королівства Швеція. Політичні науки та методика викладення соціально-політичнх дисциплін. Серія 22. Вип. 33(2). С. 54-63.

12. Грищук Р.В., Жовноватюк Р.М., Носова Г.Д. Гібридні загрози укіберпросторі: фактори впливу на природу виникнення. Modern InformationTechnologies in the Sphere of Security and Defence. 2019. No 3(36). С. 52-58.

13. Громико І. Державна домінантність визначення інформаційної безпеки України в умовах протидії загрозам. Право України. 2008. № 8. С. 130-134.

14. Гурковський В. І. Безпека як об’єкт правовідносин в умовах глобального інформаційного суспільства. Правова інформатика. 2010. № 2(26). С. 72–77.

15. Демидюк І. Л. Державна політика у сфері розвитку медіа як фактор забезпечення інформаційної безпеки України: роб. на здоб. освіт. ступ. Магістр. Луцьк: Волинський нац. ун-т ім. Л. Українки, 2024. 70 с.

16. Деркаченко Я. (2016). Інформаційно-психологічні операції як сучасний інструмент геополітики. URL: https://goal-int.org/informacijno-psixologichni-operacii-yak-suchasnij-instrument-geopolitiki/ (дата звернення: 18.08.2025).

17. Дикий А. П., Наумчук К. М., Тростенюк Т. М. (2021). Аналіз сучасних загроз інформаційній безпеці держави. *Економічний простір*, №176, С. 155-158.

18. Довгань О.Д. Соціальні мережі як чинник впливу на інформаційну безпеку. Правова інформатика. 2015. № 2(46). С. 25–31.

19. Дрига Д. Аналіз правових механізмів забезпечення інформаційної безпеки інформаційної інфраструктури Європейського Союзу. Економічні наук. Вісник Хмельницького національного університету. №5. 2024. С. 46-51.

20. Загрози інформаційної безпеки. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Загрози_інформаційної_безпеки (дата звернення: 18.08.2025).

21. Закон України «Про інформацію» за редакцією від 14.06.2025 URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення 18.08.2025).

22. Закон України «Про Концепцію Національної програми інформатизації» за редакцією від 01.01.2022. URL: https://zakon.rada.gov.ua/laws/show/75/98-вр#Text (дата звернення 18.08.2025).

23. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.2007. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text (дата звернення 18.08.2025).

24. Захист інформації. Технічний захист інформації. Терміни та визначення : ДСТУ 3396.2-97. Чинний від 01.01.1998 р. URL: https://tzi.com.ua/478.html (дата звернення 18.08.2025).

25. Звіт Міністерства культури та інформаційної політики України за 2023 рік щодо виконання Плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року. Міністерство культури України. URL: https://mcsc.gov.ua/wp-content/uploads/2025/01/zvit-shhodo-vykonannya-planu-zahodiv-z-realizacziyi-strategiyi-informaczijnoyi-bezpeky-za-2023-rik.pdf (дата звернення: 23.09.2025).

26. Золотар О. О., Трубін І. О. Класифікація загроз інформаційній безпеці. Інформація і право. 2013. № 3(9). С. 105-114.

27. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам / У. Ільницька // Humanitarian vision. - 2016. - Vol. 2, Num. 1. - С. 27-32.

28. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека»/ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 166 с.

29. Інформаційна безпека сучасного суспільства : Навчальний посібник. / За загальною ред. А. І. Міночкіна. – К.: ВІТІ НТУУ «КПІ». 2006. – 188с.

30. Калюжний Р. Питання концепції реформування інформаційного законодавства України. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : збірник Київ : НТУУ "КПІ", Міністерство освіти і науки України, СБУ. 2000. С. 17–21.

31. Каменчук Т. О. Державна політика України у сфері інформаційної безпеки. Науковий журнал «Політикус». Вип. 1. 2025. С. 46-54.

32. Кіянка І. Б. Політична стабільність: суть і основні засоби її досягнення в Україні : автореф. дис. ... канд. політ. наук: 23.00.02 / І. Б. Кіянка. Львів : Львів нац. ун-т ім. І. Франка, 2003. 18 с.

33. Козьміних А. Основні механізми та особливості політичної стабільності в Україні в умовах політичного транзиту. Філософія та політологія в контексті сучасної культури. 2020. Т. 12; № 1. С. 123–132.

