МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ
ІНСТИТУТ ЗАОЧНОГО ТА ДИСТАНЦІЙНОГО НАВЧАННЯ

КАФЕДРА КРИМІНОЛОГІЇ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА
ДЛЯ ЗДОБУТТЯ СТУПЕНЯ ВИЩОЇ ОСВІТИ МАГІСТРА

на тему: «**Національний інформаційний простір в публічному управлінні МВС України**»

Виконав: здобувач 2 курсу 2 групи
Спеціальність: 281 «Публічне управління та адміністрування»

Федієнко Денис Олександрович
Індивідуальний навчальний план № Мобільний телефон: +380504246455

Науковий керівник:
кандидат юридичних наук, доцент, доцент кафедри кримінології та інформаційних технологій Чукаєва Аліна Валеріївна

(підпис)

Кваліфікаційна робота допущена до захисту
«11» грудня 2025 р., протокол № 07
завідувач кафедри, доктор філософії в галузі права, доцент
Владислав ШКОЛЬНИКОВ

КИЇВ – 2025

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ГО	громадська організація
ДССЗЗІ	Державна служба спеціального зв'язку та захисту інформації України
ЗМІ	засоби масової інформації
ІБ	інформаційна безпека
ІКТ	інформаційно-комунікаційні технології
КІ	критична інфраструктура
КІІ	критична інформаційна інфраструктура
КСЗІ	комплексна система захисту інформації
МКІП	Міністерство культури та інформаційної політики України
НІП	національний інформаційний простір
НКЦК	Національний координаційний центр кібербезпеки
РНБО	Рада національної безпеки і оборони України
СК	стратегічні комунікації
США	Сполучені Штати Америки
ЄС	Європейський Союз
CERT-UA	Урядова команда реагування на комп'ютерні надзвичайні події України
OSINT	розвідка з відкритих джерел (Open Source Intelligence)

ВСТУП

Актуальність дослідження. У сучасних умовах глобалізації, стрімкого розвитку цифрових технологій та зростання ролі інформації як стратегічного ресурсу національний інформаційний простір МВС України набуває визначального значення для забезпечення суверенітету, стабільності та безпеки держави. Інформація перетворюється на ключовий чинник впливу на політичні процеси, суспільну свідомість, економічний розвиток та обороноздатність країн, що зумовлює формування нових форм і методів міждержавного протиборства. У цьому контексті особливої актуальності набувають проблеми вразливості національного інформаційного простору та забезпечення його стійкості до деструктивних впливів.

Для України питання захисту національного інформаційного простору має екзистенційний характер. Збройна агресія Російської Федерації, що супроводжується масштабними інформаційно-психологічними операціями, кібератаками, кампаніями дезінформації та маніпуляції громадською думкою, засвідчила, що інформаційна сфера є одним із ключових театрів сучасної гібридної війни. Вразливості національного інформаційного простору використовуються як інструмент підриву довіри до державних інститутів, дестабілізації суспільно-політичної ситуації, формування викривленої картини реальності та ослаблення національної єдності.

Водночас внутрішні фактори, зокрема фрагментарність державної інформаційної політики, недосконаліть нормативно-правового регулювання, інституційна слабкість системи забезпечення інформаційної безпеки, низький рівень медіаграмотності населення та технологічна залежність від іноземних інформаційних платформ, суттєво підсилюють інформаційну вразливість держави. За таких умов постає необхідність комплексного наукового осмислення природи національного інформаційного простору, ідентифікації його ключових вразливостей та обґрунтування ефективних механізмів підвищення його стійкості в системі публічного управління.

Мета і завдання дослідження. Метою дослідження є комплексний аналіз вразливостей національного інформаційного простору України в умовах сучасних викликів та обґрунтування пріоритетних напрямів підвищення його стійкості в контексті публічного управління.

Для досягнення поставленої мети у роботі передбачається розв'язання таких **завдань**:

- проаналізувати генезу та сучасні наукові підходи до визначення поняття національного інформаційного простору;
- розкрити місце та роль інформаційної безпеки в системі забезпечення національної безпеки держави;
- узагальнити концептуальні підходи до ідентифікації вразливостей національного інформаційного простору;
- здійснити системний аналіз внутрішніх та зовнішніх інформаційних загроз національному інформаційному простору України;
- дослідити інституційно-правові детермінанти вразливості системи забезпечення інформаційної безпеки;
- охарактеризувати соціально-комунікаційні та технологічні фактори формування інформаційної вразливості;
- обґрунтувати напрями удосконалення механізмів публічного управління у сфері захисту національного інформаційного простору;
- визначити шляхи оптимізації нормативно-правового забезпечення інформаційної безпеки України;
- розкрити значення формування суспільної стійкості до інформаційних загроз як чинника зміцнення національної безпеки.

Об'єкт і предмет дослідження. Об'єктом дослідження є національний інформаційний простір МВС України як складова системи національної безпеки держави. **Предметом дослідження** є вразливості національного інформаційного простору МВС України та механізми їх подолання в системі публічного управління.

Методологічну основу дослідження становить сукупність загальнонаукових та спеціальних методів пізнання. Зокрема, у роботі використано: аналіз і синтез – для дослідження сутності національного інформаційного простору та систематизації наукових підходів; системний підхід – для комплексного аналізу вразливостей інформаційного простору та взаємозв'язку їх складових; структурно-функціональний метод – для вивчення інституційних та правових механізмів забезпечення інформаційної безпеки; порівняльний метод – для зіставлення національних і зарубіжних підходів до захисту інформаційного простору; формально-юридичний метод – для аналізу нормативно-правових актів у сфері інформаційної безпеки; соціально-комунікаційний аналіз – для дослідження впливу інформаційних загроз на суспільну свідомість.

Елементи наукової новизни отриманих результатів. Наукова новизна одержаних результатів полягає в тому, що:

– уточнено зміст поняття вразливості національного інформаційного простору з урахуванням сучасних гібридних загроз;

– систематизовано основні групи вразливостей національного інформаційного простору України (інституційні, нормативно-правові, соціально-комунікаційні та технологічні);

– обґрунтовано роль публічного управління як ключового чинника формування стійкості національного інформаційного простору;

– визначено напрями підвищення інформаційної стійкості держави в умовах гібридної війни.

Практичне значення здобутих результатів. Практичне значення результатів дослідження полягає у можливості їх використання в діяльності органів публічного управління під час розроблення та вдосконалення державної інформаційної політики, стратегій інформаційної та кібербезпеки, а також у процесі підготовки фахівців у сфері публічного управління та національної безпеки.

РОЗДІЛ 1. ТЕОРЕТИКО-КОНЦЕПТУАЛЬНІ ТА МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ НАЦІОНАЛЬНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ МВС УКРАЇНИ

1.1. Генеза та сучасні наукові підходи до визначення поняття національного інформаційного простору

Формування та еволюція поняття національного інформаційного простору нерозривно пов’язані з розвитком інформаційного суспільства, трансформацією державних функцій та зростанням ролі інформації як стратегічного ресурсу. У науковому дискурсі проблема визначення національного інформаційного простору набула особливої актуальності наприкінці XX – на початку XXI століття, коли інформаційні технології стали ключовим чинником соціально-політичних, економічних і безпекових процесів. У цей період інформація почала розглядатися не лише як засіб комунікації, а і як інструмент впливу, управління та протиборства.

Перші підходи до осмислення інформаційного простору ґрунтувалися на технократичному баченні, у межах якого основна увага приділялася сукупності інформаційно-телекомунікаційних систем, каналів передачі даних і технічної інфраструктури. Такий підхід був характерний для ранніх досліджень у сфері зв’язку та кібернетики, де інформаційний простір ототожнювався з мережею передачі інформації та її технічним забезпеченням [1, с. 8–10; 7, с. 36–38]. Водночас подібне розуміння не враховувало соціально-політичний, правовий і культурний виміри інформаційних процесів. Подальший розвиток наукової думки зумовив перехід до соціально-комунікаційного підходу, в межах якого інформаційний простір почав розглядатися як середовище взаємодії суб’єктів суспільних відносин, у якому формуються, поширюються та сприймаються інформаційні повідомлення. Згідно з цим підходом, інформаційний простір охоплює не лише технічні засоби, а й інформаційні потоки, комунікаційні практики, символи, смисли та цінності, що циркулюють у суспільстві [16, с. 130–132; 27, с. 45–47]. Саме в цей період у науковий обіг активно вводиться

категорія «національний інформаційний простір», що відображає прив'язку інформаційних процесів до державних кордонів, політичної системи та національних інтересів.

У вітчизняній науковій традиції поняття національного інформаційного простору почало активно використовуватися з початку 2000-х років у контексті досліджень національної безпеки. Українські науковці дедалі частіше наголошували на тому, що інформаційний простір держави є самостійним об'єктом захисту поряд із територією, населенням та суверенітетом. Так, С. Глобенко визначає інформаційний простір держави як сукупність інформаційних ресурсів, інфраструктури, суб'єктів інформаційної діяльності та правових норм, що регулюють інформаційні відносини в межах національної юрисдикції [4, с. 197–199]. У цьому визначенні чітко простежується інституційно-правовий вимір інформаційного простору.

Водночас у наукових працях наголошується, що національний інформаційний простір не є ізольованим утворенням, а функціонує в умовах глобального інформаційного середовища. Глобалізація інформаційних потоків, домінування транснаціональних медіаплатформ та соціальних мереж значно ускладнюють контроль держави над власним інформаційним простором, що підвищує рівень його вразливості [20; 39]. У цьому контексті поняття національного інформаційного простору набуває динамічного характеру, оскільки його межі дедалі більше визначаються не лише територіальними, а й функціональними та нормативними чинниками. Значний внесок у розвиток концептуальних засад дослідження національного інформаційного простору зроблено в межах теорії національної безпеки. Відповідно до Закону України «Про національну безпеку України», інформаційна безпека визначається як один із ключових напрямів забезпечення національних інтересів [25]. Це законодавче положення закріплює розуміння інформаційного простору як сфери, у якій реалізуються життєво важливі інтереси держави, суспільства й особи. Як зазначає Х. Маркович, сучасна система національної безпеки

неможлива без чіткого усвідомлення ролі інформаційного простору як середовища формування політичних рішень і громадської думки [13, с. 12–14].

У контексті гібридних загроз і інформаційних війн національний інформаційний простір дедалі частіше розглядається як арена цілеспрямованого протиборства. Дослідження українських і зарубіжних учених свідчать, що інформаційний простір використовується для здійснення психологічного тиску, маніпулювання масовою свідомістю, поширення дезінформації та підриву довіри до державних інститутів [5, с. 54–57; 33; 40]. У цьому зв'язку Б. Гривнак, І. Лопушинський та І. Сапіжак підкреслюють, що дезінформація стала системним інструментом впливу на національний інформаційний простір України в умовах російсько-української війни [5, с. 58–61].

Сучасні наукові підходи до визначення національного інформаційного простору можна умовно поділити на кілька основних напрямів. Перший із них – нормативно-правовий – акцентує увагу на сукупності правових норм, інституцій та механізмів регулювання інформаційних відносин. У межах цього підходу національний інформаційний простір розглядається як об'єкт державної політики та правового захисту [19, с. 102–105; 24]. Важливу роль відіграють стратегічні документи, зокрема Стратегія інформаційної безпеки України, яка визначає пріоритети держави щодо захисту інформаційного простору від внутрішніх і зовнішніх загроз [21].

Другий підхід – системний – передбачає розгляд національного інформаційного простору як складної багаторівневої системи, що включає технічні, організаційні, соціальні та культурні компоненти. У межах цього підходу інформаційний простір розуміється як цілісне середовище взаємодії інформаційних потоків, суб'єктів комунікації та технологічних платформ [9, с. 99–103; 18]. Системний підхід дозволяє виявляти вразливості інформаційного простору, що виникають на стику різних підсистем.

Третій підхід – безпековий – фокусується на загрозах, ризиках і вразливостях національного інформаційного простору. У його межах інформаційний простір МВС України розглядається як критична сфера

національної безпеки, що потребує постійного моніторингу та захисту [8; 12]. Як зазначає І. Ломака, інформаційна безпека держави безпосередньо залежить від здатності протидіяти інформаційно-психологічним операціям і кіберзагрозам [12]. Аналогічної позиції дотримується М. Шевчук, який підкреслює, що сучасні виклики у сфері інформаційної безпеки мають комплексний характер і потребують міждисциплінарного підходу [29].

Важливим елементом сучасних наукових підходів є усвідомлення ролі суспільства в функціонуванні національного інформаційного простору. Соціально-орієнтовані концепції наголошують на значенні медіаграмотності, критичного мислення та громадянської відповідальності як чинників стійкості інформаційного середовища [15; 27]. У цьому контексті національний інформаційний простір МВС України розглядається не лише як об’єкт державного управління, а і як результат взаємодії держави, громадянського суспільства та медіа.

Отже, аналіз генези та сучасних наукових підходів до визначення поняття національного інформаційного простору свідчить про його багатовимірний і динамічний характер. У сучасних умовах національний інформаційний простір доцільно розглядати як комплексне соціально-технологічне та політико-правове утворення, у межах якого реалізуються національні інтереси, формується суспільна свідомість і забезпечується інформаційна безпека держави. Таке розуміння створює теоретичне підґрунтя для подальшого аналізу вразливостей національного інформаційного простору України та визначення ефективних механізмів його захисту.

1.2. Інформаційна безпека в системі забезпечення національної безпеки держави

Інформаційна безпека в сучасних умовах розвитку держави та суспільства посідає особливе місце в системі забезпечення національної безпеки, оскільки інформаційна сфера перетворилася на один із ключових вимірів реалізації національних інтересів. Зміна характеру загроз, поява гібридних форм протиборства, цифровізація управлінських процесів і зростання впливу масових комунікацій зумовили необхідність переосмислення ролі інформаційної безпеки як фундаментального елемента національної безпеки держави.

У науковому дискурсі поняття «інформаційна безпека» сформувалося на перетині теорій національної безпеки, інформаційного права, кібернетики та соціальних комунікацій. Як зазначає М. Шевчук, генеза поняття інформаційної безпеки безпосередньо пов’язана з еволюцією уявлень про безпеку держави – від суто воєнно-політичного розуміння до комплексного, що охоплює всі сфери суспільного життя [30, с. 135–137]. У цьому контексті інформаційна безпека поступово виокремилася як самостійний напрям національної безпеки, що відображає специфіку загроз в інформаційній сфері.

Теоретичне осмислення інформаційної безпеки ґрунтується на розумінні інформації як стратегічного ресурсу. Вона впливає на процеси прийняття політичних рішень, формування громадської думки, легітимність державної влади та соціальну стабільність. Саме тому порушення інформаційної рівноваги може мати наслідки, співмірні з традиційними загрозами безпеці, такими як економічна криза чи воєнна агресія [12]. У цьому сенсі інформаційна безпека розглядається не лише як технічний або правовий феномен, а як комплексна категорія, що поєднує політичні, соціальні та культурні виміри. У межах теорії національної безпеки інформаційна безпека визначається як стан захищеності життєво важливих інтересів особи, суспільства та держави в інформаційній сфері. Такий підхід знайшов відображення як у наукових працях, так і в нормативно-правових актах України. Зокрема, Закон України «Про національну

безпеку України» закріплює положення, відповідно до якого інформаційна безпека є складовою системи національної безпеки та передбачає захист інформаційного простору від загроз, що можуть завдати шкоди суверенітету й конституційному ладу держави [25].

Правове осмислення інформаційної безпеки в Україні розвивалося паралельно з формуванням законодавства у сфері інформаційних відносин. Прийняття Закону України «Про інформацію» стало важливим етапом у закріпленні основних принципів інформаційної діяльності та визначенні правових засад захисту інформації [24]. У подальшому ці положення були деталізовані в спеціальних законах і стратегічних документах, що відображають еволюцію державної політики у сфері інформаційної безпеки.

Значний внесок у теоретико-правове обґрунтування інформаційної безпеки зроблено українськими науковцями. Так, Д. Казмірук визначає інформаційну безпеку як системний стан захищеності інформаційної сфери держави, що забезпечує стійке функціонування політичної системи та захист національних інтересів в умовах внутрішніх і зовнішніх загроз [8]. У свою чергу, В. Білий і В. Михальчук наголошують, що інформаційна безпека є інтегруючою складовою національної безпеки, оскільки пронизує всі її інші елементи – воєнну, економічну, політичну та соціальну [3, с. 94–96].

Важливою особливістю сучасного теоретичного підходу є розуміння інформаційної безпеки як багаторівневої категорії. Вона охоплює безпеку особи, суспільства та держави, що відповідає класичній тріаді національної безпеки. У цьому контексті інформаційна безпека особи пов’язана із захистом прав на інформацію, приватність та свободу слова, інформаційна безпека суспільства – зі збереженням національної ідентичності та соціальної згуртованості, а інформаційна безпека держави – із захистом суверенітету та ефективного державного управління [27, с. 46–49]. Особливу увагу в наукових дослідженнях приділено співвідношенню понять «інформаційна безпека» та «кібербезпека». Хоча ці категорії часто використовуються як взаємопов’язані, більшість учених наголошують на їх відмінності. Кібербезпека зосереджується

передусім на захисті інформаційних систем і мереж, тоді як інформаційна безпека має ширший зміст і включає також захист інформаційного впливу, комунікаційних процесів і масової свідомості [23; 14, с. 48–50]. Такий підхід дозволяє розглядати інформаційну безпеку як концептуально ширшу категорію в системі національної безпеки.

Нормативно-правове закріплення інформаційної безпеки в Україні зазнало суттєвої трансформації в умовах збройної агресії та гібридної війни. Прийняття Стратегії інформаційної безпеки України стало відповіддю на зростання інформаційних загроз і закріпило комплексне бачення захисту національного інформаційного простору [21]. У цьому документі інформаційна безпека визначається як ключовий чинник забезпечення національної стійкості, що підкреслює її системоутворюючу роль у національній безпеці.

У теоретико-правовому вимірі інформаційна безпека дедалі більше розглядається як динамічний процес, а не як статичний стан. Такий підхід відображає змінний характер загроз і необхідність постійної адаптації правових та інституційних механізмів. Як зазначає І. Яковюк, сучасна національна безпека потребує гнучких моделей реагування, у яких інформаційна безпека виступає не допоміжним, а визначальним елементом [32].

Таким чином, теоретико-правове осмислення інформаційної безпеки як складової національної безпеки дозволяє зробити висновок, що вона є інтегральною, багатовимірною та стратегічно важливою категорією. Інформаційна безпека не лише доповнює класичні напрями національної безпеки, а й значною мірою визначає їх ефективність у сучасних умовах. Це створює концептуальне підґрунтя для подальшого аналізу функціональної ролі інформаційної безпеки в системі державного управління та протидії сучасним загрозам.

У сучасних умовах інформаційна безпека дедалі чіткіше проявляється не лише як теоретико-правова категорія, а як функціональний елемент системи державного управління, спрямований на забезпечення стійкості держави до комплексу внутрішніх і зовнішніх загроз. Зміна характеру безпекового

середовища, зокрема поява гібридних загроз, інформаційно-психологічних операцій та масштабних кібератак, зумовлює необхідність інтеграції інформаційної безпеки у всі рівні управлінських рішень.

У наукових дослідженнях підкреслюється, що інформаційна безпека виконує системоутворюючу функцію в національній безпеці, оскільки забезпечує координацію між політичними, воєнними, економічними та соціальними складовими [8; 29]. Саме через інформаційні канали здійснюється управління кризовими ситуаціями, комунікація влади з населенням, формування міжнародного іміджу держави та легітимація владних рішень. Порушення інформаційної безпеки безпосередньо впливає на ефективність державного управління та здатність держави реагувати на загрози.

Особливого значення інформаційна безпека набуває в умовах гібридної війни, де поєднуються воєнні, інформаційні, кібернетичні та політико-дипломатичні інструменти впливу. Досвід України переконливо свідчить, що інформаційні атаки можуть передувати або супроводжувати воєнні дії, створюючи сприятливе середовище для дестабілізації держави зсередини [5, с. 55–58; 40]. У цьому контексті інформаційна безпека виконує превентивну функцію, спрямовану на раннє виявлення загроз і мінімізацію їх негативного впливу. У системі державного управління інформаційна безпека реалізується через комплекс стратегічних, інституційних і правових механізмів. Прийняття Стратегії інформаційної безпеки України та Стратегії кібербезпеки України закріпило розуміння інформаційної безпеки як одного з пріоритетних напрямів державної політики [21; 22]. Ці документи визначають основні загрози, суб’єкти забезпечення інформаційної безпеки та механізми міжвідомчої координації.

Функціональна роль інформаційної безпеки полягає також у забезпеченні захисту критичної інформаційної інфраструктури. За даними Державного центру кіберзахисту, кількість кібератак на державні інформаційні ресурси України зростає, що свідчить про системний характер загроз у цифровій сфері [6]. У цьому аспекті інформаційна безпека тісно пов’язана з кібербезпекою, але

не зводиться до неї, оскільки охоплює також інформаційно-психологічний та комунікаційний виміри.

Для узагальнення місця інформаційної безпеки в системі забезпечення національної безпеки доцільно розглянути її функціональні характеристики у співвідношенні з іншими складовими національної безпеки, що подано в таблиці 1.1.

