

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА**

**Навчально-науковий інститут бізнес-освіти імені А. Поручника
Кафедра політичних технологій**

Освітньо-професійна програма «Публічна політика та лідерство»
Галузь знань 05 «Соціальні та поведінкові науки»
Спеціальність 052 «Політологія»

Форма здобуття освіти: заочна

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

**на тему «Політична опозиція: сутність, особливості та роль в умовах військової
агресії.»**

здобувача **Прохорчука Юрія Юрійовича**_____

(підпис)

Науковий керівник: к.політ.н., доцент кафедри
політичних технологій **Мордзинська Н.А.** _____

(підпис)

**Робота допущена до захисту перед екзаменаційною
комісією з атестації здобувачів вищої освіти (ЕК)
Завідувач кафедри: д.політ.н., проф., Гапоненко В.А.**

(підпис)

Київ 2026

Роль держави у забезпеченні інформаційної безпеки

ЗМІСТ

ВСТУП.....	3
РОЗДІЛ 1. Теоретико-методологічні засади інформаційної безпеки в політичній системі держави.....	7
1.1. Поняття інформаційної безпеки: політико-правовий аспект.....	8
1.2. Інформаційна безпека як політична функція держави.....	15
1.3. Міжнародні стандарти у сфері інформаційної безпеки (НАТО, ЄС, приклади Естонії, Литви, Польщі, Німеччини).....	19
РОЗДІЛ 2. Політика України у сфері інформаційної безпеки.....	29
2.1. Інституційна система забезпечення інформаційної безпеки України.....	29
2.2. Загрози інформаційній безпеці в умовах гібридної війни.....	42
2.3. Стратегії, ініціативи та державні програми у сфері інформаційної безпеки.....	49
РОЗДІЛ 3. Баланс між інформаційною безпекою та демократичними свободами.....	59
3.1. Свобода слова і державна політика протидії дезінформації.....	59
3.2. Роль громадянського суспільства та незалежних медіа.....	67
3.3. Перспективи розвитку державної інформаційної політики в Україні.....	72
ВИСНОВКИ.....	77
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	80

ВСТУП

Актуальність теми «Роль держави у забезпеченні інформаційної безпеки» зумовлена стрімким розвитком інформаційних технологій та зростанням кіберзагроз, що становлять небезпеку для національної безпеки України. В умовах воєнної агресії особливої ваги набуває захист інформаційного простору від пропаганди, дезінформації та кібератак. Ефективна державна політика у сфері інформаційної безпеки є запорукою стабільності, довіри громадян до влади та захисту державного суверенітету. Водночас наукові дослідження з даної проблематики свідчать про недостатню узгодженість між нормативно-правовим забезпеченням, інституційними механізмами реалізації державної політики та практичними заходами у сфері кібербезпеки. Потребує глибшого аналізу питання взаємодії державних структур із громадянським суспільством у протидії інформаційним загрозам, а також пошуку балансу між безпековими інтересами держави та дотриманням демократичних стандартів свободи слова. Проблема полягає у недостатній узгодженості між безпековими заходами держави та дотриманням демократичних принципів свободи слова.

Аналіз останніх досліджень і публікацій. У наукових працях В. В. Ковальчук висвітлено ключову роль держави у забезпеченні інформаційної безпеки в умовах гібридної війни. Автор підкреслює, що стрімкий розвиток інформаційних технологій створює нові виклики для державного управління, а захист інформаційного простору має бути одним із пріоритетів національної політики [35, с.45]. Українські дослідники В. М. Вовк і У. М. Олійник розглядають інформаційну безпеку крізь призму права людини на доступ до Інтернету, що тісно пов'язане із забезпеченням як особистої, так і державної безпеки [19, с.112]. На відміну від них, Ю. І. Крилова робить акцент на нормативно-правових механізмах протидії дезінформації та потребі впровадження просвітницьких заходів серед населення для формування культури інформаційної безпеки [40, с.77]. Позиція Крилової відрізняється від

підходу В. Вовк тим, що вона фокусується на інституційному управлінні та правових інструментах, тоді як Вовк і Олійник – на ціннісно-демократичному аспекті проблеми. Західні дослідники, такі як А. Рац і А. Бугар, аналізують інформаційні війни як складову гібридних загроз у міжнародній політиці. У праці «Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist» А. Рац детально розкриває етапи інформаційних впливів, серед яких стратегічні, політичні та оперативні заходи, спрямовані на дестабілізацію держави-жертви. На відміну від українських учених, які зосереджуються на внутрішніх механізмах державної політики, західні дослідники розглядають інформаційне протистояння як глобальний феномен неконвенційного протиборства [71, с.18].

У науковому дискурсі можна виокремити три основні напрями дослідження інформаційної безпеки:

1. Правовий напрям (Ю. Крилова, В. Дзюба, О. Косілова) – удосконалення нормативно-правової бази та регуляторних механізмів.
2. Політичний напрям (В. Вовк, У. Олійник, В. Ковальчук) – інституційна роль держави та співвідношення безпеки і демократії.
3. Стратегічний напрям (А. Рац, А. Бугар) – інформаційні війни і гібридні загрози як інструмент геополітичного впливу.

Отже, українські науковці переважно зосереджуються на розробці правових і політичних засад інформаційної безпеки, тоді як зарубіжні автори – на аналізі глобальних механізмів і технологічних інструментів впливу. Поєднання цих підходів дає змогу комплексно дослідити роль держави у забезпеченні інформаційної безпеки в умовах сучасних гібридних загроз.

Методологічну основу дослідження становлять концепції інформаційного суспільства (М. Кастельс), теорія національної безпеки (Б. Бузан), підходи до аналізу гібридних загроз (Ф. Гофман), а також інституціональний підхід у політичній науці (Д. Норт, Г. Алмонд). Зазначені теоретичні підходи дають можливість розглядати інформаційну безпеку не лише як технічну чи правову категорію, а як складну соціально-політичну систему, що визначає стабільність держави та її суверенітет. Вони також

забезпечують міждисциплінарний характер дослідження, поєднуючи політичні, правові й комунікаційні аспекти інформаційної безпеки.

Мета дослідження: з'ясувати особливості політичних, правових та інституційних механізмів, за допомогою яких держава забезпечує інформаційну безпеку, та оцінити їх ефективність в умовах гібридних загроз і воєнного стану

Завдання дослідження:

1. Розкрити сутність поняття «інформаційна безпека» та охарактеризувати її політико-правовий зміст.
2. Проаналізувати інформаційну безпеку як одну з ключових політичних функцій держави.
3. Дослідити міжнародні стандарти та практики забезпечення інформаційної безпеки (на прикладі країн НАТО та ЄС).
4. Визначити основні загрози інформаційній безпеці України в умовах гібридної війни та шляхи їх нейтралізації.
5. Оцінити ефективність інституційної системи та державних програм України у сфері інформаційної безпеки.
6. Розглянути взаємозв'язок між забезпеченням інформаційної безпеки та дотриманням демократичних свобод.
7. Запропонувати напрями вдосконалення державної інформаційної політики України з урахуванням європейських стандартів.

Об'єкт дослідження: процес формування та реалізації державної політики у сфері забезпечення інформаційної безпеки.

Предмет дослідження: роль держави в організації, регулюванні та гарантуванні інформаційної безпеки в умовах сучасних політичних і безпекових викликів.

Методи дослідження: у роботі застосовано системний, аналітичний, порівняльно-правовий, історичний, інституційний та структурно-функціональний методи. Використано також методи контент-аналізу офіційних

документів, нормативно-правових актів та міжнародних стратегій у сфері інформаційної безпеки.

Теоретична значущість отриманих результатів: полягає у поглибленні наукових уявлень про сутність, структуру та механізми забезпечення інформаційної безпеки держави, а також у систематизації підходів до формування національної інформаційної політики.

Практична значущість отриманих результатів: полягає у можливості використання висновків і пропозицій дослідження у процесі вдосконалення державних стратегій, нормативно-правових актів та програм із забезпечення інформаційної безпеки України, а також у навчальному процесі при вивченні політичних та правових дисциплін.

Інформаційну базу дослідження становлять наукові праці українських і зарубіжних учених, зокрема: Ю. І. Крилової, К. М. Зоріна, В. А. Дзюби, В. О. Шумейка, А. Бугар, А. Раца, У. М. Олійник, В. М. Вовка, Г. Куспляк, О. Дуліної, К. Ровинської, О. І. Косілової, О. Б. Березовської-Чміль, Ю. В. Кобець, М. Б. Міщук та інших. Їхні праці присвячені проблемам державної політики у сфері кібербезпеки, нормативно-правового регулювання інформаційних процесів, впливу гібридних загроз, а також розвитку інформаційного суспільства в умовах глобалізації.

Структура дослідження: робота складається із вступу, основної частини, яка, у свою чергу, має три розділи із підрозділами, висновки та список використаної літератури. Загальний обсяг роботи складає 79 сторінок, список використаних джерел вміщує 71 найменування.

РОЗДІЛ 1. Теоретико-методологічні засади інформаційної безпеки в політичній системі держави

Інформаційна безпека в сучасному суспільстві виступає не лише техніко-правовим явищем, а передусім політичним феноменом, що відображає стан і механізми взаємодії держави, суспільства та інститутів влади у сфері інформаційної комунікації. У контексті політичної системи держави вона є складовою механізму забезпечення легітимності влади, керованості суспільних процесів і стабільності політичного режиму.

З політико-теоретичної точки зору, інформаційна безпека - це інструмент політичного управління інформаційними потоками, спрямований на підтримку балансу між відкритістю суспільства і захистом його стратегічних інтересів. У цьому сенсі вона є засобом формування інформаційного суверенітету, який визначає спроможність держави контролювати простір політичних комунікацій, протидіяти деструктивним інформаційним впливам і забезпечувати довіру громадян до інститутів влади.

Мій авторський підхід полягає у трактуванні інформаційної безпеки як системної політичної практики, що об'єднує стратегічні рішення, управлінські механізми та символічні ресурси легітимації. Інформаційна безпека не може бути зведена лише до юридичних норм чи технологічних бар'єрів – вона є динамічним процесом політичної взаємодії, у якому держава виступає не лише охоронцем, а й активним суб'єктом конструювання інформаційної реальності.

Політичний аспект інформаційної безпеки охоплює:

- державну політику у сфері інформації, що визначає стратегічні пріоритети, концепції та програми захисту інформаційного простору;
- легітимацію рішень у сфері інформаційної політики через суспільне схвалення та політичну комунікацію;
- взаємодію політичних інституцій (парламенту, уряду, президента, громадянського суспільства, медіа), що координують інформаційні потоки і визначають межі свободи слова, доступу до інформації та контролю над нею.

Натомість правовий аспект інформаційної безпеки зводиться до формалізованої системи норм, стандартів і регламентів, які забезпечують захист інформації, визначають відповідальність за порушення, регулюють права суб'єктів інформаційних відносин. Якщо політична складова формує зміст, то правова - задає форму його інституційного оформлення [66, с.50].

Таким чином, політична природа інформаційної безпеки полягає у здатності держави створювати та підтримувати політичний порядок через контроль інформаційного простору, забезпечуючи при цьому баланс між свободою комунікації та захистом національних інтересів. Інформаційна безпека як політичний феномен відображає рівень зрілості політичної системи, її спроможність до діалогу з громадянським суспільством та ефективності у реагуванні на інформаційні виклики глобалізованого світу.

1.1. Поняття інформаційної безпеки: політико-правовий аспект

Сутність поняття «інформаційна безпека» розкривається через його багатовимірний характер, що поєднує політичні, правові, технічні та соціальні аспекти. У науковій літературі цей термін тлумачиться як стан захищеності інформаційного простору держави, за якого забезпечується збереження, достовірність, цілісність і доступність інформації, а також гарантується можливість її вільного обігу без загрози національним інтересам. У правовому полі України поняття інформаційної безпеки закріплене у «Стратегії національної безпеки» та в низці нормативних актів, де воно визначається як частина системи національної безпеки, спрямована на захист інформаційних ресурсів, технологій і комунікацій від внутрішніх і зовнішніх загроз.

Інформаційна безпека виступає однією з ключових складових національної безпеки, адже саме інформаційна сфера визначає рівень політичної стабільності, довіри до влади, суспільної згуртованості та здатності держави протидіяти деструктивним інформаційним впливам. В умовах гібридної війни та активного використання інформаційних технологій у політичних процесах зростає роль держави як гаранта інформаційного

суверенітету, що передбачає ефективну взаємодію між інституціями, медіа, громадянами та цифровими платформами [33, с.19].

До структури інформаційної безпеки входять такі взаємопов'язані елементи, як інформаційні ресурси, інформаційні технології, а також суб'єкти і об'єкти захисту. Інформаційні ресурси охоплюють масиви даних, бази знань, комунікаційні канали, які формують інформаційний потенціал держави. Інформаційні технології забезпечують створення, обробку та передачу інформації, а суб'єкти - державні органи, організації та громадяни - виступають носіями і захисниками цього ресурсу. Об'єктами захисту є інформація, інфраструктура та права людини у сфері доступу й поширення даних. Таким чином, інформаційна безпека є системною категорією, що охоплює як технічний, так і гуманітарний вимір, забезпечуючи гармонійний баланс між захистом інформаційного простору та збереженням демократичних цінностей.

Тож розуміння сутності інформаційної безпеки як комплексного явища дає змогу перейти до розгляду її політичного аспекту, який безпосередньо пов'язаний із роллю держави у формуванні та реалізації інформаційної політики. У сучасних умовах саме держава виступає основним суб'єктом, відповідальним за створення нормативно-правової бази, інституційних механізмів і стратегічних програм, спрямованих на захист інформаційного простору. Її завдання полягає не лише у протидії зовнішнім інформаційним загрозам, а й у формуванні внутрішньої системи комунікації між владою, громадянським суспільством та медіа, що забезпечує стійкість політичної системи.

Інформаційна безпека у цьому контексті розглядається як важливий інструмент державного управління, який дозволяє підтримувати суспільно-політичну стабільність, запобігати деструктивним інформаційним впливам та забезпечувати легітимність державної влади. Ефективна державна політика у сфері інформаційної безпеки сприяє формуванню позитивного іміджу держави, підвищенню рівня довіри до інституцій влади та зменшенню ризиків політичної поляризації суспільства. У демократичних державах така політика базується на

принципах відкритості, відповідальності та прозорості, що дозволяє забезпечити баланс між безпекою та свободою слова [16, с.12].

Особливу увагу слід приділити впливу інформаційних процесів на політичну свідомість і громадську думку, адже саме через інформаційне середовище формується ставлення громадян до державної політики, політичних інститутів та соціальних цінностей. Маніпуляції інформацією, пропаганда, фейки та дезінформаційні кампанії можуть суттєво впливати на поведінку виборців, підривати довіру до влади та створювати передумови для політичної нестабільності. Тому ефективне управління інформаційним простором, розвиток медіаграмотності та контроль за дотриманням стандартів журналістики стають ключовими елементами державної стратегії інформаційної безпеки. Тож, політичний аспект інформаційної безпеки полягає у забезпеченні гармонійної взаємодії між владою, суспільством і медіа задля зміцнення демократичної стабільності та захисту національних інтересів [20, с.195].

Правовий аспект інформаційної безпеки становить фундаментальну основу її функціонування, адже саме через систему нормативно-правових актів держава визначає засади, принципи та механізми захисту інформаційного простору. Конституція України гарантує право кожного громадянина на свободу думки, слова, доступ до інформації та її поширення, одночасно передбачаючи обмеження у випадках, коли це необхідно для захисту національної безпеки, громадського порядку чи прав інших осіб. Базовими нормативними документами, що регулюють сферу інформаційної безпеки, є закони України «Про національну безпеку України», «Про інформацію», «Про основні засади забезпечення кібербезпеки України», «Про доступ до публічної інформації», а також низка підзаконних актів, стратегій і концепцій. Ці документи визначають основні напрями державної політики у сфері інформаційного захисту, коло суб'єктів, відповідальних за її реалізацію, та порядок взаємодії між ними.

Важливе значення у формуванні правового середовища мають міжнародно-правові акти та стандарти, які Україна імплементує у власну систему. Зокрема, це документи ООН, Ради Європи, ОБСЄ, директиви та рекомендації Європейського Союзу, а також стандарти НАТО у сфері кібер- та інформаційної безпеки. Впровадження європейських і міжнародних принципів сприяє підвищенню рівня захисту інформаційного простору, зміцненню співпраці у сфері протидії кіберзлочинності, дезінформації та гібридним загрозам. Прикладом є Будапештська конвенція про кіберзлочинність, до якої приєдналася Україна, та Резолюції Генеральної Асамблеї ООН щодо протидії інформаційним загрозам [17, с. 25].

Ключовими принципами правового регулювання інформаційної безпеки виступають законність, пропорційність та баланс між забезпеченням безпеки і дотриманням демократичних свобод. Законність означає, що будь-які обмеження у сфері інформаційної діяльності повинні ґрунтуватися на чітких правових нормах, тоді як принцип пропорційності передбачає, що заходи із захисту інформаційного простору мають бути співмірними із реальною загрозою. Баланс між безпекою та свободою слова є надзвичайно важливим у демократичному суспільстві, адже надмірне втручання держави може призвести до цензури, тоді як її бездіяльність - до посилення інформаційної вразливості. Інституційний механізм забезпечення інформаційної безпеки України становить цілісну систему органів державної влади, які здійснюють координацію, регулювання та контроль за станом інформаційного простору держави. Центральне місце у цій системі належить Раді національної безпеки і оборони України (РНБО), яка визначає основні напрями державної політики у сфері інформаційної та кібербезпеки, координує діяльність інших органів виконавчої влади, затверджує відповідні стратегії та програми. РНБО виступає стратегічним центром прийняття рішень, що стосуються захисту інформаційного суверенітету держави, зокрема в умовах воєнної агресії та гібридних загроз. Важливу роль відіграє Служба безпеки України (СБУ), на яку покладено завдання з виявлення, запобігання та нейтралізації інформаційних і

кіберзагроз, що посягають на конституційний лад, державну таємницю і стабільність суспільства. СБУ здійснює контррозвідувальні заходи, розслідує випадки інформаційних диверсій, а також бере участь у формуванні нормативної бази з питань інформаційної безпеки [22, с.86].

Значну управлінську та координаційну функцію виконує Міністерство цифрової трансформації України (Мінцифри), яке відповідає за розвиток цифрової інфраструктури, кіберзахист державних електронних ресурсів і впровадження інновацій у сфері інформаційних технологій. Водночас Національна рада України з питань телебачення і радіомовлення здійснює регуляторну діяльність у медіапросторі, контролюючи дотримання законодавства про інформацію, свободу слова, запобігаючи поширенню пропаганди та мови ворожнечі. До системи також входять Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації (ДССЗІ), Міністерство культури та інформаційної політики, Міністерство внутрішніх справ, кожне з яких реалізує свої функції у межах компетенції - від кіберзахисту військових інформаційних систем до моніторингу інформаційних кампаній та інформаційної протидії ворожим впливам. Взаємодія між цими структурами здійснюється на основі принципів узгодженості, субординації та міжвідомчої координації, що забезпечує комплексний підхід до захисту інформаційного простору держави. Такий інституційний механізм дозволяє об'єднати зусилля політичних, безпекових, технічних і медійних інституцій задля створення ефективної системи інформаційної безпеки, здатної адаптуватися до нових викликів цифрової епохи [28, с.95].