34. Конституція України від 26.06.1996 р. Відомості Верховної Ради України, №30, 141. URL: «https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text» (дата звернення: 20.09.2025).

35. Концепція «гібридної» війни та її складові. (2024). «СЕНС». URL: https://censs.org/concept-of-hybrid-warfare-and-its-components/ (дата звернення: 18.08.2025).

36. Кормич Б. А. Інформаційна безпека: організаційно-правові основи: Навч. Посібник. – К.: Кондор, 2004. – 384 с.

37. Леснік Р. М. Державна політика забезпечення інформаційної безпеки України: основні напрямки та особливості здійснення: роб. на здоб. освіт. ступ. магістр. Острог: Нац. ун-т «Острозька академія», 2022. 67 с.

38. Ліпсет С. М. Політична людина. Соціальні основи політики / С. М. Ліпсет // Політична наука. 2011. № 3. С. 195–245.

39. Мазепа С. Міжнародний досвід захисту інформаційної безпеки: імплементація європейських правових норм в законодавство України. Науковий вісник Ужгородського Національного Університету. Серія ПРАВО. Вип. 90: частина 3. 2025. С. 289-296.

40. Марценко М. С. Поняття та види інформаційних війн // Матеріали VI Міжнародної науково-практичної конференції «Російсько-українська війна: право, безпека, світ» (29–30 квітня 2022 р.). – Тернопіль, 2022. URL: http://confuf.wunu.edu.ua/index.php/confuf/article/view/943 (дата звернення: 20.09.2025).

41. Милосердна І. М. Інформаційна безпека як елемент національної безпеки: теоретичний вимір та особливості впровадження / І.М. Милосердна // Політикус : наук. журнал. 2024. № 4. С. 179-185.

42. Міненко Є. С. Сутність політичної стабільності в умовах інформаційного суспільства. Науковий журнал «Politicus». 2023. № 5. С. 155–160.

43. Мужанова Т. М. Інформаційна безпека держави: навч. посіб. Київ : ДУТ, ННІЗІ, 2019. 131 с.

44. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с.

45. Панарін А. Політична стабільність: визначення та підходи до розуміння. Соціогуманітарні проблеми людини № 7, 2013. С. 106-112.

46. Пастернак А. В. Державна політика у сфері інформаційної безпеки: роб. на здоб. освіт. ступ. магістра. Івано-Франківськ: Заклад вищої освіт ун-т короля Данила, 2024. 98 с.

47. Пашковський В. Ф. Інституційний механізм інформаційної безпеки України в умовах гібридної війни: характер та перспективи трансформацій.

Політичні інститути та процеси. Науковий журнал «Політикус». Вип. 1. 2021. С. 69-78.

48. Погромський М. В. Національна безпека України в умовах гібридних загроз (2014-2024 рр.): роб. на здоб. освіт. ступ. бакалавр. Київ: Київський столичний ун-т ім. Б. Грінченка, 2025. 97 с.

49. Постанова Кабінету Міністрів України "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" від 29.03.2006 № 373. URL: https://zakon.rada.gov.ua/laws/main/373-2006-%D0%BF (дата звернення: 18.08.2025).

50. Прокопенко Л. С. Інформація. Українська бібліотечна енциклопедія. 2022. URL: https://ube.nlu.org.ua/article/Інформація (дата звернення 18.08.2025).

51. Проноза І. І. (2018). Інформаційна війна: сутність та особливості прояву. Актуальні проблеми політики, Вип. 61, 76-84.

52. Прямоухіна Н. В., Бойко Ю. В. Соціальні мережі як інструмент забезпечення державної безпеки. Вінниця: ДНУ ім. В. Стуса, 2021. С. 280–282.

53. Пугачов О.І. Зарубіжний досвід забезпечення інформаційної безпеки держави. Проблеми сучасних трансформацій. Серія право. Публічне управління та адміністрування. 2024. № 13.

54. Ребкало В., Шахов В. Політична стабільність і політична безпека: характер та механізми взаємозв'язку. Вісник Національної академії державного управління при Президентові України. 2011. No 3. С. 159–169.

55. Розпорядження Кабінету Міністрів України від 30 березня 2023 р. № 272-р «Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року». URL: https://zakon.rada.gov.ua/laws/show/272-2023-р#n14 (дата звернення: 23.09.2025).