Таблиця 1.1

Місце та функції інформаційної безпеки в системі забезпечення національної безпеки держави

Складова національної безпеки	Основний об'єкт захисту	Ключові загрози	Роль інформаційної безпеки
Воєнна безпека	Суверенітет, територіальна цілісність	Інформаційно-психологічні операції, деморалізація населення	Інформаційний супровід оборони, протидія пропаганді
Політична безпека	Стабільність політичної системи	Дезінформація, втручання у виборчі процеси	Захист легітимності влади, стратегічні комунікації
Економічна безпека	Економічна стабільність	Кіберзлочинність, витоки даних	Захист економічної інформації та цифрових систем
Соціальна безпека	Суспільна згуртованість	Маніпуляція суспільною свідомістю	Формування медіастійкості та довіри
Кібербезпека	Інформаційні системи	Кібератаки, шкідливе ПЗ	Комплексний захист інформаційного середовища

Джерело: узагальнено автором на основі [21; 22; 29]

Як видно з таблиці 1.1, інформаційна безпека пронизує всі основні складові національної безпеки, виконуючи інтегруючу та координаційну функції. Вона забезпечує не лише захист інформаційних ресурсів, а й стійкість управлінських процесів, ефективність державної комунікації та здатність суспільства протистояти деструктивним інформаційним впливам.

Аналіз сучасних досліджень свідчить, що інформаційна безпека є ключовим інструментом публічного управління в кризових і надзвичайних ситуаціях. Саме через інформаційні канали держава може запобігати паніці, поширювати достовірну інформацію та координувати дії різних суб'єктів

безпеки [2; 11]. Водночас неефективна інформаційна політика або відсутність узгоджених комунікаційних стратегій суттєво підвищує рівень вразливості держави.

У науковій літературі наголошується, що сучасна інформаційна безпека має ґрунтуватися на принципах відкритості, законності та дотримання прав людини. Надмірні обмеження в інформаційній сфері можуть призводити до зниження довіри громадян до держави та створювати додаткові ризики [15; 27]. Тому інформаційна безпека в системі державного управління має балансувати між потребами захисту національних інтересів і забезпеченням демократичних свобод.

Особливу роль у функціонуванні інформаційної безпеки відіграють інституційні механізми. Координація між органами державної влади, сектором безпеки й оборони, медіа та громадянським суспільством є необхідною умовою ефективної протидії сучасним загрозам [19, с. 104–107]. Досвід провідних держав свідчить, що успішні моделі інформаційної безпеки базуються на міжвідомчій взаємодії та стратегічному плануванні [38].

Інформаційна безпека виступає не лише складовою національної безпеки, а й важливим функціональним елементом системи державного управління. Вона забезпечує здатність держави адекватно реагувати на сучасні виклики, зберігати стабільність політичної системи та формувати стійке інформаційне середовище. Це зумовлює необхідність подальшого аналізу вразливостей національного інформаційного простору України.

1.3. Концептуальні підходи до ідентифікації вразливостей національного інформаційного простору МВС України

У сучасних умовах трансформації безпекового середовища проблема вразливостей національного інформаційного простору набуває особливої

актуальності, оскільки саме інформаційна сфера дедалі частіше стає об’єктом цілеспрямованого деструктивного впливу. Усвідомлення сутності та природи вразливостей є необхідною передумовою для розроблення ефективних механізмів забезпечення інформаційної безпеки та підвищення стійкості держави до сучасних загроз.

У загальнонауковому розумінні вразливість трактується як властивість системи, що зумовлює її схильність до порушення нормального функціонування під впливом внутрішніх або зовнішніх факторів. У сфері національної безпеки вразливість розглядається як поєднання структурних, функціональних і ресурсних обмежень, які можуть бути використані суб’єктами загроз для досягнення власних цілей [37]. Застосування цього підходу до інформаційної сфери дозволяє розглядати національний інформаційний простір як складну соціально-технологічну систему, у якій вразливості виникають на різних рівнях.

Теоретичне осмислення вразливостей національного інформаційного простору базується на системному підході, який передбачає аналіз взаємозв’язків між елементами інформаційного середовища. Як зазначають Ю. Кучеренко та інші дослідники, інформаційна безпека держави не може бути забезпечена без комплексного врахування організаційних, технічних і соціальних чинників, оскільки саме на їх перетині формуються найбільш критичні зони ризику [9, с. 100–103]. У цьому контексті вразливість постає не як ізольована характеристика окремого елементу, а як результат дисбалансу всієї системи.

Важливим теоретичним підходом до ідентифікації вразливостей є безпековий, у межах якого інформаційний простір розглядається як поле реалізації загроз національній безпеці. У цьому підході вразливості трактуються як умови або обставини, що полегшують реалізацію загроз, зокрема дезінформації, інформаційно-психологічних операцій і кібернетичних атак [12; 29]. Як підкреслює І. Ломака, наявність вразливостей у інформаційному просторі свідчить про недостатню адаптивність держави до

змін у характері інформаційних загроз [12]. Суттєвий внесок у розвиток теоретичних підходів до аналізу вразливостей зроблено в межах концепції критичної інформаційної інфраструктури. Згідно з цією концепцією, інформаційний простір МВС України складається з низки критично важливих елементів, порушення функціонування яких може мати системні наслідки для національної безпеки [6]. Дослідження у сфері кіберзахисту демонструють, що технічні вразливості часто поєднуються з організаційними та кадровими проблемами, що значно підвищує ризик масштабних інцидентів.

Окрему увагу в наукових працях приділено методологічним аспектам ідентифікації вразливостей. Зокрема, пропонується застосування ризик-орієнтованого підходу, який передбачає оцінювання ймовірності реалізації загроз та потенційних наслідків їх впливу на інформаційний простір МВС України [18]. Такий підхід дозволяє визначати пріоритетні напрями захисту та раціонально розподіляти ресурси системи інформаційної безпеки.

У межах міждисциплінарного підходу вразливості національного інформаційного простору розглядаються також крізь призму соціальних і комунікаційних процесів. Як свідчать дослідження з інформаційних війн, значна частина вразливостей пов’язана не з технічними недоліками, а з особливостями сприйняття інформації, рівнем довіри до медіа та здатністю суспільства критично осмислювати інформаційні повідомлення [33; 39]. Це дозволяє говорити про існування когнітивних і культурних вразливостей, які є складними для ідентифікації, але мають значний вплив на національну безпеку.

Методологічно важливим є також розмежування понять «загроза» та «вразливість». У науковій літературі наголошується, що загроза є зовнішнім або внутрішнім чинником потенційного негативного впливу, тоді як вразливість характеризує внутрішній стан системи, який робить можливим або полегшує реалізацію цієї загрози [4, с. 200–203]. Таке розмежування має принципове значення для побудови ефективної системи ідентифікації та нейтралізації ризиків у національному інформаційному просторі.

У сучасних дослідженнях дедалі більше уваги приділяється динамічному характеру вразливостей. Вони розглядаються як змінні параметри, що еволюціонують разом із розвитком технологій, трансформацією суспільних відносин і зміною геополітичної ситуації [29]. Це зумовлює необхідність постійного моніторингу інформаційного простору та оновлення методологічних підходів до його аналізу.

Теоретико-методологічні підходи до розуміння вразливостей національного інформаційного простору ґрунтуються на системному, безпековому та міждисциплінарному баченні інформаційної сфери. Вразливості постають як комплексне явище, що формується на стику технічних, організаційних і соціальних чинників. Це створює наукове підґрунтя для подальшого дослідження конкретних інституційних, соціально-комунікаційних і технологічних факторів формування інформаційної вразливості.

Сучасні наукові дослідження засвідчують, що вразливості національного інформаційного простору формуються під впливом сукупності інституційних, соціально-комунікаційних і технологічних чинників, які перебувають у тісному взаємозв’язку. На відміну від суто теоретичного рівня аналізу, ідентифікація вразливостей у прикладному вимірі передбачає виявлення конкретних слабких місць у функціонуванні державних інституцій, комунікаційних процесів та інформаційно-технологічної інфраструктури.

Інституційний підхід до ідентифікації вразливостей зосереджується на аналізі системи публічного управління у сфері інформаційної безпеки. У межах цього підходу вразливості розглядаються як наслідок неузгодженості повноважень між органами державної влади, фрагментарності інформаційної політики, недостатнього рівня міжвідомчої координації та обмеженості ресурсного забезпечення [4, с. 202–205; 19, с. 103–106]. Як зазначають дослідники, навіть за наявності належної нормативно-правової бази слабкість інституційних механізмів суттєво знижує ефективність захисту національного інформаційного простору.

В умовах гібридної війни інституційні вразливості проявляються, зокрема, у запізнілому реагуванні на інформаційні атаки, відсутності єдиного центру стратегічних комунікацій та недостатній інтеграції інформаційної безпеки в процес ухвалення управлінських рішень [2; 21]. Це створює сприятливі умови для реалізації деструктивних інформаційних впливів і підвищує загальний рівень уразливості держави.

Соціально-комунікаційний підхід акцентує увагу на ролі суспільства як активного учасника інформаційних процесів. У межах цього підходу вразливості національного інформаційного простору пов'язуються з низьким рівнем медіаграмотності, поширенням недовіри до офіційних джерел інформації, поляризацією суспільства та домінуванням емоційно забарвленого контенту в інформаційному середовищі [5, с. 59–61; 27, с. 48–51]. Саме ці чинники створюють умови для ефективного поширення дезінформації та маніпуляцій громадською свідомістю.

Дослідження у сфері протидії дезінформації свідчать, що соціально-комунікаційні вразливості є одними з найбільш складних для нейтралізації, оскільки вони пов'язані з ціннісними орієнтаціями, рівнем політичної культури та інформаційними звичками населення [11; 15]. У цьому контексті національний інформаційний простір виступає не лише як об'єкт захисту, а і як простір формування суспільної стійкості.

Технологічний підхід до ідентифікації вразливостей зосереджується на аналізі стану інформаційно-комунікаційної інфраструктури, цифрових платформ і систем передачі даних. Сучасні дослідження вказують на те, що технологічні вразливості часто зумовлені застарілими інформаційними системами, залежністю від іноземного програмного забезпечення, недостатнім рівнем кіберзахисту та дефіцитом кваліфікованих кадрів [1, с. 10–13; 6]. За даними CERT-UA, більшість кібератак спрямовані саме на використання відомих, але неусунених вразливостей у державних і корпоративних системах [34].

Водночас технологічні вразливості не існують ізольовано, а взаємодіють із соціальними та інституційними чинниками. Як зазначає М. Мусієнко, навіть найсучасніші технологічні рішення не забезпечують належного рівня інформаційної безпеки без відповідної культури безпеки та чітких управлінських процедур [17, с. 60–63]. Це підтверджує необхідність комплексного підходу до ідентифікації вразливостей національного інформаційного простору.

Для узагальнення основних підходів до ідентифікації вразливостей доцільно систематизувати їх за ключовими напрямами, що подано в таблиці 1.2.

Таблиця 1.2

Підходи до ідентифікації вразливостей національного інформаційного простору

Підхід	Об’єкт аналізу	Основні вразливості	Потенційні наслідки
Інституційний	Система публічного управління	Фрагментарність політики, слабка координація	Неефективне реагування на загрози
Соціально-комунікаційний	Суспільна свідомість, медіасередовище	Дезінформація, низька медіаграмотність	Поляризація суспільства
Технологічний	Інформаційна інфраструктура	Кібервразливості, технічна залежність	Порушення функціонування систем
Нормативно-правовий	Правове регулювання	Прогалини та застарілі норми	Правова невизначеність
Когнітивний	Сприйняття інформації	Маніпулятивний вплив	Викривлення картини реальності

Джерело: узагальнено автором на основі [17; 29; 34]

Як свідчать дані таблиці 1.2, вразливості національного інформаційного простору мають багаторівневий характер і формуються під впливом різних груп чинників. Жоден із підходів не є самодостатнім, оскільки ігнорування хоча б одного з них призводить до неповного розуміння природи інформаційних загроз.

Комплексний аналіз інституційних, соціально-комунікаційних і технологічних підходів дозволяє зробити висновок, що ефективна ідентифікація вразливостей можлива лише за умови міждисциплінарної

взаємодії та системного моніторингу інформаційного простору. Такий підхід відповідає сучасним тенденціям розвитку державної політики у сфері інформаційної безпеки та створює методологічне підґрунтя для подальшого аналізу конкретних вразливостей національного інформаційного простору України, що стане предметом дослідження другого розділу роботи.

Отже, нами здійснено теоретико-концептуальне та методологічне осмислення національного інформаційного простору як самостійного об'єкта наукового дослідження та ключової складової системи національної безпеки держави. Аналіз генези та сучасних наукових підходів до визначення поняття національного інформаційного простору засвідчив його багатовимірний і динамічний характер, що поєднує технологічні, соціально-комунікаційні, правові та політичні компоненти. Обґрунтовано, що в умовах глобалізації та цифровізації національний інформаційний простір МВС України функціонує в тісному взаємозв'язку з глобальним інформаційним середовищем, що суттєво ускладнює процеси його державного регулювання та захисту.

Дослідження інформаційної безпеки в системі забезпечення національної безпеки дозволило встановити її інтегруючу та системоутворюючу роль у сучасній моделі державного управління. Інформаційна безпека постає не лише як окремий напрям безпекової політики, а як чинник, що безпосередньо впливає на ефективність воєнної, політичної, економічної та соціальної безпеки. Теоретико-правовий аналіз засвідчив, що інформаційна безпека в Україні набула чіткого нормативного закріплення та стратегічного значення, особливо в умовах гібридних загроз і збройної агресії, водночас її практична реалізація значною мірою залежить від узгодженості управлінських та інституційних механізмів.

Розкриття концептуальних підходів до ідентифікації вразливостей національного інформаційного простору дало змогу визначити їх комплексну природу та багаторівневий характер. Вразливості формуються на перетині інституційних, соціально-комунікаційних, технологічних і когнітивних чинників, що зумовлює необхідність застосування системного та

міждисциплінарного підходу до їх аналізу. Узагальнення теоретичних положень першого розділу створює науково-методологічне підґрунтя для подальшого дослідження конкретних проявів вразливості національного інформаційного простору України в умовах сучасних викликів.

РОЗДІЛ 2. СИСТЕМНИЙ АНАЛІЗ ВРАЗЛИВОСТІ НАЦІОНАЛЬНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ МВС УКРАЇНИ В УМОВАХ СУЧАСНИХ ВИКЛИКІВ

2.1. Деструктивний вплив внутрішніх та зовнішніх інформаційних загроз на національний інформаційний простір МВС України

Сучасний національний інформаційний простір МВС України формується та функціонує в умовах системного зовнішнього тиску, що зумовлено передусім збройною агресією Російської Федерації та застосуванням нею інструментів гібридної війни. У цих умовах інформаційна сфера перетворилася на самостійний об’єкт цілеспрямованого деструктивного впливу, а зовнішні інформаційні загрози набули комплексного, організованого та довготривалого характеру. Як зазначають вітчизняні дослідники, інформаційні загрози в сучасних конфліктах спрямовані не лише на порушення функціонування інформаційних систем, а й на трансформацію суспільної свідомості, підрив довіри до державних інституцій і дестабілізацію політичних процесів [5, с. 54–57; 12].

Ключовою особливістю зовнішніх інформаційних загроз для України є їх системність і поєднання різних інструментів впливу. Інформаційно-психологічні операції, кампанії дезінформації та кібератаки застосовуються не ізольовано, а як взаємопов’язані елементи єдиної стратегії інформаційного протиборства. За спостереженнями Б. Гривнака, І. Лопушинського та І. Сапіжака, дезінформація використовується як базовий механізм формування викривленої картини реальності, що створює сприятливе середовище для подальших деструктивних дій у політичній, соціальній та безпековій сферах [5, с. 58–61]. У цьому контексті національний інформаційний простір МВС України розглядається зовнішнім агресором як арена постійного впливу, а не як тимчасовий об’єкт атаки.

Вагомим проявом зовнішніх інформаційних загроз є масштабні кампанії дезінформації, що реалізуються через традиційні та цифрові медіа, соціальні

мережі й месенджери. Дослідження засвідчують, що ключовими цілями таких кампаній є делегітимація органів державної влади, підрив довіри до Збройних Сил України, поширення панічних настроїв та стимулювання соціальної поляризації [11, с. 470–472; 20]. Використання бот-мереж і координованих інформаційних вкидів дозволяє швидко масштабувати дезінформаційні повідомлення та охоплювати значні аудиторії, що істотно ускладнює протидію таким впливам у межах публічного управління.

Поряд із дезінформацією важливим компонентом зовнішніх загроз є кібероперації, які дедалі частіше поєднуються з інформаційно-психологічними впливами. За даними Державного центру кіберзахисту Держспецзв'язку України, у 2024 році було зафіксовано суттєве зростання кількості кіберінцидентів, спрямованих проти державних інформаційних ресурсів, критичної інфраструктури та інформаційних систем органів влади [6]. Аналітика CERT-UA свідчить, що значна частина таких атак має не лише технічну, а й інформаційну мету, оскільки супроводжується поширенням дискредитаційних матеріалів і спробами підірвати довіру громадян до здатності держави забезпечувати безпеку в цифровому середовищі [34].

Протягом року фахівці ОЦРК було виявлено 277 кіберінцидентів, що атрибутуються до активності, яка відслідковується CERT-UA за ідентифікатором UAC-0010. Серед досліджених кіберінцидентів первинним вектором ураження було розповсюдження ШПЗ засобами електронної пошти та за допомогою флешносіїв.

Кластери UAC є аналітичними ідентифікаторами, які застосовуються CERT-UA для групування кіберінцидентів зі спільними характеристиками. Номер кластера виконує виключно облікову та аналітичну функцію і не пов'язаний із рівнем небезпеки, а використовується для системного моніторингу активності кіберзагроз.

Рис. 2.1. Таймлайн кіберінцидентів, пов'язаних з діяльністю кластеру UAC-0010 у 2024 році

Джерело: узагальнено автором на основі [34]

У 2024 році фахівці ОЦРК виявили 174 кіберінциденти, що атрибутуються до активності, яка відслідковується CERT-UA за ідентифікатором UAC-0006. Серед досліджених кіберінцидентів найчастіше первинним вектором ураження було розповсюдження ШПЗ SmokeLoader засобами електронної пошти.

Рис. 2.2. Таймлайн кіберінцидентів, пов'язаних з діяльністю кластеру UAC-0006 у 2024 році

Джерело: узагальнено автором на основі [34]

Упродовж року фахівці ОЦРК виявили 99 кіберінцидентів, що атрибутуються до активності, яка відслідковується CERT-UA за ідентифікатором UAC-0050. Серед досліджених кіберінцидентів первинним вектором ураження було розповсюдження ШПЗ засобами електронної пошти.

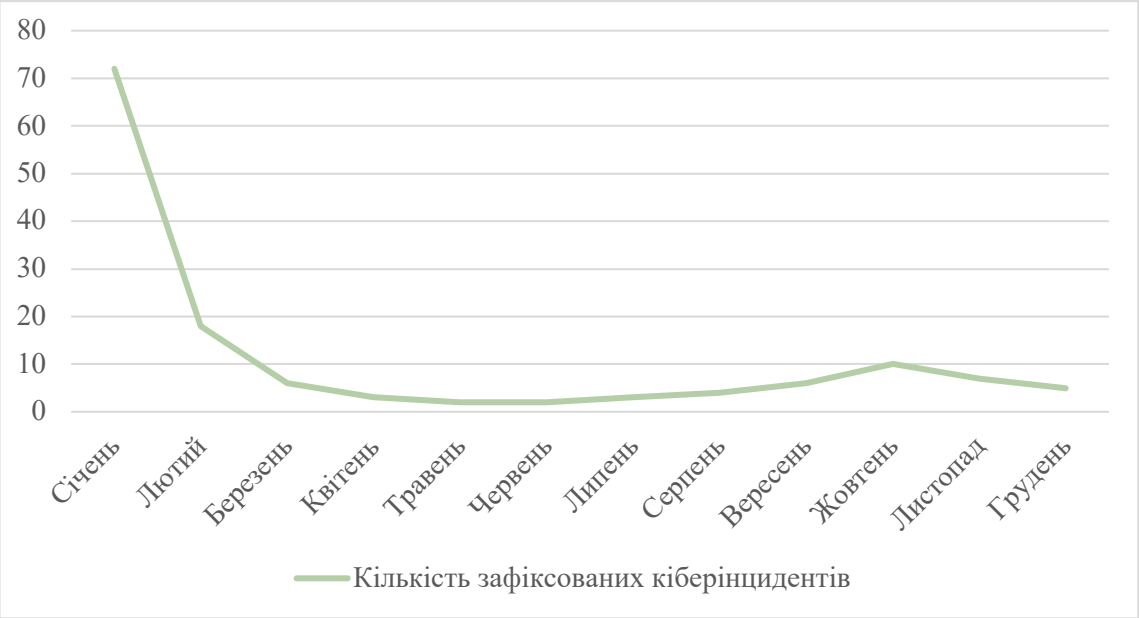


Рис. 2.3. Таймлайн кіберінцидентів, пов'язаних з діяльністю кластеру UAC-0050 у 2024 році

Джерело: узагальнено автором на основі [34]

Наведені таймлайни активності кластерів кіберзагроз UAC-0010, UAC-0050 та UAC-0006 відображають нерівномірний і хвилеподібний характер кіберінцидентів протягом 2024 року. Пікові значення активності свідчать про цілеспрямоване планування та координацію кібератак, що корелює з етапами загострення безпекової ситуації та адаптацією противника до заходів кіберзахисту. Загалом отримані дані підтверджують системний характер зовнішніх кіберзагроз і наявність технологічних вразливостей національного інформаційного простору України, що потребує постійного моніторингу та превентивних управлінських рішень.