У науковому дискурсі інформаційну безпеку визначають як стан захищеності інформаційного простору держави, що забезпечує збереження, достовірність і цілісність інформації, а також її вільний обіг без шкоди національним інтересам. В українському правовому полі поняття інформаційної безпеки закріплено у «Стратегії національної безпеки України», де вона визначається як складова національної безпеки, спрямована на захист інформаційних ресурсів і комунікацій від зовнішніх і внутрішніх загроз.

Водночас науковий аналіз показує, що інформаційна безпека виходить за межі суто правового розуміння - вона є системною політичною категорією, яка безпосередньо пов'язана з державним управлінням, формуванням політичної стабільності та довіри громадян до влади.

Таблиця 1.1.

Порівняльна таблиця підходів до визначення сутності інформаційної безпеки

Підхід	Сутність	Основний суб'єкт	Мета	Ключові індикатори ефективності
Політичний	Інформаційна безпека розглядається як інструмент державної політики, спрямований на підтримку легітимності влади, інформаційного суверенітету та стабільності політичної системи	Держава, політичні інститути, медіа, громадянське суспільство	Координація інформаційних потоків, протидія пропаганді, забезпечення єдності та довіри громадян	Політична стабільність, рівень довіри до влади, стійкість до дезінформації
Правовий	Інформаційна безпека трактується як система правових норм, що регулюють захист інформаційного простору, права суб'єктів інформаційних відносин і відповідальність за порушення	Держава як гарант законності	Захист прав і свобод громадян, регулювання обігу інформації	Відповідність законодавству, ефективність нормативно-правових механізмів
Технологічний	Зосереджується на технічних і кібернетичних засобах захисту інформації, створенні безпечної цифрової інфраструктури	Спеціальні служби, ІТ-сектор, кіберпідрозділи	Забезпечення кіберзахисту, недопущення втручання в інформаційні системи	Кількість відбитих атак, рівень кіберстійкості систем

Із таблиці 1.1. ми бачимо, що порівняльна таблиця відображає багатовимірність поняття інформаційної безпеки, демонструючи різні підходи до її тлумачення – політичний, правовий і технологічний. Політичний підхід

розкриває інформаційну безпеку як інструмент державної політики, спрямований на забезпечення легітимності влади, інформаційного суверенітету та стабільності політичної системи. Тут ключову роль відіграє держава у взаємодії з політичними інститутами, медіа та громадянським суспільством, а показниками ефективності виступають рівень довіри до влади та стійкість суспільства до дезінформації. Правовий підхід має більш нормативний характер і ґрунтується на регламентації інформаційних відносин через систему законів і стандартів. Його мета – забезпечення захисту прав суб'єктів інформаційного простору, дотримання законності та створення правових гарантій інформаційної безпеки. Ефективність цього виміру оцінюється через відповідність національного законодавства міжнародним нормам та дієвість правозастосовних механізмів. Технологічний підхід фокусується на практичному вимірі – створенні захищеної цифрової інфраструктури, протидії кіберзагрозам і недопущенні несанкціонованого втручання в інформаційні системи. Його реалізація залежить від координації дій державних і приватних структур у сфері ІТ та кібербезпеки. Узагальнюючи порівняння, можна зазначити, що політичний аспект інформаційної безпеки має системоутворюючий характер, оскільки інтегрує правові та технологічні компоненти в єдину державну політику, спрямовану на зміцнення легітимності влади та стабільності політичного середовища.

У сучасних умовах війни інформаційна безпека виконує не лише функцію захисту від загроз, а й ціннісно-ідеологічну функцію - забезпечує збереження національної ідентичності, консолідацію суспільства та довіру до держави. Саме через інформаційне середовище формується спільна система цінностей, визначається сприйняття ворога і союзника, а отже, підтримується внутрішня єдність нації. Особливої ваги набуває суб'єктна роль держави, яка виступає не лише гарантом, а й координатором взаємодії між органами влади, медіа, громадянським суспільством і міжнародними партнерами. Ефективна державна політика у сфері інформаційної безпеки сьогодні вимагає мережевої моделі управління, коли держава формує правила і забезпечує баланс інтересів усіх

учасників інформаційного простору. У цьому контексті інформаційна безпека стає інструментом політичного управління, який дозволяє забезпечувати легітимність влади, нейтралізувати деструктивні інформаційні впливи та підтримувати комунікаційний баланс у суспільстві [28, с.96].

У демократичній моделі розвитку держава не обмежується контролем, а діє через прозорість, довіру і стратегічну комунікацію. Це передбачає не тільки протидію фейкам і дезінформації, а й розвиток медіаграмотності, підтримку незалежних ЗМІ та створення умов для відповідальної журналістики. Відтак, інформаційна безпека у політико-правовому вимірі - це не лише захист ресурсів, а динамічна політична система взаємодії, у якій держава, медіа і суспільство спільно формують стійкість нації до інформаційних викликів. Саме така інтегративна модель є запорукою інформаційного суверенітету України в умовах гібридної війни та глобальної цифрової конкуренції.

1.2. Інформаційна безпека як політична функція держави

Сутність інформаційної безпеки як політичної функції держави полягає у її розгляді як одного з ключових інструментів реалізації завдань державного управління та підтримки політичної стабільності. Політичні функції держави традиційно охоплюють регулювання суспільних процесів, забезпечення порядку, захист національних інтересів та формування умов для розвитку демократичних інститутів. У цьому контексті інформаційна безпека займає особливе місце, оскільки вона гарантує захист інформаційного простору, контроль над обігом інформації та протидію дезінформаційним загрозам, що безпосередньо впливає на ефективність державного управління.

Зв'язок між інформаційною безпекою, державною владою та політичним управлінням проявляється у здатності держави формувати стратегічні рішення, координувати діяльність інституцій, впливати на інформаційні потоки та забезпечувати стійкість політичної системи. Через контроль за інформаційними процесами держава не лише захищає національні інтереси, але й формує

суспільну думку, підтримує легітимність влади та довіру громадян до політичних інститутів [26, с.32].

Інформаційна безпека, таким чином, виступає важливим елементом політичної стабільності та легітимності влади, оскільки вона забезпечує рівновагу між потребами держави у захисті інформаційного простору та правами громадян на доступ до інформації. Ефективне здійснення цієї функції дозволяє державі оперативно реагувати на загрози, запобігати політичним маніпуляціям, підтримувати соціальну згуртованість і сприяти розвитку демократичних процесів.

Інформаційна політика держави виступає ключовим інструментом реалізації завдань інформаційної безпеки, оскільки саме через неї формуються стратегічні підходи до захисту інформаційного простору та управління інформаційними потоками. Державна інформаційна політика передбачає визначення цілей, принципів і конкретних заходів, спрямованих на протидію інформаційним загрозам, забезпечення безпеки комунікацій і підтримку стабільності політичної системи [31, с.53].

Серед основних напрямів інформаційної політики виділяють захист національного інформаційного простору, що передбачає охорону державних інформаційних ресурсів і критичної інфраструктури; протидію дезінформації та маніпуляціям, зокрема через розвиток систем раннього виявлення фейкових повідомлень і запровадження нормативно-правових механізмів; підвищення цифрової грамотності громадян, що дозволяє суспільству ефективно орієнтуватися в інформаційному середовищі; а також підтримку національного медіапростору, що включає розвиток українських медіа, забезпечення доступу до достовірної інформації та стимулювання плюралізму думок.

Інформаційна політика тісно пов'язана з іншими сферами державного управління. Вона інтегрується у систему національної безпеки та оборони, забезпечуючи захист від зовнішніх і внутрішніх загроз; у сферу культури та освіти, формуючи інформаційно-грамотне та критично мисляче суспільство; а також впливає на роботу органів влади, відповідальних за правове регулювання

та контроль за дотриманням стандартів інформаційної діяльності. Такий комплексний підхід забезпечує гармонійне поєднання захисту державних інтересів із правами громадян та розвитком демократичного суспільства.

Механізми реалізації політичної функції інформаційної безпеки забезпечують практичне втілення державної політики у сфері захисту інформаційного простору та управління інформаційними потоками. Центральну роль у цьому процесі відіграють органи державної влади, кожен із яких має чітко визначені повноваження. Президент України формує стратегічні напрямки інформаційної політики, забезпечує її відповідність національним інтересам та координацію дій державних органів. Верховна Рада ухвалює закони, які регламентують порядок обігу інформації, права та обов'язки суб'єктів інформаційної діяльності, а уряд забезпечує їх реалізацію через відповідні міністерства та відомства. Особливе значення мають РНБО, що визначає загальні напрями національної безпеки та контролює виконання стратегій, СБУ, яка займається протидією кіберзагрозам і дезінформаційним атакам, Мінцифри, що відповідає за розвиток цифрової інфраструктури та кіберзахист, та Нацрада з питань телебачення і радіомовлення, яка здійснює регуляторну функцію у медіапросторі та контролює дотримання стандартів інформаційної діяльності [34, с.38].

Державне регулювання та контроль у сфері інформаційної безпеки здійснюються через нормативно-правові акти, інституційні механізми та міжвідомчу координацію, що дозволяє оперативно реагувати на загрози, запобігати деструктивним впливам і забезпечувати стабільність політичної системи. Крім того, значну роль відіграють інформаційні технології, які використовуються як інструмент політичного впливу та управління. Через цифрові платформи, медіаресурси та аналітичні системи держава може ефективно поширювати достовірну інформацію, протидіяти пропаганді та фейкам, формувати суспільну думку і підвищувати рівень медіаграмотності громадян.

Інформаційна безпека в умовах демократичного розвитку держави є складовою частиною забезпечення національної стабільності та одночасно показником зрілості політичної системи. Її ефективність значною мірою визначається здатністю держави поєднувати заходи з охорони інформаційного простору з дотриманням фундаментальних свобод громадян, зокрема свободи слова та доступу до інформації. Баланс між безпекою та демократичними правами є критично важливим, оскільки надмірний контроль може призводити до цензури та обмеження громадянських прав, тоді як недостатній захист відкриває простір для дезінформації, маніпуляцій та зовнішніх впливів, що підривають довіру до державних інститутів [14, с.95].

Важливою умовою формування стійкого інформаційного середовища є активна участь громадянського суспільства, незалежних медіа та міжнародних партнерів, які сприяють контролю за діяльністю держави та забезпечують плюралізм інформаційних джерел. Незалежні медіа відіграють ключову роль у підтримці об'єктивної інформації, розвитку критичного мислення громадян і протидії дезінформації, тоді як міжнародне співробітництво дозволяє впроваджувати сучасні стандарти інформаційної безпеки та обмінюватися досвідом у боротьбі з кіберзагрозами.

Прозорість, відкритість і довіра є фундаментальними чинниками, які визначають ефективність інформаційної політики у демократичному суспільстві. Довіра громадян до державних інститутів підсилює легітимність політичних рішень та сприяє їх ефективній реалізації, тоді як відкритість і прозорість у прийнятті рішень мінімізують ризики маніпуляцій та формують відчуття участі суспільства у державотворчих процесах. Таким чином, інформаційна безпека в контексті демократичного розвитку не обмежується технічним або правовим захистом даних, а передбачає комплексний підхід, що інтегрує політичні, соціальні та правові механізми задля створення надійного, безпечного та демократично збалансованого інформаційного простору.

Отже, інформаційна безпека виступає ключовою політичною функцією держави, спрямованою на забезпечення стабільності, захист національного

суверенітету та підтримку демократичного розвитку. Вона поєднує стратегічні, нормативні та інституційні механізми, які дозволяють державі контролювати інформаційні потоки, протидіяти загрозам і водночас зберігати баланс між безпекою та фундаментальними правами громадян. Через формування ефективної інформаційної політики, розвиток цифрової грамотності, забезпечення прозорості та підтримку незалежних медіа держава здатна зміцнювати довіру суспільства до політичних інститутів і забезпечувати легітимність своїх рішень. Інформаційна безпека, таким чином, не обмежується лише технічним або правовим захистом даних, а є комплексним інструментом управління, який інтегрує політичні, соціальні та правові аспекти для зміцнення національної стійкості і демократичного розвитку держави.

1.3. Міжнародні стандарти у сфері інформаційної безпеки (НАТО, ЄС, приклади Естонії, Литви, Польщі, Німеччини)

Міжнародні норми і стандарти відіграють ключову роль у формуванні національної політики інформаційної безпеки, оскільки вони визначають базові принципи захисту інформаційного простору, узгоджують підходи до кіберзахисту та протидії дезінформації, а також сприяють інтеграції держави у глобальну систему безпеки. Дотримання міжнародних стандартів дозволяє забезпечити сумісність національних систем захисту інформації з практиками інших країн, підвищує ефективність взаємодії у сфері кібербезпеки та сприяє оперативному обміну даними про загрози та інциденти [19, с.113]. Крім того, міжнародні норми створюють правову та методологічну основу для розробки національних стратегій, програм і нормативно-правових актів, визначають критерії оцінки ризиків та стандарти управління інформаційними ресурсами. Імплементация таких стандартів також підвищує довіру міжнародних партнерів і суспільства, демонструючи відповідність держави світовим вимогам безпеки та захисту даних. Тож міжнародні норми та стандарти виступають орієнтиром для побудови ефективної та гармонізованої національної системи

інформаційної безпеки, здатної протистояти сучасним викликам цифрової епохи [41, с.32].

Гармонізація національного законодавства з міжнародними практиками у сфері інформаційної безпеки має низку важливих переваг, оскільки дозволяє державі підвищити ефективність захисту інформаційного простору та забезпечити відповідність сучасним глобальним стандартам. По-перше, вона сприяє уніфікації підходів до кіберзахисту, що полегшує взаємодію з міжнародними партнерами, обмін інформацією про загрози та координацію спільних заходів у протидії кібератакам. По-друге, гармонізація забезпечує підвищення правової визначеності та передбачуваності, оскільки національні закони і нормативні акти стають сумісними з міжнародними стандартами, що створює стабільне середовище для державних органів, бізнесу та громадян. По-третє, приведення законодавства у відповідність із міжнародними нормами сприяє підвищенню довіри міжнародного співтовариства та інвесторів, демонструючи, що держава дотримується світових стандартів кібербезпеки та захисту даних. По-четверте, така гармонізація дозволяє запроваджувати передові технологічні та організаційні практики, перевірені у інших державах, що підвищує ефективність національної системи інформаційної безпеки та сприяє розвитку цифрової економіки. В цілому, інтеграція міжнародних практик у національне законодавство створює основу для комплексного, сучасного та гнучкого підходу до забезпечення інформаційної безпеки, здатного реагувати на нові виклики глобального цифрового середовища.

Основні принципи кіберзахисту та інформаційної безпеки НАТО базуються на колективній відповідальності держав-членів і спрямовані на забезпечення безперервності, стійкості та захисту інформаційних та комунікаційних систем Альянсу. Ключовим принципом є колективна оборона у кіберпросторі, коли кібератака на одну державу-члена розглядається як потенційна загроза всьому Альянсу, що передбачає координацію заходів реагування та підтримку постраждалої країни. НАТО дотримується превентивного підходу, активно виявляючи кіберзагрози, здійснюючи аналіз

ризиків і впроваджуючи превентивні заходи для мінімізації можливих наслідків атак.

Ще одним принципом є інформаційна стійкість, яка передбачає захист критичних інформаційних систем і мереж від зовнішніх та внутрішніх загроз, підтримання безперервності функціонування командних і керівних структур, а також забезпечення швидкого відновлення після інцидентів. НАТО також приділяє значну увагу співпраці та обміну інформацією між державами-членами, об'єднуючи зусилля у сфері моніторингу загроз, аналізу інцидентів і розробки спільних стандартів безпеки. Нарешті, принцип постійного вдосконалення та навчання передбачає регулярне тестування систем, обмін досвідом, підготовку кадрів і розробку новітніх технологічних рішень для протидії сучасним кіберзагрозам. Ці принципи дозволяють НАТО формувати комплексну, координаційну і адаптивну систему інформаційної безпеки, здатну протистояти швидкозмінним викликам цифрового середовища [44, с.6].

НАТО розробляє низку рекомендацій для держав-членів, спрямованих на ефективну протидію кіберзагрозам та дезінформації, які враховують сучасні виклики цифрового середовища та гібридних конфліктів. Серед ключових рекомендацій – побудова національних систем кіберзахисту, які включають розбудову інфраструктури для моніторингу, виявлення та реагування на кіберінциденти, а також інтеграцію цих систем у спільну мережу Альянсу. НАТО наголошує на неперервному обміні інформацією між державами-членами, що дозволяє своєчасно виявляти загрози, поширювати дані про інциденти та координувати спільні заходи реагування [57, с.47].

Велике значення приділяється підвищенню кіберграмотності та цифрової свідомості громадян, оскільки стійкість суспільства до маніпуляцій та фейкових повідомлень є ключовим фактором протидії дезінформації. НАТО також рекомендує співпрацю між державними органами, приватним сектором та громадянським суспільством, створюючи багаторівневу систему захисту від кібератак і інформаційного впливу. Крім того, Альянс пропонує постійне вдосконалення нормативно-правової бази та впровадження передових

технологій для забезпечення кіберстійкості критичної інфраструктури та медіапростору. Виконання цих рекомендацій дозволяє державам-членам НАТО не лише ефективно протидіяти зовнішнім і внутрішнім загрозам, а й зміцнювати національну безпеку та стійкість демократичних інститутів у цифрову епоху.

Європейські директиви та регламенти у сфері кібербезпеки та захисту даних відіграють фундаментальну роль у формуванні національної та наднаціональної політики безпеки інформаційного простору. Директива NIS (Network and Information Systems Directive) встановлює мінімальні стандарти кібербезпеки для держав-членів ЄС, визначає обов'язки операторів критичної інфраструктури та цифрових служб, а також закладає механізми обміну інформацією про інциденти та координацію між національними органами. Ця директива спрямована на підвищення стійкості ключових систем до кібератак та забезпечення безперервності критично важливих послуг, що є основою функціонування економіки та державного управління [63, с.7].

Регламент GDPR (General Data Protection Regulation) встановлює єдині правила захисту персональних даних громадян ЄС, визначає права користувачів на контроль над власною інформацією та зобов'язує організації впроваджувати комплексні механізми безпеки даних. GDPR забезпечує підвищений рівень прозорості у зборі, обробці та зберіганні інформації, а також передбачає суворі санкції за порушення, що стимулює держави і бізнес до належного управління даними.

У поєднанні NIS Directive і GDPR створюють комплексний правовий та організаційний каркас, який дозволяє ЄС підвищувати кіберстійкість держав, гарантувати захист персональних і критично важливих даних та формувати стандарти для інтеграції національних систем у єдиний безпечний цифровий простір. Впровадження цих директив сприяє уніфікації підходів до кібербезпеки та формуванню надійної системи захисту інформації на рівні як держав, так і приватних структур [68, с.34].

Європейський Союз відіграє ключову роль у формуванні стандартів цифрової безпеки, створюючи правові, організаційні та технічні рамки, які

забезпечують захист інформаційного простору держав-членів та підвищують їхню стійкість до кіберзагроз. Через прийняття директив, регламентів і стратегій, таких як NIS Directive і GDPR, ЄС встановлює єдині стандарти кіберзахисту, що сприяють уніфікації підходів до безпеки цифрової інфраструктури, обміну інформацією про інциденти та реагування на кіберзагрози.

