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: **«Концептуальні засади забезпечення інформаційної безпеки МВС України»**

Виконав: здобувач 2 курсу 4 групи
Спеціальність: 281 «Публічне управління та адміністрування»

Оніщук Павло Сергійович
Індивідуальний навчальний план №14-77
Мобільний телефон: +380 66-445-71-04

Науковий керівник:
старший викладач кафедри,
кандидат юридичних наук
Пустовий Олександр Олександрович
(підпис)

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

Київ 2025

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: **«Концептуальні засади забезпечення інформаційної безпеки МВС України»**

Виконав: здобувач 2 курсу 4 групи
Спеціальність: 281 «Публічне управління та адміністрування»

Оніщук Павло Сергійович
Індивідуальний навчальний план №
Мобільний телефон**:** +380 66-445-71-04

Науковий керівник:
старший викладач кафедри,
кандидат юридичних наук
Пустовий Олександр Олександрович _____
(підпис)

Кваліфікаційна робота допущена до захисту
«____» _____20____р., протокол № ____
завідувач кафедри, доктор філософії в галузі
права, доцент
_____ Владислав ШКОЛЬНІКОВ

Київ 2025

ЗМІСТ

ВСТУП

Актуальність теми. В сучасному світі загрози, які існують в сфері інформаційної безпеки (ІБ) стрімко ускладнюються в умовах глобальної цифрової трансформації. Практично всі сфери життя переходять в цифровий формат, що робить суспільство вразливішим до кібератак і інформаційних впливів. Одночасно зростає кількість цілеспрямованих інформаційних впливів від дезінформації в соціальних мережах до масштабних пропагандистських кампаній, покликаних маніпулювати громадською думкою. Інформаційні атаки нині розглядаються як серйозна небезпека, що здатна ставити під загрозу національну безпеку держави, адже стратегічні противники використовують відкритість і цифрову взаємопов'язаність сучасних демократичних суспільств для підриву їхньої стабільності.

В умовах еволюції загроз особливої ваги набуває дослідження концептуальних засад інформаційної безпеки. Науковці відзначають, що державна політика у зазначеній сфері потребує чіткої науково обґрунтованої основи – єдиної концепції, яка об'єднує національні цілі, інтереси і цінності та визначає стратегію і тактику захисту інформаційного простору. Лише на основі цілісних концепцій можна розробити ефективні механізми протидії сучасним загрозам, впровадити новітні технології захисту і вдосконалити нормативно-правове регулювання. Іншими словами, актуальність дослідження концептуальних засад інформаційної безпеки зумовлена необхідністю випереджати дії ворога – мати наперед вироблені стратегії реагування на новітні інформаційні атаки.

Зазначені фактори визначають актуальність наукового дослідження, орієнтованого на аналіз та перспективу удосконалення концептуальних засад інформаційної безпеки МВС України. Розв'язання цих завдань сприятиме розробці ефективної моделі цифрової трансформації відповідно до світових тенденцій, державних стратегічних документів і політики безпеки.

Мета дослідження полягає у комплексному теоретико-правовому та прикладному обґрунтуванні концептуальних засад інформаційної безпеки України з урахуванням цифрової трансформації суспільства та потреб інтеграції цифрової складової в систему національної безпеки.

Для досягнення мети в передбачається виконання таких завдань:

– окреслити теоретико-методологічні підходи до ІБ МВС України;

– визначити зміст та структуру поняття інформаційна безпека в українському законодавстві та науковому дискурсі;

– проаналізувати чинну нормативно-правову базу у сфері ІБ;

– охарактеризувати інституційну структуру органів забезпечення ІБ;

– висвітлити ключові проблеми та виклики забезпечення інформаційної безпеки України в сучасних умовах;

– визначити шляхи удосконалення механізмів безпеки в інформаційній сфері.

Об’єкт дослідження – система забезпечення інформаційної безпеки МВС України як складової національної безпеки в умовах зовнішніх загроз, цифрової трансформації та правового реформування.