Особливу небезпеку становить поєднання кібератак із подальшими інформаційними кампаніями, спрямованими на перебільшення наслідків

інцидентів або формування уявлення про «недієздатність» державних інституцій. Як зазначає І. Ломака, саме такий комбінований характер зовнішніх загроз дозволяє досягати значно більшого деструктивного ефекту, ніж у разі застосування окремих інструментів впливу [12]. У результаті порушується не лише технічна стабільність інформаційних систем, а й інформаційна рівновага в суспільстві, що безпосередньо впливає на рівень національної безпеки. Важливою рисою сучасних зовнішніх інформаційних загроз є їх адаптивність і динамічність. Зовнішні суб'єкти впливу активно використовують зміни в інформаційному середовищі, зокрема зростання ролі соціальних мереж, алгоритмічну персоналізацію контенту та зниження рівня довіри до традиційних медіа [39]. Це дозволяє їм оперативно коригувати наративи та канали поширення інформації, що істотно ускладнює реагування з боку держави. У таких умовах навіть наявність нормативно-правових механізмів захисту інформаційного простору не гарантує його стійкості без належної інституційної та комунікаційної спроможності [19, с. 104–106].

Для узагальнення основних видів зовнішніх інформаційних загроз та механізмів їх деструктивного впливу на національний інформаційний простір України доцільно звернутися до таблиці 2.1.

Таблиця 2.1

Основні зовнішні інформаційні загрози національному інформаційному простору України та їх деструктивний вплив

Вид загрози	Основні інструменти	Об'єкт впливу	Наслідки для інформаційного простору
Дезінформаційні кампанії	Фейкові новини, маніпулятивні наративи, бот-мережі	Суспільна свідомість, медіасередовище	Викривлення інформаційної картини, зниження довіри
Інформаційно-психологічні операції	Психологічний тиск, деморалізаційні меседжі	Населення, військовослужбовці	Поширення паніки, соціальна дестабілізація
Кібератаки	Зломи, DDoS-атаки, шкідливе ПЗ	Державні інформаційні системи	Порушення функціонування, дискредитація влади
Комбіновані інформаційні	Кібератаки + інформаційні	Інститути державної влади	Посилення вразливостей

операції	кампанії		управління

Джерело: узагальнено автором на основі [5; 6; 12; 19; 34]

Аналіз даних, наведених у таблиці 2.1, свідчить, що зовнішні інформаційні загрози впливають на національний інформаційний простір України багатовимірно та системно. Їх деструктивний ефект проявляється не лише у тимчасових порушеннях функціонування інформаційних ресурсів, а й у довгостроковому підриві інформаційної стійкості держави. Поєднання дезінформації, інформаційно-психологічних операцій і кібератак створює умови для накопичення вразливостей, які можуть бути використані для досягнення політичних і безпекових цілей зовнішнього агресора. Це підтверджує необхідність комплексного підходу до аналізу зовнішніх загроз та зумовлює перехід до дослідження внутрішніх чинників, що посилюють вразливість національного інформаційного простору України.

Внутрішні інформаційні загрози відіграють ключову роль у формуванні вразливості національного інформаційного простору України, оскільки саме вони створюють сприятливе середовище для реалізації зовнішніх деструктивних впливів. На відміну від зовнішніх загроз, що мають чітко визначене джерело та цілеспрямований характер, внутрішні загрози формуються внаслідок особливостей функціонування державних інституцій, соціально-комунікаційних процесів та управлінських практик у сфері інформаційної політики. У наукових дослідженнях наголошується, що навіть за умов потужного зовнішнього інформаційного тиску саме внутрішні слабкості визначають рівень стійкості або вразливості інформаційного простору держави [4, с. 202–205; 12].

Однією з ключових внутрішніх інформаційних загроз є фрагментарність та недостатня узгодженість державної інформаційної політики. Попри наявність стратегічних документів у сфері інформаційної та кібербезпеки, практична реалізація державної інформаційної політики нерідко характеризується відсутністю єдиного центру стратегічних комунікацій, розпорошеністю повноважень між органами влади та несистемністю

інформаційних рішень [2, с. 46–48; 19, с. 103–105]. Це призводить до появи інформаційних вакуумів, які оперативно заповнюються неофіційними або маніпулятивними джерелами, що суттєво підвищує вразливість національного інформаційного простору.

Вагомим чинником внутрішньої інформаційної вразливості є низький рівень медіаграмотності населення та обмежена здатність громадян критично оцінювати інформаційні повідомлення. Як зазначають І. Сопілко та Л. Рапацька, недостатній рівень інформаційної культури сприяє некритичному сприйняттю дезінформації, поширенню чуток і маніпулятивних наративів, що особливо небезпечно в умовах кризових ситуацій та воєнного стану [27, с. 48–51]. За таких умов громадяни стають не лише об’єктами інформаційного впливу, а й мимовільними ретрансляторами деструктивного контенту, що значно ускладнює протидію інформаційним загрозам на рівні державного управління.

Суттєвою внутрішньою загрозою для національного інформаційного простору є також зниження рівня довіри до офіційних джерел інформації. Дослідження у сфері стратегічних комунікацій свідчать, що несвоєчасне інформування, суперечливі повідомлення різних органів влади та відсутність зрозумілої комунікаційної стратегії призводять до делегітимації офіційного дискурсу в очах суспільства [2, с. 49–50; 11, с. 471–473]. У таких умовах громадяни дедалі частіше звертаються до альтернативних джерел інформації, зокрема соціальних мереж і месенджерів, які є менш контрольованими та більш уразливими до маніпулятивного впливу.

Окрему групу внутрішніх інформаційних загроз становлять соціально-комунікаційні чинники, пов’язані з поляризацією суспільства та емоційною насиченістю інформаційного простору. В умовах воєнного протистояння та тривалого стресу зростає попит на емоційно забарвлений контент, що часто супроводжується спрощеними або радикалізованими інтерпретаціями подій [5, с. 59–61; 29]. Це створює сприятливі умови для маніпуляцій громадською

свідомістю, посилює соціальні розколи та знижує рівень суспільної згуртованості, що є критично важливим чинником національної безпеки.

Не менш важливою внутрішньою інформаційною загрозою є технологічна та організаційна неготовність окремих суб'єктів інформаційних відносин до сучасних викликів. За даними Державного центру кіберзахисту Держспецзв'язку України, значна частина інформаційних інцидентів зумовлена використанням застарілих інформаційних систем, недостатнім рівнем захисту даних і дефіцитом кваліфікованих кадрів у сфері інформаційної безпеки [6]. Як зазначає Д. Мусієнко, навіть за наявності сучасних технологічних рішень відсутність культури інформаційної безпеки та чітких управлінських процедур значно підвищує ризик успішної реалізації деструктивних впливів [17, с. 60–63].

У контексті публічного управління внутрішні інформаційні загрози проявляються також у недостатній інтеграції інформаційної безпеки в процес ухвалення управлінських рішень. Інформаційна складова часто розглядається як допоміжний елемент, а не як стратегічний ресурс, що знижує ефективність реагування на кризові ситуації та інформаційні атаки [8; 18]. Такий підхід обмежує можливості держави щодо формування проактивної інформаційної політики та підвищення стійкості національного інформаційного простору. Для систематизації основних внутрішніх інформаційних загроз та визначення їх впливу на вразливість національного інформаційного простору України доцільно звернутися до таблиці 2.2.

Таблиця 2.2

Внутрішні інформаційні загрози та їх вплив на вразливість національного інформаційного простору України

Внутрішня загроза	Основні прояви	Сфера впливу	Наслідки для інформаційної безпеки
Фрагментарність інформаційної політики	Неузгоджені меседжі, інформаційні вакууми	Державне управління	Зниження ефективності стратегічних комунікацій
Низький рівень	Некритичне	Суспільна	Поширення

медіаграмотності	сприйняття контенту	свідомість	дезінформації
Недовіра до офіційних джерел	Переорієнтація на альтернативні канали	Медіасередовище	Делегітимація державного дискурсу
Соціальна поляризація	Радикалізація, емоційний контент	Соціальні комунікації	Ослаблення суспільної згуртованості
Технологічна неготовність	Застарілі системи, кадровий дефіцит	Інформаційна інфраструктура	Підвищення ризику інцидентів

Джерело: узагальнено автором на основі [11; 17; 27; 29]

Аналіз даних, наведених у таблиці 2.2, дозволяє зробити висновок, що внутрішні інформаційні загрози мають системний характер і безпосередньо впливають на рівень вразливості національного інформаційного простору України. Вони не лише ускладнюють реалізацію державної інформаційної політики, а й створюють умови для ефективного впливу зовнішніх суб'єктів, посилюючи деструктивний ефект інформаційних атак. У сукупності внутрішні загрози формують критичні «точки напруги» в інформаційному середовищі, що знижують здатність держави та суспільства протистояти сучасним інформаційним викликам. Таким чином, внутрішні інформаційні загрози виступають не другорядним, а визначальним чинником формування вразливості національного інформаційного простору України. Їх подолання потребує комплексних рішень у сфері публічного управління, стратегічних комунікацій, розвитку медіаграмотності та інституційної спроможності держави. Усвідомлення цієї обставини створює логічне підґрунтя для подальшого аналізу синергетичного впливу внутрішніх і зовнішніх загроз.

У сучасних умовах забезпечення національної інформаційної безпеки ключового значення набуває усвідомлення синергетичного характеру дії внутрішніх і зовнішніх інформаційних загроз. Національний інформаційний простір України зазнає не лише окремих деструктивних впливів, а комплексного тиску, у межах якого внутрішні слабкості держави та суспільства істотно підсилюють ефективність зовнішніх інформаційних атак. Саме взаємодія цих чинників формує системну вразливість інформаційного середовища, яка не може бути пояснена дією лише одного типу загроз [12; 29].

У наукових дослідженнях наголошується, що зовнішні інформаційні загрози, зокрема дезінформаційні кампанії та інформаційно-психологічні операції, рідко досягають стратегічних цілей без опори на внутрішні інформаційні проблеми держави [5, с. 59–61; 40]. Внутрішні загрози, такі як фрагментарність державної інформаційної політики, низький рівень медіаграмотності населення та недовіра до офіційних джерел, створюють сприятливе середовище, у якому зовнішній вплив набуває значно більшої результативності. У цьому контексті вразливість національного інформаційного простору постає як результат накладання та взаємного посилення загроз різної природи.

Одним із ключових проявів синергетичного ефекту є поєднання дезінформаційних кампаній із кризами довіри до державних інституцій. Як зазначають дослідники у сфері стратегічних комунікацій, за умов несвоєчасного або суперечливого інформування з боку органів влади навіть обмежені за масштабом інформаційні вкиди можуть мати значний суспільний резонанс [2, с. 48–50; 11, с. 471–473]. У таких ситуаціях зовнішні інформаційні наративи легко інтегруються в внутрішній дискурс, трансформуючись у чинник внутрішньої дестабілізації.

Синергетичний характер загроз особливо чітко проявляється у взаємодії кібератак та інформаційно-психологічних операцій. За даними аналітичних матеріалів CERT-UA, значна частина кіберінцидентів супроводжується інформаційними кампаніями, спрямованими на перебільшення масштабів шкоди або дискредитацію здатності держави забезпечувати кіберзахист [6; 34]. За відсутності ефективної кризової комунікації такі кампанії посилюють відчуття небезпеки та невизначеності в суспільстві, що негативно впливає на рівень національної стійкості. Таким чином, технічні вразливості поєднуються з комунікаційними, формуючи багаторівневу загрозу для інформаційного простору.

Важливим елементом синергетичного впливу є також соціально-психологічний вимір. Тривалий стрес, спричинений воєнними діями,

економічними труднощами та інформаційним перенасиченням, знижує здатність громадян до критичного мислення й підвищує сприйнятливість до маніпулятивного контенту [27, с. 48–51; 39]. За таких умов зовнішні інформаційні загрози використовують внутрішні психологічні чинники для посилення поляризації суспільства, що ускладнює формування консолідованої позиції щодо ключових питань національної безпеки.

У межах публічного управління синергетичний вплив загроз проявляється також у недостатній інтеграції інформаційної безпеки в систему стратегічного планування.

Для наочного відображення механізму синергетичного впливу внутрішніх і зовнішніх інформаційних загроз на вразливість національного інформаційного простору України доцільно звернутися до рисунка 2.4.

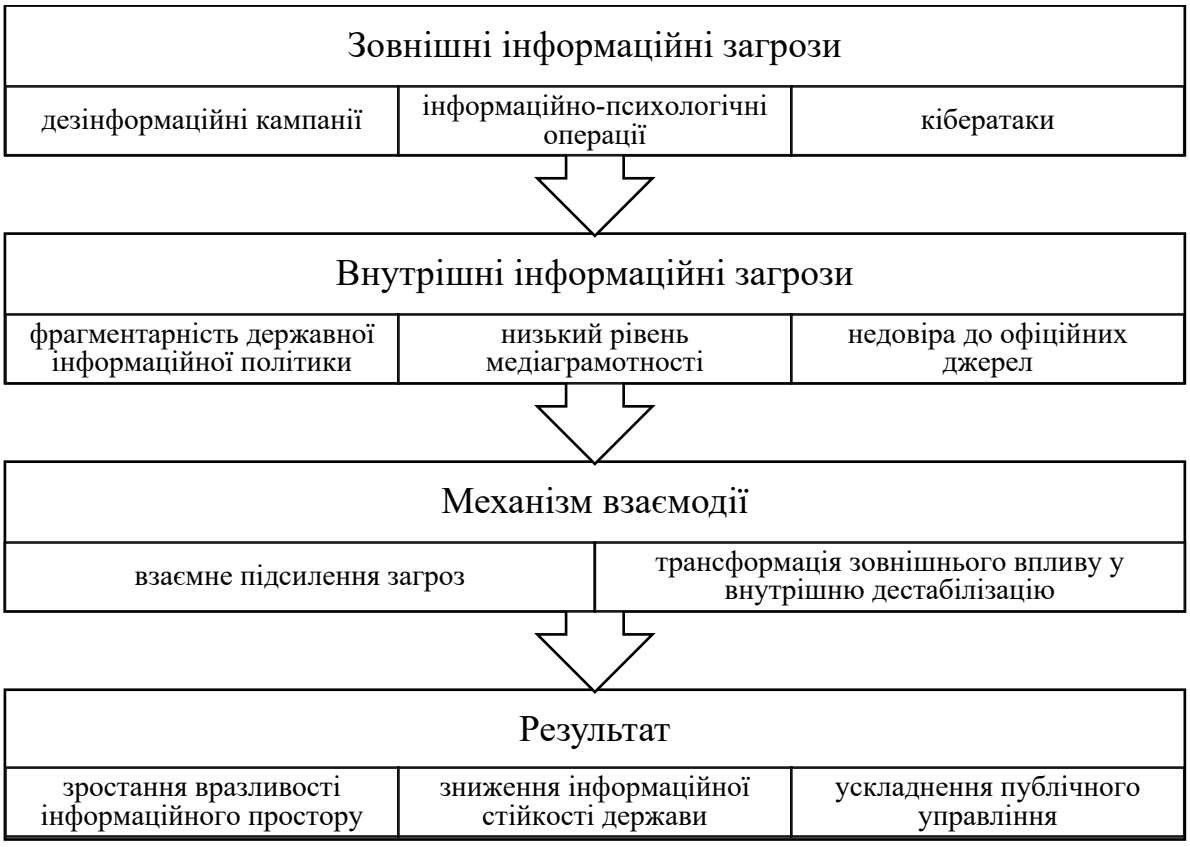


Рис. 2.4. Синергетичний вплив внутрішніх і зовнішніх інформаційних загроз на вразливість національного інформаційного простору України

Джерело: розроблено автором

Як показано на рисунку 2.4, зовнішні та внутрішні загрози перебувають у постійній взаємодії, формуючи замкнений цикл деструктивного впливу, що ускладнює процеси державного управління та знижує рівень інформаційної стійкості.

Узагальнюючи викладене, слід зазначити, що синергетичний вплив внутрішніх і зовнішніх інформаційних загроз є одним із ключових чинників формування вразливості національного інформаційного простору України. Він зумовлює перехід від локальних інформаційних проблем до системних криз, що охоплюють політичну, соціальну та безпекову сфери. Подолання таких загроз потребує комплексного підходу, що поєднує інституційні, правові, комунікаційні та соціальні інструменти публічного управління

2.2. Інституційно-правові детермінанти вразливості системи забезпечення інформаційної безпеки

Система забезпечення інформаційної безпеки України характеризується значною кількістю задіяних інституцій, кожна з яких виконує окремі функції у сфері протидії інформаційним та кібернетичним загрозам. До ключових суб’єктів належать Рада національної безпеки і оборони України, Служба безпеки України, Державна служба спеціального зв’язку та захисту інформації України, Національна поліція (кіберполіція), а також профільні органи виконавчої влади, відповідальні за інформаційну політику та стратегічні комунікації [21; 22; 23]. Формально така багаторівнева структура має забезпечувати комплексний захист національного інформаційного простору, однак на практиці вона створює низку інституційних уразливостей, пов’язаних із координацією та узгодженістю дій.

Практика реагування на інформаційні та кібернетичні загрози свідчить, що основною проблемою є фрагментація управлінських рішень і відсутність

постійного єдиного центру оперативної координації. Згідно з даними Державного центру кіберзахисту Держспецзв'язку України, у 2024 році було зафіксовано 4315 кіберінцидентів, що майже на 70 % більше, ніж у 2023 році [6]. Значна частина з них потребувала одночасної участі кількох суб'єктів – технічного реагування з боку CERT-UA, правової оцінки з боку правоохоронних органів та інформаційної комунікації з боку органів виконавчої влади. Однак на практиці ці процеси часто відбувалися паралельно, а не скоординовано, що знижувало ефективність реагування.

Статистичні дані CERT-UA також засвідчують, що більшість кіберінцидентів у 2024 році мали міжсекторальний характер, тобто торкалися одночасно державних інформаційних систем, об'єктів критичної інфраструктури та інформаційного простору в цілому [34]. За таких умов відсутність уніфікованих протоколів взаємодії між інституціями призводила до затримок у прийнятті рішень, дублювання функцій та розмивання відповідальності. Це, своєю чергою, створювало додаткові «вікна вразливості», якими користувалися зовнішні суб'єкти впливу.

Практичним індикатором інституційної перевантаженості є також динаміка реагування на інциденти. За інформацією Держспецзв'язку, у 2024 році значна частина ресурсів CERT-UA була зосереджена на ліквідації наслідків атак, а не на превентивних заходах [6]. Це свідчить про домінування реактивної моделі управління інформаційною безпекою, за якої інституції змушені працювати в режимі постійного кризового реагування. В умовах такої моделі навіть незначні управлінські збої або комунікаційні затримки набувають системного характеру та підсилюють загальну вразливість інформаційного простору.

Окремої уваги потребує проблема координації інформаційних комунікацій у кризових ситуаціях. Аналіз практики публічного інформування під час кібератак або масштабних інформаційних кампаній засвідчує, що різні органи влади часто поширюють повідомлення з різним рівнем деталізації та часовими розривами [2, с. 48–50]. У результаті виникає інформаційна

асиметрія, яка негативно впливає на рівень довіри громадян до офіційних джерел та посилює ефект дезінформаційних вкидів. Такі комунікаційні розриви мають інституційний характер і є наслідком відсутності єдиного алгоритму стратегічних комунікацій у сфері інформаційної безпеки.

Статистичні огляди у сфері кібербезпеки також демонструють нерівномірність інституційної спроможності на різних рівнях управління. Зокрема, за даними огляду подій у сфері кібербезпеки, підготовленого апаратом РНБО, більшість ефективних механізмів моніторингу та реагування зосереджені на центральному рівні, тоді як місцеві органи влади та підпорядковані установи часто не мають достатніх ресурсів і підготовленого персоналу для оперативного реагування [35]. Це створює додаткові ризики для цілісності національного інформаційного простору, оскільки саме регіональний рівень нерідко стає первинною точкою проникнення інформаційних і кіберзагроз.

Практика функціонування інституційної системи інформаційної безпеки України засвідчує, що зростання кількості інцидентів не супроводжується пропорційним посиленням координаційних механізмів. За умов, коли одна інституція відповідає за технічний захист, інша – за кримінальне переслідування, а третя – за інформаційні комунікації, відсутність чітко визначеного центру управління кризовими ситуаціями призводить до фрагментації зусиль і втрати часу [19, с. 104–106]. Саме ця фрагментація виступає однією з ключових інституційних детермінант вразливості системи забезпечення інформаційної безпеки. Для наочного відображення інституційної архітектури та координаційних зв’язків у системі забезпечення інформаційної безпеки України доцільно звернутися до рисунка 2.5. Як видно з рисунка, наявність значної кількості суб’єктів безпеки без чітко вибудуваного механізму постійної взаємодії створює умови для виникнення управлінських розривів та зниження ефективності реагування на загрози. Рисунок наочно демонструє складну, багаторівневу інституційну архітектуру системи забезпечення інформаційної безпеки України, яка характеризується значною кількістю

суб'єктів із частково перехресними повноваженнями. Як видно з рисунка, ключові функції розподілені між органами стратегічного рівня (РНБО України та її координаційні центри), органами оперативно-технічного реагування (Держспецзв'язку, Державний центр кіберзахисту, CERT-UA), правоохоронними структурами (СБУ, кіберполіція) та органами виконавчої влади, відповідальними за комунікаційну політику.