Крім правових ініціатив, ЄС активно підтримує держави-члени у впровадженні технологічних і організаційних рішень, надаючи консультації, методичну допомогу та ресурси для розвитку національних систем кібербезпеки. Важливою складовою є також партнерство з міжнародними організаціями, академічними установами та приватним сектором, що дозволяє ефективно протидіяти дезінформації, кібератакам і цифровим маніпуляціям. Завдяки цим заходам ЄС сприяє формуванню безпечного, прозорого і стійкого цифрового середовища, де держави здатні захищати національні інтереси, критичну інфраструктуру та права громадян, одночасно інтегруючись у єдиний європейський інформаційний простір [67, с.39].

Досвід Естонії у реалізації міжнародних стандартів інформаційної безпеки є одним із найбільш системних і технологічно розвинених у світі, що обумовлено високою залежністю країни від цифрових технологій у державному управлінні та суспільному житті. Країна впровадила комплексну модель електронного урядування, яка охоплює практично всі державні послуги - від податкових операцій до систем охорони здоров'я та виборчого процесу. Ця модель передбачає централізовану ідентифікацію користувачів через систему eID, яка дозволяє здійснювати безпечний доступ до державних сервісів, підписувати документи в електронній формі та захищає персональні дані громадян на рівні міжнародних стандартів, зокрема GDPR.

Ключовим елементом національної системи є Естонський центр кібербезпеки (CERT-EE), який відповідає за моніторинг кіберзагроз, аналіз інцидентів та розробку рекомендацій для державних установ і приватного сектору. Центр працює за методологіями НАТО та ЄС, координуючи дії між

різними державними органами та забезпечуючи швидке реагування на кібератаки і спроби дезінформації. Значна увага приділяється також навчанню та сертифікації фахівців, що дозволяє створювати високопрофесійну спільноту кіберекспертів і підвищує загальний рівень кіберстійкості суспільства.

Особливістю естонської моделі є інтеграція заходів інформаційної безпеки у повсякденне функціонування державних інститутів і соціальних процесів, що забезпечує одночасно ефективний захист критичної інфраструктури та розвиток цифрового суспільства. Завдяки цьому Естонія демонструє, як міжнародні стандарти та рекомендації можуть бути системно імplementовані в національну політику, створюючи стійку, прозору і технологічно адаптивну систему інформаційної безпеки [59, с.59].

Досвід Литви у реалізації міжнародних стандартів інформаційної безпеки демонструє системний підхід до формування національної кіберстійкості та інтеграції кращих європейських практик. Основою цієї системи є Комплексна національна стратегія кібербезпеки, затверджена урядом, яка визначає ключові напрями державної політики: захист критичної інфраструктури, протидію кібератакам і дезінформації, підвищення кіберграмотності громадян та розвиток цифрових сервісів. Стратегія ґрунтується на принципах превентивності, комплексності та взаємодії державних органів, приватного сектору та громадянського суспільства, що дозволяє координовано протидіяти сучасним кіберзагрозам.

Одним із важливих компонентів литовської моделі є підготовка кадрів у сфері кібербезпеки, що включає спеціалізовані навчальні програми у вищих навчальних закладах, курси підвищення кваліфікації для державних службовців, а також тренінги для приватного сектору. Ця система забезпечує формування високопрофесійних фахівців, здатних ефективно реагувати на інциденти, проводити аудит інформаційних систем і впроваджувати сучасні технологічні рішення.

Крім того, Литва активно інтегрує міжнародні стандарти та рекомендації НАТО і ЄС у свої національні практики, що дозволяє забезпечувати сумісність

з європейським законодавством і ефективну взаємодію з партнерами у сфері кіберзахисту. Такий підхід створює комплексну, адаптивну систему інформаційної безпеки, здатну реагувати на сучасні виклики та забезпечувати захист критично важливих державних і приватних ресурсів, одночасно підтримуючи прозорість і стійкість цифрового середовища [61, с.13].

Досвід Польщі у сфері забезпечення інформаційної безпеки характеризується високим рівнем інституційного розвитку та чітко вибудованою системою державного управління у галузі кіберзахисту. У країні створено Національний центр кібербезпеки (NC Cyber), який координує дії державних органів, військових структур, приватного сектору та наукових установ у протидії кіберзагрозам. Його діяльність спрямована на виявлення, моніторинг та нейтралізацію інцидентів у кіберпросторі, а також на впровадження стандартів НАТО та ЄС у сфері кіберзахисту. Важливу роль також відіграє Урядовий центр безпеки (RCB), який забезпечує координацію дій у кризових ситуаціях, зокрема пов'язаних із кібератаками чи інформаційними операціями проти державних інституцій.

Польща активно розвиває нормативно-правову базу інформаційної політики, що регулює питання кібербезпеки, цифрового управління та захисту персональних даних. Основу цієї системи становлять Закон про національну систему кібербезпеки (2018 р.) та інші підзаконні акти, що імплементують положення Директиви NIS та Регламенту GDPR. Ці документи визначають обов'язки державних і приватних суб'єктів у сфері кіберзахисту, порядок взаємодії з Національним центром кібербезпеки та механізми інформування про інциденти.

Крім того, Польща послідовно впроваджує інформаційну політику, спрямовану на розвиток цифрового суверенітету, протидію дезінформації та зміцнення довіри громадян до державних інституцій. Значну увагу приділено співпраці з Європейським союзом і НАТО, участі у спільних навчаннях і проєктах з кіберстійкості. Такий підхід дозволяє Польщі поєднувати захист національних інтересів із дотриманням демократичних принципів,

забезпечуючи стабільність інформаційного простору та підвищення готовності держави до сучасних викликів у сфері безпеки.

Досвід Німеччини у сфері забезпечення інформаційної безпеки є одним із найсистемніших у Європі та базується на комплексній законодавчій і інституційній моделі кіберзахисту. Основу правового регулювання становить Закон про безпеку інформаційних технологій (IT-Sicherheitsgesetz), ухвалений у 2015 році та оновлений у 2021 році (IT-Sicherheitsgesetz 2.0). Цей нормативний акт визначає обов'язки державних органів і приватних компаній у сфері кіберзахисту, встановлює вимоги до критичної інфраструктури, запроваджує механізми обміну інформацією про інциденти та передбачає адміністративну відповідальність за недотримання стандартів безпеки. Важливим доповненням є Закон про захист персональних даних (BDSG), який імплементує норми Регламенту ЄС про захист даних (GDPR), створюючи правові засади для захисту приватності громадян в умовах цифровізації [56, с.68].

Центральним органом, відповідальним за реалізацію державної політики у сфері інформаційної безпеки, є Федеральне управління з безпеки інформаційних технологій (Bundesamt für Sicherheit in der Informationstechnik - BSI). Його діяльність охоплює розробку технічних стандартів і сертифікаційних вимог у сфері кіберзахисту, проведення моніторингу загроз, координацію реагування на кіберінциденти, а також підвищення обізнаності населення та організацій щодо цифрової безпеки. BSI також виконує консультативну функцію при Федеральному уряді, забезпечуючи стратегічну взаємодію між міністерствами, службами безпеки та приватним сектором.

У Німеччині розроблено високі національні стандарти кіберзахисту, зокрема IT-Grundschutz, який визначає базові вимоги до організації систем інформаційної безпеки в державних і приватних установах. Ця система стандартизації стала еталоном не лише для німецьких, а й для європейських структур, адже поєднує технічні, організаційні та управлінські аспекти безпеки. Окрім того, Німеччина активно співпрацює з Європейським агентством з кібербезпеки (ENISA) та бере участь у програмах НАТО, спрямованих на

розвиток спільної кіберстійкості. Тож німецький підхід до забезпечення інформаційної безпеки вирізняється поєднанням жорсткої нормативної регламентації, ефективного державного управління та постійного оновлення технічних стандартів, що дозволяє країні утримувати високий рівень захищеності інформаційного простору та слугувати прикладом для інших держав-членів ЄС [56, с.74].

Узагальнюючи результати аналізу міжнародних стандартів і практик у сфері інформаційної безпеки, слід підкреслити їхню визначальну роль у формуванні ефективної національної політики України. Досвід НАТО, Європейського Союзу та окремих європейських держав - зокрема Естонії, Литви, Польщі та Німеччини – демонструє, що стійкість держави в інформаційному просторі забезпечується завдяки поєднанню чіткої законодавчої бази, розвиненої інституційної структури, високого рівня міжвідомчої координації та активної участі громадянського суспільства. Міжнародні стандарти, такі як Директива NIS, Регламент GDPR, а також рекомендації НАТО щодо кіберзахисту, створюють основу для гармонізації національних систем безпеки й підвищення їхньої сумісності у межах глобальної безпекової архітектури. Для України імплементація цих підходів має особливе значення в умовах гібридної війни та постійних інформаційних атак. Адаптація міжнародних практик дозволить посилити нормативно-правове забезпечення, розвинути систему кіберзахисту критичної інфраструктури, підвищити рівень цифрової грамотності населення та зміцнити довіру до державних інституцій. Водночас впровадження таких стандартів повинно враховувати національні особливості, політичний контекст та стратегічні пріоритети України, зокрема забезпечення балансу між інформаційною безпекою і демократичними цінностями. Таким чином, міжнародні норми й досвід інших держав виступають не лише орієнтиром, але й практичним інструментом для побудови сучасної, гнучкої та демократичної системи інформаційної безпеки України, здатної ефективно реагувати на глобальні виклики та зміцнювати її суверенітет у цифрову епоху.

РОЗДІЛ 2. Політика України у сфері інформаційної безпеки

2.1. Інституційна система забезпечення інформаційної безпеки України

Поняття інституційної системи у сфері національної безпеки охоплює сукупність державних органів, інституцій та механізмів, які забезпечують реалізацію державної політики, спрямованої на захист суверенітету,

територіальної цілісності, конституційного ладу та життєво важливих інтересів суспільства. У контексті інформаційної безпеки така система виступає структурованим організаційно-правовим утворенням, що забезпечує розроблення, координацію й виконання заходів, спрямованих на захист інформаційного простору держави від внутрішніх і зовнішніх загроз.

Інституційна система базується на взаємодії політичних, адміністративних і правоохоронних інститутів, діяльність яких регламентується Конституцією України, законами та державними стратегіями. Вона функціонує за принципами єдності державного управління, системності, підзвітності та координації між різними рівнями влади – від вищих органів держави до спеціалізованих служб і відомств [57, с.39].

У сфері інформаційної безпеки така система не обмежується лише органами влади, адже включає елементи громадянського суспільства, наукові установи, засоби масової інформації та приватний сектор, які відіграють роль у формуванні безпечного інформаційного середовища. Саме комплексність і взаємопов'язаність усіх цих суб'єктів забезпечують ефективність функціонування інституційної системи, її здатність оперативно реагувати на динамічні інформаційні загрози та підтримувати стабільність політичної системи держави.

Структура системи забезпечення інформаційної безпеки України являє собою багаторівневу, цілісну організаційну модель, у межах якої реалізуються політичні, правові, адміністративні та технічні механізми захисту інформаційного простору держави. Її основу становлять вищі органи державної влади (Президент України, Верховна Рада, Кабінет Міністрів), які визначають стратегічні напрями розвитку інформаційної політики та ухвалюють ключові нормативно-правові акти. Координаційну роль у системі виконує Рада національної безпеки і оборони України, що формує та контролює реалізацію державної стратегії у сфері інформаційної безпеки. На виконавчому рівні діють спеціалізовані органи - Служба безпеки України, Міністерство цифрової трансформації, Державна служба спеціального зв'язку та захисту інформації,

Національна рада з питань телебачення і радіомовлення, кожен з яких відповідає за окремий напрям - від кіберзахисту до інформаційної політики та регулювання медіа [50, с.40].

Система забезпечення інформаційної безпеки побудована на низці фундаментальних принципів, серед яких - законність, пріоритет національних інтересів, системність, координація та відповідальність суб'єктів за виконання своїх повноважень. Важливим є принцип балансу між безпекою і свободою слова, який гарантує, що заходи захисту не обмежуватимуть демократичні права громадян. Окрім того, ключовим є принцип інтеграції та взаємодії, що передбачає тісну співпрацю між державними органами, приватним сектором і громадянським суспільством у реалізації політики безпеки.

Взаємозв'язок між державними, недержавними та міжнародними суб'єктами у сфері інформаційної безпеки являється чинником ефективного функціонування всієї системи національної безпеки. У сучасних умовах глобалізації та розвитку цифрового середовища жодна держава не може самостійно забезпечити повний захист інформаційного простору, оскільки інформаційні загрози мають транскордонний характер. Державні суб'єкти – це насамперед органи законодавчої, виконавчої та судової влади, а також спеціалізовані установи, що відповідають за формування, реалізацію та контроль політики у сфері інформаційної безпеки. До них належать Рада національної безпеки і оборони України, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації, Міністерство цифрової трансформації, Міністерство оборони, Національний центр кібербезпеки при РНБО. Їхнє завдання – розроблення нормативно-правових актів, координація дій різних органів, реагування на кіберінциденти та забезпечення захисту державних інформаційних ресурсів. Недержавні суб'єкти (зокрема ІТ-компанії, громадські організації, аналітичні центри, навчальні заклади, засоби масової інформації) відіграють важливу роль у практичній реалізації заходів безпеки, підвищенні цифрової грамотності населення, розробці інноваційних технологій кіберзахисту та формуванні суспільної свідомості у сфері інформаційної

культури. Взаємодія держави з приватним сектором (Public-Private Partnership) є необхідною умовою для створення ефективних механізмів моніторингу, запобігання та реагування на інформаційні атаки. Міжнародні суб'єкти - це Європейський Союз, НАТО, ООН, ОБСЄ, а також міжнародні організації з кібербезпеки (наприклад, Європейська агенція з кібербезпеки ENISA). Їхня участь полягає у формуванні спільних стандартів, обміні інформацією, спільних навчаннях, фінансовій та технічній підтримці національних програм безпеки. Співпраця України з цими інституціями сприяє інтеграції в європейський безпековий простір і підвищенню рівня сумісності із західними системами реагування [51, с.112].

Конституційно-правові засади діяльності органів у сфері інформаційної безпеки ґрунтуються на нормах Конституції України, яка визначає фундаментальні принципи побудови та функціонування системи національної безпеки, у тому числі й у сфері інформаційної безпеки. Конституція виступає основоположним документом, що закріплює права, свободи громадян і визначає обов'язки держави щодо їх забезпечення, у тому числі в інформаційному просторі. Насамперед, стаття 17 Конституції України проголошує, що забезпечення державної безпеки та захист державного суверенітету є найважливішими функціями держави. У цьому контексті інформаційна безпека розглядається як складова національної безпеки, адже інформаційні загрози можуть мати прямий вплив на обороноздатність, політичну стабільність, економічну незалежність і територіальну цілісність держави.

Стаття 34 Конституції гарантує кожному право на свободу думки і слова, а також на вільний збір, зберігання, використання та поширення інформації. Разом із тим ця стаття встановлює межі реалізації інформаційних прав – вони не можуть порушувати права інших осіб, підривати національну безпеку, громадський порядок або територіальну цілісність держави. Такий баланс між свободою інформації та безпекою є основою конституційної політики України в цій сфері. Крім того, статті 85, 106 і 107 Конституції України визначають

повноваження Верховної Ради, Президента України та Ради національної безпеки і оборони у формуванні та реалізації політики національної, у тому числі інформаційної, безпеки. Верховна Рада ухвалює закони, що регулюють захист інформаційного простору, Президент забезпечує керівництво у сфері безпеки, а РНБО координує діяльність усіх державних органів у цій галузі.

Законодавча база України у сфері інформаційної безпеки становить системну основу формування, реалізації та координації державної політики в цій галузі. Ключовими нормативно-правовими актами є закони «Про національну безпеку України», «Про інформацію» та «Про основні засади забезпечення кібербезпеки України», які визначають стратегічні цілі, принципи, суб'єктів і механізми забезпечення інформаційної безпеки держави.

Закон «Про національну безпеку України» (2018 р.) закріплює інформаційну безпеку як один із головних складників національної безпеки. У ньому підкреслюється, що держава має забезпечувати захист свого інформаційного простору, протидію дезінформації, інформаційно-психологічним операціям та кіберзагрозам. Закон визначає основні напрями державної політики у сфері інформаційної безпеки – зокрема, розвиток національної системи стратегічних комунікацій, підвищення медіаграмотності населення, а також взаємодію державних і недержавних інституцій у сфері захисту інформації [49, с.61].

Закон «Про інформацію» (в редакції 2011 року з подальшими змінами) встановлює правові засади інформаційних відносин, визначає поняття інформації, її види, принципи доступу до неї, права і обов'язки суб'єктів інформаційної діяльності. Він гарантує право громадян на отримання достовірної, повної й об'єктивної інформації, а також визначає правові межі поширення відомостей, які можуть загрожувати державній безпеці. У цьому контексті закон формує правову основу для забезпечення балансу між свободою інформації та захистом національних інтересів.

Закон «Про основні засади забезпечення кібербезпеки України» (2017 р.) регламентує організаційні та технічні механізми кіберзахисту. Він визначає

ключові суб'єкти у сфері кібербезпеки – Раду національної безпеки і оборони, Службу безпеки України, Державну службу спеціального зв'язку та захисту інформації, Міністерство оборони та інші органи. У документі також закріплені принципи співпраці між державними структурами, приватним сектором і міжнародними партнерами у протидії кіберзагрозам. Закон спрямований на створення цілісної системи реагування на інциденти у кіберпросторі, удосконалення захисту критичної інформаційної інфраструктури та розвиток національного потенціалу кібероборони.

Стратегічні документи, зокрема Стратегія національної безпеки України та Доктрина інформаційної безпеки, визначають не лише загальні напрями державної діяльності, а й пріоритети, механізми реалізації, відповідальних суб'єктів та очікувані результати у сфері захисту інформаційного простору. Стратегія національної безпеки України (затверджена Указом Президента України у 2020 році) є базовим документом, що окреслює фундаментальні засади державної політики безпеки. У ній інформаційна безпека розглядається як один із ключових компонентів національної безпеки поряд із воєнною, економічною, екологічною, кібербезпекою тощо. Стратегія визначає головну мету у цій сфері – забезпечення стійкості держави до інформаційних загроз, зокрема до інформаційно-психологічних операцій, кібернетичних атак, дезінформації та пропаганди, що підривають довіру громадян до інститутів влади. Серед пріоритетних завдань – створення ефективної системи стратегічних комунікацій, посилення кіберзахисту критичної інфраструктури, розвиток національного інформаційного простору та підвищення інформаційної грамотності громадян.

Доктрина інформаційної безпеки України (затверджена у 2017 році) конкретизує положення Стратегії, надаючи детальне бачення принципів, напрямів і механізмів реалізації державної політики у сфері інформаційної безпеки. У документі визначено, що головною метою є захист національних інтересів у інформаційній сфері, забезпечення інформаційного суверенітету, формування сприятливого середовища для розвитку українського

медіапростору та протидія зовнішнім інформаційним впливам, передусім гібридним загрозам з боку інших держав. Доктрина також підкреслює важливість співпраці держави з громадянським суспільством, ЗМІ та міжнародними партнерами у протидії дезінформації, а також потребу у формуванні національної культури безпечного використання інформаційних технологій [28, с.99].