Предмет дослідження – концептуальні засади та механізм реалізації ІБ МВС України.

Наукова новизна отриманих результатів полягає у науковому обґрунтуванні та удосконаленні концептуальних засад інформаційної безпеки МВС України в умовах цифровізації сучасного суспільства в контексті війни; розробці авторської структурно-функціональної моделі механізму забезпечення інформаційної безпеки України, як інтегрованого комплексу інструментів, зорієнтованого на повний цикл управління ризиками.

Методологічну основу дослідження становлять системний, порівняльно-правовий, структурно-функціональний і прогностичний методи, метод контент-аналізу, аналіз нормативно-правових актів, а також аналіз кращих міжнародних практик у сфері забезпечення інформаційної безпеки. Дослідження ґрунтується

на положеннях теорії публічного адміністрування, інституційного аналізу, концепції цифрової трансформації та сучасного державного управління.

Практичне значення результатів полягає у можливості використання отриманих висновків та рекомендацій для підготовки стратегічних документів та програм; розроблення прикладних рішень і пілотних проєктів в сфері ІБ; оптимізації організаційної структури та підвищення ефективності діяльності підрозділів МВС України.

Апробація результатів може бути здійснена під час участі в науково-практичних конференціях, круглих столах та семінарах з питань публічного управління, цифрових трансформацій концептуальних засад ІБ.

Таким чином, обрана тема відповідає сучасним потребам публічного управління, характеризується високою практичною значущістю і відкриває можливості для впровадження новітніх технологічних рішень, що є актуальним у контексті євроінтеграційного курсу держави, необхідності посилення спроможності правоохоронних органів і формування безпечного цифрового середовища.

РОЗДІЛ І

ТЕОРЕТИЧНІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МВС УКРАЇНИ

1.1. Теоретико-концептуальні підходи до визначення поняття та механізму інформаційної безпеки

В сучасній державі в усіх сферах життєдіяльності дедалі виразніше проявляються нові типи загроз і ризиків, зумовлені стрімким прогресом інформаційно-комунікаційних технологій. Вони реалізуються, зокрема, у формах спотворення змісту інформації, маніпулювання масовою свідомістю, ведення інформаційних війн та інших деструктивних інформаційних впливів. Сформований унаслідок глобалізаційних процесів світовий інформаційний простір дедалі більше набуває рис простору конфронтації та змагання між державами. Прискорене впровадження цифрових технологій спричинило суттєву трансформацію ціннісних орієнтацій, що, своєю чергою, поглибило глобальну ціннісну кризу сучасного суспільства.

В умовах інформаційного суспільства розвиток держави значною мірою спирається на продукування, накопичення та використання науково-технічної й іншої суспільно значущої інформації. Кодифікація знань, інноваційний і технологічний поступ виступають базовими детермінантами соціального прогресу. Як наслідок, економічні процеси, культурний розвиток, формування масової свідомості та суспільної психології відбуваються в ситуації домінування технологічних чинників.

В умовах інтенсивної цифровізації зростає значення системного захисту інформаційних процесів як у технічному, так і в соціально-нормативному вимірах. Це актуалізує філософсько-аксіологічний аналіз цифрової трансформації, насамперед її впливу на структуру цінностей, механізми соціальної довіри та критерії суспільної стійкості [74]. Відтак постає завдання визначити базові цінності, які мають виконувати функцію стратегічних

орієнтирів розвитку й водночас слугувати нормативною основою формування відповідальної інформаційної поведінки індивіда та спільноти.

У концептуальному вимірі інформаційна безпека постає як частина національної безпеки, яка відображає рівень стійкості інформаційного середовища та здатність держави зменшити руйнівні впливи, які здатні змінити структуру цінностей, моделі прийняття рішень і механізми соціальної довіри. Відповідно, актуалізується дослідження поняття інформаційна безпека, що дає змогу виокремити його ключові ознаки та межі застосування [53].