Рис. 2.5. Інституційна система забезпечення інформаційної безпеки України та координаційні розриви

Джерело: розроблено автором на основі [6; 19; 21; 34; 35]

Водночас відсутність чітко визначеного постійного центру оперативного управління інформаційними кризами зумовлює виникнення координаційних розривів між зазначеними суб'єктами. На практиці це проявляється у несинхронності дій під час реагування на кіберінциденти та інформаційні атаки, що підтверджується зростанням кількості інцидентів, які потребують залучення кількох інституцій одночасно [6; 34]. У таких умовах інформаційний обмін між суб'єктами часто має фрагментарний характер, що призводить до затримок у прийнятті управлінських рішень та зниження оперативності реагування.

Особливої уваги заслуговує дисбаланс між центральним і регіональним рівнями управління, який чітко простежується на рисунку 2.5. Концентрація основних ресурсів, експертного потенціалу та аналітичних інструментів на центральному рівні за одночасної обмеженості спроможностей місцевих органів влади створює структурну вразливість інформаційного простору. Саме регіональні та підпорядковані установи нерідко стають первинною мішенню інформаційних і кібернетичних атак, що підтверджується аналітичними оглядами у сфері кібербезпеки [35].

Таким чином, аналіз рисунка 2.2 дозволяє дійти висновку, що інституційна складність та недостатній рівень координації між суб'єктами забезпечення інформаційної безпеки виступають самостійною детермінантою вразливості національного інформаційного простору України. За умов зростання кількості та складності загроз такі координаційні розриви не лише знижують ефективність реагування, а й створюють сприятливі умови для масштабування деструктивних інформаційних впливів, що вимагає подальшого вдосконалення як управлінських, так і нормативно-правових механізмів у цій сфері.

Нормативно-правове забезпечення інформаційної безпеки України формально охоплює широкий спектр суспільних відносин і включає закони, укази Президента України, стратегії, концепції та підзаконні акти. Водночас практичний аналіз їх реалізації засвідчує наявність низки стійких проблем, які

безпосередньо впливають на ефективність функціонування системи забезпечення інформаційної безпеки та формують її вразливість.

Однією з ключових практичних проблем є фрагментарність нормативно-правового поля. Законодавче регулювання інформаційної безпеки розподілене між різними галузями права – інформаційним, адміністративним, кримінальним, безпековим і кібернетичним. На практиці це призводить до ситуації, коли окремі аспекти інформаційної безпеки регламентуються кількома нормативними актами без чіткого визначення механізмів їх взаємодії [19, с. 101–110]. Як наслідок, суб'єкти забезпечення інформаційної безпеки змушені діяти в умовах нормативної невизначеності, що знижує оперативність і правову обґрунтованість управлінських рішень.

Практичним підтвердженням зазначеної проблеми є реалізація Стратегії інформаційної безпеки України. Аналіз виконання заходів, передбачених планами імплементації стратегічних документів, свідчить, що значна частина нормативних завдань має декларативний характер і не супроводжується чіткими індикаторами результативності [21]. У результаті контроль за виконанням таких заходів ускладнений, а відповідальність за їх невиконання є розмитою. Це створює нормативні «прогалини», які можуть бути використані в умовах інформаційного протиборства.

Суттєвою детермінантою вразливості є застарілість окремих правових норм, які не відповідають сучасним умовам цифровізації та гібридних загроз. Частина законодавчих положень була сформована в період, коли інформаційні загрози мали переважно традиційний характер і не охоплювали масове використання соціальних мереж, месенджерів та цифрових платформ як інструментів впливу [26]. На практиці це ускладнює правове реагування на дезінформаційні кампанії та маніпулятивні інформаційні впливи, що поширюються через транснаціональні платформи.

Окремою проблемою нормативно-правового характеру є розмежування інформаційної безпеки та кібербезпеки. Хоча в законодавстві ці сфери визначені як взаємопов'язані, на практиці вони регулюються різними актами та

перебувають у віданні різних органів влади [22; 23]. Це призводить до ситуацій, коли кіберінциденти з потужним інформаційно-психологічним ефектом розглядаються виключно як технічні порушення без належної правової та комунікаційної реакції. Такий підхід знижує комплексність протидії загрозам і підсилює вразливість інформаційного простору.

Практичні труднощі виникають і у сфері правозастосування. За результатами аналітичних оглядів, значна частина норм, спрямованих на протидію дезінформації, реалізується вибірково або з істотним часовим лагом [11]. Це пояснюється складністю доказування, відсутністю уніфікованих процедур фіксації інформаційних правопорушень та обмеженими повноваженнями окремих суб’єктів у цифровому середовищі. У підсумку правові механізми часто не встигають за динамікою інформаційних загроз.

Практика 2023–2024 років також засвідчила проблему нерівномірності нормативної реалізації на центральному та місцевому рівнях. У той час як на загальнодержавному рівні приймаються стратегічні документи та методичні рекомендації, їх впровадження на рівні органів місцевого самоврядування часто є фрагментарним або формальним [35]. Це створює асиметрію в рівнях захищеності інформаційного простору та робить окремі територіальні сегменти більш уразливими до інформаційних атак. Для узагальнення основних нормативно-правових проблем, що формують вразливість системи забезпечення інформаційної безпеки України, доцільно звернутися до рисунка 2.6, який відображає структуру ключових детермінант у відсотковому співвідношенні.

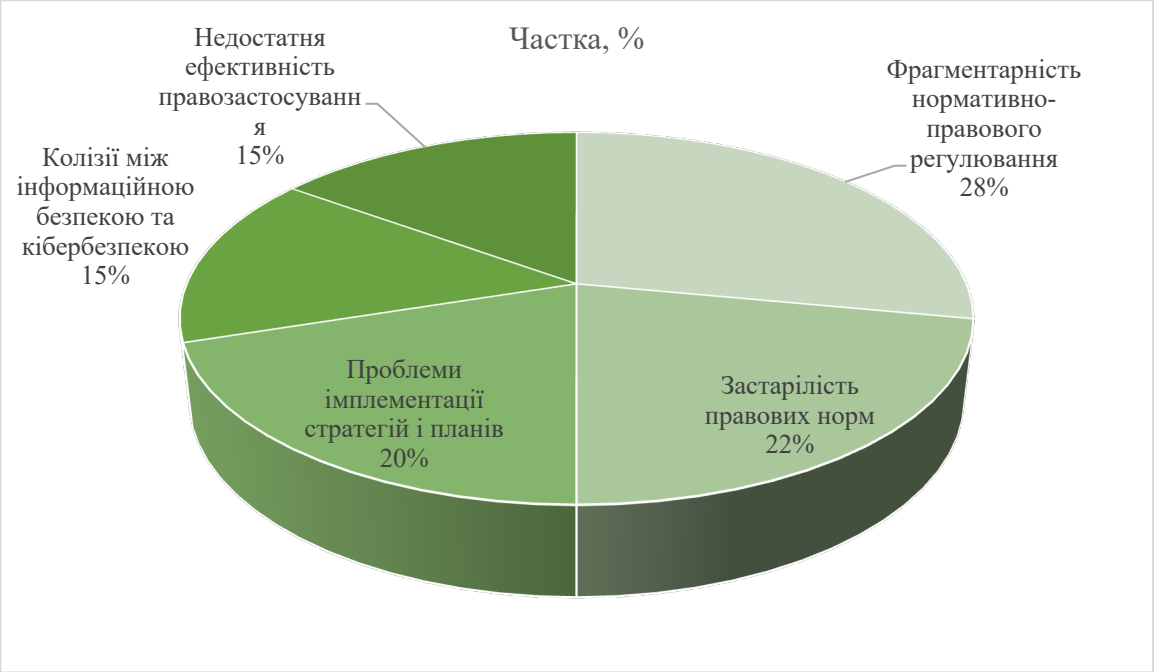


Рис. 2.6. Структура нормативно-правових детермінант вразливості системи забезпечення інформаційної безпеки України

Джерело: узагальнено автором на основі [21; 22; 26; 35]

Дані рисунка 2.6 свідчать, що найбільший вплив на формування нормативно-правової вразливості системи інформаційної безпеки мають фрагментарність регулювання та застарілість окремих правових норм, сумарна частка яких становить 50 %. Це означає, що навіть за наявності значної кількості нормативних актів їх неузгодженість і невідповідність сучасним загрозам істотно знижують ефективність правового захисту інформаційного простору.

Вагому частку (20 %) становлять проблеми імплементації стратегічних документів, що підтверджує розрив між декларованими цілями державної політики та практикою їх реалізації. Колізії між правовим регулюванням інформаційної безпеки та кібербезпеки, а також низька ефективність правозастосування, у сукупності формують ще 30 % нормативних ризиків, що свідчить про необхідність комплексного оновлення та систематизації законодавства.

Загалом аналіз нормативно-правових детермінант підтверджує, що вразливість системи забезпечення інформаційної безпеки України значною мірою має не технічний, а саме правовий і управлінський характер.

Ресурсно-спроможнісні чинники відіграють визначальну роль у формуванні практичної ефективності системи забезпечення інформаційної безпеки України. Навіть за наявності розгалуженої інституційної структури та сформованої нормативно-правової бази, обмеженість фінансових, кадрових і технологічних ресурсів суттєво знижує здатність держави своєчасно реагувати на сучасні інформаційні та кібернетичні загрози. Практика функціонування відповідних інституцій у 2022–2024 роках переконливо свідчить, що саме ресурсні обмеження є одним із ключових чинників системної вразливості національного інформаційного простору.

Однією з основних проблем є дисбаланс між зростанням кількості загроз і рівнем фінансового забезпечення суб’єктів інформаційної безпеки. За даними Державного центру кіберзахисту, у 2024 році кількість зафіксованих кіберінцидентів зросла майже на 70 % порівняно з попереднім роком, тоді як бюджетні асигнування на окремі напрями кіберзахисту та інформаційної безпеки зросли значно повільніше [6; 34]. Це призводить до ситуації, коли більшість ресурсів спрямовується на ліквідацію наслідків атак, а не на розвиток превентивних механізмів.

Фінансування системи забезпечення інформаційної безпеки України здійснюється через різні бюджетні програми, розпорошені між кількома головними розпорядниками коштів. Така модель ускладнює стратегічне планування та не дозволяє сформувати єдиний фінансовий контур інформаційної безпеки. У результаті окремі напрями, зокрема розвиток аналітичних центрів, модернізація систем моніторингу та підготовка кадрів, фінансуються за залишковим принципом [19, с. 104–106].

Особливо гостро проблема ресурсної обмеженості проявляється на **регіональному рівні**. Аналітичні огляди у сфері кібербезпеки свідчать, що більшість сучасних технічних засобів захисту та висококваліфікованих

спеціалістів зосереджені в центральних органах влади, тоді як місцеві органи влади часто не мають достатнього фінансування для впровадження навіть базових заходів кіберзахисту [35]. Це створює асиметрію в рівнях захищеності інформаційного простору та робить окремі сегменти державної інфраструктури більш уразливими.

Кадровий аспект також є критичною ресурсною детермінантою. За даними профільних аналітичних матеріалів, дефіцит фахівців з інформаційної та кібернетичної безпеки в державному секторі залишається системною проблемою [14; 17]. Конкуренція з приватним сектором, обмежені можливості матеріального стимулювання та високе професійне навантаження призводять до плинності кадрів і втрати інституційної пам’яті. У результаті навіть наявні технологічні рішення не використовуються повною мірою через нестачу підготовленого персоналу.

Ресурсна вразливість проявляється і в обмеженості аналітичних та прогнозних спроможностей. Як засвідчують щомісячні та щоквартальні огляди подій у сфері кібербезпеки, більшість аналітичних матеріалів мають описовий характер і спрямовані на фіксацію вже реалізованих інцидентів, а не на прогнозування майбутніх загроз [35]. Такий підхід обумовлений, зокрема, браком фінансування для впровадження систем великих даних, штучного інтелекту та автоматизованого аналізу інформаційних потоків.

Для ілюстрації фінансового аспекту ресурсної вразливості системи забезпечення інформаційної безпеки України доцільно звернутися до таблиці 2.7, у якій узагальнено дані щодо орієнтовного розподілу бюджетного фінансування за основними напрямами.

Рис. 2.7. Орієнтовний розподіл фінансування у сфері забезпечення інформаційної безпеки України (2022–2024 рр.)

Джерело: узагальнено автором на основі відкритих бюджетних даних та аналітичних матеріалів [17; 19; 35]

Дані рисунка свідчать, що майже половина фінансових ресурсів у сфері інформаційної безпеки спрямовується на технічний кіберзахист та реагування на інциденти. Така структура фінансування підтверджує домінування реактивного підходу до забезпечення інформаційної безпеки, за якого основні ресурси витрачаються на ліквідацію наслідків атак, а не на їх попередження.

Водночас фінансування розвитку аналітичних систем, підготовки кадрів і стратегічних комунікацій у сукупності не перевищує 30 %, що є недостатнім з огляду на комплексний характер сучасних інформаційних загроз. Мінімальна частка коштів, спрямованих на наукові дослідження та інновації (5 %), свідчить про обмежені можливості довгострокового розвитку системи та її адаптації до нових форм інформаційного протиборства.

Отже, ресурсно-спроможнісні детермінанти формують стійку вразливість системи забезпечення інформаційної безпеки України, яка проявляється у фінансовій розпорошеності, кадровому дефіциті та обмежених можливостях

аналітичного прогнозування. За умов зростання кількості та складності загроз такі обмеження суттєво знижують загальну інформаційну стійкість держави та підсилюють негативний ефект інституційних і нормативно-правових проблем, розглянутих у попередніх підрозділах.

2.3. Соціально-комунікаційні та технологічні фактори формування інформаційної вразливості

У сучасних умовах ключовим чинником формування інформаційної вразливості національного інформаційного простору України стає не лише інституційна або нормативна спроможність держави, а й особливості інформаційної поведінки населення. Практичні дослідження останніх років свідчать, що структура споживання інформації, рівень довіри до різних джерел та способи поширення контенту безпосередньо впливають на здатність суспільства протидіяти дезінформації та маніпулятивним впливам [5, с. 59–61; 27, с. 48–51].

Однією з ключових тенденцій є зміщення центрів споживання суспільно-політичної інформації з традиційних медіа до цифрових платформ і месенджерів. За результатами соціологічних досліджень 2023–2024 років, більшість громадян України отримують новини насамперед із соціальних мереж, месенджерів і неофіційних онлайн-ресурсів, тоді як роль телебачення та офіційних державних каналів поступово зменшується [27; 29]. Така трансформація інформаційного середовища ускладнює централізоване інформування населення та створює умови для фрагментації інформаційного простору.

Практичний аналіз показує, що месенджери, зокрема Telegram, відіграють домінуючу роль у поширенні оперативної інформації. Їхня популярність зумовлена швидкістю поширення повідомлень, зручністю доступу та

можливістю анонімного адміністрування каналів [17, с. 58–61]. Водночас саме ці характеристики значно знижують рівень контролю за достовірністю інформації та полегшують масове поширення неперевірених або маніпулятивних повідомлень. За таких умов інформаційна поведінка користувачів дедалі частіше ґрунтується не на перевірці джерел, а на емоційній реакції та довірі до «свого» каналу комунікації.

Суттєвим чинником вразливості є поширення інформації через горизонтальні соціальні зв'язки – родичів, друзів, колег. Соціологічні опитування засвідчують, що значна частина користувачів сприймає інформацію, отриману від знайомих, як більш надійну порівняно з офіційними джерелами [15]. У результаті дезінформаційні наративи, інтегровані в особисте спілкування, поширюються швидше та сприймаються менш критично. Такий механізм комунікації суттєво ускладнює протидію інформаційним загрозам, оскільки вони набувають «соціально легітимованого» характеру.

Окремої уваги потребує інформаційне перенасичення як фактор зниження стійкості суспільства. Постійний потік новин, повідомлень і коментарів у цифровому середовищі призводить до інформаційної втоми, що знижує здатність користувачів до аналітичного осмислення отриманих даних [39]. У таких умовах люди дедалі частіше обирають прості й емоційно забарвлені пояснення складних подій, що підвищує ефективність маніпулятивних інформаційних впливів.

Практичні результати оцінювання медіаграмотності населення підтверджують наявність когнітивних уразливостей, пов'язаних зі сприйняттям інформації. Попри активізацію державних і громадських програм з підвищення медіаграмотності, значна частина населення демонструє обмежені навички критичного аналізу інформаційних повідомлень, зокрема у цифровому середовищі [15; 27]. Це створює ситуацію, коли навіть за наявності офіційних спростувань дезінформаційні наративи зберігають вплив і продовжують циркулювати в інформаційному просторі.

Інформаційна поведінка населення також характеризується поляризацією інформаційного споживання. Алгоритмічні механізми соціальних мереж формують персоналізовані стрічки новин, які підсилюють уже наявні переконання користувачів [33]. У практичному вимірі це призводить до формування інформаційних «бульбашок», у межах яких альтернативні точки зору або офіційні позиції держави сприймаються з недовірою. Такий стан інформаційного середовища ускладнює формування єдиного національного інформаційного наративу та підвищує ризики внутрішньої дезінтеграції.

Для узагальнення ключових соціально-комунікаційних чинників, пов’язаних з інформаційною поведінкою населення, доцільно звернутися до рисунка 2.8, який відображає основні канали споживання інформації та пов’язані з ними вразливості.

Рисунок 2.8 демонструє, що основні соціально-комунікаційні вразливості національного інформаційного простору формуються на перетині цифрових каналів комунікації та особливостей інформаційної поведінки населення. Домінування соціальних мереж і месенджерів як джерел новин поєднується з низьким рівнем перевірки достовірності інформації та високим рівнем довіри до неформальних каналів поширення.

Як видно з рисунка, саме горизонтальні соціальні зв’язки та алгоритмічні механізми платформ виступають каталізаторами фрагментації інформаційного простору. У результаті навіть за наявності інституційних і правових механізмів захисту інформаційного середовища, соціально-комунікаційні фактори значно підсилюють загальну вразливість та ускладнюють реалізацію державної інформаційної політики.

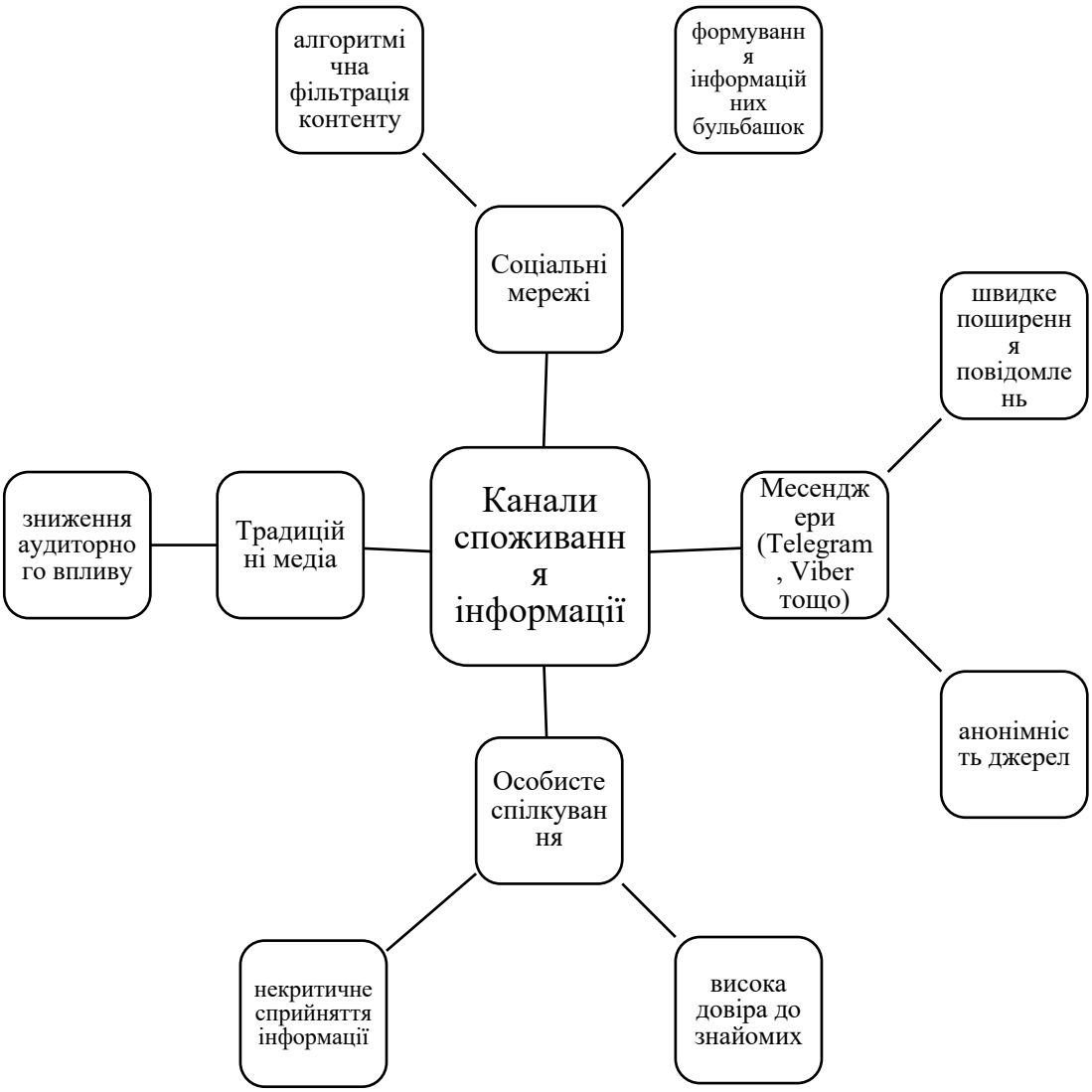


Рис. 2.8. Канали споживання інформації та соціально-комунікаційні чинники формування інформаційної вразливості

Джерело: узагальнено автором на основі [5; 15; 27; 29]

Одним із ключових соціально-комунікаційних чинників формування інформаційної вразливості національного інформаційного простору України є рівень довіри до джерел інформації та здатність громадян критично оцінювати інформаційні повідомлення. Практичні дослідження останніх років засвідчують, що навіть за умов активної інформаційної політики держави та наявності офіційних каналів комунікації значна частина населення залишається

вразливою до маніпулятивного контенту та дезінформації [5, с. 59–61; 27, с. 48–51].