Взаємодія цих двох документів забезпечує стратегічну узгодженість і наступність політики: Стратегія задає загальну рамку, визначає загальнодержавні пріоритети, тоді як Доктрина деталізує інституційні, правові й організаційні механізми їх реалізації. У сукупності вони утворюють методологічну основу для розроблення галузевих стратегій, державних програм і законодавчих актів у сфері інформаційної та кібербезпеки.

Президент України відіграє центральну роль у системі державного управління інформаційною безпекою, оскільки виступає гарантом національної безпеки та територіальної цілісності держави. Конституційно закріплені повноваження Президента дозволяють йому визначати стратегічні пріоритети у сфері захисту інформаційного простору, затверджувати ключові державні програми та стратегічні документи, зокрема Стратегію національної безпеки та Доктрину інформаційної безпеки.

Президент координує діяльність Ради національної безпеки і оборони (РНБО), яка формує та контролює реалізацію політики держави у сфері інформаційної безпеки, а також забезпечує взаємодію між усіма ключовими органами влади – Верховною Радою, Кабінетом Міністрів, спеціалізованими силовими та технічними структурами. Він визначає пріоритети розвитку кіберзахисту, протидії дезінформації та забезпечення безпеки критичної інформаційної інфраструктури, а також встановлює рамки для взаємодії з міжнародними партнерами у сфері інформаційної безпеки.

Рада національної безпеки і оборони України (РНБО) є ключовим органом державного управління, що відповідає за координацію та контроль реалізації політики інформаційної безпеки. Вона створює єдину платформу для

взаємодії всіх гілок влади та спеціалізованих відомств, що забезпечує комплексний підхід до захисту національного інформаційного простору. РНБО формує стратегічні напрямки діяльності держави у сфері інформаційної безпеки, затверджує національні програми протидії кіберзагрозам та дезінформації, а також визначає пріоритети розвитку критичної інформаційної інфраструктури. Організаційна структура РНБО передбачає участь Президента України як голови, ключових міністрів, керівників силових і спеціалізованих органів (СБУ, Мінцифри, Держспецзв'язку), що забезпечує системну координацію між виконавчою, законодавчою та правоохоронною гілками влади. Рада здійснює контроль за виконанням стратегічних документів у сфері інформаційної безпеки, аналізує поточні загрози, готує пропозиції щодо удосконалення нормативно-правової бази та розвитку інституційної системи. Тож РНБО виступає центром стратегічного управління інформаційною безпекою, що забезпечує узгодженість дій усіх державних суб'єктів, оперативне реагування на інформаційні загрози та реалізацію комплексної політики захисту національного інформаційного простору [21, с.13].

Кабінет Міністрів України забезпечує реалізацію державних програм та стратегій у сфері інформаційної політики і кіберзахисту. Він відповідає за практичне втілення стратегічних рішень, ухвалених Президентом та РНБО, та організовує координацію діяльності центральних органів виконавчої влади, що займаються питаннями захисту інформаційного простору. Кабінет Міністрів контролює виконання законів та державних програм, спрямованих на розвиток цифрової інфраструктури, кібербезпеку критичних об'єктів, протидію дезінформації, а також підтримку національного медіапростору та інформаційної грамотності населення. Він здійснює міжвідомчу координацію, виділяє ресурси на реалізацію заходів у сфері інформаційної безпеки та забезпечує підготовку нормативно-правових актів, необхідних для ефективного функціонування державної системи захисту інформації [23, с.9].

У системі державного управління інформаційною безпекою України спеціалізовані органи та установи виконують критично важливу роль у

забезпеченні захисту національного інформаційного простору, протидії кіберзагрозам та формуванні безпечного цифрового середовища. Вони забезпечують реалізацію політики держави у сфері інформаційної безпеки на практичному рівні, координуючи свою діяльність із стратегічними органами влади та міжнародними партнерами, що робить систему комплексною та адаптивною до сучасних викликів.

Служба безпеки України (СБУ) є основним державним органом, який забезпечує захист державних інформаційних ресурсів та критичної інфраструктури від внутрішніх і зовнішніх загроз. До її завдань належить виявлення, запобігання та нейтралізація кіберінцидентів, розслідування інформаційних атак і протидія діяльності суб'єктів, які можуть підривати національну безпеку у інформаційній сфері. СБУ здійснює координацію між різними державними структурами, що забезпечує швидке реагування на інформаційні загрози та мінімізацію наслідків атак на державні системи. Окрім цього, служба бере участь у міжнародних обмінах інформацією щодо кіберзагроз і співпрацює з партнерами у розробці сучасних механізмів захисту інформаційного простору.

Міністерство цифрової трансформації України (Мінцифри) відповідає за розвиток цифрової інфраструктури, впровадження електронного врядування та забезпечення кіберстійкості державних інформаційних систем. Воно реалізує проекти, спрямовані на розвиток національного цифрового простору, підтримку інновацій, створення електронних сервісів для громадян і бізнесу та підвищення цифрової грамотності населення. Міністерство координує стандарти безпеки в державних органах, проводить аудит кіберзахисту інформаційних систем і забезпечує інтеграцію українських цифрових платформ у міжнародні стандарти безпеки.

Національна рада з питань телебачення і радіомовлення виконує важливу функцію у контролі за інформаційним простором та медіа. Вона здійснює моніторинг змісту інформаційних потоків, регулює діяльність мовників, забезпечує протидію поширенню дезінформації, пропаганди та шкідливого

контенту, що може підривати суспільну довіру та демократичні інститути. Рада також формує стандарти прозорості та етики у медіа, сприяє розвитку національного медіапростору та підтримує участь громадянського суспільства у контролі за інформаційною політикою.

Державна служба спеціального зв'язку та захисту інформації України (ДССЗІ) відповідає за технічний захист інформації, стандарти безпеки та сертифікацію систем захисту інформаційних ресурсів. Вона розробляє методології і технології захисту критичної інформаційної інфраструктури, контролює впровадження технічних засобів кіберзахисту та забезпечує відповідність державних інформаційних систем міжнародним стандартам безпеки. ДССЗІ також координує питання криптографічного захисту, захищеного зв'язку та організовує навчання спеціалістів із кібербезпеки.

Узагальнюючи, взаємодія цих органів формує комплексну систему забезпечення інформаційної безпеки України, де кожен суб'єкт відповідає за окремий напрям – стратегічне планування, технічний захист, цифрову трансформацію або регулювання медіапростору. Їхня спільна діяльність забезпечує ефективне протидіяння інформаційним і кіберзагрозам, зміцнення національної стійкості та підтримку демократичного розвитку, а також дозволяє державі інтегрувати власну політику інформаційної безпеки у міжнародні стандарти та практики.

З огляду на глобальний характер інформаційних потоків, високий рівень технологічної динаміки та домінування приватного сектору в ІТ-сфері, досягнення стійкості інформаційного простору потребує скоординованої взаємодії державних і недержавних суб'єктів. Така взаємодія формується як багаторівнева система партнерства, що включає співпрацю держави з медіа, ІТ-компаніями, науковими установами, громадськими організаціями та міжнародними інституціями. Передусім варто відзначити, що держава, реалізуючи політику у сфері інформаційної безпеки, виконує стратегічно координуючу функцію. Її завдання полягає не лише у створенні правових і технологічних умов для захисту національних інтересів, а й у налагодженні

комунікації між усіма учасниками інформаційного середовища. Зокрема, співпраця з медіа дозволяє державі реалізовувати інформаційну політику, спрямовану на протидію дезінформації, формування медіаграмотності населення, а також зміцнення довіри до офіційних джерел інформації. Медіа у цьому контексті виступають не лише інструментом поширення контенту, а й партнером у забезпеченні відкритості влади, зворотного зв'язку з громадськістю та підвищенні рівня критичного мислення суспільства.

Водночас вирішальну роль у сучасній системі інформаційної безпеки відіграють ІТ-компанії, що володіють інфраструктурою, технологіями і знаннями, без яких неможливо ефективно реагувати на кіберзагрози. Партнерство держави з технологічним сектором дає змогу реалізовувати спільні програми з кіберзахисту, розробляти національні стандарти безпеки інформаційних систем, здійснювати моніторинг кіберінцидентів та оперативно реагувати на загрози. У цьому аспекті особливого значення набуває концепція публічно-приватного партнерства, що передбачає розподіл відповідальності та ресурсів між державою й бізнесом. Вона забезпечує не лише підвищення технічної спроможності країни до протидії кіберзлочинності, але й стимулює інноваційний розвиток цифрової інфраструктури.

В умовах гібридної та кібервійни особливого значення набуває публічно-приватне партнерство як один із ключових механізмів забезпечення інформаційної та кібербезпеки держави. Традиційна модель, у межах якої провідна роль у захисті інформаційного простору належить виключно державним інституціям, виявляється недостатньо ефективною з огляду на динамічний характер сучасних кіберзагроз, високу швидкість технологічних змін та складність цифрових інфраструктур. Саме тому залучення приватного сектору, насамперед ІТ-компаній, телекомунікаційних операторів та розробників програмного забезпечення, стає необхідною умовою формування стійкої системи інформаційної безпеки.

У сучасних умовах кібервійни приватні ІТ-компанії часто виступають першими об'єктами кібератак, оскільки вони забезпечують функціонування критично важливих цифрових сервісів, хмарних платформ, платіжних систем та інформаційних ресурсів державних органів. Атаки на приватний сектор мають не лише економічні, а й стратегічні наслідки, адже можуть призводити до порушення роботи державних сервісів, витоку конфіденційної інформації та дестабілізації суспільних процесів. У цьому контексті приватні компанії фактично стають «першою лінією оборони» у кіберпросторі, що обумовлює потребу у тісній координації їхніх дій з державними структурами.

Механізми публічно-приватного партнерства у сфері інформаційної безпеки реалізуються через декілька ключових напрямів. По-перше, це обмін інформацією про кіберінциденти та загрози, який дозволяє оперативно виявляти нові вектори атак, шкідливе програмне забезпечення та уразливості в інформаційних системах. Державні органи, зокрема Державна служба спеціального зв'язку та захисту інформації та Служба безпеки України, отримують від приватних компаній аналітичні дані та технічні індикатори компрометації, що значно підвищує ефективність реагування на кібератаки.

По-друге, важливим механізмом співпраці є спільна розробка та впровадження стандартів кіберзахисту. Приватні ІТ-компанії, володіючи сучасними технологічними рішеннями та експертизою, беруть участь у створенні рекомендацій щодо захисту критичної інфраструктури, хмарних сервісів і державних інформаційних ресурсів. Такий підхід дозволяє адаптувати державну політику до реальних технологічних викликів та зменшити розрив між нормативним регулюванням і практикою кіберзахисту.

По-третє, значну роль відіграє участь приватного сектору у підготовці кадрів у сфері кібербезпеки. Спільні освітні програми, тренінги та симуляційні навчання сприяють формуванню професійної спільноти фахівців, здатних діяти в умовах масштабних кібератак. У цьому аспекті публічно-приватне партнерство виконує не лише захисну, але й превентивну функцію, знижуючи вразливість держави до майбутніх загроз.

Окрему увагу доцільно приділити аналізу кластерів кібербезпеки як інституційної форми публічно-приватної взаємодії. Кібербезпекові кластери являють собою мережеві об'єднання державних органів, приватних компаній, наукових установ та освітніх центрів, діяльність яких спрямована на спільне вирішення завдань у сфері кіберзахисту. Ефективність таких кластерів полягає у концентрації ресурсів, знань і технологій, що дозволяє швидко реагувати на нові загрози та розробляти інноваційні рішення.

Практика функціонування кібербезпекових кластерів демонструє їхню здатність підвищувати рівень стійкості інформаційної інфраструктури держави. Завдяки горизонтальній взаємодії між учасниками кластера скорочується час реагування на інциденти, покращується координація дій та зменшується дублювання функцій між державним і приватним секторами. Крім того, кластери сприяють інтеграції України у міжнародні мережі кібербезпеки, що є особливо важливим в умовах транснаціонального характеру кібератак.

Водночас ефективність публічно-приватного партнерства та кібербезпекових кластерів залежить від рівня довіри між державою та бізнесом, чіткості правового регулювання та наявності прозорих механізмів відповідальності. За відсутності належних гарантій захисту комерційної таємниці та персональних даних приватні компанії можуть бути обмежені у готовності до глибокої співпраці з державними органами. Тому формування правових і організаційних умов для сталого партнерства є одним із пріоритетів державної політики у сфері інформаційної безпеки.

Тож публічно-приватне партнерство в умовах кібервійни виступає не допоміжним, а системоутворювальним елементом інституційної моделі забезпечення інформаційної безпеки України. Залучення приватних ІТ-компаній і розвиток кластерів кібербезпеки дозволяють підвищити адаптивність держави до сучасних кіберзагроз, забезпечити більш ефективний захист критичної інфраструктури та сформувати комплексну модель реагування на інформаційні виклики.

Наукові установи та громадські організації виступають у системі інформаційної безпеки джерелом аналітичних даних, експертних оцінок і методологічних рекомендацій. Академічне середовище формує наукові підходи до аналізу інформаційних ризиків, розробляє нові моделі кіберзахисту, прогнозує тенденції розвитку інформаційного простору. Громадські організації, у свою чергу, беруть участь у просвітницьких і моніторингових ініціативах, сприяють підвищенню рівня цифрової культури населення, а також контролюють прозорість дій державних інституцій у сфері інформаційної політики. Їхня діяльність створює необхідний баланс між безпекою і свободою слова, попереджаючи можливі зловживання владними повноваженнями у сфері інформаційного контролю.

Міжнародне співробітництво є невід'ємним елементом стратегії інформаційної безпеки України. В умовах глобальних інформаційних загроз, що не визнають державних кордонів, партнерство з міжнародними структурами, такими як НАТО, Європейський Союз та Європейська агенція з мережевої та інформаційної безпеки (ENISA), забезпечує доступ до передових технологій, експертизи та координаційних механізмів. Зокрема, співпраця з НАТО дозволяє інтегрувати українські стандарти кіберзахисту до євроатлантичних норм, отримувати технічну підтримку та брати участь у спільних навчаннях із кібероборони. Участь у програмах ЄС сприяє гармонізації національного законодавства з європейським правовим полем, а партнерство з ENISA розширює можливості для аналізу інцидентів та впровадження сучасних методів управління інформаційними ризиками.

Важливою умовою результативності зазначених форм співпраці є міжвідомча координація. Ефективне функціонування системи інформаційної безпеки передбачає синхронізацію дій між різними державними органами — від спеціальних служб і силових структур до органів виконавчої влади, відповідальних за освіту, науку та цифровізацію. Лише комплексна взаємодія дозволяє забезпечити єдність стратегічного бачення, уникнути дублювання функцій і створити гнучкий механізм реагування на загрози [11, с.54].

Отже, взаємодія державних і недержавних суб'єктів у системі інформаційної безпеки є ключовою умовою збереження інформаційного суверенітету України. Її ефективність визначається рівнем довіри між учасниками, наявністю нормативної бази, що регулює партнерські відносини, та готовністю усіх сторін до відкритого обміну знаннями, технологіями і ресурсами. Така модель співпраці формує не лише стійкий інформаційний простір, але й підґрунтя для побудови цифрової держави, здатної забезпечити безпечний розвиток громадянського суспільства в умовах глобальних викликів.

2.2. Загрози інформаційній безпеці в умовах гібридної війни

Гібридна війна є однією з найхарактерніших форм сучасних конфліктів, у яких поєднуються військові, політичні, економічні, інформаційні, кібернетичні та психологічні засоби впливу. На відміну від традиційних війн, де протиборство здійснюється переважно у військовій площині, гібридна війна розмиває межі між станом миру і війни, між військовими та невійськовими інструментами, створюючи складну багатовимірну систему впливів. Її сутність полягає у досягненні стратегічних цілей агресора без офіційного оголошення війни, шляхом використання непрямих, асиметричних методів, які спрямовані на дестабілізацію супротивника зсередини [18, с.19].

Поняття «гібридна війна» відображає нову парадигму ведення конфліктів, де військові операції поєднуються з інформаційно-психологічними кампаніями, кібератаками, економічним тиском, політичним шантажем і навіть маніпуляцією гуманітарними питаннями. Якщо традиційні війни орієнтувалися на фізичне знищення або окупацію територій, то гібридна агресія має на меті підірвати довіру до державних інститутів, деморалізацію суспільства та зміну політичного курсу держави-мішені. Її основним інструментом стає не зброя у прямому розумінні, а інформація, перетворена на засіб стратегічного впливу.

У сучасному світі саме інформаційний простір стає ключовим полем бою у гібридних війнах. Інформація здатна формувати або руйнувати національну єдність, створювати альтернативні реальності, керувати громадськими

настроями і навіть визначати політичні рішення. Через медіа, соціальні мережі, цифрові платформи та кібератаки агресор отримує можливість впливати на масову свідомість, підмінювати факти, поширювати дезінформацію та маніпулювати емоціями. Такі операції часто супроводжують військові або економічні дії, створюючи ілюзію легітимності агресії або дискредитуючи сторону, що зазнала нападу.

Інформаційний компонент гібридної війни вирізняється високим рівнем прихованості, масштабністю та швидкістю поширення. Маніпулятивні технології, фейкові новини, бот-мережі, підконтрольні медіа та кібердиверсії використовуються для того, щоб змінити інформаційний баланс, нав'язати суспільству викривлені наративи, посіяти сумніви у правдивості офіційної інформації. У результаті держава-жертва стикається не лише з військовим або політичним тиском, але й з підривом власного інформаційного суверенітету, що є критичним чинником її національної безпеки [17, с.25].

Через інформаційну складову відбувається вплив на свідомість людей, формування спотвореного сприйняття реальності та підриг внутрішньої стабільності держави-жертви. На відміну від класичних воєн, у яких головним інструментом є фізична сила, у гібридному конфлікті інформація стає зброєю, здатною руйнувати державу зсередини без прямого застосування військових засобів. Інформація використовується як інструмент маніпуляції, дезорієнтації та психологічного тиску. Агресор цілеспрямовано створює потік викривлених повідомлень, що підмінюють факти емоційними оцінками, апелюють до страху, образи чи відчуття безнадії. Такі повідомлення поширюються через телебачення, інтернет-ресурси, соціальні мережі, ботоферми та навіть через «незалежних експертів», які насправді працюють на інтереси ворожої сторони. Головна мета цих інформаційних операцій – вплинути не лише на окремі групи, а на всю систему суспільних комунікацій, спрямовуючи її в потрібному агресору напрямку.

Одним із ключових завдань інформаційної агресії є підриг довіри до державних інститутів. Через масове поширення дезінформації ворог

намагається створити враження некомпетентності або корумпованості влади, зруйнувати авторитет силових структур, посіяти сумніви в легітимності політичного керівництва. В умовах війни це має особливо небезпечні наслідки, адже підриває суспільну єдність, деморалізує військових і громадян, знижує готовність до спротиву. Деструктивна інформація часто поширюється у вигляді фейкових новин про поразки на фронті, зраду, внутрішні конфлікти або змови, що має спричинити паніку, зневіру й відчуття безсилля. Іншою важливою метою є деморалізація населення через тривале інформаційне навантаження, апеляцію до емоційного виснаження, страху, втрати віри в майбутнє. Противник розраховує, що в умовах постійного потоку негативних повідомлень громадяни почнуть сприймати дійсність у викривленому світлі, втратять відчуття реальності та здатність до критичного мислення. Така стратегія дозволяє агресору досягати політичних і соціальних результатів без необхідності масштабних військових дій, адже розхитане, деморалізоване суспільство саме стає джерелом внутрішньої нестабільності [22, с.94].