56. Савлюк М. Важливість інформаційної безпеки в соціальних мережах для загальнонаціональної безпеки: безпековий вимір України. Вісник

Прикарпатського університету. Серія: Політологія. 2024. Випуск 18. С. 300-309.

57. Сасин Г. В. Інформаційна війна: сутність, засоби реалізації, результати та можливості протидії (на прикладі російської експансії в український простір) / Г. В. Сасин // Грані. - 2015. - № 3. - С. 18-23. - URL: http://nbuv.gov.ua/UJRN/Grani_2015_3_5 (дата звернення 19.08.2025).

58. Свідерська О. (2020). Теоретико-методологічний аналіз впливу соціальних мереж на формування політичної поведінки в сучасному суспільстві (на прикладі Facebook, Twitter, Instagram, WhatsApp). Регіональні студії, 20, 184-190.

59. Сливка М. М. Правове забезпечення інформаційної безпеки: досвід країн Європейського Союзу. Юридичний науковий електронний журнал. №11. 2021. С. 514-516.

60. Солодка О.М. Пріоритети удосконалення інформаційної безпеки України. Інформація і право. № 3(15). 2015. С. 36-42.

61. Стрільчук, Л. (2023). Інформаційна війна як складова сучасних гібридних воєн (на прикладі Грузії та України). *Літопис Волині*, (28), 235-239. URL: https://doi.org/10.32782/2305-9389/2023.28.33 (дата звернення 18.08.2025).

62. Ткачук Т.Ю., Довгань О.Д. Система інформаційної безпеки України: онтологічні виміри. Інформація і право. 2018. № 1 (24). С. 89–104.

63. Тлуста А. О. Вплив соціальних мереж на політичну стабільність держави. Сучасна система міжнародного права. 2011. С. 195–201.

64. Турчак А. Основні складові інформаційної безпеки держави. Аспекти публічного управління. 2019. № 5, т. 7. С. 44–56.

65. Уздєнова, Ю. М. (2024). Гібриднавійна: сутність, складовітаключовіпоняття. Вчені записки ТНУ ім. В. І. Вернадського. Серія: Публічне управління та адміністрування. Т. 35(74). №4. 2024. С. 172-179.

66. Указ Президента України №685/2021 «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегії інформаційної безпеки». URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення 18.08.2025).

67. Федорова Н. Є., Смєсова В. Л. Інформаційна безпека та шляхи її забезпечення на етапі інформаційно-технологічної революції. Причорноморські економічні студії. 2020. Вип. 57. С. 13–16.

68. Феськов І. В. НУ «ОЮА» Основні методи ведення гібридної війни в сучасному інформаційному суспільстві. Актуальні проблеми політики. 2016. Вип. 58. С. 66–76.

69. Харченко С.О. Наукові підходи до класифікації загроз інформаційній безпеці. Держава та регіони. Серія : Державне управління. 2019. № 2 (66).

70. Четверик Г. Мережа інтернет та політична стабільність. Філософія та політологія в контексті сучасної культури. 2012. Вип.3. С. 279–286.

71. Шевчук М. О. До питання генези поняття інформаційної безпеки як складової національної безпеки. Науковий вісник Ужгородського університету: серія: Право / голов. ред. Ю. М. Бисага. Ужгород, 2023. Т. 2. Вип. 78. С. 134–139.

72. Шемаєв В. М., Присяжнюк М. М., Онофрійчук А. П. Соціальні мережі в аспекті інформаційної безпеки. Наука і оборона. 2019. №3. С. 36-40.

73. Шпига П. С., Рудник Р. М. Основні технології та закономірності інформаційної війни. Проблеми міжнародних відносин. 2014. Вип. 8. С. 326-339.

74. Шульга В. І. Сучасні підходи до трактування поняття інформаційна безпека. Ефективна економіка. 2015. №4. URL: http://www.economy.nayka.com.ua/?op=1&z=5514 (дата звернення 18.08.2025).

75. Шульська, Н. М., Букіна, Н. В., Адамчук, Н. В. (2023). Типологічні маркери інформаційнопсихологічних операцій (ІПСО) в умовах війни в медіа.

Науковий журнал «Вчені записки ТНУ імені В. І. Вернадського. Серія: Філологія. Журналістика». Том 34 (73). № 1. Частина 2. С. 268–274.

76. Яворський М. Політична стабільність: сутність та основні підходи до класифікації. Вісник Національного університету «Львівська політехніка» Серія «Політичні науки». 2017. № 1. С. 62–66.