Соціологічні опитування демонструють нестабільність довіри до різних джерел інформації. З одного боку, зберігається відносно високий рівень довіри до окремих державних інституцій у кризових ситуаціях, з іншого – спостерігається зростання скептицизму щодо офіційних повідомлень у повсякденному інформаційному споживанні [29]. Така диференційована довіра створює сприятливі умови для альтернативних, неофіційних джерел, які не завжди дотримуються стандартів достовірності та відповідальності.

Практичним індикатором когнітивної вразливості є результати оцінювання медіаграмотності населення. За даними Національного тесту з медіаграмотності, проведеного у 2024 році, тест розпочали понад 230 тис. осіб, проте завершили його лише близько третини учасників, що свідчить про обмежену готовність до системного опанування навичок критичного аналізу інформації [15]. Навіть серед тих, хто завершив тестування, значна частина демонструвала труднощі з розпізнаванням маніпулятивних заголовків, емоційно забарвлених повідомлень і прихованої реклами.

Додатковим підтвердженням наявності когнітивних уразливостей є результати соціологічних досліджень, згідно з якими понад половина респондентів визнають, що стикалися з неправдивою інформацією, але не завжди могли однозначно визначити її недостовірність [11]. Це означає, що проблема полягає не лише у факті поширення дезінформації, а й у недостатній здатності аудиторії до її ідентифікації.

Важливим чинником інформаційної вразливості є емоційне сприйняття інформації. Дослідження у сфері соціальних комунікацій засвідчують, що повідомлення, які апелюють до страху, обурення або співчуття, поширюються значно швидше та сприймаються менш критично [39]. У контексті воєнного стану та тривалого психологічного напруження такі повідомлення мають підвищений вплив, що посилює ризики маніпулювання суспільною свідомістю.

Практика функціонування цифрових платформ також свідчить про вплив інформаційних «бульбашок» на формування когнітивних вразливостей. Алгоритмічне персоналізоване подання контенту знижує ймовірність зіткнення користувачів з альтернативними точками зору та сприяє закріпленню вже сформованих переконань [33]. За таких умов навіть офіційні спростування або коригування інформації мають обмежений ефект, оскільки не завжди потрапляють до відповідних аудиторій.

Для узагальнення основних когнітивних і поведінкових чинників інформаційної вразливості доцільно звернутися до рисунка 2.9, який відображає структуру ключових проблем у сфері довіри та медіаграмотності населення у відсотковому співвідношенні.

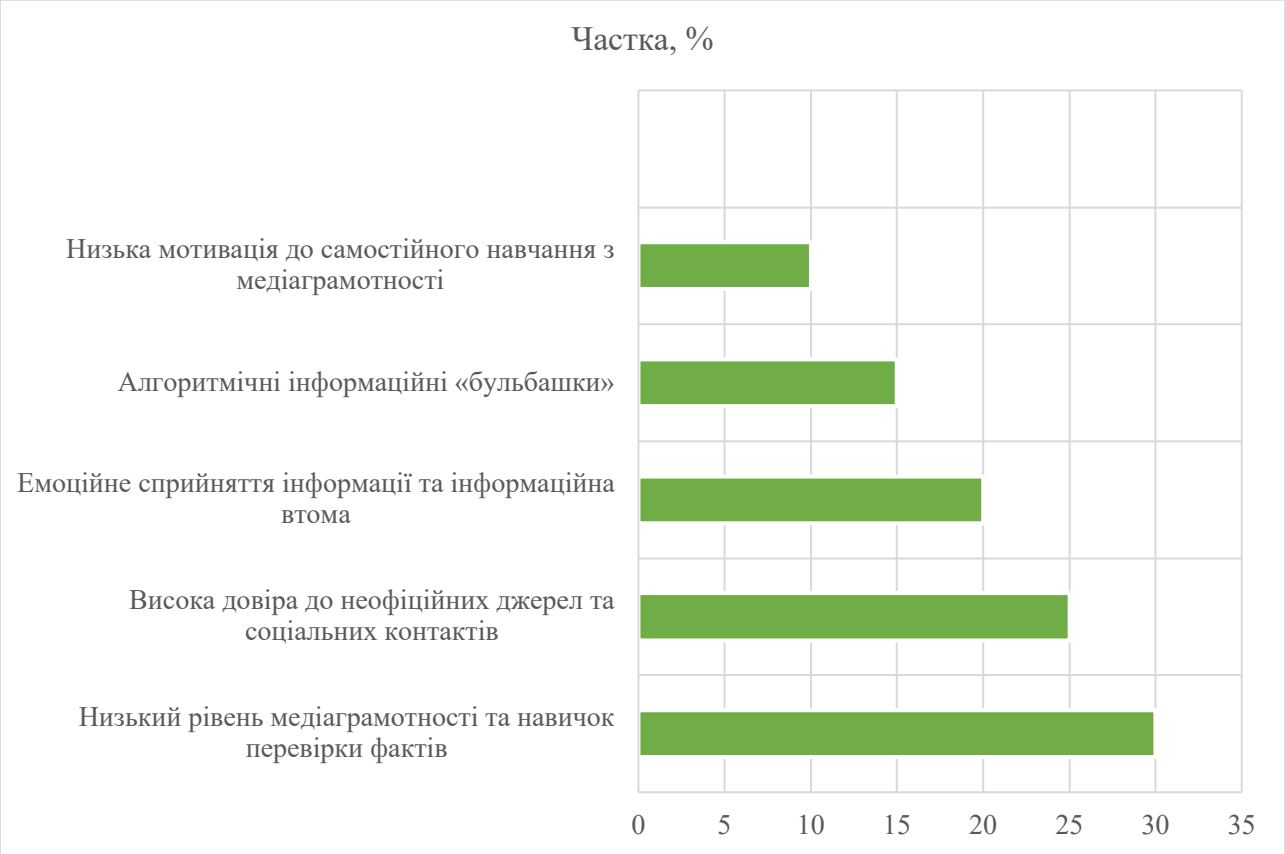


Рис. 2.9. Структура когнітивних і поведінкових чинників інформаційної вразливості населення України

Джерело: узагальнено автором на основі [29; 33; 39]

Дані рисунка 2.9 свідчать, що домінуючим чинником когнітивної інформаційної вразливості є низький рівень медіаграмотності та обмежені навички перевірки інформації, частка яких становить 30 %. Це підтверджує, що навіть за умов активного інформаційного середовища значна частина населення не має достатніх інструментів для критичного аналізу контенту.

Висока довіра до неофіційних джерел і соціальних контактів (25 %) у поєднанні з емоційним сприйняттям інформації (20 %) створює сприятливі умови для швидкого поширення маніпулятивних повідомлень. Меншою, але системно значущою є роль алгоритмічних інформаційних «бульбашок» (15 %), які ускладнюють корекцію дезінформаційних наративів. Низька мотивація до підвищення медіаграмотності (10 %) свідчить про необхідність переорієнтації державних і суспільних програм із формального інформування на довгострокове формування культури критичного мислення.

У сукупності ці чинники формують стійку когнітивну вразливість, яка значно ускладнює реалізацію інституційних і правових механізмів забезпечення інформаційної безпеки та підсилює негативний вплив сучасних інформаційних загроз.

У сучасному цифровому середовищі технологічні фактори відіграють самостійну роль у формуванні інформаційної вразливості національного інформаційного простору України. Йдеться не лише про кібератаки як такі, а про сукупність технологічних умов, архітектурних рішень і платформних особливостей, які визначають спосіб створення, поширення та сприйняття інформації. Практика останніх років засвідчує, що навіть за наявності інституційних і правових механізмів захисту, технологічні характеристики цифрового середовища часто створюють сприятливі умови для деструктивних інформаційних впливів [6; 34].

Одним із ключових технологічних факторів є домінування глобальних цифрових платформ у національному інформаційному просторі. Соціальні мережі, відеохостинги та месенджери, що використовуються громадянами України, функціонують за правилами, визначеними транснаціональними

компаніями, а не національними регуляторами. Це обмежує можливості держави щодо оперативного впливу на модерацію контенту, алгоритмічне просування повідомлень і видалення дезінформаційних матеріалів [33]. У практичному вимірі це означає, що значна частина інформаційних процесів відбувається поза межами прямого державного контролю.

Суттєвим технологічним чинником уразливості є алгоритмічна логіка поширення контенту. Алгоритми рекомендацій соціальних мереж оптимізовані на утримання уваги користувачів, що часто призводить до пріоритетного поширення емоційно забарвленого, конфліктного або сенсаційного контенту [39]. У таких умовах дезінформаційні повідомлення та маніпулятивні наративи отримують конкурентну перевагу над перевіреною та збалансованою інформацією, що підсилює інформаційну вразливість суспільства.

Окрему увагу слід приділити анонімності та слабкій ідентифікації користувачів у цифровому середовищі. Анонімні акаунти, боти та автоматизовані мережі дозволяють здійснювати масове поширення інформаційних повідомлень без можливості оперативного встановлення джерела впливу [33; 39]. Практичні огляди у сфері кібербезпеки засвідчують, що значна частина інформаційних кампаній супроводжується використанням автоматизованих інструментів, які імітують активність реальних користувачів і штучно формують інформаційні тренди [34].

Важливим технологічним фактором є також інтеграція соціальної інженерії в цифрові сервіси. За даними CERT-UA, значна кількість інцидентів пов’язана не зі складними технічними зломами, а з використанням фішингових повідомлень, підроблених сайтів і маніпулятивних сценаріїв, спрямованих на експлуатацію людського фактора [6]. Такі технології поєднують інформаційний та кібернетичний вплив, що ускладнює їх своєчасне виявлення та нейтралізацію.

Додатковим чинником уразливості є фрагментація технологічної інфраструктури державних і суспільних інформаційних систем. Різні програмні рішення, рівні захисту та стандарти безпеки, що використовуються в органах

влади та підпорядкованих установах, створюють нерівномірний рівень захищеності інформаційного простору [1, с. 10–13; 6]. У практичному вимірі це означає, що навіть одиничні технологічні збої можуть мати каскадний ефект і використовуватися для ширших інформаційних впливів.

Технологічна вразливість також посилюється швидкими темпами впровадження нових цифрових рішень, які не завжди супроводжуються належною оцінкою ризиків. Використання хмарних сервісів, сторонніх програмних продуктів і зовнішніх платформ без повноцінної адаптації до національних вимог безпеки створює додаткові точки потенційного впливу на інформаційний простір МВС України [7]. За таких умов технологічний розвиток без належного управління ризиками перетворюється з інструменту підвищення ефективності на джерело нових вразливостей.

Для узагальнення ключових технологічних факторів, що формують інформаційну вразливість національного інформаційного простору України, доцільно звернутися до рисунка 2.10, який відображає їх взаємозв’язок і практичні наслідки.

Рис. 2.10. Технологічні фактори формування інформаційної вразливості національного інформаційного простору України

Джерело: розроблено автором на основі [33; 34; 39]

Рисунок 2.10 демонструє, що технологічні фактори інформаційної вразливості мають комплексний і взаємопов'язаний характер. Домінування глобальних платформ і алгоритмічних механізмів поширення контенту поєднується з анонімністю та автоматизацією інформаційних процесів, що суттєво ускладнює ідентифікацію джерел деструктивного впливу.

Як видно з рисунка, технологічні чинники не лише створюють самостійні ризики, а й підсилюють соціально-комунікаційні вразливості, зокрема емоційне сприйняття інформації та низький рівень критичного аналізу. У результаті інформаційна вразливість національного інформаційного простору формується як наслідок поєднання технологічної складності цифрового середовища та обмежених можливостей його регулювання.

Загалом аналіз технологічних факторів підтверджує, що підвищення стійкості національного інформаційного простору потребує не лише технічних рішень, а й системного управління цифровими ризиками, що має стати одним із пріоритетів публічного управління у сфері інформаційної безпеки.

Отже, здійснено системний аналіз вразливості національного інформаційного простору України в умовах сучасних викликів, що дозволило виявити комплекс внутрішніх і зовнішніх чинників, які мають деструктивний вплив на його стійкість. Доведено, що інформаційні загрози мають багаторівневий і взаємопов'язаний характер, а їхній вплив посилюється через поєднання дезінформаційних кампаній, інформаційно-психологічних операцій та кібератак із внутрішніми слабкостями державного управління та суспільного середовища. Синергетичний ефект таких загроз зумовлює трансформацію локальних інформаційних інцидентів у системні ризики для національної безпеки.

Аналіз інституційно-правових та ресурсно-спроможнісних детермінант вразливості засвідчив, що ключовими проблемами є фрагментарність координації між суб'єктами забезпечення інформаційної безпеки, неузгодженість нормативно-правового регулювання та обмеженість фінансових і кадрових ресурсів. Практичні дані свідчать про домінування реактивного підходу до протидії загрозам, за якого основні зусилля зосереджуються на ліквідації наслідків інцидентів, тоді як превентивні механізми залишаються недостатньо розвиненими. Наявні управлінські та правові обмеження знижують ефективність реалізації державної інформаційної політики та підсилюють вразливість інформаційного простору.

Дослідження соціально-комунікаційних і технологічних факторів дозволило встановити, що інформаційна вразливість формується також на рівні поведінки, сприйняття та цифрових практик суспільства. Домінування соціальних мереж і месенджерів як каналів споживання інформації, низький рівень медіаграмотності, емоційне сприйняття контенту та алгоритмічні механізми цифрових платформ створюють сприятливе середовище для

поширення дезінформації. У сукупності результати аналізу підтверджують необхідність переходу до комплексної моделі підвищення стійкості національного інформаційного простору, що поєднуватиме інституційні, нормативно-правові, соціально-комунікаційні та технологічні інструменти публічного управління, обґрунтування яких здійснюватиметься в третьому розділі роботи.

РОЗДІЛ 3. ПРІОРИТЕТНІ НАПРЯМИ ПІДВИЩЕННЯ СТІЙКОСТІ НАЦІОНАЛЬНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ МВС УКРАЇНИ В КОНТЕКСТІ ПУБЛІЧНОГО УПРАВЛІННЯ

3.1. Удосконалення механізмів публічного управління у сфері захисту національного інформаційного простору МВС України

Підвищення стійкості національного інформаційного простору в сучасних умовах потребує насамперед удосконалення інституційно-координаційних механізмів публічного управління. Результати аналізу вразливостей, здійсненого у другому розділі роботи, свідчать, що ключовими проблемами у сфері інформаційної безпеки залишаються фрагментарність управлінських рішень, розпорошення повноважень між суб'єктами забезпечення безпеки та недостатня узгодженість дій органів державної влади в умовах кризових інформаційних ситуацій. За таких обставин першочергового значення набуває формування цілісної системи координації, здатної забезпечити своєчасне виявлення загроз і скоординовану реакцію на них.

Одним із пріоритетних інституційних механізмів є посилення ролі центрального координуючого органу у сфері інформаційної безпеки. Йдеться не стільки про створення нової структури, скільки про чітке закріплення координаційних повноважень та відповідальності за стратегічне управління інформаційною безпекою. Такий орган має забезпечувати інтеграцію діяльності суб'єктів сектору безпеки й оборони, органів виконавчої влади, комунікаційних підрозділів та регіональних структур. Централізація координації дозволяє мінімізувати дублювання функцій, скоротити час ухвалення рішень і забезпечити єдність державної позиції в інформаційному просторі.

Важливим напрямом є формування постійно діючих міжвідомчих механізмів взаємодії. На практиці це передбачає запровадження стандартизованих протоколів обміну інформацією між державними органами, чітке визначення відповідальних осіб і процедур реагування на інформаційні інциденти. Інституційна координація має ґрунтуватися не на ситуативних

домовленостях, а на формалізованих управлінських процедурах, що забезпечують безперервність реагування незалежно від кадрових або політичних змін.

Окремої уваги потребує інституціоналізація стратегічних комунікацій як складової публічного управління. В умовах інформаційних криз ключовим чинником стійкості є здатність держави оперативно формувати та транслювати узгоджену позицію. Для цього доцільно запровадити механізм єдиного інформаційного центру кризових комунікацій, який би координував публічні заяви органів влади, забезпечував їхню узгодженість і мінімізував ризики суперечливих повідомлень. Такий підхід сприяє зростанню довіри громадян до офіційної інформації та знижує ефективність дезінформаційних кампаній.

Підвищення стійкості національного інформаційного простору неможливе без залучення регіонального рівня публічного управління. Децентралізація управлінських процесів зумовлює необхідність створення в регіонах спеціалізованих підрозділів або визначення відповідальних посадових осіб з питань інформаційної безпеки та стратегічних комунікацій. Регіональні структури мають бути інтегровані в загальнонаціональну систему координації та діяти відповідно до єдиних стандартів і протоколів реагування, що дозволить оперативно враховувати місцеву специфіку інформаційних загроз.

Ще одним важливим інституційним механізмом є розвиток міжсекторальної взаємодії. Забезпечення інформаційної стійкості держави вимагає системної співпраці органів влади з громадянським суспільством, експертним середовищем і науковими установами. Формалізація такої взаємодії через дорадчі органи, експертні платформи та консультативні ради дозволяє залучати незалежну аналітику, підвищувати якість управлінських рішень і своєчасно виявляти нові інформаційні ризики.

Інституційна спроможність системи публічного управління у сфері інформаційної безпеки також залежить від кадрового забезпечення. Запровадження спеціалізованих програм підготовки та підвищення кваліфікації державних службовців, відповідальних за інформаційну політику та безпеку, є

необхідною умовою ефективної координації. Формування професійної управлінської культури у сфері інформаційної безпеки сприяє зменшенню управлінських помилок і підвищенню адаптивності системи до нових викликів.

Для узагальнення запропонованих інституційно-координаційних механізмів підвищення стійкості національного інформаційного простору доцільно систематизувати їх у таблиці 3.1.

Таблиця 3.1

Інституційно-координаційні механізми підвищення стійкості національного інформаційного простору

Механізм	Зміст управлінського рішення	Очікуваний ефект
Центральна координація	Закріплення єдиного координуючого органу у сфері інформаційної безпеки	Єдність управлінських рішень, зменшення дублювання функцій
Міжвідомча взаємодія	Запровадження формалізованих протоколів обміну інформацією	Оперативне реагування на інформаційні інциденти
Стратегічні комунікації	Створення єдиного центру кризових комунікацій	Підвищення довіри до офіційної інформації
Регіональний рівень	Інтеграція регіональних структур у загальнонаціональну систему	Урахування локальних загроз і швидке реагування
Міжсекторальна співпраця	Залучення громадянського суспільства та експертів	Підвищення якості управлінських рішень
Кадрове забезпечення	Підготовка та навчання фахівців з інформаційної безпеки	Зростання інституційної спроможності

Джерело: розроблено автором

Отже, удосконалення інституційно-координаційних механізмів публічного управління є базовою передумовою підвищення стійкості національного інформаційного простору. Запропоновані управлінські рішення спрямовані на подолання фрагментарності управління, посилення взаємодії між суб’єктами забезпечення інформаційної безпеки та формування цілісної системи реагування на сучасні інформаційні загрози. Реалізація цих механізмів створює підґрунтя для впровадження інструментальних і технологічних рішень.

Підвищення стійкості національного інформаційного простору неможливе без упровадження дієвих управлінських та інструментальних механізмів, спрямованих на превенцію, раннє виявлення та оперативне реагування на інформаційні загрози. Якщо інституційно-координаційні

механізми забезпечують організаційну цілісність системи публічного управління, то інструментальні механізми визначають її практичну спроможність діяти в режимі реального часу. Саме на цьому рівні формується здатність держави не лише реагувати на вже реалізовані загрози, а й запобігати їх масштабуванню.