Особливу роль відіграє також дезорієнтація міжнародної спільноти. Через глобальні медіа, дипломатичні канали й соціальні мережі агресор прагне представити свої дії як «захист», «вимушену реакцію» або «боротьбу з нацизмом», намагаючись виправдати вторгнення у свідомості іноземних громадян. Це створює ефект інформаційного шуму, у якому правду важко відокремити від брехні, а міжнародна підтримка держави-жертви поступово підважується. Така тактика, відома як “постправда”, дає змогу агресору зберігати контроль над інформаційним порядком денним, навіть коли факти свідчать про протилежне. Усі ці інформаційні механізми діють у тісній взаємодії з іншими складовими гібридної агресії – військовими, економічними, енергетичними, дипломатичними. Їхня ефективність ґрунтується на тому, що вони впливають на глибинні структури суспільної свідомості, змінюючи не лише уявлення про події, а й систему цінностей, мотивацію та колективну поведінку. Саме тому інформаційна складова гібридної війни є не допоміжним,

а рівнозначним фронтом, на якому вирішується доля національної безпеки, державної цілісності та моральної стійкості суспільства [29, с.118].

Гібридна війна створює нову архітектуру загроз, у якій інформаційна сфера стає не лише засобом комунікації, а й ключовим полем бою. У цьому контексті інформаційна безпека набуває стратегічного значення, адже будь-який збій або порушення в інформаційному просторі може мати руйнівні наслідки для національної стабільності, обороноздатності та економічної безпеки держави. Основні загрози проявляються у п'яти взаємопов'язаних напрямках – кіберзагрозах, дезінформації та пропаганді, психологічному впливі, маніпуляції громадською думкою та витоку інформації.

Першочерговим викликом є кіберзагрози, що стали органічною частиною гібридних воєн. Кібератаки спрямовуються на інформаційні ресурси органів державної влади, енергетичну та транспортну інфраструктуру, банківську систему, об'єкти оборонного та телекомунікаційного секторів. Їхня мета полягає не лише у викраденні або знищенні даних, а й у порушенні безперервності функціонування критично важливих систем, що може паралізувати діяльність держави. Приклади таких атак, зокрема український досвід зі шкідливими програмами типу NotPetya або злам державних вебресурсів, свідчать, що кіберпростір став ареною реальних бойових дій, де зброєю виступають коди, а мішенню – інформаційні системи [25, с.61].

Не менш небезпечною є дезінформація та пропаганда, що використовуються агресором для підриву внутрішньої єдності суспільства. Поширення фейкових новин, маніпулятивних наративів, напівправди та чуток відбувається через підконтрольні медіа, псевдоаналітичні ресурси, блогерів і соціальні мережі. У результаті формується альтернативна інформаційна реальність, де істину складно відокремити від вигадки. Пропагандистські кампанії будуються на викривленні історичних фактів, створенні образу ворога, розпалюванні ворожнечі між регіонами або соціальними групами. Такі технології мають на меті не лише дезорієнтувати населення, а й зруйнувати

довіру до національних ЗМІ, інституцій влади та міжнародних партнерів України.

Психологічний вплив виступає окремим і водночас невід’ємним інструментом інформаційної агресії. Його суть полягає у цілеспрямованому впровадженні в суспільну свідомість страху, відчаю та недовіри. Через масові інформаційні кампанії створюється атмосфера паніки, нестабільності, відчуття беззахисності перед ворогом. Особливо ефективними ці методи стають у періоди активних бойових дій або економічної нестабільності, коли населення є психологічно вразливим. Такі атаки знижують моральний дух армії, демотивують громадян до спротиву, породжують апатію та взаємні звинувачення. Зрештою, психологічний вплив може бути не менш руйнівним, ніж фізичні удари, адже він підриває основи суспільної солідарності.

Ще одним механізмом дестабілізації є маніпуляція громадською думкою через соціальні мережі. Цей інструмент особливо ефективний через швидкість поширення контенту та можливість адресного впливу на різні аудиторії. Використовуючи ботоферми, тролів і алгоритмічні механізми підсилення окремих тем, агресор може формувати потрібний інформаційний порядок денний, підмінюючи суспільні дискусії нав’язаними сюжетами. Зокрема, через соціальні мережі поширюються фейки, організовуються інформаційні «вкиди», що викликають політичні скандали або масову паніку. Крім того, агресор використовує аналітику користувацьких даних для створення психопрофілів, що дозволяє застосовувати технології мікротаргетингу – тобто впливу на конкретні групи людей із певними емоційними тригерами [32, с.57].

Не менш серйозною загрозою є витік та викрадення інформації, що включає кібершпигунство, злам баз даних, компрометацію службових або комерційних відомостей. Такі дії мають подвійний ефект: по-перше, агресор отримує доступ до конфіденційних даних, які можуть бути використані для шантажу, економічного тиску чи дестабілізації; по-друге, факт самого витіку підриває довіру до національної системи безпеки. У гібридній війні інформаційне шпигунство охоплює не лише державні структури, але й приватні

компанії, банківські установи, ЗМІ, а також окремих громадян – через злам електронної пошти, соціальних мереж чи мобільних додатків.

Усі зазначені загрози утворюють взаємопов'язану систему, у якій кожен елемент підсилює інші. Кібератаки можуть створювати технічні умови для поширення дезінформації, а психологічний тиск підвищує її ефективність. Маніпуляція в соцмережах забезпечує швидке розповсюдження фейків, тоді як витік інформації дає ворогу нові інструменти впливу. Саме така багатовекторність робить інформаційні загрози в умовах гібридної війни особливо небезпечними. Вони здатні паралізувати державні механізми, деморалізувати суспільство й змінити стратегічний баланс без масштабного застосування збройної сили. Тому розуміння природи та механізмів цих загроз є необхідною передумовою для формування ефективної системи національної інформаційної безпеки [67, с.39].

В умовах гібридної війни, що триває з 2014 року та особливо загострилася після повномасштабного вторгнення Російської Федерації у 2022 році, Україна стала мішенню безпрецедентного інформаційного тиску. Інформаційні загрози для нашої держави мають системний і багаторівневий характер, охоплюючи всі сфери суспільного життя – від політики та економіки до культури й особистісних орієнтирів громадян. Основна мета цих деструктивних впливів – підірвати єдність українського суспільства, знизити довіру до влади та інститутів безпеки, а також спотворити імідж України на міжнародній арені. Одним із найпомітніших проявів таких загроз є масштабні інформаційні атаки та пропагандистські кампанії, що реалізуються з боку Російської Федерації. Вони охоплюють як традиційні медіа (телебачення, радіо, друковані видання), так і цифровий простір – соціальні мережі, месенджери, відеоплатформи. Кремлівські пропагандистські ресурси систематично продукують контент, спрямований на дискредитацію української державності, заперечення права України на суверенітет і незалежність, спотворення фактів щодо перебігу бойових дій. Наприклад, у російських ЗМІ активно поширюються наративи про «штучність української нації», «зовнішнє управління Україною» чи

«громадянську війну на Донбасі», що мають на меті розмити межу між агресором і жертвою агресії.

Особливу небезпеку становить інформаційна війна проти українських ЗМІ. Російські структури намагаються впливати на інформаційний простір України через створення псевдопатріотичних медіа, підконтрольних блогерів, або через мережі «ботоферм», які масово поширюють потрібні меседжі. Такі інформаційні операції супроводжуються кампаніями дискредитації українських журналістів, підривом довіри до офіційних джерел інформації та розпалюванням ворожнечі всередині українського медіапростору. Внаслідок цього формується спотворене сприйняття реальності, у якому правду важко відрізнити від маніпуляції.

Російська пропаганда активно використовує чутливі соціальні теми, перетворюючи їх на інструменти тиску. Особливо активно експлуатується тема війни, яку агресор подає як «захисну операцію» або «боротьбу з нацизмом», а також тема енергетичної безпеки, де через інформаційні кампанії створюється враження, ніби Україна не здатна забезпечити власне енергопостачання без допомоги Росії. Подібна риторика спрямована на деморалізацію населення, підрив віри у спроможність держави впоратися з викликами [66, с.57].

Крім того, маніпулятивно подається інформація щодо питань біженців і соціальної нестабільності. У медіапросторі поширюються повідомлення, що українські переселенці створюють «проблеми» у країнах ЄС або що українське суспільство «втомилося від війни». Такі меседжі мають подвійний ефект: у міжнародній площині вони спрямовані на зменшення підтримки України з боку партнерів, а всередині країни – на провокування апатії, соціальної напруги та недовіри до уряду.

Варто зазначити, що інформаційні атаки часто супроводжуються кіберактивністю – спробами зламів офіційних сайтів, витоками даних, публікацією фейкових документів. Такі акції мають на меті створити враження беззахисності держави, підірвати довіру до її інституцій, а також сприяти поширенню панічних настроїв серед населення.

2.3. Стратегії, ініціативи та державні програми у сфері інформаційної безпеки

Державна політика у сфері інформаційної безпеки України є складовою частиною системи національної безпеки та спрямована на забезпечення захисту інформаційного простору держави, збереження інформаційного суверенітету й гарантування прав громадян на достовірну інформацію. В умовах гібридної війни та глобальної цифровізації саме інформаційна безпека набуває стратегічного значення, оскільки інформаційна сфера перетворилася на самостійний простір протистояння, де формуються суспільні настрої, політичні рішення і навіть результати воєнних дій.

Метою державної політики у цій сфері є створення стійкої системи захисту національних інтересів у інформаційному просторі, попередження деструктивних впливів, забезпечення стабільності суспільства та підвищення довіри до державних інституцій. Держава прагне сформувати безпечне, конкурентоспроможне і технологічно розвинене інформаційне середовище, у якому гарантовано права громадян на свободу слова, доступ до інформації та захист від дезінформації, кібератак і маніпуляцій [60, с.9].

Серед основних завдань державної політики інформаційної безпеки можна виокремити кілька взаємопов'язаних напрямів. По-перше, це формування ефективної системи моніторингу, виявлення та нейтралізації інформаційних загроз, включно з кіберзлочинністю, пропагандою, інформаційним шпигунством і маніпуляцією суспільною думкою. По-друге, розроблення й реалізація нормативно-правових та організаційних механізмів, що регулюють діяльність у цифровій та медіасферах, з урахуванням міжнародних стандартів і європейських практик. По-третє, створення умов для розвитку національної інфраструктури кіберзахисту, захисту державних інформаційних ресурсів та критичних об'єктів інфраструктури. Важливим завданням є також підвищення рівня медіаграмотності громадян і формування культури безпечного користування інформаційними технологіями.

Роль інформаційної безпеки в системі національної безпеки України визначається тим, що інформаційна сфера інтегрує всі інші складові – політичну, економічну, оборонну, гуманітарну. Порушення стабільності інформаційного середовища може призвести до глибоких кризових явищ у суспільстві, зниження рівня довіри до влади, дестабілізації політичної системи та навіть до втрати територіальної цілісності держави. Саме тому інформаційна безпека виступає не лише як окремий напрям державної політики, а як базовий елемент суверенітету, що забезпечує здатність держави самостійно визначати інформаційний порядок денний і протидіяти зовнішнім впливам. Важливим аспектом державної політики є також баланс між безпекою та демократичними принципами. Україна, орієнтуючись на європейські стандарти, прагне вибудовувати політику інформаційної безпеки не як засіб цензури, а як інструмент захисту прав і свобод громадян. Йдеться про необхідність створення відкритого, але захищеного інформаційного простору, у якому держава виступає гарантом не лише безпеки, а й прозорості, доступності й правдивості інформації [59, с.64].

Сьогодні політика України у сфері інформаційної безпеки має дві ключові тенденції. З одного боку – це реактивна функція, спрямована на протидію загрозам, зокрема з боку агресора, через інформаційні операції, кібератаки, дезінформаційні кампанії. З іншого боку – проактивна функція, яка полягає у формуванні національної інформаційної культури, розвитку цифрових компетентностей громадян, стимулюванні розвитку українського медіапростору, технологічних інновацій та безпечного цифрового контенту.

Нормативно-правова база у сфері інформаційної безпеки України формує правові засади захисту національних інтересів у інформаційному просторі, визначає принципи державної політики, повноваження суб'єктів забезпечення безпеки та механізми координації їхньої діяльності. Ця система документів є динамічною, оскільки реагує на нові виклики, пов'язані з гібридною агресією, розвитком цифрових технологій і трансформацією глобального інформаційного середовища.

Конституційні засади інформаційної безпеки визначають фундаментальні принципи, на яких ґрунтується державна політика в цій сфері. Конституція України гарантує кожному громадянину право на свободу думки й слова, на вільне вираження своїх поглядів та переконань (ст. 34), а також право на захист персональних даних і приватного життя (ст. 32). Водночас стаття 17 закріплює, що захист суверенітету, територіальної цілісності та інформаційного простору України є найважливішою функцією держави і справою всього народу. Тож, інформаційна безпека постає як складова загальної системи національної безпеки, а забезпечення безпечного інформаційного середовища – як конституційний обов’язок держави.

Ключовим законодавчим актом є Закон України «Про національну безпеку» (2018 р.), який визначає інформаційну безпеку як один із пріоритетних напрямів державної політики у сфері захисту національних інтересів. У ньому наголошується, що основними загрозами є поширення дезінформації, кібератаки, втручання у роботу інформаційних систем, маніпуляції суспільною свідомістю та порушення цілісності інформаційної інфраструктури. Закон закладає правові засади функціонування сектору безпеки і оборони, визначає роль Ради національної безпеки і оборони України (РНБО) як координаційного органу у сфері інформаційної політики, а також окреслює необхідність формування системи кіберзахисту критичної інфраструктури [55, с.188].

Важливу роль у сучасній архітектурі безпеки відіграють Стратегія національної безпеки України (2020 р.) та Стратегія інформаційної безпеки (2021 р.). У першому документі підкреслюється, що основою стійкості держави є «людина, суспільство і держава», які разом формують трикутник безпеки. Інформаційна безпека тут визначена як ключовий елемент протидії гібридним загрозам. Основні цілі стратегії полягають у забезпеченні спроможності держави реагувати на інформаційні впливи, зміцненні кіберзахисту, розвитку національного медіапростору та підвищенні рівня медіаграмотності населення.

Стратегія інформаційної безпеки України (2021 р.) конкретизує механізми реалізації цих цілей. Вона ґрунтується на принципах верховенства

права, прозорості, балансу між свободою слова та захистом державних інтересів. Серед ключових напрямів реалізації визначено:

- створення ефективної системи моніторингу інформаційного простору та оперативного реагування на загрози;
- розвиток національного контенту і підтримку незалежних ЗМІ;
- зміцнення кіберзахисту державних інформаційних ресурсів;
- формування стійкого до маніпуляцій суспільства через освіту і просвітницькі програми;
- удосконалення міжнародного співробітництва у сфері інформаційної безпеки [53, с.82].

Ця стратегія стала першим комплексним документом, який поєднав безпековий, комунікаційний і технологічний виміри інформаційної політики держави.

До важливих елементів нормативної бази належать також Концепція кібербезпеки України (затверджена Указом Президента № 96/2017), Доктрина інформаційної безпеки України (Указ Президента № 47/2017) та Національна стратегія розвитку інформаційного суспільства. Концепція кібербезпеки визначає засади створення національної системи кіберзахисту, розвиток державно-приватного партнерства у цій сфері, підготовку фахівців і впровадження інноваційних технологій для захисту критичної інфраструктури. Доктрина інформаційної безпеки встановлює основні напрями державної політики щодо протидії деструктивним інформаційним впливам, зокрема в умовах зовнішньої агресії. У свою чергу, Національна стратегія розвитку інформаційного суспільства визначає ціль – побудову «цифрової України», де інформаційна безпека виступає гарантією сталого розвитку, інноваційності та конкурентоспроможності держави.

Реалізація державної політики у сфері інформаційної безпеки в Україні здійснюється через складну багаторівневу інституційну систему, яка охоплює органи державної влади, правоохоронні та спеціальні служби, а також органи місцевого самоврядування. Така структура покликана забезпечити ефективну

координацію дій, оперативне реагування на загрози та інтеграцію інформаційної безпеки у загальну систему національної безпеки [46, с.13].

Координаційну роль у цій системі відіграє Рада національної безпеки і оборони України (РНБО), яка формує стратегічні напрями державної політики, визначає пріоритети захисту інформаційного простору та контролює виконання державних програм у сфері інформаційної безпеки. РНБО виступає центральним органом, що інтегрує діяльність всіх суб'єктів сектору безпеки та оборони, забезпечує міжвідомчу координацію та ухвалює рішення у надзвичайних ситуаціях, пов'язаних з інформаційними загрозами.

Одним із ключових виконавців політики у сфері інформаційної безпеки є Міністерство цифрової трансформації України, яке відповідає за розвиток національної цифрової інфраструктури, управління державними інформаційними ресурсами, впровадження електронних сервісів та забезпечення кіберзахисту. Міністерство координує дії з іншими державними органами у сфері захисту інформаційних систем та цифрових платформ, а також реалізує освітні програми з підвищення цифрової грамотності населення та медіаосвіти.

Служба безпеки України (СБУ) виконує роль головного спеціалізованого органу з протидії інформаційній агресії, кібершпигунству, терористичним та деструктивним інформаційним впливам. СБУ здійснює розвідувальні, контррозвідувальні та превентивні заходи, спрямовані на виявлення і нейтралізацію загроз на національному і регіональному рівнях. Особливе значення має контроль за забезпеченням захисту критичної інформаційної та телекомунікаційної інфраструктури, а також протидія внутрішнім і зовнішнім дезінформаційним кампаніям.

Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку) відповідає за організаційно-технічний захист інформаційних ресурсів держави, розробку та впровадження стандартів безпеки, адміністрування систем захисту інформації у державних органах. Держспецзв'язку забезпечує контроль за виконанням нормативних вимог до

кіберзахисту, технічного захисту персональних даних та конфіденційної інформації, а також координує роботу з приватним сектором у сфері кібербезпеки. Ефективність інституційної системи забезпечується через взаємодію центральних органів виконавчої влади та місцевих адміністрацій. Центральні органи формують стратегічні документи, визначають стандарти і правила, а місцеві адміністрації реалізують їх на територіальному рівні, здійснюють моніторинг загроз та координують локальні заходи безпеки. Взаємодія включає обмін інформацією про кібератаки, дезінформаційні кампанії та інші загрози, проведення навчань і тренінгів, організацію превентивних та оперативних заходів. Такий підхід дозволяє створити багаторівневу систему захисту, де центральна влада визначає загальні стандарти, а регіони забезпечують оперативну адаптацію до локальних викликів [47, с.76].