Одним із ключових управлінських механізмів є впровадження системи раннього виявлення інформаційних загроз. Така система має ґрунтуватися на постійному моніторингу інформаційного середовища, зокрема соціальних мереж, месенджерів, онлайн-медіа та цифрових платформ. Йдеться не про ситуативний аналіз, а про безперервний процес збору, фільтрації та первинної оцінки інформаційних сигналів, які можуть свідчити про початок або підготовку деструктивних інформаційних кампаній. Раннє виявлення дозволяє зменшити часовий лаг між появою загрози та управлінською реакцією, що є критично важливим в умовах швидкого поширення інформації.

Наступним важливим механізмом є створення єдиної інформаційно-аналітичної платформи для суб’єктів публічного управління. Така платформа має забезпечувати консолідацію даних із різних джерел, їх аналітичну обробку та формування управлінських рекомендацій. У практичному вимірі це означає перехід від фрагментарного використання інформації до інтегрованої моделі ухвалення рішень, коли всі зацікавлені органи влади працюють з узгодженими даними та єдиною аналітичною картиною інформаційного середовища.

Ефективність управлінських рішень у сфері інформаційної безпеки значною мірою залежить від інтеграції оцінки інформаційних ризиків у процес публічного управління. Інформаційні ризики мають розглядатися нарівні з фінансовими, кадровими чи безпековими ризиками під час розроблення політик, програм і стратегічних документів. Запровадження обов’язкової процедури аналізу інформаційних наслідків управлінських рішень дозволяє мінімізувати небажані комунікаційні ефекти, зокрема викривлення повідомлень, втрату довіри або використання управлінських рішень у дезінформаційних кампаніях.

Важливим інструментальним механізмом є проведення регулярних аудитів інформаційної стійкості органів державної влади. Такі аудити мають охоплювати не лише технічний стан інформаційних систем, а й комунікаційні процеси, організацію роботи з інформацією, готовність персоналу до кризових ситуацій. Результати аудитів повинні використовуватися для коригування внутрішніх процедур, оновлення протоколів реагування та підвищення загального рівня готовності органів влади до інформаційних викликів.

Окреме місце серед управлінських механізмів займає запровадження показників ефективності (KPI) у сфері інформаційної безпеки для керівників органів публічної влади. Такі показники можуть включати швидкість реагування на інформаційні інциденти, якість кризових комунікацій, рівень узгодженості публічних повідомлень та ефективність превентивних заходів. Інституціоналізація відповідальності за стан інформаційної безпеки сприяє переходу від формального виконання функцій до результатоорієнтованого управління.

Не менш важливим є використання механізмів публічно-приватного партнерства у сфері захисту інформаційного простору. Співпраця з аналітичними центрами, науковими установами, IT-компаніями та медіаорганізаціями дозволяє розширити аналітичні можливості держави, впроваджувати сучасні інструменти аналізу даних і швидше адаптуватися до технологічних змін. Формалізація такої взаємодії через угоди, меморандуми та спільні проєкти сприяє підвищенню гнучкості управлінської системи.

Сукупність зазначених управлінських та інструментальних механізмів формує практичну основу для підвищення стійкості національного інформаційного простору. Їх реалізація потребує не лише технічних рішень, а й зміни управлінської культури, орієнтованої на превенцію, аналітичність і міжсекторальну взаємодію.

Для наочного узагальнення запропонованих механізмів доцільно звернутися до рисунка 3.1.

Рис. 3.1. Управлінські та інструментальні механізми підвищення стійкості національного інформаційного простору

Рис. 3.1 ілюструє, що ефективне публічне управління у сфері захисту національного інформаційного простору ґрунтується на поєднанні управлінських і інструментальних механізмів. Системи раннього виявлення, аналітичні платформи та регулярні аудити забезпечують інформаційну основу для прийняття рішень, тоді як управлінські інструменти відповідальності та координації формують організаційні умови для їх реалізації.

Запропонована модель дозволяє перейти від реактивного реагування на інформаційні загрози до проактивного управління ризиками, що є ключовою умовою підвищення стійкості національного інформаційного простору в умовах сучасних викликів. Реалізація цих механізмів створює практичне підґрунтя для подальшого вдосконалення нормативно-правового забезпечення інформаційної безпеки.

3.2. Оптимізація нормативно-правового забезпечення інформаційної безпеки України

Оптимізація нормативно-правового забезпечення інформаційної безпеки України є необхідною умовою підвищення стійкості національного інформаційного простору, оскільки саме правова база визначає межі, інструменти та відповідальність суб'єктів публічного управління в цій сфері. Аналіз чинних стратегічних і рамкових актів свідчить, що, попри наявність значної кількості нормативних документів, система правового регулювання залишається фрагментованою, що знижує її прикладну ефективність у протидії сучасним інформаційним загрозам.

Однією з ключових проблем є відсутність цілісної нормативної архітектури, у межах якої стратегічні документи, закони та підзаконні акти були б узгоджені за цілями, термінологією та механізмами реалізації. На практиці це призводить до ситуації, коли окремі положення стратегій мають декларативний характер і не підкріплюються нормами прямої дії. У результаті суб'єкти забезпечення інформаційної безпеки змушені діяти в умовах правової невизначеності або покладатися на тимчасові управлінські рішення.

Пріоритетним напрямом оптимізації нормативно-правового забезпечення є уніфікація та уточнення базової термінології. Наразі в різних нормативних актах використовуються різні підходи до визначення понять «інформаційна безпека», «інформаційна загроза», «дезінформація», «інформаційний вплив», що ускладнює правозастосовну практику. Закріплення єдиного понятійного апарату на рівні рамкових актів дозволить забезпечити однакове розуміння завдань і повноважень усіма суб'єктами публічного управління.

Важливим кроком є синхронізація стратегічних документів у сфері національної, інформаційної та кібербезпеки. Стратегії мають утворювати єдину ієрархічну систему, у межах якої чітко визначені пріоритети, індикатори досягнення цілей і механізми координації. Відсутність такої узгодженості

знижує ефективність реалізації стратегічних положень і створює ризики дублювання функцій між органами влади.

Окремої уваги потребує закріплення поняття інформаційної стійкості як самостійного об’єкта правового регулювання. На сьогодні це поняття активно використовується в управлінській та експертній практиці, однак не має достатнього нормативного наповнення. Його інтеграція в рамкові акти дозволить перейти від реагування на окремі загрози до системного управління ризиками та стійкістю інформаційного середовища.

Ще одним напрямом оптимізації є посилення ролі норм прямої дії у стратегічних і рамкових документах. Практика показує, що значна частина положень має рекомендаційний характер і не супроводжується чітко визначеними обов’язками, строками виконання та відповідальністю. Запровадження обов’язкових процедур, стандартів і мінімальних вимог до суб’єктів інформаційної безпеки підвищить дієвість правового регулювання.

Доцільним також є впровадження механізму регулярного перегляду стратегічних і рамкових актів. Динаміка інформаційних загроз зумовлює необхідність періодичного оновлення нормативної бази з урахуванням технологічних і соціально-комунікаційних змін. Формалізація такого механізму дозволить уникнути застарівання стратегічних документів і підвищить адаптивність правової системи.

Для узагальнення ключових напрямів оптимізації стратегічних і рамкових нормативно-правових актів у сфері інформаційної безпеки доцільно систематизувати їх у таблиці 3.2.

Таблиця 3.2

Напрями оптимізації стратегічних і рамкових нормативно-правових актів у сфері інформаційної безпеки

Проблемний аспект	Суть проблеми	Запропонований напрям оптимізації
Термінологічна неузгодженість	Різні трактування ключових понять	Уніфікація понятійного апарату
Фрагментарність стратегій	Відсутність єдиної ієрархії документів	Синхронізація стратегічних актів

Декларативність норм	Обмежена кількість норм прямої дії	Посилення обов'язкових правових приписів
Відсутність поняття стійкості	Нечітке нормативне закріплення	Інтеграція поняття інформаційної стійкості
Застарілі положення	Неврахування нових викликів	Регулярний перегляд і оновлення актів

Джерело: розроблено автором

Отже, оптимізація стратегічних і рамкових нормативно-правових актів має бути спрямована на формування цілісної, узгодженої та адаптивної правової системи у сфері інформаційної безпеки. Реалізація запропонованих напрямів дозволить підвищити ефективність правового регулювання, зменшити рівень правової невизначеності та створити надійне нормативне підґрунтя для впровадження спеціальних правових механізмів реагування на сучасні інформаційні загрози.

Сучасні інформаційні загрози характеризуються високою динамікою, гібридним характером та поєднанням інформаційно-психологічних, технологічних і кібернетичних впливів. За таких умов ефективність системи інформаційної безпеки держави значною мірою залежить від наявності спеціальних правових механізмів, здатних забезпечити оперативне реагування на деструктивні інформаційні процеси без порушення базових демократичних принципів. Оптимізація нормативно-правового забезпечення в цій площині має бути спрямована не на розширення декларативних заборон, а на створення гнучких і пропорційних правових інструментів.

Одним із ключових напрямів є запровадження правових механізмів швидкого реагування на інформаційні інциденти. У чинному правовому полі процедури обмеження доступу до деструктивного контенту або реагування на масові інформаційні атаки часто є надмірно складними та тривалими. Це знижує ефективність державних дій в умовах, коли швидкість поширення інформації вимірюється хвилинами. Тому доцільним є нормативне закріплення спрощених і тимчасових процедур реагування, які можуть застосовуватися в умовах кризових ситуацій, воєнного стану або масових інформаційних атак.

Важливим правовим інструментом є регулювання взаємодії держави з цифровими платформами та онлайн-сервісами. Значна частина деструктивного інформаційного контенту поширюється через соціальні мережі, відеохостинги та месенджери, діяльність яких регулюється переважно правилами самих платформ. У цьому контексті розвиток спеціальних правових механізмів має передбачати встановлення чітких процедур співпраці державних органів із провайдерами цифрових послуг, зокрема щодо оперативного реагування на запити про обмеження поширення дезінформації або шкідливого контенту.

Окремої уваги потребує правове врегулювання режимів інформаційної безпеки в особливих умовах. Йдеться про визначення правових підстав і меж застосування тимчасових інформаційних режимів у період воєнного стану, надзвичайних ситуацій або масштабних інформаційних кампаній. Чітке нормативне визначення таких режимів дозволяє уникнути правової невизначеності та забезпечити баланс між потребами безпеки й дотриманням прав людини.

Суттєвим напрямом оптимізації є диференціація юридичної відповідальності за правопорушення в інформаційній сфері. Практика засвідчує, що універсальні підходи до відповідальності не завжди є ефективними, оскільки не враховують характер, масштаб і наслідки інформаційного впливу. Доцільним є запровадження градації правових наслідків залежно від ступеня суспільної небезпеки інформаційних дій, що дозволить підвищити превентивну функцію права без надмірної криміналізації інформаційної діяльності.

Важливим спеціальним механізмом є правове оформлення державно-приватної взаємодії у сфері інформаційної безпеки. Аналітичні центри, медіаорганізації, ІТ-компанії та експертні спільноти відіграють значну роль у виявленні та аналізі інформаційних загроз, однак їх участь у системі безпеки часто має неформальний характер. Закріплення правових форм співпраці, зокрема через угоди, меморандуми та спеціальні правові режими, дозволить

інтегрувати потенціал недержавних акторів у загальнодержавну систему реагування.

Не менш важливим є нормативне забезпечення захисту прав і свобод людини в процесі реалізації спеціальних правових механізмів. Будь-які обмеження в інформаційній сфері мають бути чітко визначені законом, мати тимчасовий характер і супроводжуватися ефективними механізмами контролю. Це дозволяє запобігти зловживанням і зберегти довіру громадян до державної інформаційної політики навіть у кризових умовах.

Таким чином, розвиток спеціальних правових механізмів реагування має базуватися на принципах оперативності, пропорційності та правової визначеності. Їх упровадження створює умови для ефективного протистояння сучасним інформаційним загрозам без підриву демократичних засад функціонування держави.

Для узагальнення ключових спеціальних правових механізмів реагування на сучасні інформаційні загрози доцільно звернутися до рисунка 3.2.

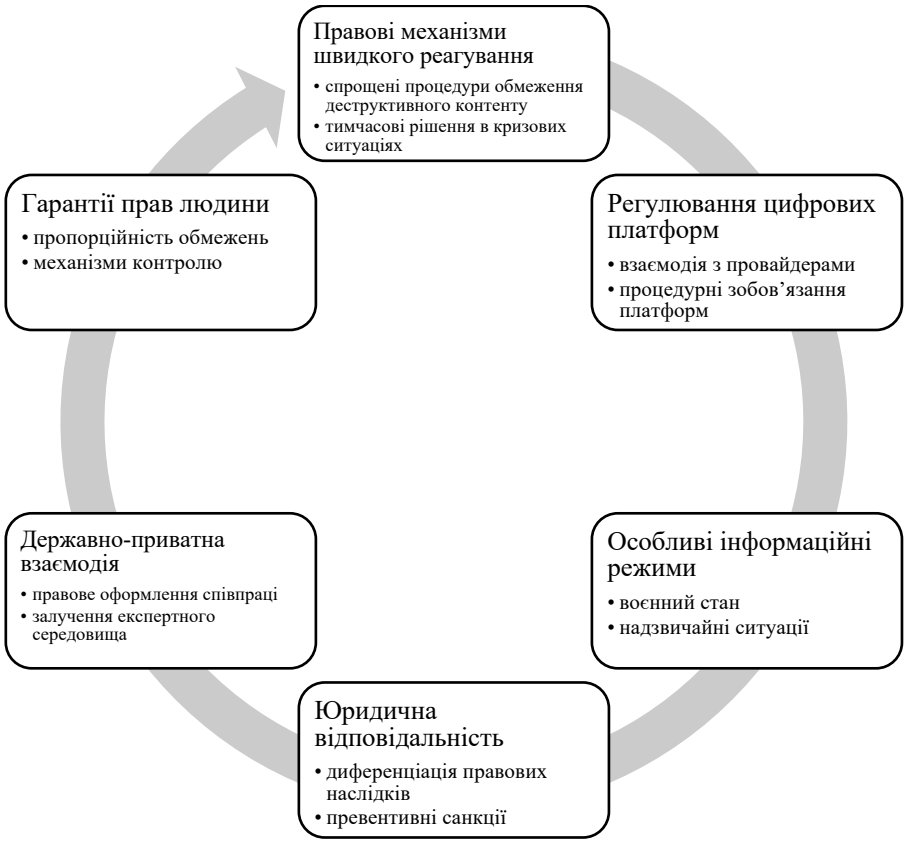


Рис. 3.2. Спеціальні правові механізми реагування на сучасні інформаційні загрози

Джерело: розроблено автором

Рисунок 3.2 демонструє, що спеціальні правові механізми реагування на сучасні інформаційні загрози формують багаторівневу систему правового впливу, яка охоплює як оперативні, так і довгострокові інструменти. Центральне місце в цій системі посідають механізми швидкого реагування та регулювання цифрових платформ, які дозволяють мінімізувати масштаби деструктивних інформаційних впливів на ранніх етапах їх реалізації.

Водночас наявність правових гарантій захисту прав людини та чітко визначених меж застосування обмежень забезпечує легітимність державних дій у сфері інформаційної безпеки. Запропонована система правових механізмів сприяє переходу від ситуативного реагування до структурованої моделі правового управління інформаційними ризиками, що є необхідною умовою підвищення стійкості національного інформаційного простору України.

3.3. Формування суспільної стійкості до інформаційних загроз як чинник зміцнення національної безпеки МВС України

Формування суспільної стійкості до інформаційних загроз є одним із ключових чинників зміцнення національної безпеки України, оскільки саме суспільство виступає головним середовищем сприйняття, інтерпретації та поширення інформації. Навіть за умов ефективних інституційних, управлінських і правових механізмів держава залишається вразливою, якщо значна частина населення не володіє навичками критичного аналізу інформаційних повідомлень. У цьому контексті розвиток медіаграмотності та критичного мислення набуває стратегічного значення і має розглядатися як довгострокова інвестиція в національну безпеку.

Практичний досвід протидії інформаційним загрозам свідчить, що більшість дезінформаційних кампаній орієнтовані не на фахівців або державні інституції, а саме на масову аудиторію. Маніпулятивні повідомлення розраховані на емоційне сприйняття, спрощене мислення та довіру до звичних джерел інформації. За таких умов підвищення рівня медіаграмотності населення є одним із найбільш ефективних способів зменшення вразливості інформаційного простору без застосування обмежувальних або репресивних інструментів.

Важливим напрямом формування суспільної стійкості є інституціоналізація медіаграмотності в системі освіти. Йдеться не лише про запровадження окремих навчальних курсів, а про системне формування навичок критичного мислення, аналізу джерел, розпізнавання маніпуляцій та фейкових повідомлень на всіх рівнях освіти. Такий підхід дозволяє закладати основи інформаційної стійкості ще на ранніх етапах соціалізації особистості та формувати покоління громадян, менш уразливих до дезінформаційних впливів.

Окремої уваги потребує розвиток медіаграмотності серед дорослого населення та професійних груп, діяльність яких пов’язана з ухваленням рішень або поширенням інформації. Державні службовці, представники органів місцевого самоврядування, освітяни, журналісти та громадські активісти мають бути носіями високих стандартів інформаційної культури. Підвищення їхніх компетенцій у сфері медіаграмотності сприяє зменшенню ризиків поширення недостовірної інформації на інституційному рівні та підвищує загальну стійкість інформаційного середовища.

Суттєвим чинником суспільної стійкості є формування культури критичного споживання інформації. Критичне мислення має сприйматися не як спеціалізована навичка, а як соціальна норма повсякденної поведінки. Це передбачає розвиток звички перевіряти джерела, порівнювати інформацію з різних каналів, відокремлювати факти від оцінок та усвідомлювати власні когнітивні упередження. У практичному вимірі така культура значно знижує ефективність маніпулятивних інформаційних впливів.

Важливою складовою є цільові програми для вразливих груп населення, які найбільше піддаються інформаційному впливу. До таких груп належать особи похилого віку, внутрішньо переміщені особи, мешканці прифронтових територій, а також громадяни з обмеженим доступом до якісних інформаційних ресурсів. Адаптовані освітні та просвітницькі програми для цих категорій дозволяють зменшити асиметрію інформаційної стійкості в суспільстві та підвищити загальний рівень національної безпеки.

Формування суспільної стійкості також потребує регулярного оцінювання рівня медіаграмотності населення. Моніторинг таких показників дозволяє виявляти слабкі місця в інформаційній підготовці суспільства, коригувати державні та громадські програми й оцінювати ефективність реалізованих заходів. Наявність чітких індикаторів медіастійкості дає змогу перейти від декларативних ініціатив до результатоорієнтованої політики.

Для узагальнення основних напрямів формування суспільної стійкості через розвиток медіаграмотності та критичного мислення доцільно звернутися до рисунка 3.3.

Рис. 3.3. Основні напрями формування суспільної стійкості до інформаційних загроз

Джерело: розроблено автором

Рисунок 3.3 демонструє, що формування суспільної стійкості до інформаційних загроз є багаторівневим процесом, який охоплює освітній, професійний і соціальний виміри. Центральне місце в цій системі посідає розвиток критичного мислення як універсальної навички, що забезпечує здатність громадян самостійно протидіяти маніпулятивним інформаційним впливам.

Водночас цільова робота з вразливими групами та регулярне оцінювання рівня медіаграмотності дозволяють зменшити нерівномірність інформаційної стійкості в суспільстві. У сукупності ці напрями формують фундамент довгострокової інформаційної безпеки, що підсилює ефективність державних управлінських і правових механізмів та сприяє зміцненню національної безпеки України.

У сучасних умовах забезпечення інформаційної безпеки держави неможливе виключно силами органів публічної влади. Масштаб і динаміка інформаційних загроз, зростання ролі цифрових платформ та фрагментація інформаційного середовища зумовлюють необхідність активного залучення громадянського суспільства та медіа до формування стійкого національного інформаційного простору. У цьому контексті суспільство постає не як об’єкт захисту, а як повноцінний учасник системи інформаційної безпеки.

Одним із ключових напрямів формування суспільної стійкості є інституціоналізація участі громадянського суспільства у процесах забезпечення інформаційної безпеки. На практиці громадські організації, аналітичні центри та експертні спільноти часто виконують функції раннього виявлення дезінформаційних кампаній, аналізу інформаційних наративів і роз’яснення складних суспільно-політичних процесів. Формалізація їх участі через дорадчі органи, консультативні ради та партнерські платформи дозволяє інтегрувати

незалежну експертизу в систему публічного управління та підвищити якість ухвалюваних рішень.

Важливим елементом суспільної стійкості є підтримка незалежних і відповідальних медіа. Якісна журналістика відіграє роль буфера між державними інституціями та суспільством, забезпечуючи перевірку фактів, пояснення управлінських рішень і протидію маніпулятивним повідомленням. Публічне управління у сфері інформаційної безпеки має бути спрямоване не на обмеження свободи медіа, а на створення умов для їх сталого розвитку, зокрема через підтримку професійних стандартів, прозорих механізмів фінансування та саморегулювання.

Окремої уваги потребує розвиток фактчекінгових ініціатив як елементу суспільної протидії дезінформації. Такі ініціативи виконують функцію незалежної перевірки інформації, сприяють підвищенню рівня довіри до перевірених джерел і формують у громадян навички самостійного аналізу контенту. Інтеграція фактчекінгових проєктів у ширші інформаційні екосистеми, зокрема через співпрацю з медіа та освітніми установами, посилює їхній вплив на формування суспільної стійкості.

Суттєвим чинником є забезпечення ефективного зворотного зв’язку між владою і суспільством. Відкриті комунікаційні канали, прозорість рішень і готовність державних органів до діалогу знижують рівень недовіри та мінімізують ґрунт для поширення дезінформації. У практичному вимірі це означає перехід від одностороннього інформування до інтерактивних форматів комунікації, у межах яких громадяни можуть отримувати пояснення, ставити запитання та брати участь у формуванні інформаційної політики.

Важливим напрямом залучення суспільства є підтримка локальних ініціатив і регіональних медіа. Місцевий рівень інформаційного простору часто є найбільш уразливим до дезінформаційних впливів через обмежені ресурси та слабку інституційну підтримку. Сприяння розвитку локальних інформаційних проєктів, громадських медіа та регіональних аналітичних центрів дозволяє

підвищити стійкість інформаційного середовища на місцях і зменшити вплив зовнішніх інформаційних акторів.

Не менш значущим є формування партнерських моделей взаємодії між державою, медіа та громадянським суспільством. Такі моделі можуть включати спільні інформаційні кампанії, обмін аналітичними даними, навчальні програми та координацію дій у кризових ситуаціях. Партнерський підхід дозволяє поєднати ресурси різних акторів і забезпечити комплексну відповідь на інформаційні загрози.

Для узагальнення ключових напрямів залучення громадянського суспільства та медіа до системи забезпечення інформаційної безпеки доцільно систематизувати їх у таблиці 3.3.

Таблиця 3.3

Напрями залучення громадянського суспільства та медіа до забезпечення інформаційної безпеки

Напрям	Зміст заходів	Очікуваний результат
Інституційна участь	Дорадчі ради, експертні платформи	Підвищення якості управлінських рішень
Підтримка медіа	Сприяння незалежній журналістиці	Зміцнення довіри до інформації
Фактчекінг	Розвиток перевірки фактів	Зменшення впливу дезінформації
Зворотний зв’язок	Діалог влади з громадянами	Зниження інформаційної напруги
Локальні ініціативи	Підтримка регіональних медіа	Підвищення стійкості на місцях
Партнерські моделі	Спільні проєкти держави і суспільства	Синергія ресурсів

Джерело: розроблено автором

Отже, залучення громадянського суспільства та медіа до системи забезпечення інформаційної безпеки є необхідною умовою формування довгострокової стійкості національного інформаційного простору. Активна участь суспільства дозволяє не лише посилити ефективність державних механізмів захисту, а й створити середовище довіри, відповідальності та критичного ставлення до інформації. У сукупності це сприяє зміцненню

національної безпеки України та підвищує її здатність протидіяти сучасним інформаційним загрозам.

Таким чином, обґрунтовано пріоритетні напрями підвищення стійкості національного інформаційного простору України в контексті публічного управління, що дозволило перейти від ідентифікації вразливостей до формування комплексної системи управлінських, правових і суспільних рішень. Запропоновані інституційно-координаційні та управлінсько-інструментальні механізми спрямовані на подолання фрагментарності державної політики, підвищення узгодженості дій суб'єктів інформаційної безпеки та запровадження превентивного підходу до протидії сучасним інформаційним загрозам.

Аналіз напрямів оптимізації нормативно-правового забезпечення інформаційної безпеки засвідчив необхідність формування цілісної та адаптивної правової системи, здатної оперативно реагувати на динамічні виклики інформаційного середовища. Обґрунтовано доцільність удосконалення стратегічних і рамкових нормативних актів, а також розвитку спеціальних правових механізмів реагування, які поєднують ефективність державного втручання з дотриманням демократичних стандартів і прав людини. Реалізація цих заходів створює нормативне підґрунтя для підвищення інформаційної стійкості держави в умовах гібридних загроз.

Доведено, що формування суспільної стійкості до інформаційних загроз є невід'ємною складовою зміцнення національної безпеки України. Розвиток медіаграмотності, критичного мислення та активне залучення громадянського суспільства і медіа до системи забезпечення інформаційної безпеки сприяють зниженню ефективності дезінформаційних впливів і підвищенню рівня довіри в суспільстві. У сукупності запропоновані напрями формують комплексну модель підвищення стійкості національного інформаційного простору, що поєднує державне управління, правове регулювання та активну участь суспільства, забезпечуючи довгострокову стабільність і безпеку держави.

ВИСНОВКИ

У процесі виконання дослідження здійснено комплексний аналіз вразливостей національного інформаційного простору України в умовах сучасних викликів та обґрунтовано пріоритетні напрями підвищення його стійкості в контексті публічного управління. Актуальність обраної теми підтверджується трансформацією інформаційної сфери у ключовий вимір національної безпеки, а також практичним досвідом України, яка в умовах збройної агресії та гібридної війни стикається з масштабними інформаційними, психологічними та кібернетичними загрозами.

У першому розділі роботи здійснено теоретико-концептуальне та методологічне осмислення національного інформаційного простору як самостійного об’єкта наукового дослідження та складової системи національної безпеки держави. Аналіз генези та сучасних наукових підходів до визначення поняття національного інформаційного простору засвідчив його багатовимірний і динамічний характер, що поєднує технологічні, соціально-комунікаційні, правові та політичні компоненти. Обґрунтовано, що в умовах глобалізації та цифровізації національний інформаційний простір МВС України не є замкненим утворенням, а функціонує у взаємодії з глобальним інформаційним середовищем, що суттєво ускладнює процеси його державного регулювання та захисту.

Дослідження інформаційної безпеки в системі забезпечення національної безпеки дозволило встановити її інтегруючу та системоутворюючу роль. Інформаційна безпека постає не лише як окремий напрям державної політики, а як чинник, що безпосередньо впливає на ефективність воєнної, політичної, економічної та соціальної безпеки. Теоретико-правовий аналіз засвідчив, що в Україні інформаційна безпека набула нормативного закріплення та стратегічного значення, однак її практична реалізація значною мірою залежить від узгодженості управлінських і інституційних механізмів.

У межах першого розділу також розкрито концептуальні підходи до ідентифікації вразливостей національного інформаційного простору. Доведено, що вразливості мають комплексну природу та формуються на перетині інституційних, соціально-комунікаційних, технологічних і когнітивних чинників. Це зумовлює необхідність застосування системного та міждисциплінарного підходу до їх аналізу й подолання, а також створює методологічне підґрунтя для подальшого практичного дослідження.

Другий розділ роботи присвячено системному аналізу вразливості національного інформаційного простору України в умовах сучасних викликів. У результаті дослідження деструктивного впливу внутрішніх і зовнішніх інформаційних загроз встановлено, що інформаційний простір МВС України зазнає постійного цілеспрямованого впливу, який реалізується через дезінформаційні кампанії, інформаційно-психологічні операції, кібератаки та маніпуляцію суспільною свідомістю. Ці загрози мають системний характер, поєднують воєнні, політичні та соціальні інструменти впливу і спрямовані на підрив довіри до державних інститутів, дестабілізацію суспільства та ослаблення національної єдності.

Аналіз інституційно-правових детермінант вразливості системи забезпечення інформаційної безпеки засвідчив наявність низки проблем, серед яких фрагментарність державної інформаційної політики, недостатня міжвідомча координація, прогалини нормативно-правового регулювання та обмеженість ресурсного забезпечення. Виявлено, що навіть за наявності стратегічних документів та законодавчої бази відсутність чітких механізмів реалізації та відповідальності суттєво знижує ефективність системи інформаційної безпеки.

Дослідження соціально-комунікаційних і технологічних факторів формування інформаційної вразливості дозволило встановити, що значна частина загроз реалізується через особливості сприйняття інформації населенням, низький рівень медіаграмотності, поширення емоційно забарвленого контенту та технологічну залежність від іноземних цифрових

платформ. Технологічні вразливості, зокрема застаріла інфраструктура та дефіцит кваліфікованих кадрів, у поєднанні з соціальними чинниками значно підсилюють загальний рівень уразливості національного інформаційного простору.

У третьому розділі роботи обґрунтовано пріоритетні напрями підвищення стійкості національного інформаційного простору в контексті публічного управління. Запропоновані механізми удосконалення публічного управління спрямовані на подолання фрагментарності інформаційної політики, посилення координації між суб'єктами інформаційної безпеки та впровадження превентивного підходу до протидії загрозам. Обґрунтовано доцільність створення ефективних управлінських інструментів, які забезпечують системне реагування на інформаційні виклики та інтеграцію інформаційної безпеки в процес ухвалення державних рішень.

Особливу увагу приділено оптимізації нормативно-правового забезпечення інформаційної безпеки України. Доведено необхідність удосконалення стратегічних і рамкових нормативних актів, уніфікації понятійного апарату, посилення норм прямої дії та впровадження механізмів регулярного оновлення правової бази. Обґрунтовано важливість розвитку спеціальних правових механізмів реагування на інформаційні загрози, які поєднують ефективність державного втручання з дотриманням демократичних стандартів і прав людини.

Важливим результатом дослідження є обґрунтування ролі суспільної стійкості як чинника зміцнення національної безпеки. Доведено, що розвиток медіаграмотності, критичного мислення та залучення громадянського суспільства і медіа до системи забезпечення інформаційної безпеки суттєво знижують ефективність дезінформаційних впливів. Суспільство, здатне критично сприймати інформацію, виступає активним суб'єктом інформаційної безпеки, доповнюючи інституційні та правові механізми держави.

Узагальнюючи результати дослідження, можна зробити висновок, що підвищення стійкості національного інформаційного простору України

можливе лише за умови комплексного підходу, який поєднує ефективне публічне управління, адаптивне нормативно-правове регулювання та активну участь суспільства. Реалізація запропонованих у роботі заходів сприятиме зміцненню інформаційної безпеки, підвищенню національної стійкості та забезпеченню довгострокової стабільності держави в умовах сучасних глобальних і регіональних викликів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аналіз технологій побудови мережі передавання даних із високими вимогами щодо інформаційної безпеки, надійності та затримки / В. О. Власенко, Ю. В. Щавінський, М. М. Запорожченко, В. С. Тищенко. Зв'язок. 2023. № 3(163). С. 8-15.

2. Антіпова О. Стратегічні комунікації як складова інформаційної безпеки держави. Law Journal of the National Academy of Internal Affairs. 2023. Vol. 13, No. 1. P. 44-52.

3. Білий В. І., Михальчук В. М. Основні напрями забезпечення національної безпеки держави. Інвестиції: практика та досвід, 2021. № 17. С. 92–98.

4. Глобенко С. Інформаційний простір держави та проблеми забезпечення його захисту в Україні. Науковий вісник: Державне управління. 2023. № 1(13). С. 195-210.

5. Гривнак Б., Лопушинський І., Сапіжак І. Дезінформація як загроза національній безпеці України в умовах неоголошеної російсько-української війни. Науковий вісник Вінницької академії безперервної освіти. Серія «Екологія. Публічне управління та адміністрування». 2024. Вип. 1. С. 53–63. URL: https://journals.academ.vinnica.ua/index.php/eco-pa/article/download/122/115/119 (дата звернення: 19.12.2025)

6. Державний центр кіберзахисту Держспецзв'язку України. Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки : річний звіт (2024). 2024. URL: https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006 (дата звернення: 19.12.2025)

7. Єсіна М. В. Моделі загроз для хмарних послуг / М. В. Єсіна, В. В. Онопріенко, А. В. Толок. Радіотехніка. 2023. Вип. 212. С. 36-41

8. Казмірук Д. М. Інформаційна безпека як складова національної безпеки в умовах сучасних викликів. Politicus. 2025. № 1. URL: http://politicus.od.ua/1_2025/5.pdf (дата звернення: 18.12.2025).

9. Кучеренко Ю. Ф., Александров О. В., Носик А. М., Камак Д. О. Методологічні основи інформаційної безпеки країни з урахуванням умов сучасного періоду її державотворення. С. 99-109.

10. Кучеренко Ю. Ф., Власік С. М., Сальник О. В., Воробйов О. Г. Методологічні аспекти щодо розробки системи захисту інформації в системах управління військового призначення. С. 65-70.

11. Кушнір І. П., Адамчук С. В. Протидія дезінформації: організаційно-правовий аспект. Аналітично-порівняльне правознавство. 2025. Вип. 01. С. 470–475. URL: https://app-journal.in.ua/wp-content/uploads/2025/02/80.pdf (дата звернення: 19.12.2025)

12. Ломака І. І. Інформаційна безпека держави: концептуальні засади та загрози. Регіональні студії. 2023. № 31. URL: https://regionalstudies.uzhnu.uz.ua/archive/31/21.pdf (дата звернення: 18.12.2025).

13. Маркович Х. М. Національна безпека України: понятійно-категоріальне осмислення. Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична, 2023. Вип. 38. С. 10–15.

14. Методичний посібник з кібербезпеки для військових та держслужбовців. Бізнес і безпека. 2023. № 1(149). С. 47-56.

15. Методичні рекомендації щодо протидії поширенню неправдивої інформації та дезінформації в інтернеті через перевірку фактів та розробку рішень для платформ з дотриманням прав людини 2023. URL: https://mcsc.gov.ua/wp-content/uploads/2024/03/cdmsi2023015-msi-inf-guidance-note_uk.pdf (дата звернення: 19.12.2025).

16. Микитин М. Значення інформаційного простору в контексті національної безпеки держави. Вісник Прикарпатського університету. Серія: Політологія. 2024. Вип. 19. С. 129–136. URL: https://journals.pnu.if.ua/index.php/politology/article/download/189/185/382 (дата звернення: 19.12.2025)

17. Мусієнко Д. Безпека використання месенджерів. Бізнес і безпека. 2023. № 2- 3(150). С. 58-65.

18. Основні критерії інформаційної політики України: монографія / І. Р. Боднар; Центральна спілка споживчих товариств України, Львівський торговельно-економічний ун-т. Львів : Вид-во Львів. торг.-екон. ун-ту, 2023. 144 с.

19. Правові механізми забезпечення інформаційної безпеки України в умовах гібридної війни / С. В. Легомінова, Ю. В. Щавінський, Т. М. Мужанова [та ін.]. Телекомунікаційні та інформаційні технології. 2023. № 1(78). С. 101-110.

20. Присяжнюк Т. О. Інформаційно-політичні конфлікти як загроза національній безпеці України. Політичне життя. 2024. № 2. URL: https://jpl.donnu.edu.ua/article/view/17922/17814 (дата звернення: 18.12.2025).

21. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки" : Указ Президента України; Стратегія від 28.12.2021 № 685/2021. База даних «Законодавство України». Верховна Рада України. URL: https://zakon.rada.gov.ua/go/685/2021 (дата звернення: 19.12.2025).

22. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" : Указ Президента України; Стратегія від 26.08.2021 № 447/2021. База даних «Законодавство України». Верховна Рада України. URL: https://zakon.rada.gov.ua/go/447/2021 (дата звернення: 19.12.2025).

23. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. База даних «Законодавство України». Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2163-19 (дата звернення: 19.12.2025).

24. Про інформацію : Закон України від 02.10.1992 № 2657-XII. База даних «Законодавство України». Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2657-12 (дата звернення: 19.12.2025).

25. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. База даних «Законодавство України». Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2469-19 (дата звернення: 19.12.2025).

26. Смотрич Д. В. Інформаційна безпека України в умовах воєнного стану. Науковий вісник Ужгородського національного університету. Серія: Право. 2023. Вип. 22(2). URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2023/06/22-2.pdf (дата звернення: 18.12.2025).

27. Сопілко І. Соціально-правові основи інформаційної безпеки держави, суспільства й особи в Україні / І. Сопілко, Л. Рапацька. Scientific Journal of the National Academy of Internal Affairs. 2023. Vol. 28, № 1. P. 44-54.

28. Чубаєвський В. Світова практика управління подіями інформаційної безпеки корпорацій. Зовнішня торгівля: економіка, фінанси, право. 2022. № 6. С. 73-82

29. Шевчук М. О. Сучасні виклики і загрози у сфері національної інформаційної безпеки. Актуальні проблеми наукових досліджень. 2024. № 6. URL: https://apnl.dnu.in.ua/6_2024/27.pdf (дата звернення: 18.12.2025).

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

31. Юровський А. Г. Поширення недостовірної інформації про особу в мережі Інтернет: актуальні питання судового захисту. С. 140-147.

32. Яковюк І. В., Білоусов Є. М. Національна безпека України в умовах нових викликів європейській та євроатлантичній солідарності: монографія. Харків: ФОП Рубан В. В., 2022. 148 с.

33. Bakirov A. Theoretical bases of methods of counteraction to modern information warfare. Computers. 2025. Vol. 14. No. 10. P. 410. DOI: 10.3390/computers14100410. URL: https://www.mdpi.com/2073-431X/14/10/410 (дата звернення: 19.12.2025)

34. CERT-UA. Російські кібер-операції : аналітика за І півріччя 2024 року. 2024. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=68771 (дата звернення: 19.12.2025)

35. CYBER DIGEST. Огляд подій в сфері кібербезпеки, вересень 2024. 2024. URL: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20241022/Cyber%20digest_Sep_2024_UA.pdf (дата звернення: 19.12.2025)

36. DevOps. Посібник: Як домогтися гнучкості, надійності і безпеки світового рівня в технологічних компаніях / Джин Кім, Джез Хамбл, Патрік Дебуа і Джон Вілліс. Харків: Видавничий Дім "Фабула",2023. 384 с

37. Gorman S., Schintler L., Kulkarni R., Stough R. The revenge of distance: vulnerability analysis of critical information infrastructure. arXiv preprint. 2003. URL: https://arxiv.org/abs/cond-mat/0310427 (дата звернення: 19.12.2025)

38. Ngobeni H., Nkongolo M. Integrating public input and technical expertise for effective cybersecurity policy formulation. arXiv preprint. 2025. URL: https://arxiv.org/abs/2512.08575 (дата звернення: 19.12.2025)

39. Stetter S. Online disinformation and cyber insecurities. Munich. Universität der Bundeswehr München. 2023. 56 p. URL: https://www.unibw.de/politikwissenschaft/professuren/lehrstuhl-ikf/stetter/odiscye-brochure_online.pdf (дата звернення: 19.12.2025)

40. Sipper J. A. The combined power of information warfare threats. Journal of Information Warfare. 2022. Vol. 21. No. 3. P. 45–60. URL: https://www.jstor.org/stable/27199993 (дата звернення: 19.12.2025)

41. U.S. Senate Select Committee on Intelligence. Russian interference in the 2016 United States presidential election. Washington. U.S. Government Publishing Office. 2019. URL: https://www.intelligence.senate.gov (дата звернення: 19.12.2025)

ДОДАТКИ

Додаток А

Статистичні дані щодо кіберінцидентів в Україні за матеріалами річного звіту CERT-UA

За понад три роки повномасштабної війни ворогу так і не вдалося досягти цілей, так званої спеціальної військової операції. Тому щодня він збільшує кількість своїх атак: як число випущених дронів та ракет по Україні, так і кібератак.

У кожному піврічному звіті ми звертали увагу на те, що кількість кіберінцидентів, опрацьованих CERT-UA та SOC Державного центру кіберзахисту, лише збільшується.

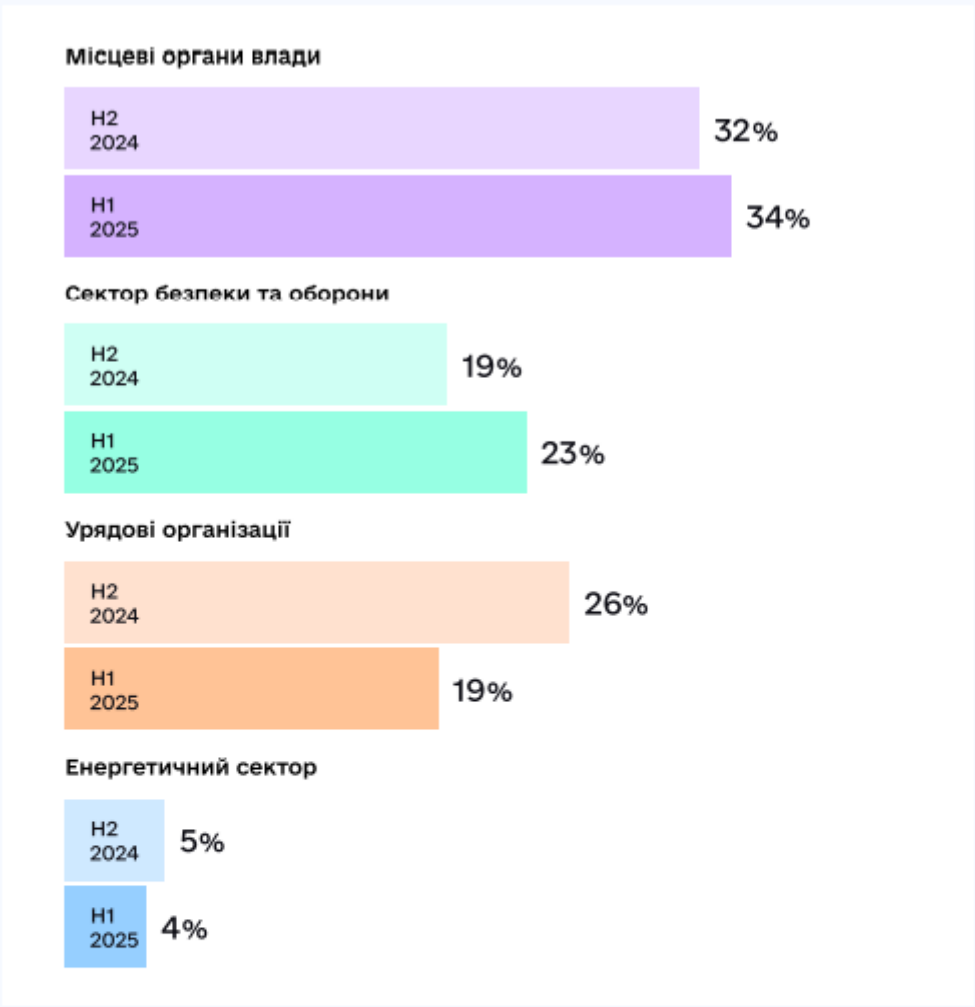
Перше півріччя 2025 року не стало винятком.