У контексті сучасних викликів гібридної війни та швидкої цифровізації українська держава реалізує низку цільових програм та ініціатив, спрямованих на зміцнення інформаційної безпеки. Вони охоплюють різні аспекти – від кіберзахисту критичної інфраструктури до протидії дезінформації та розвитку цифрової грамотності населення. Такі ініціативи мають стратегічне значення для забезпечення стійкості держави, підвищення довіри до інформаційного простору та формування суспільної стійкості до інформаційних впливів. Одним із пріоритетних напрямів є програми кіберзахисту критичної інфраструктури. Вони передбачають створення багаторівневої системи захисту державних інформаційних ресурсів, енергетичних, транспортних, фінансових та комунікаційних систем. Основні завдання таких програм – виявлення уразливостей, запобігання кібератакам, оперативне реагування на інциденти та підготовка фахівців у сфері кібербезпеки. Особлива увага приділяється державно-приватному партнерству, що дозволяє інтегрувати національні та міжнародні технології кіберзахисту, а також забезпечувати координацію між державними органами та приватними компаніями, відповідальними за критичні об'єкти. Не менш важливою є протидія дезінформації, що реалізується через

національні кампанії на кшталт «Фільтр» та «Медіаграмотність – щит проти фейків». Ці ініціативи спрямовані на підвищення обізнаності громадян щодо методів поширення фейкових новин, маніпулятивних наративів та інформаційних атак. Вони включають публікацію навчальних матеріалів, проведення просвітницьких кампаній у медіа та соціальних мережах, а також створення онлайн-платформ для перевірки фактів. Завдяки таким програмам держава не лише реагує на інформаційні загрози, а й формує у суспільстві критичне мислення та здатність самостійно оцінювати достовірність інформації [44, с.16].

Важливим критерієм оцінки ефективності державних стратегій і програм у сфері протидії дезінформації є не лише їх формальне впровадження, але й реальні зміни у рівні інформаційної стійкості населення. У цьому контексті доцільним є звернення до результатів соціологічних досліджень, які дозволяють простежити динаміку здатності громадян України розпізнавати фейкову інформацію та протистояти маніпулятивному впливу в умовах гібридної війни. Особливу цінність становлять емпіричні дані за останні два роки, адже саме цей період характеризується інтенсифікацією державних і громадських ініціатив у межах програм «Фільтр» та «Медіаграмотність – щит проти фейків».

Одним із найбільш авторитетних і системних досліджень у цій сфері є щорічний «Індекс медіаграмотності українців», який проводиться громадською організацією «Детектор медіа» за участю національних і міжнародних експертів. Результати хвиль 2023–2025 років засвідчують поступові, хоча й нерівномірні зміни у рівні стійкості громадян до дезінформації. Зокрема, у 2023 році близько 37 % опитаних зазначали, що при сумнівах у достовірності інформації вони звертають увагу на першоджерело або намагаються перевірити інформацію в альтернативних джерелах. У 2024 році цей показник зріс до приблизно 43 %, що свідчить про позитивну тенденцію формування навичок критичного аналізу медіаконтенту.

Водночас рівень впевненості громадян у власній здатності розпізнавати фейки залишається відносно низьким. За даними дослідження, лише близько 17–18 % респондентів у 2024–2025 роках вважають, що можуть завжди відрізнити неправдиву інформацію від достовірної. Це вказує на те, що, попри зростання усвідомлення проблеми дезінформації, значна частина населення все ще перебуває у зоні ризику інформаційного впливу, особливо в умовах емоційного тиску та кризових подій. Таким чином, зростання обізнаності не завжди автоматично трансформується у впевнені практичні навички, що є важливим викликом для державної політики у сфері інформаційної безпеки.

Разом з тим, зафіксовано зростання загальної чутливості суспільства до проблеми фейків і маніпуляцій. У 2024 році понад 60 % українців визнали дезінформацію серйозною загрозою для держави та суспільної стабільності, що корелює з активною інформаційною кампанією, яка проводиться в межах програми «Фільтр». Дана програма, координована Міністерством культури та інформаційної політики України, має на меті не лише інформування громадян про загрози дезінформації, але й формування у них відповідального ставлення до споживання інформації. Акцент на поясненні механізмів створення фейків, ролі емоційних тригерів та алгоритмів соціальних мереж сприяє підвищенню рівня рефлексії щодо отримуваного медіаконтенту.

Подібну функцію виконує і програма «Медіаграмотність – щит проти фейків», яка орієнтована на освітній компонент та довгострокове формування навичок критичного мислення. За результатами соціологічних опитувань, у 2025 році зросла частка громадян, які не лише пасивно споживають інформацію, а й намагаються аналізувати мотиви її поширення, перевіряти фото- та відеоконтент, а також звертатися до професійних фактчекінгових ресурсів. Це свідчить про поступовий перехід від інтуїтивного сприйняття інформації до більш раціональної моделі медіаспоживання.

Водночас соціологічні дані демонструють і наявність суттєвих обмежень. Близько 35–40 % респондентів у 2024–2025 роках визнавали, що практично не перевіряють інформацію, яку отримують із соціальних мереж або месенджерів.

Така ситуація особливо характерна для швидких інформаційних потоків, де домінує емоційний контент і де фактор часу часто переважає над раціональним аналізом. Це підкреслює необхідність подальшого розвитку державних програм медіаграмотності, зокрема через інтеграцію освітніх модулів у шкільну та університетську освіту, а також через спеціалізовані курси для дорослого населення.

Узагальнюючи наведені статистичні дані, можна зробити висновок, що за останні два роки в Україні спостерігається помірне, але стабільне зростання рівня інформаційної стійкості населення. Це зростання проявляється насамперед у підвищенні усвідомленості проблеми дезінформації та поширенні практик перевірки джерел. Водночас обмежена впевненість громадян у власних навичках розпізнавання фейків свідчить про те, що державні програми «Фільтр» і «Медіаграмотність – щит проти фейків» перебувають на етапі формування довготривалого ефекту і потребують подальшого системного розвитку. Таким чином, поєднання нормативно-правових, освітніх і просвітницьких заходів залишається ключовою умовою підвищення стійкості українського суспільства до дезінформаційних загроз у сучасному інформаційному середовищі.

Важливим елементом державної політики є освітні програми з розвитку цифрової грамотності населення. Вони передбачають навчання громадян основам безпечного користування інтернетом, захисту персональних даних, роботи з електронними сервісами та виявлення маніпулятивного контенту. Особлива увага приділяється школам, університетам та державним установам, де підвищення цифрової компетентності сприяє формуванню стійкості до інформаційних атак, зменшенню ризику кіберзлочинності та активному використанню цифрових технологій у повсякденному житті.

Ще одним стратегічним напрямом є підтримка незалежних ЗМІ та фактчекінгових платформ, що сприяє забезпеченню об'єктивного й прозорого інформаційного середовища. Держава стимулює розвиток медіа через гранти, освітні проєкти, технічну підтримку та участь у міжнародних програмах

співробітництва. Підтримка незалежних журналістів і фактчекінгових платформ дозволяє протидіяти дезінформаційним кампаніям, підвищувати довіру до офіційних джерел і формувати культуру відповідального споживання інформації серед громадян.

Така багаторівнева архітектура забезпечує комплексний захист інформаційного простору, оперативне реагування на загрози і інтеграцію всіх суб'єктів у систему національної безпеки.

РОЗДІЛ 3. Баланс між інформаційною безпекою та демократичними свободами

3.1. Свобода слова і державна політика протидії дезінформації

У сучасних умовах гібридної війни та стрімкої цифровізації особливого значення набуває проблема поєднання національної безпеки з демократичними правами громадян, зокрема свободою слова. Інформаційний простір стає не лише ареною для розвитку суспільства і реалізації громадянських прав, а й потенційною зоною загроз, де поширення дезінформації, пропаганди або маніпулятивних наративів може негативно впливати на політичну стабільність, соціальну згуртованість та безпеку держави. Саме тому виникає необхідність у формуванні концепції балансу, яка дозволяє одночасно захищати інтереси держави й зберігати фундаментальні права громадян.

Концепція балансу між національною безпекою та демократичними правами передбачає, що держава має забезпечувати захист суспільства від загроз, не вдаючись до надмірного обмеження свобод, що є невід'ємною

частиною демократичного устрою. Вона ґрунтується на принципах пропорційності, мінімізації втручання та дотримання прав людини, передбачених національним законодавством і міжнародними стандартами. З одного боку, держава здійснює превентивні заходи для протидії інформаційним загрозам, кіберзлочинності та деструктивним інформаційним кампаніям. З іншого боку, вона не повинна обмежувати доступ громадян до інформації, цензурувати медіа або створювати умови для надмірного контролю над громадською думкою [34, с. 40].

Баланс між безпекою та свободою слова стає особливо актуальним у країнах, що перебувають під загрозою гібридної агресії, де інформаційні атаки є частиною комплексної стратегії зовнішнього впливу. Недотримання цього балансу може призвести до політичної дестабілізації, втрати довіри до державних інституцій та порушення прав громадян. Водночас ефективний баланс дозволяє формувати стійке, критично мисляче суспільство, яке здатне самостійно протидіяти дезінформації та маніпуляціям, не обмежуючи при цьому основоположні демократичні свободи.

Тож національна безпека і свобода слова не є антагоністами, а мають розглядатися як взаємодоповнюючі складові сучасної державної політики. Забезпечення безпеки в інформаційному просторі повинно здійснюватися через прозорі, правомірні та пропорційні механізми, що гарантують громадянам право на свободу думки, вираження поглядів і доступ до достовірної інформації. Такий підхід формує основу для подальшого аналізу державної політики протидії дезінформації та механізмів, що дозволяють зберігати демократичні свободи в умовах сучасних інформаційних викликів.

Свобода слова є одним із базових принципів демократичного суспільства і виступає фундаментальною умовою реалізації громадянських прав та свобод. В Україні цей принцип закріплений у Конституції, яка визначає свободу думки та слова, право на вільне вираження поглядів і переконань як невід'ємні права кожного громадянина. Зокрема, стаття 34 Конституції України проголошує, що кожна особа має право вільно шукати, отримувати, передавати, виробляти та

поширювати інформацію будь-якими законними способами, а держава гарантує свободу преси, незалежність засобів масової інформації та заборону цензури. Ці конституційні гарантії створюють правову основу для забезпечення відкритого і прозорого інформаційного простору, де кожен громадянин може брати активну участь у суспільному житті та реалізовувати свої демократичні права [25, с. 58].

Свобода слова має ключове значення для формування відкритого суспільства. Вона дозволяє громадянам обмінюватися ідеями, критично оцінювати дії влади, впливати на прийняття рішень та контролювати діяльність державних інституцій. В умовах демократичного суспільства свобода слова стимулює розвиток публічної дискусії, сприяє політичній прозорості та підзвітності влади, а також забезпечує можливість протистояти монополії на інформацію. Відкритий інформаційний простір, у якому реалізується свобода слова, є запорукою розвитку громадянського суспільства, формування критичного мислення і підвищення рівня політичної культури населення [60, с. 8].

Одним із ключових критеріїв оцінки допустимості обмежень свободи слова в демократичному суспільстві є принцип пропорційності, який посідає центральне місце у практиці Європейського суду з прав людини. Згідно з усталеною юриспруденцією ЄСПЛ, будь-яке втручання держави у здійснення права на свободу вираження поглядів, гарантованого статтею 10 Конвенції про захист прав людини і основоположних свобод, має відповідати трьом основним умовам: бути «встановленим законом», переслідувати легітимну мету та бути «необхідним у демократичному суспільстві». Саме останній критерій передбачає перевірку пропорційності втручання, тобто співмірності між обраними засобами та задекларованою метою.

У контексті державної політики України у сфері протидії дезінформації питання пропорційності особливо гостро постає у зв'язку з рішеннями щодо блокування окремих вебресурсів, телеканалів та онлайн-платформ, які розглядаються владою як інструменти інформаційного впливу держави-

агресора. Прикладом таких заходів є рішення Ради національної безпеки і оборони України про застосування санкцій, що передбачали припинення мовлення низки телевізійних каналів та обмеження доступу до певних інтернет-ресурсів. Ці дії були обґрунтовані необхідністю захисту національної безпеки в умовах гібридної війни та системного поширення дезінформації.

З позиції практики ЄСПЛ, легітимна мета у вигляді захисту національної безпеки або територіальної цілісності держави визнається допустимою підставою для обмеження свободи слова. Зокрема, у рішенні у справі *Leander v. Sweden* Суд підкреслив, що держави мають певний «простір розсуду» у питаннях національної безпеки. Водночас цей простір не є необмеженим, а втручання повинно бути пропорційним і супроводжуватися достатніми процесуальними гарантіями.

Особливе значення для аналізу українських кейсів має рішення ЄСПЛ у справі *Ahmet Yildirim v. Turkey*, у якій Суд визнав порушення статті 10 Конвенції у зв'язку з блокуванням доступу до платформи Google Sites. Суд наголосив, що загальне та невибіркове блокування інтернет-ресурсу, яке унеможлиблює доступ до значного обсягу законного контенту, не відповідає вимогам пропорційності. У цьому контексті українська практика блокування інформаційних ресурсів потребує оцінки з точки зору того, чи є застосовані обмеження точковими, обґрунтованими та мінімально необхідними для досягнення заявленої мети.

Аналогічний підхід простежується і в рішенні *Cengiz and Others v. Turkey*, де ЄСПЛ підкреслив, що обмеження доступу до інформації в інтернеті мають враховувати суспільну цінність свободи вираження поглядів та право громадян отримувати інформацію. Суд зазначив, що навіть за наявності загрози громадському порядку або безпеці держава повинна обирати такі заходи, які найменше втручаються у свободу слова.

У застосуванні до українських реалій це означає, що рішення щодо блокування телеканалів або вебресурсів мають супроводжуватися чітким правовим обґрунтуванням, прозорими процедурами ухвалення та можливістю

судового перегляду. В іншому випадку існує ризик трансформації інструментів протидії дезінформації у механізми надмірного контролю над інформаційним простором, що може суперечити демократичним стандартам.

Водночас практика ЄСПЛ визнає, що в умовах збройного конфлікту або гібридної агресії держава може застосовувати більш жорсткі заходи захисту, за умови доведення їх необхідності та тимчасового характеру. Так, у низці справ Суд наголошував, що свобода слова не є абсолютною і може зазнавати обмежень, якщо діяльність медіа або інформаційних ресурсів сприяє підриву демократичного ладу чи поширенню ворожої пропаганди. Таким чином, ключовим завданням держави є забезпечення балансу між ефективною протидією інформаційним загрозам і дотриманням принципів правової держави.

Тож аналіз українських рішень щодо блокування інформаційних ресурсів крізь призму практики Європейського суду з прав людини дозволяє зробити висновок, що принцип пропорційності має стати визначальним орієнтиром державної інформаційної політики. Лише поєднання легітимної мети, чіткої правової процедури та мінімізації втручання у свободу слова здатне забезпечити ефективний захист інформаційної безпеки без порушення демократичних свобод, що є особливо важливим для України як держави, яка декларує європейський вектор розвитку.

Крім того, свобода слова є важливим механізмом зміцнення демократичних інститутів. Вона сприяє ефективній роботі незалежних медіа, дозволяє проводити журналістські розслідування, виявляти корупційні практики та інші порушення прав людини. У такий спосіб держава отримує ефективний контрольний механізм через громадську думку та відкриті джерела інформації, що запобігає концентрації влади і підвищує рівень підзвітності органів державного управління. Свобода слова також забезпечує платформу для реалізації політичних, культурних і соціальних ініціатив, підтримуючи плюралізм думок і політичну конкуренцію - основні ознаки демократичного розвитку.

Дезінформація є однією з ключових загроз сучасного інформаційного простору, що має здатність суттєво впливати на суспільну свідомість, політичну стабільність та національну безпеку. Дезінформація визначається як навмисне поширення недостовірної або спотвореної інформації з метою введення громадськості в оману, формування хибних уявлень, маніпулювання емоціями та прийняттям рішень. В умовах гібридної війни дезінформаційні кампанії стають інструментом зовнішнього впливу, що дозволяє агресору підривати довіру до державних інституцій, деморалізувати населення, створювати соціальну поляризацію та дискредитувати політичні процеси. Наслідки дезінформації можуть бути критичними: від масових протестів і панічних настроїв до ослаблення державного управління та підриву міжнародної підтримки [50, с. 42].

Державна політика протидії дезінформації в Україні реалізується через комплекс нормативно-правових, організаційних та інформаційних заходів. Серед основних інструментів можна виділити:

1. Нормативно-правова база, що закріплює механізми запобігання деструктивному інформаційному впливу. Вона включає Конституцію України, Закон України «Про національну безпеку», Стратегію національної безпеки (2020 р.), Стратегію інформаційної безпеки (2021 р.) та Доктрину інформаційної безпеки. Ці документи визначають поняття інформаційних загроз, закладають правові підстави для моніторингу, аналізу та нейтралізації дезінформаційних кампаній, а також встановлюють повноваження органів державної влади та координаційні механізми між ними [53, с. 72].

2. Національні стратегії та програми, спрямовані на підвищення інформаційної стійкості суспільства. Прикладами є програми «Фільтр» та «Медіаграмотність - щит проти фейків», які передбачають систематичне навчання населення розпізнаванню фейків, поширення методологій фактчекінгу та створення інформаційного середовища, стійкого до маніпуляцій. Такі ініціативи поєднують освітні, просвітницькі та технологічні заходи, що сприяють формуванню критичного мислення і підвищенню медіаграмотності.

3. Створення фактчекінгових платформ та незалежних медіа, які забезпечують оперативну перевірку інформації, виявлення фейків і спростування дезінформації. Держава підтримує розвиток таких платформ як національних, так і регіональних, а також співпрацює з міжнародними організаціями для інтеграції глобальних практик фактчекінгу. Цей інструмент дозволяє не лише протидіяти дезінформації, а й підвищувати рівень довіри громадян до достовірних джерел інформації.

Державна політика у сфері протидії дезінформації базується на комплексному підході, який поєднує превентивні заходи, технологічні інструменти та правове регулювання. Вона спрямована на зменшення шкоди від дезінформаційних атак без надмірного обмеження свободи слова та доступу громадян до інформації. Тож політика протидії дезінформації виконує дві взаємопов'язані функції: захисну, що забезпечує стійкість держави і суспільства до зовнішніх та внутрішніх загроз, та просвітницьку, що формує критичне мислення і медійну компетентність населення [56, с. 98].

Однією з ключових проблем у сфері інформаційної безпеки є збалансування заходів держави щодо протидії дезінформації з гарантуванням свободи слова. Надмірне втручання у інформаційний простір може перетворитися на цензуру, підривати демократичні засади та порушувати права громадян. Тому основою сучасної політики є застосування принципу пропорційності, який передбачає, що будь-які державні дії щодо обмеження інформації мають бути обґрунтованими, чітко визначеними, необхідними та мінімально обмежувальними для громадян. Пропорційність передбачає, що заходи реагування повинні точно відповідати рівню загрози: наприклад, обмеження доступу до джерел дезінформації повинно застосовуватися лише у випадках систематичних, навмисних та потенційно небезпечних інформаційних атак, а не до легальних висловлювань громадян або критики влади.

Важливою складовою системи балансу є роль незалежних медіа та громадських організацій. Вони виконують функцію моніторингу та контролю за діями держави, оцінюючи, чи відповідають заходи протидії дезінформації

принципам законності та прав людини. Незалежні журналісти, медіа-організації та правозахисні інститути здійснюють аудит інформаційної політики, публікують аналітичні матеріали, перевіряють факти та повідомляють про можливі зловживання владою. Така взаємодія забезпечує прозорість державних дій і створює механізми громадського контролю, що є критично важливими для збереження демократичних стандартів [59, с. 60].