Безсумнівно, постійно збільшується видимість (можливість виявлення інфікувань), але водночас інтенсивність кібератак також зростає, і це має значний вплив на статистику, представлену далі.

Інциденти за рівнем критичності	H2 2024	H1 2025	Зміна за період
Критичні	1	1	0
Високі	10	6	-40%
Середні	2 454	2 944	+20%
Низькі	110	67	-39%
Загалом	**2 575**	**3 018**	**+17%**

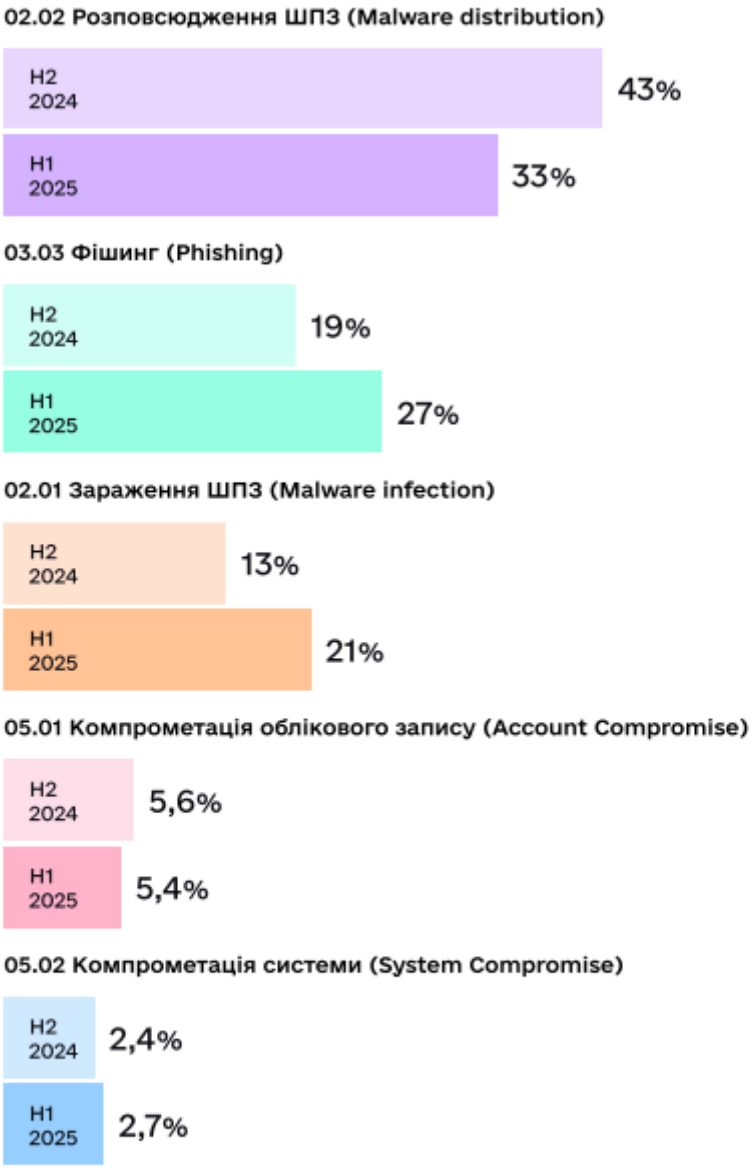
Як і раніше, топцілями ворога є об'єкти, де циркулює найбільше інформації, яку вони можуть використати у воєнних діях, або надаються сервіси, зупинка яких матиме значний вплив на безпеку та добробут цивільного населення.

Якщо поглянути на відсоткове співвідношення кібератак на конкретний сектор до загальної кількості атак, то спостерігається незначна зміна фокусу проросійських хакерів, але при цьому топ залишається незмінним.



Якщо брати до уваги типи кіберінцидентів, то можемо констатувати факт, що зміни тактик, технік і процедур під час розповсюдження шкідливого програмного забезпечення, на жаль, мають позитивні результати для ворога. Проте кількість виявлених інфікованих систем водночас відповідає кількості нейтралізованих загроз.

Позитивним є те, що люди стали більш обізнаними в питаннях кібергігієни та дотримуються її принципів, про що свідчить майже незмінний відсоток кіберінцидентів типу «05.01 Компрометація облікового запису (Account compromise)», незважаючи на зростання інтенсивності фішингових атак.


02.02 Розповсюдження ШПЗ (Malware distribution)
H2 2024
43%
H1 2025
33%
03.03 Фішинг (Phishing)
H2 2024
19%
H1 2025
27%
02.01 Зараження ШПЗ (Malware infection)
H2 2024
13%
H1 2025
21%
05.01 Компрометація облікового запису (Account Compromise)
H2 2024
5,6%
H1 2025
5,4%
05.02 Компрометація системи (System Compromise)
H2 2024
2,4%
H1 2025
2,7%

Додаток Б

Позиція України в міжнародних індексах кібер- та інформаційної безпеки (за даними National Cyber Security Index)

NCSI

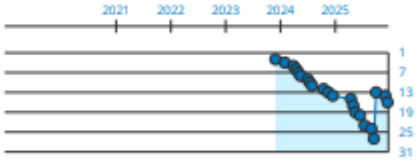
16. Ukraine 88.33

Population	37.7 million
Area (km²)	603.6 thousand
GDP per capita ($)	17.6 thousand

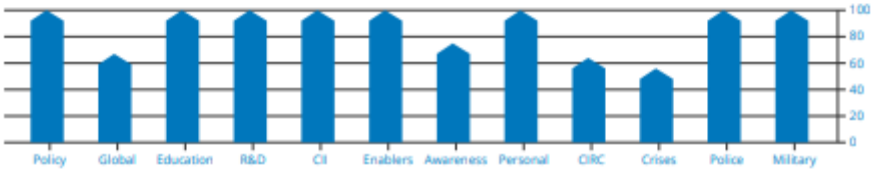
16th	National Cyber Security Index	88 %
N/A	Global Cybersecurity Index	84 %
30th	E-Government Development Index	88 %
43rd	Network Readiness Index	55 %

NCSI DEVELOPMENT TIMELINE

RANKING TIMELINE



NCSI FULFILMENT PERCENTAGE



STRATEGIC CYBERSECURITY INDICATORS

1. CYBERSECURITY POLICY	15	(100%)
1.1. High-level cybersecurity leadership	3	
1.2. Cybersecurity policy development	3	
1.3. Cybersecurity policy coordination	3	
1.4. National cybersecurity strategy	3	
1.5. National cybersecurity strategy action plan	3	
2. GLOBAL CYBERSECURITY CONTRIBUTION	4 / 6	(67%)
2.1. Cyber diplomacy engagements	3	
2.2. Commitment to international law in cyberspace	1	
2.3. Contribution to international capacity building in cybersecurity	0 / 2	
3. EDUCATION AND PROFESSIONAL DEVELOPMENT	10	(100%)
3.1. Cyber safety competencies in primary education	2	
3.2. Cyber safety competencies in secondary education	2	
3.3. Undergraduate cybersecurity education	2	
3.4. Graduate cybersecurity education	3	
3.5. Association of cybersecurity professionals	1	
4. CYBERSECURITY RESEARCH AND DEVELOPMENT	4	(100%)
4.1. Cybersecurity research and development programmes	2	
4.2. Cybersecurity doctoral studies	2	

PREVENTIVE CYBERSECURITY INDICATORS

5. CYBERSECURITY OF CRITICAL INFORMATION INFRASTRUCTURE	12	(100%)
5.1. Identification of critical information infrastructure	3	
5.2. Cybersecurity requirements for operators of critical information infrastructure	3	
5.3. Cybersecurity requirements for public sector organisations	3	
5.4. Competent supervisory authority	3	
6. CYBERSECURITY OF DIGITAL ENABLERS	12	(100%)
6.1. Secure electronic identification	2	
6.2. Electronic signature	2	
6.3. Trust services	2	
6.4. Supervisory authority for trust services	2	
6.5. Cybersecurity requirements for cloud services	2	
6.6. Supply chain cybersecurity	2	
7. CYBER THREAT ANALYSIS AND AWARENESS RAISING	9/12	(75%)
7.1. Cyber threat analysis	3	
7.2. Public cyber threat reports	3	
7.3. Public cybersecurity awareness resources	3	
7.4. Cybersecurity awareness raising coordination	0/3	
8. PROTECTION OF PERSONAL DATA	4	(100%)
8.1. Personal data protection legislation	2	
8.2. Personal data protection authority	2	

RESPONSIVE CYBERSECURITY INDICATORS

9. CYBER INCIDENT RESPONSE	9/14	(64%)
9.1. National incident response capacity	3	
9.2. Incident reporting obligations	3	
9.3. Cyber incident reporting tool	0/2	
9.4. Single point of contact for international cooperation	0/3	
9.5. Participation in international incident response cooperation	3	
10. CYBER CRISIS MANAGEMENT	5/9	(56%)
10.1. Cyber crisis management plan	0/2	
10.2. National cyber crisis management exercises	3	
10.3. Participation in international cyber crisis exercises	2	
10.4. Operational crisis reserve	0/2	
11. FIGHT AGAINST CYBERCRIME	16	(100%)
11.1. Cybercrime offences in national law	3	
11.2. Procedural law provisions	3	
11.3. Ratification of or accession to the Convention on Cybercrime	2	
11.4. Cybercrime investigation capacity	3	
11.5. Digital forensics capacity	2	
11.6. 24/7 contact point for international cybercrime	3	
12. MILITARY CYBER DEFENCE	6	(100%)
12.1. Military cyber defence capacity	2	
12.2. Military cyber doctrine	2	
12.3. Military cyber defence exercises	2	

Додаток В

Витяг із річного звіту системи виявлення вразливостей і реагування на кіберінциденти та кібератаки за 2024 рік


СТАТИСТИКА МОНІТОРИНГУ
КІЛЬКІСНІ ПОКАЗНИКИ ЗІБРАНИХ ТА ОПРАЦЬОВАНИХ ДАНИХ
За допомогою системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було оброблено сотні мільярдів подій телеметрії та зафіксовано майже 3 мільйони подій інформаційної безпеки.
Основними джерелами даних є засоби захисту ІКС об'єктів кіберзахисту, а саме: інструменти для виявлення загроз у мережі (NDR) - сенсори підсистеми збору телеметрії, інструменти для аналізу даних із робочих станцій та серверів (EDR) - сенсори підсистеми захисту кінцевих точок, а також дані розвідки загроз щодо скомпрометованих облікових записів та інших індикаторів компрометації (TI).
NDR
EDR
ASM
TI
~2.95 МЛН
Подій безпеки
Виявлено та опрацьовано подій інформаційної безпеки засобами платформи SIEM та SOAR
1.9 МЛН
Info & Low
509 ТИС
Medium
436 ТИС
High
28 ТИС
Critical
ПРИМІТКА
Варто зауважити, що показники моніторингу суттєво відрізняються порівняно з минулим роком, оскільки в системі було здійснено модернізацію засобів збору мережевої телеметрії, а також впроваджено SOAR систему та застосовано генеративний штучний інтелект для автоматизації виявлення та опрацювання потенційних кіберінцидентів та кібератак. Це дозволило знизити навантаження на SIEM систему та аналітиків ОЦРК, проте кількість виявлених кіберінцидентів та кібератак залишається майже на тому ж рівні, що й минулого року.
2024
9

СТАТИСТИКА МОНІТОРИНГУ

КІЛЬКІСНІ ПОКАЗНИКИ ЗІБРАНИХ ТА ОПРАЦЬОВАНИХ ДАНИХ

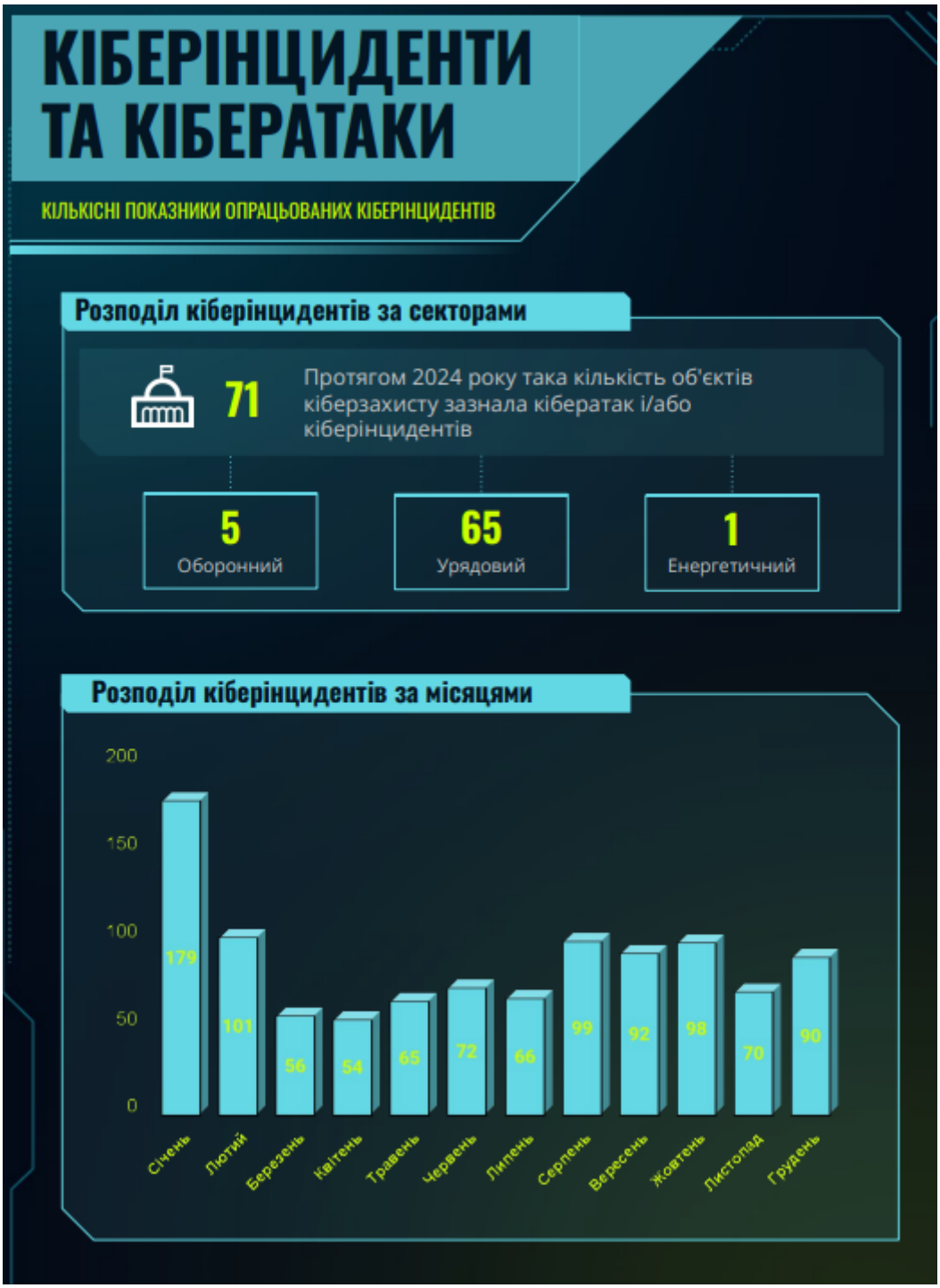
- Статистика представлена згідно з Переліком категорій кіберінцидентів, схваленим Національним координаційним центром кібербезпеки при Раді національної безпеки та оборони України

Серед виявлених подій інформаційної безпеки основну частину, а саме 58.8%, становлять події, пов'язані зі шкідливим програмним кодом (Malicious Code). Спроби втручання (Intrusion Attempts) займають 17,6%, тоді як збір інформації зловмисником (Information Gathering) становить 12,1%. Інші події (Other) складають 8,3%, порушення властивостей інформації (Information Content Security) та порушення доступності (Availability) займають 2,7% та 0,5% відповідно.

Ці дані про типи подій, що були опрацьовані ОЦРК протягом звітного періоду, допомагають визначити пріоритетні напрямки для посилення заходів кіберзахисту.

2024

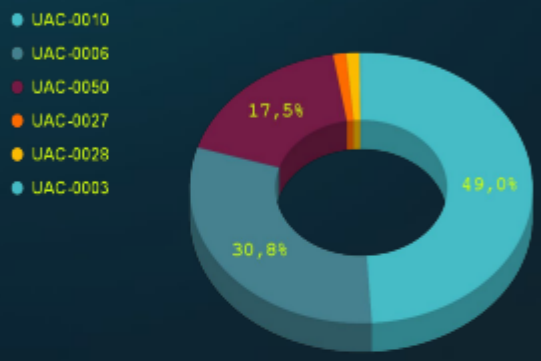

КІБЕРІНЦИДЕНТИ ТА КІБЕРАТАКИ
КІЛЬКІСНІ ПОКАЗНИКИ ОПРАЦЬОВАНИХ КІБЕРІНЦИДЕНТІВ
Розподіл за типами джерел
1042
Протягом 2024 року аналітиками ОЦРК зареєстровано та опрацьовано кіберінцидентів
249
EDR
739
NDR
54
TI
Розподіл за типами кіберінцидентів
02.04 407
02.01 352
03.03 94
02.02 86
05.01 77
01.01 12
05.02 9
04.01 2
07.01 2
09.01 1
1
5
10
50
100
Понад 90% опрацьованих кіберінцидентів стосуються організацій урядового сектору.
За класифікацією, найбільше кіберінцидентів належать до типу «02.04 Шкідливе підключення» – спроби з'єднання від/до URL або IP-адреси, пов'язаної з відомим ШПЗ, наприклад C&C, або ресурсом розповсюдження компонентів, пов'язаних з активністю певної бот-мережі.
2024
12


КІБЕРІНЦИДЕНТИ ТА КІБЕРАТАКИ
КІЛЬКІСНІ ПОКАЗНИКИ ОПРАЦЬОВАНИХ КІБЕРІНЦИДЕНТІВ
Розподіл кіберінцидентів за секторами
71
Протягом 2024 року така кількість об'єктів кіберзахисту зазнала кібератак і/або кіберінцидентів
5
Оборонний
65
Урядовий
1
Енергетичний
Розподіл кіберінцидентів за місяцями
200
150
100
50
0
179
101
56
54
65
72
66
99
92
98
70
90
Січень
Лютий
Березень
Квітень
Травень
Червень
Липень
Серпень
Вересень
Жовтень
Листопад
Грудень

КІБЕРЗАГРОЗИ

КІЛЬКІСНІ ПОКАЗНИКИ КІБЕРЗАГРОЗ

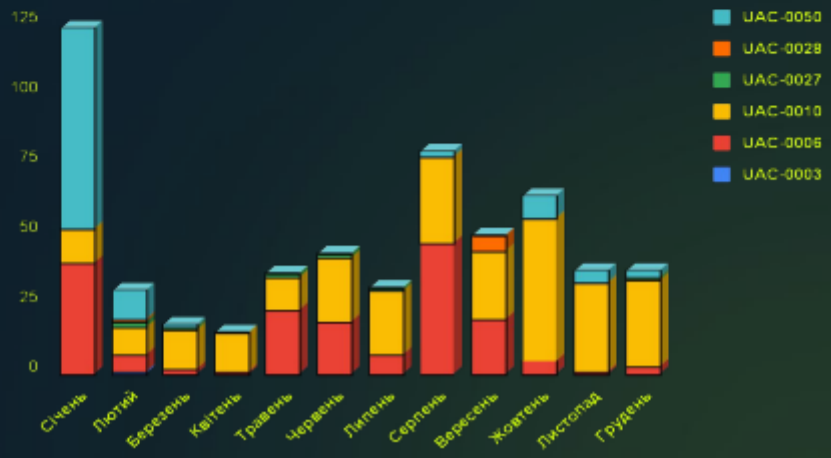
Розподіл кіберінцидентів



Найактивнішими кластерами кіберзагроз, які були виявлені Оперативним центром реагування на кіберінциденти, у 2024 році стали **UAC-0010**, **UAC-0006** та **UAC-0050** (за класифікацією CERT-UA).

Основним початковим вектором кібератак було розповсюдження ШПЗ засобами електронної пошти – **T1566.001** Phishing: Spearphishing Attachment (за класифікацією MITRE ATT&CK).

Часовий розподіл кіберінцидентів, що були атрибутовані до кіберзагроз



2024