Не менш ефективним механізмом є використання освіти та медіаграмотності як превентивного інструменту. Замість цензури та обмежень держава може інвестувати в підвищення критичного мислення громадян, навчання розпізнаванню маніпулятивного контенту, розвитку навичок перевірки фактів та оцінки джерел інформації. Освітні програми у школах, університетах та громадських центрах дозволяють формувати у населення стійкість до дезінформації, зменшують ризики паніки чи соціальної поляризації та водночас не порушують права громадян на доступ до законної інформації. Медіаграмотність стає запобіжним механізмом, який зменшує потребу у жорстких регуляторних заходах та забезпечує природний баланс між безпекою і свободою [68, с. 38].

Таким чином, забезпечення балансу між захистом від дезінформації та свободою слова стикається з низкою серйозних викликів, що пов'язані з особливостями сучасного інформаційного середовища та характером гібридної війни. Одним із головних ризиків є надмірне втручання держави в інформаційний простір, яке може проявлятися у формі цензури, обмеження доступу до певних джерел інформації або надмірного контролю за діяльністю медіа [20, с. 196]. Такі дії, навіть якщо вони мотивовані боротьбою з дезінформацією, здатні підривати довіру громадян до державних інституцій, обмежувати політичну конкуренцію та негативно впливати на розвиток демократичного суспільства. Ризик надмірного втручання особливо загострюється в умовах інформаційної війни, коли необхідність оперативного реагування на загрози стикається з правами громадян на свободу вираження поглядів. Ще одним важливим аспектом є необхідність гармонізації

українського законодавства з міжнародними стандартами щодо свободи слова та прав людини. Успішна політика протидії дезінформації потребує правової бази, яка враховує вимоги міжнародних угод, практику Європейського суду з прав людини та рекомендації міжнародних організацій щодо захисту інформаційних прав. Це дозволяє забезпечити прозорість і законність державних заходів, уникати конфліктів між національною безпекою та фундаментальними свободами, а також підтримувати позитивний імідж України на міжнародній арені.

Водночас існують значні перспективи розвитку ефективної системи протидії дезінформації без порушення демократичних свобод. До них належать інтеграція превентивних освітніх програм з медіаграмотності, розвиток незалежних фактчекінгових платформ, активне залучення громадських організацій до моніторингу інформаційного простору, а також використання сучасних технологій для виявлення та нейтралізації загроз. Подальший розвиток такої системи передбачає поєднання правового регулювання, технологічних інструментів та громадської участі, що дозволяє створити стійкий механізм протидії дезінформації, який не обмежує права громадян і зберігає відкритий та плюралістичний інформаційний простір. Отже, подолання викликів у сфері інформаційної безпеки та дотримання балансу між захистом від дезінформації і свободою слова є комплексним завданням, що потребує чіткого визначення меж державного втручання, правового забезпечення відповідності міжнародним стандартам та активного розвитку громадянського суспільства. Реалізація цих заходів дозволить сформувати ефективну, збалансовану систему інформаційної безпеки, здатну протистояти загрозам гібридної війни та водночас підтримувати демократичні принципи розвитку України.

3.2. Роль громадянського суспільства та незалежних медіа

Громадянське суспільство та незалежні медіа відіграють ключову роль у формуванні стійкої демократії та розвитку відкритого інформаційного

простору. Активне громадянське суспільство виступає як соціальний інститут, здатний контролювати діяльність держави, впливати на прийняття рішень, відстоювати права і свободи громадян та сприяти розвитку демократичних практик. Організації громадянського суспільства забезпечують платформу для участі громадян у суспільному житті, мобілізують ресурси для просвітницької діяльності, підтримують механізми перевірки фактів і моніторингу дій влади, що особливо важливо в умовах поширення дезінформації та гібридних загроз.

Незалежні медіа виступають важливим гарантом плюралізму думок і прозорості інформаційного простору. Вони забезпечують доступ громадян до різних точок зору, створюють умови для публічної дискусії, сприяють підзвітності державних інституцій та підвищенню політичної культури населення. Через журналістські розслідування, фактчекінг та аналітичні матеріали незалежні медіа здатні протидіяти маніпуляціям, викривати неправдиву інформацію та сприяти формуванню критично мислячого суспільства [21, с. 37]. Поєднання активного громадянського суспільства та незалежних медіа створює систему природного стримування і протидії, яка забезпечує не лише ефективну протидію дезінформації, а й підтримку демократичних свобод. Така взаємодія формує відкритий та прозорий інформаційний простір, здатний протистояти загрозам гібридної війни, зберігаючи при цьому фундаментальні принципи демократичного розвитку держави.

Громадянське суспільство виконує ключові функції у забезпеченні інформаційної безпеки, особливо в умовах сучасних гібридних загроз та широкого поширення дезінформації. Однією з основних функцій є моніторинг діяльності державних органів та контроль за дотриманням прав людини. Громадські організації та активісти здійснюють аудит рішень влади, перевіряють законність та прозорість її дій у сфері інформаційної політики, оцінюють дотримання конституційних прав громадян та міжнародних стандартів. Така діяльність дозволяє зменшити ризики зловживання владою,

забезпечує підзвітність державних інституцій та формує довіру населення до системи управління [64].

Ще однією важливою функцією є просвітницька діяльність та розвиток медіаграмотності населення. Громадянські організації проводять навчальні програми, тренінги, вебінари та інформаційні кампанії, спрямовані на підвищення критичного мислення, навчання розпізнаванню фейків та маніпуляцій у медіа. Такі ініціативи дозволяють формувати стійкість громадян до дезінформації, зменшувати панічні настрої та соціальну поляризацію, а також сприяють розвитку активної громадянської позиції, яка є фундаментальною для демократичного суспільства.

Крім того, громадянське суспільство бере активну участь у перевірці фактів, розкритті фейків та протидії дезінформаційним кампаніям. Фактчекінгові ініціативи та незалежні аналітичні платформи дозволяють виявляти неправдиву інформацію, оперативно спростовувати маніпулятивні наративи та забезпечувати достовірний доступ до інформації для широкого кола громадян. Це особливо важливо під час гібридних атак, коли дезінформація використовується як засіб психологічного тиску, дискредитації держави або впливу на міжнародну спільноту [56, с. 458].

Незалежні медіа відіграють ключову роль у формуванні достовірного та прозорого інформаційного середовища, яке є фундаментом демократичного суспільства та важливим елементом інформаційної безпеки. Вони забезпечують громадян доступом до різноманітних джерел інформації, сприяють плюралізму думок і створюють умови для відкритої публічної дискусії. Завдяки незалежності від державного контролю та комерційних впливів, такі медіа здатні подавати об'єктивну інформацію, оцінювати її достовірність і забезпечувати баланс між різними точками зору, що знижує ризик маніпуляцій та формування односторонніх наративів.

Однією з ключових функцій незалежних медіа є проведення журналістських розслідувань та контроль за діяльністю влади і бізнесу. Через розслідувальну журналістику медіа виявляють корупційні практики,

порушення прав людини та інші зловживання, які можуть негативно впливати на соціальну і політичну стабільність. Такі розслідування не лише інформують громадян, а й підвищують рівень підзвітності державних і приватних структур, створюючи ефективний механізм контролю та стримування потенційних порушень [47, с. 92].

Крім того, незалежні медіа відіграють критичну роль у протидії маніпуляціям та дезінформації. Вони використовують методи фактчекінгу, публікують аналітичні матеріали та роз'яснення щодо поширених фейків, що дозволяє громадянам відокремлювати достовірну інформацію від маніпулятивної. Це особливо важливо в умовах гібридних інформаційних атак, коли дезінформація може мати стратегічний характер і загрожувати національній безпеці, деморалізувати населення або підривати довіру до державних інституцій.

Ефективне функціонування системи інформаційної безпеки неможливе без транспарентної та взаємодіючої моделі між державою, громадянським суспільством і незалежними медіа. Одним із важливих механізмів такої взаємодії є партнерство у реалізації освітніх і просвітницьких програм. Спільні ініціативи державних органів, громадських організацій і медіа спрямовані на розвиток медіаграмотності, навчання критичному мисленню та підвищення здатності населення розпізнавати дезінформацію. Таке партнерство дозволяє поєднувати державні ресурси та експертний потенціал громадянського суспільства, забезпечуючи широку охоплюваність освітніх заходів і їх практичну ефективність [43, с. 202].

Другим важливим механізмом є спільний моніторинг інформаційних загроз та оцінка ефективності державних заходів. Громадські організації та медіа здійснюють незалежну перевірку дій влади у сфері інформаційної безпеки, аналізують інформаційні кампанії, оцінюють вплив законодавчих та організаційних рішень на суспільство. Такий контроль забезпечує оперативне виявлення проблем у політиці протидії дезінформації, своєчасне внесення

коректив та підтримує баланс між національною безпекою і правами громадян [40, с. 82].

Важливою складовою є також забезпечення прозорості і відкритості державних рішень без порушення свободи слова. Взаємодія з громадянським суспільством і незалежними медіа дозволяє державі демонструвати легітимність своїх дій, своєчасно інформувати суспільство про загрози, проводити консультації та відкриті обговорення ключових рішень. Це створює атмосферу довіри та взаємної відповідальності, зменшує ризик соціальної напруги та забезпечує демократичну легітимність заходів у сфері інформаційної безпеки.

Тож роль громадянського суспільства та незалежних медіа у забезпеченні інформаційної безпеки стикається з низкою значних викликів, які потребують системного і стратегічного підходу. Одним із основних ризиків є поява елементів цензури та тиску на незалежні медіа. Спроби обмежити діяльність журналістів, впливати на редакційну політику або блокувати доступ до інформаційних ресурсів можуть не лише підривати плюралізм думок, а й створювати небезпечні прецеденти для демократії та свободи слова. Такий тиск особливо загрозливий у періоди політичної або інформаційної кризи, коли незалежні медіа є критично важливим механізмом перевірки фактів і протидії дезінформації [38, с. 105].

Не менш важливим є забезпечення фінансової та правової незалежності ЗМІ. Для збереження об'єктивності та здатності виконувати контрольну функцію медіа потребують стабільних джерел фінансування, захисту від політичного та корпоративного тиску, а також правових гарантій, що обмежують втручання у редакційну діяльність. Державна підтримка у формі грантів, розвиток незалежних платформ та сприяння міжнародним партнерствам можуть стати ефективними інструментами підтримки незалежності медіа. Перспективи розвитку системи громадянського суспільства у сфері інформаційної безпеки пов'язані зі зміцненням ролі активних громадських організацій і незалежних медіа у протидії дезінформації

та формуванні критично мислячого населення. Інвестиції у медіаграмотність, розвиток освітніх програм та створення платформ для громадського моніторингу дозволяють формувати суспільство, здатне самостійно оцінювати достовірність інформації та протидіяти маніпуляціям. Збільшення участі громадськості у контролі за державними рішеннями підвищує прозорість влади і зміцнює демократичні інститути, одночасно підтримуючи ефективну інформаційну безпеку [60, с. 9].

Отже, виклики у сфері інформаційної безпеки пов'язані з ризиками цензури та фінансової залежності медіа, а перспективи полягають у розвитку громадянського суспільства та незалежних медіа як ключових чинників протидії дезінформації. Такий підхід дозволяє одночасно підтримувати демократичні свободи та забезпечувати стійкість держави до інформаційних загроз.

3.3. Перспективи розвитку державної інформаційної політики в Україні

Інформаційна політика є однією з ключових складових національної безпеки держави, оскільки сучасні загрози часто мають не тільки фізичний, але й інформаційний характер. У контексті гібридних конфліктів, кіберзагроз і поширення дезінформації стратегічно розроблена державна політика в інформаційній сфері дозволяє своєчасно реагувати на загрози, захищати національний інформаційний простір та підтримувати стійкість суспільства. Вона визначає пріоритети у сфері кібербезпеки, протидії дезінформації, розвитку медіаграмотності населення та забезпеченні прозорості діяльності державних органів.

Ефективна державна інформаційна політика впливає на формування стійкого та прозорого інформаційного середовища, яке забезпечує громадянам доступ до достовірної інформації, підтримує плюралізм думок і сприяє відкритим публічним дискусіям. Вона створює умови для балансування між захистом національних інтересів і дотриманням демократичних прав, зменшуючи ризики маніпуляцій, соціальної дезорієнтації та політичної

нестабільності. Тож стратегічний розвиток інформаційної політики є критично важливим для забезпечення не лише національної безпеки, а й формування громадянського суспільства, здатного критично оцінювати інформаційні потоки, що, у свою чергу, зміцнює демократичні інститути та стійкість держави перед сучасними інформаційними викликами [67, с. 41].

Одним із ключових напрямів розвитку державної інформаційної політики є підвищення рівня кібербезпеки державних і критичних інфраструктур. Сучасні загрози все частіше мають цифрову природу, включаючи кібератаки на урядові системи, енергетичні та фінансові мережі, комунікаційні платформи та об'єкти критичної інфраструктури. Високий рівень кіберзахисту дозволяє забезпечити безперервність роботи державних органів, зберегти цілісність даних та протидіяти спробам зовнішнього втручання, що є критично важливим у періоди гібридних конфліктів.

Другим важливим напрямом є розвиток систем протидії дезінформації та фейковим новинам. Державна політика передбачає створення правових, організаційних та технологічних механізмів, які дозволяють виявляти, аналізувати та нейтралізувати інформаційні загрози. Сюди входить підтримка фактчекінгових платформ, розвиток національних кампаній з медіаграмотності, а також співпраця з громадянським суспільством та незалежними медіа для забезпечення достовірної інформації та формування критично мислячого населення [71, с. 98].

Третім важливим аспектом є інтеграція міжнародних стандартів щодо свободи слова та захисту прав людини у національне законодавство та практику реалізації інформаційної політики. Дотримання цих стандартів дозволяє забезпечити баланс між необхідністю протидії дезінформації та захистом демократичних свобод громадян. Використання міжнародного досвіду і рекомендацій Європейського Союзу, Організації Об'єднаних Націй та інших міжнародних структур сприяє підвищенню прозорості, законності та легітимності державних заходів у сфері інформаційної безпеки [45, с. 201].

Сучасна державна інформаційна політика в Україні передбачає впровадження інноваційних механізмів та технологічних інструментів, що дозволяють ефективно реагувати на складні та швидкозмінні загрози інформаційної безпеки. Одним із ключових напрямів є використання сучасних цифрових платформ для виявлення загроз та моніторингу інформаційного середовища. Ці платформи дозволяють аналізувати потоки даних у реальному часі, виявляти фейкові новини, кібератаки, дезінформаційні кампанії та інші ризики, що впливають на національну безпеку. Автоматизовані системи збору та обробки інформації забезпечують оперативність реагування та зменшують можливість поширення паніки чи маніпуляцій у суспільстві.

Другим важливим напрямом є підтримка освітніх ініціатив у сфері медіаграмотності та цифрової безпеки. Це включає впровадження навчальних програм, тренінгів, онлайн-курсів та інформаційних кампаній, спрямованих на підвищення здатності громадян критично оцінювати інформаційні потоки та розпізнавати маніпуляції. Освітні заходи сприяють формуванню стійкого та свідомого населення, здатного протидіяти дезінформаційним загрозам та забезпечувати безпеку власних даних у цифровому середовищі [46, с. 10].

Третім напрямом є розвиток партнерства з міжнародними організаціями та приватним сектором. Співпраця з такими структурами дозволяє впроваджувати передові технології, обмінюватися досвідом та кращими практиками у сфері кібербезпеки та протидії дезінформації. Залучення приватних ІТ-компаній та міжнародних експертів підвищує ефективність моніторингу та реагування на інформаційні загрози, а також сприяє інтеграції української системи інформаційної безпеки у глобальний цифровий простір.

Ефективна державна інформаційна політика неможлива без транспарентної взаємодії з громадянським суспільством та незалежними медіа, які виступають важливими партнерами у формуванні безпечного та відкритого інформаційного середовища. Однією з основних форм такої взаємодії є спільна реалізація освітніх і просвітницьких програм. Державні органи у партнерстві з громадськими організаціями та незалежними медіа розробляють навчальні

курси, тренінги, інформаційні кампанії та освітні ресурси для підвищення медіаграмотності населення та формування критичного мислення. Це дозволяє громадянам ефективно відокремлювати достовірну інформацію від маніпулятивної та сприяє стійкості суспільства до інформаційних атак [49, с. 74].

Іншим важливим аспектом є моніторинг і оцінка ефективності державних заходів у сфері інформаційної безпеки. Громадські організації та незалежні медіа виконують функцію зовнішнього контролю, аналізуючи заходи держави щодо протидії дезінформації, кіберзагрозам та маніпуляціям у медіа. Такий моніторинг дозволяє своєчасно виявляти недоліки, оцінювати ефективність програм і забезпечувати підзвітність органів влади перед суспільством. Не менш важливою складовою є забезпечення прозорості державних рішень при збереженні демократичних свобод. Взаємодія з громадянським суспільством і медіа сприяє відкритості процесів ухвалення рішень, підвищенню довіри населення та формуванню легітимності заходів у сфері інформаційної безпеки. Такий підхід дозволяє підтримувати баланс між необхідністю захисту національних інтересів і дотриманням прав людини, запобігаючи ризикам надмірного контролю чи цензури [51, с. 116].

Розвиток державної інформаційної політики в Україні супроводжується низкою важливих викликів, які потребують уважного і збалансованого підходу. Одним із основних ризиків є надмірний централізований контроль та можливе обмеження свободи слова. Надмірна концентрація повноважень у сфері інформаційної безпеки може призвести до цензури, обмеження доступу до різноманітних джерел інформації та підриву демократичних свобод, що в свою чергу знижує довіру населення до державних інститутів і послаблює ефективність заходів протидії дезінформації.

Не менш важливим є забезпечення стабільного фінансування і правової підтримки ініціатив у сфері інформаційної політики. Для розвитку незалежних платформ, фактчекінгових ресурсів, освітніх програм і цифрових технологій державі необхідно створювати умови для фінансової підтримки та правової

гарантії діяльності медіа й громадських організацій. Це дозволяє зміцнити незалежність та ефективність партнерських структур, що беруть участь у формуванні інформаційного середовища [39, с. 106].

Серед перспектив розвитку виділяється формування комплексної, збалансованої та ефективної державної інформаційної політики, здатної протидіяти сучасним загрозам та забезпечувати стійкий розвиток демократичних інститутів. Інтеграція сучасних технологій, міжнародних стандартів, систем моніторингу та партнерства з громадянським суспільством дозволяє створити адаптивну систему, яка одночасно захищає національні інтереси, протидіє дезінформації та зберігає фундаментальні права громадян.

Отже, виклики та перспективи державної інформаційної політики зумовлюють необхідність поєднання безпеки і демократичних свобод, стабільності та інноваційності, що формує основу для ефективної та легітимної системи інформаційного захисту у сучасних умовах.

ВИСНОВКИ

Проведене дослідження дозволило комплексно розглянути проблему інформаційної безпеки як ключового аспекту національної безпеки держави в сучасних умовах політичних, технологічних та соціальних викликів. Теоретико-методологічний аналіз першого розділу показав, що інформаційна безпека є багаторівневим і багатофункціональним явищем, яке охоплює правові, політичні та організаційні аспекти функціонування держави. Було визначено сутність поняття «інформаційна безпека» у політико-правовому контексті, підкреслено її значення як складової політичної функції держави та механізм забезпечення стабільності суспільства в умовах інформаційних ризиків. Дослідження міжнародного досвіду країн НАТО та ЄС, таких як Естонія, Литва, Польща та Німеччина, показало ефективність комплексного підходу до кіберзахисту, протидії дезінформації та підвищення медіаграмотності населення. Використання передових практик цих держав може стати орієнтиром для розвитку української системи інформаційної безпеки та адаптації міжнародних стандартів до національних умов.

Другий розділ роботи підтвердив, що політика України у сфері інформаційної безпеки базується на комплексній інституційній системі, яка забезпечує координацію між центральними органами влади, правоохоронними структурами, органами місцевого самоврядування та приватними суб'єктами.

Розгляд інституційної системи засвідчив ключову роль РНБО, Міністерства цифрової трансформації, Служби безпеки України, Держспецзв'язку та інших структур у забезпеченні захисту інформаційного простору та критичної інфраструктури. Аналіз загроз інформаційній безпеці в умовах гібридної війни показав різноманітність ризиків, включаючи кіберзагрози, дезінформаційні кампанії, психологічний вплив на населення, маніпуляції громадською думкою через соціальні мережі та витік конфіденційної інформації. Важливо зазначити, що ефективна протидія цим загрозам потребує не лише державних заходів, а й активної участі суспільства та приватного сектору, що вимагає розвитку партнерських ініціатив і впровадження сучасних технологічних інструментів для моніторингу та реагування на інформаційні ризики.

Розгляд стратегій, ініціатив і державних програм у сфері інформаційної безпеки дозволив зробити висновок, що Україна поступово формує системний підхід до протидії інформаційним загрозам, який поєднує правові, освітні, технологічні та організаційні механізми. До ключових елементів таких заходів належать програми кіберзахисту критичної інфраструктури, національні кампанії протидії дезінформації («Фільтр», «Медіаграмотність – щит проти фейків»), підтримка незалежних медіа та фактчекінгових платформ, а також розвиток цифрової та медіаграмотності населення. Такий комплексний підхід дозволяє не лише протидіяти зовнішнім загрозам, а й зміцнювати стійкість суспільства до інформаційного тиску та маніпуляцій.

Третій розділ підкреслив, що баланс між інформаційною безпекою та демократичними свободами є ключовим фактором ефективності політики у цій сфері. Було детально проаналізовано значення свободи слова як фундаментального демократичного принципу та її роль у формуванні відкритого і прозорого інформаційного середовища. Досліджено державну політику протидії дезінформації, яка включає нормативно-правові механізми, національні стратегії та створення фактчекінгових платформ, водночас забезпечуючи дотримання принципу пропорційності та недопущення цензури. Висвітлено роль громадянського суспільства та незалежних медіа у контролі за

діяльністю держави, проведенні журналістських розслідувань, моніторингу загроз та формуванні критично мислячого населення. Також проаналізовано перспективи розвитку державної інформаційної політики, що включають інтеграцію сучасних цифрових технологій, міжнародних стандартів та партнерства з приватним сектором і міжнародними організаціями.

В цілому, дослідження демонструє, що ефективна інформаційна політика України має ґрунтуватися на комплексному, багаторівневому підході, який поєднує правові, організаційні, технологічні та освітні механізми. Забезпечення кібербезпеки, протидія дезінформації, розвиток медіаграмотності населення, підтримка незалежних медіа та громадянського суспільства створюють умови для стійкого та прозорого інформаційного простору. Водночас інтеграція міжнародних стандартів і практик дозволяє гарантувати дотримання демократичних свобод і прав людини, підтримуючи баланс між національною безпекою та свободою слова.

Отже, перспективи розвитку державної інформаційної політики в Україні полягають у формуванні комплексної, адаптивної та збалансованої системи, здатної ефективно протидіяти сучасним інформаційним загрозам, захищати національні інтереси та зміцнювати демократичні інститути. Використання досвіду міжнародних партнерів, активна участь громадянського суспільства та незалежних медіа, а також постійне вдосконалення технологічних та освітніх механізмів дозволяють створити стійку і легітимну систему інформаційної безпеки, яка відповідає сучасним викликам та забезпечує розвиток України як демократичної, інформаційно безпечної держави.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Конституція України: прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 р. Київ: Преса України, 1997. 80 с.
2. Закон України «Про інформацію». *Відомості Верховної Ради України*. 1992. № 48. Ст. 651; Із змінами від 06.04.2000, ВВР. 2000. № 27. Ст.213; від 07.02.2002, ВВР. 2002. № 29. Ст. 194; від 03.04.2003, ВВР. 2003. № 28.
3. Закон України «Про державну таємницю» від 21 січня 1994 р. *Відомості Верховної Ради України*. 1994. № 16.
4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 02.08.1994. *Відомості ВРУ*. 1994. № 31.
5. Закон України «Про національну програму інформатизації» від 17.07.1998. *Відомості Верховної Ради України*. 1998. № 27.
6. Закон України від 13.01.2011 № 2939-VI «Про доступ до публічної інформації». URL: <http://zakon4.rada.gov.ua/laws/show/2939-17>
7. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 9 січня 2007 року № 537–V. *Відомості Верховної Ради України*. 2007. № 12
8. Закон України «Про захист персональних даних» від 01.06.2010 р. № 2297-VI. *Відомості ВРУ*. 2010 р. № 34.

9. Закон України «Про основні засади забезпечення кібербезпеки України». *Відомості ВРУ*. 2017 р. № 45.
10. Закон України «Про національну безпеку України». *Відомості Верховної Ради України*. 2018. № 31.
11. IX Всеукраїнська науково-практична конференція «Захист прав і свобод громадян у світлі вимог Конституції України» : зб. матеріалів, 27 берез. 2024 р. / уклад.: В. В. Давиденко, А. М. Безносюк, В. В. Давиденко, А. М. Безносюк, В. А. Пригоцький, О. М. Олійник, О. І. Мисак, В. Р. Мохнатюк; Відкритий міжнародний університет розвитку людини «Україна». Вінниця : ТВОРИ, 2024. 163, [1] с.
12. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти/ За загальною редакцією д-ра юрид. наук, проф. Бандурки О.М...: Монографія. Харків: Вид-во Ун-ту внутр. Справ, 2000. 368 с.
13. Березовська І. Р. Місце та роль органів державної влади у забезпеченні інформаційної безпеки України. *Вісник Запорізького національного університету*. Юридичні науки. 2013. № 2(1). С. 115-119. URL: [http://nbuv.gov.ua/UJRN/Vznu_Jur_2013_2\(1\)_21](http://nbuv.gov.ua/UJRN/Vznu_Jur_2013_2(1)_21)
14. Бондаренко, Р. В., & Михальчук, В. М. Інформаційна безпека держави. *Інвестиції: практика та досвід*, 2021. №5, с.95-101.
15. Бугар А. Деякі аспекти формування іміджу країни в інформаційному просторі. *European political and law discoourse*. 2020. Вип. 7. С. 240–249.
16. Валюшко І. О. Інформаційна безпека України в контексті російсько-українського конфлікту : автореф. дис. ... канд. політ. наук : 23.00.04. Миколаїв, 2018. 39с.
17. Веденєєв Д.В., Семенюк О.Г. Розвиток концептуальних поглядів на особливості «гібридних» війн в євроатлантичному воєнно-політичному просторі. *Юридичний науковий електронний журнал*. 2022. №8. 25-29.
18. Вовк В. М., Олійник У. М. Право бути забутим як «нове право» людини у діджиталізованому суспільстві. *Науково-інформаційний вісник Івано-*

- Франківського університету права імені Короля Данила Галицького.* 2020. № 10 (22). С. 16–22. (Серія «Право»).
19. Вовк В. М., Олійник У. М. Право на доступ до Інтернету як елемент інформаційної безпеки особи та держави. *Інформаційне право.* 2022. № 1. С. 112–120.
 20. Глобенко, С. Інформаційний простір держави та проблеми забезпечення його захисту в Україні. *Науковий вісник: Державне управління*, 2023. № 1 (13)), с.195-210.
 21. Головка А. А. Громадянське суспільство як суб'єкт протидії загрозам національній безпеці в інформаційній сфері : автореф. дис. ...канд. політ. наук : 21.01.01. Київ, 2019
 22. Гришук, Р. В., & Молодецька-Гринчук, К. В. Постановка проблеми забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах. *Сучасний захист інформації*, 2017. №3, с.86-96.
 23. Гуцалюк О. М. Роль інформаційно-аналітичних ресурсів у фінансовому забезпеченні технологій управління економічною безпекою банківських установ. *Держава та регіони. Сер. Економіка та підприємництво.* 2015. Вип. 2. С. 9-12.
 24. Дзюба В. О. Правові засади забезпечення інформаційної безпеки в Україні. *Вісник Національної академії правових наук України.* 2020. № 3. С. 56–64.
 25. Жарков Я.М., Дзюба М.Т., Замаруєва І.В., ін. Інформаційна безпека особистості, суспільства, держави: Підручник. Київ: Видавничо-поліграфічний центр «Київський університет», 2008. 274 с.
 26. Забезпечення інформаційної безпеки держави: Навчальний посібник / В. Б. Дудикевич, І. Р. Опірський, П. І. Гаранюк, В. С. Зачепило, А. І. Партика. Львів : Видавництво Львівської політехніки, 2017. 204 с.
 27. Задувайло О. К. Розкриття інформації з обмеженим доступом як загроза внутрішньополітичній безпеці держави : автореф. дис. ... канд. політ. наук : 21.01.01. Київ, 2018. 28с.

- 28.Захаренко, К. К. Міжнародний досвід інформаційної безпеки. *Сучасне суспільство*, 2019. №1, с.95-109.
- 29.Іванченко Є.В., Іванченко І.С., Хорошко В.О., Хохлачова Ю.Є.Забезпечення інформаційної безпеки держави Є.В. Іванченко [та ін.] ; за ред. проф. В.О. Хорошка ; Вид-во Нац. авіац. ун-ту, 2016. 254 с.
- 30.Інформаційна безпека України в умовах євроінтеграції: конспект лекцій.
URL: http://pidruchniki.com/1584072028356/politologiya/informatsiyna_bezpeka_ukrayini_v_umovah_yevrointegratsiyi
- 31.Карпенко В. Інформаційна політика та безпека: підручник. – Київ, 2006.
URL: <http://ukrlife.org/main/karp/bezpeka15.htm>
- 32.Климчук О. О., Мельник Д. С., Панченко В. М., Петрик В. М. Забезпечення інформаційної безпеки у провідних країнах світу : навч. посіб. За заг. ред. В. М. Петрика. Київ. : Вид-во ІСЗЗІ НТУУ «КПІ», 2014. 260 с.
- 33.Климчук О. О., Петрик В. М., Присяжнюк М. М. Забезпечення інформаційної безпеки держави : підручник. Київ: ДНУ «Книжкова палата України», 2015. 672 с.
- 34.Ключко, А. Забезпечення інформаційної безпеки в умовах сучасного суспільства. Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління, 2022. №3 (63)), с.38-42.
- 35.Ковальчук В. В. Інформаційна безпека держави в умовах гібридної війни: політико-правовий аспект. *Державне управління: теорія та практика*. 2021. № 2. С. 45–53.
- 36.Ковальчук В. В. Роль держави у забезпеченні інформаційної безпеки в умовах гібридної війни. *Правові засади організації та здійснення публічної влади:збірник тез VI Міжнародної науково-практичної конференції, присвяченої 85-річчю від дня народження доктора юридичних наук, професора, академіка-засновника НАПрНУ, першого*

- Голови Конституційного Суду України Леоніда Петровича Юзькова (м. Хмельницький, 31 березня 2023 року). Хмельницький : Хмельницький університет управління та права імені Леоніда Юзькова, 2023. с.221-223
37. Кононенко, В. П., Здоровко, С. С., & Корольова, А. Є. Інформаційна безпека як стан. *Науковий вісник Ужгородського національного університету*. Серія: Право, 2023. №2(76), с. 244-250.
 38. Косілова О. П. Регулювання інформаційної безпеки в контексті цифрової трансформації держави. *Наукові праці Національної академії державного управління при Президентові України*. 2021. № 1. С. 101–110.
 39. Костецький П. В. Цифровізація суспільства та освіти у забезпеченні соціально-економічних трансформацій : автореферат дис. ... д.філософ : 051 / П. В. Костецький ; Сумський державний університет. 2024 укр.
 40. Крилова Ю. І. Нормативно-правові механізми протидії дезінформації в Україні. *Юридичний вісник*. 2023. № 4. С. 77–84.
 41. Кузіна І. І. Роль інституту освіти в забезпеченні інформаційної безпеки держави (з позицій неінституціонального підходу). *Вісник Харківського національного університету імені В. Н. Каразіна*. Серія : Соціологічні дослідження сучасного суспільства: методологія, теорія, методи. 2017. Вип. 38. С. 31-34. URL: http://nbuv.gov.ua/UJRN/VKhISD_2017_38_7
 42. Кунєв, Ю. Д. Я. Правове забезпечення інформаційної безпеки як предмет правового дослідження. *Scientific works of Kyiv Aviation Institute. Series Law Journal" Air and Space Law"*, 2021. №1(58), с.95-102.
 43. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. Київ: КНТ, 2006. 311с.
 44. Лісовська Ю. П. Адміністративно-правове забезпечення інформаційної безпеки в Україні : автореф. дис. ... канд. юрид. наук : 12.00.07. Київ, 2017. 34с.
 45. Магда Є.В. Гібридна війна : вижити і перемогти. Харків : Віват, 2015. 304 с.

46. Мельничук, В. В., Горохова, Л. В. Критичне мислення як складова інформаційної безпеки. Вісник Львівського університету. Серія філософські науки, 2022. №29, с.7-13.
47. Мужанова Т.М. Інформаційна безпека держави: Навчальний посібник. Київ: Київський університет комунікацій, 2019. 131с.
48. Національний інформаційний простір України: проблеми формування та державного регулювання: Аналітична доповідь НІСД України. URL: www.niss.gov.ua/public/File/2013_table/1119_dop.pdf
49. Національний інформаційний суверенітет у контексті розвитку новітніх інформаційних технологій / О. С. Онищенко, В. М. Горовий, В. І. Попик та ін. Київ: НБУВ, 2011. 154 с.
50. Неустроев, Ю. Г. Роль інформаційних технологій у забезпеченні економічної безпеки країни. *Інвестиції: практика та досвід*, 2021. №8, с.40-44.
51. Новицький, В. Я. Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах. Інформація і право, 2022. №1 (40)), с.111-118.
52. Олійник О. В., Соснін О. В., Шиманський Л. Є. Політико-правові аспекти формування інформаційного суспільства суверенної і незалежної держави. URL: http://old.niss.gov.ua/book/Sosnin_2.htm
53. Остроухов В.В., Присяжнюк М.М., Петрик В.М. та ін. Інформаційна безпека (соціально-правові аспекти): підручник. За ред. Є.Д.Скулиша. Київ: КНЕУ, 2010. 776 с.
54. Пархоменко-Куцевіл О. Проблеми забезпечення національної безпеки в умовах воєнного часу. *Науковий вісник Вінницької академії безперервної освіти*. Серія «Екологія. Публічне управління та адміністрування», 2023. №3, с.143-150.
55. Пересада О. В. Роль Національної поліції України в забезпеченні інформаційної безпеки держави: теоретико-методологічні аспекти. *Правовий часопис Донбасу*. 2019. № 4. С. 183-189. URL: http://nbuv.gov.ua/UJRN/pppd_2019_4_28

- 56.Петрик В.М., Присяжнюк М.М., Мельник Д.С. та ін. Забезпечення інформаційної безпеки держави: підручник ; за заг. ред. О.А. Семченка та В.М. Петрика. Київ: ДНУ «Книжкова палата України», 2015. 672 с.
- 57.Пєвцов Г.В., Залкін С.В., Сідченко С.О., Хударковський К.І. Інформаційна безпека у воєнній сфері: проблеми, методологія, система забезпечення: монографія. Харків : *Цифрова друкарня № 1*, 2013. 270 с.
- 58.Про Рекомендації парламентських слухань на тему: «Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України»: Постанова Верховної Ради України від 31.03.2016 № 1073-VIII. URL: <http://zakon3.rada.gov.ua/laws/show/1073-19>
- 59.Редзюк, В., Редзюк, Н. Сучасні проблеми інформаційної безпеки України та напрями їх вирішення. *Публічне управління: концепції, парадигма, розвиток, удосконаленню*. 2023. №3, с.59-65.
- 60.Самофалова О. Ю. Регулювання засобів масової комунікації у структурі державної правозахисної політики в Україні. *Вісн. Нац. акад. держ. упр. при Президентові України*. Сер. Держ. упр. 2017. № 1. с. 8-9
- 61.Саричев Ю. О. Іміджеве забезпечення як вид інформаційного забезпечення в системі державного управління. *Наук. часоп. Акад. нац. безпеки*. 2018. № 2. С.12-13
- 62.Саричев Ю. О. Організаційно-управлінське забезпечення як вид інформаційного забезпечення в системі державного управління. *Наук. часоп. Акад. нац. безпеки*. 2018. № 1. с.12-13
- 63.Сніцаренко П. М. Іміджеве забезпечення як вид інформаційного забезпечення в системі державного управління у воєнній сфері. *Наук. часоп. Акад. нац. безпеки*. 2018. № 3/4. С.7-8
- 64.Соснін О.В. Інформаційна політика України: проблеми розбудови. URL: <http://www.niisp.gov.ua/vydanna/panorama>
- 65.Тихомиров О.О. Класифікації забезпечення інформаційної безпеки. URL: http://tihomalaw.at.ua/Tihomyrov_klasifikacii_zabezpechennya_infobezpeky.pdf

- 66.Тична Б. М. Мета та принципи інформаційної діяльності збройних сил України та її роль у забезпеченні інформаційної безпеки держави в сучасних умовах. *Міжнародний науковий журнал «Інтернаука»*. Серія : Юридичні науки. 2020. № 4(1). С. 50-58. URL: [http://nbuv.gov.ua/UJRN/mnjiu_2020_4\(1\)__9](http://nbuv.gov.ua/UJRN/mnjiu_2020_4(1)__9)
67. Юдін О.К., Богуш В.М. Інформаційна безпека держави: Навч. посіб. Харків: Консул, 2005. С.39-41.
68. Bugar, A. Information Warfare and Hybrid Threats in International Relations. *Journal of Security Studies and Research*. 2020. Vol. 5, No. 2. P. 34–46.
- 69.Laichuk S. Ensuring cybersecurity in accounting in the digital economy era // Фінанс.-кредит. діяльність: проблеми теорії та практики : зб. наук. пр. 2023. Вип. 6. с.18-19
- 70.Onyshchenko S. Role and importance of information security in a pandemic environment. *Економіка і регіон*. 2020. № 2. С.22-24
71. Rácz, A. Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist. Helsinki: The Finnish Institute of International Affairs (FIIA), 2016. 98 p.