Зокрема, І. О. Громика та Т. І. Саханчук трактують ІБ як «захист державних інтересів в інформаційній сфері, що включає запобігання, виявлення та нейтралізацію внутрішніх і зовнішніх інформаційних небезпек і загроз, забезпечення інформаційного суверенітету держави, а також створення умов для безпечного розвитку міжнародного інформаційного співробітництва» [35, с. 130–134].

Л. С. Харченко визначає інформаційну безпеку як «елемент системи національної безпеки та як діяльність із керування ризиками й загрозами, що здійснюється суб’єктами публічної влади, інституціями громадянського суспільства й окремими громадянами з метою гарантування інформаційного суверенітету держави» [88, с. 65].

Натомість Б. А. Кормич пропонує розуміти ІБ як «режим охорони встановлених законом правил функціонування інформаційних процесів у державі, за якого гарантуються закріплені Конституцією умови існування й розвитку людини, суспільства та держави загалом» [44, с. 89].

Вартим уваги є підхід С. С. Єсімова, який підкреслює, що «інститут інформаційної безпеки в межах інформаційного права реалізується через комплекс правових, організаційних і технічних заходів, спрямованих на захист інформаційно-комунікаційного комплексу держави» [39, с. 75]. У складі такого комплексу автор виокремлює «інформаційні ресурси та інформаційні системи, інформаційно-комунікаційну інфраструктуру, науково-технічний і виробничий сегменти інформаційної індустрії, ринок інформаційних продуктів і послуг, а

також освітньо-просвітницький напрям і професійну підготовку кадрів» [39, с. 75].

Отже, інформаційну безпеку доцільно інтерпретувати не як набір ізольованих технічних процедур, а як інтегрований право-управлінський режим охорони національних інтересів. Його зміст охоплює управління ризиками: виявлення та оцінювання загроз, їх попередження, реагування та мінімізацію наслідків, а також орієнтує державну політику на превенцію й підвищення стійкості. У цій логіці «інформаційний суверенітет» виступає стратегічним критерієм, що означає збереження спроможності держави автономно визначати правила функціонування національного інформаційного простору та забезпечувати захист критично важливих інформаційних ресурсів.

Важливим є також наголос Н. С. Мороз на «динамічному характері інформаційної безпеки» [61, с. 136]. Дослідниця пов’язує її зміст із «забезпеченням стабільності та розвитку інформаційної сфери, яка зазнає постійних змін під впливом різноманітних потреб учасників інформаційних правовідносин» [61, с. 136]. Домінантним у літературі є розуміння інформаційної безпеки як стану стійкості та захищеності інформаційної сфери держави, який підтримує безперервність функціонування, керованість і розвиток інформаційних ресурсів та систем.

Узагальнюючи наведені позиції, вважаємо за доцільне погодитися з думкою І. І. Недохлєбова, який запропонував таке бачення поняття «інформаційна безпека»: «комплекс технічних, правових, організаційних та етичних заходів, спрямованих на захист інформаційних систем та інформації від несанкціонованого доступу, неправомірного використання, розголошення, модифікації чи знищення, що в сукупності забезпечує збереження цілісності, конфіденційності та доступності інформації» [65, с. 25].

Важливим є також уточнення змісту категорії «забезпечення», оскільки саме вона задає діяльнісну логіку аналізу: йдеться не про декларацію бажаного стану, а про організований процес досягнення визначеного результату. Сучасні дослідники трактують це поняття дещо широко, підкреслюючи його практичний

вимір. Однак, В. А. Предборський зазначає, що «забезпечення безпеки постає як специфічний соціальний феномен, пов'язаний із подоланням суперечностей між об'єктивно існуючою небезпекою та потребами людини, соціальної групи, соціуму та держави в її попередженні, локалізації та обмеженні» [78, с. 391]. У цьому контексті об'єктом такої діяльності виступають суспільні відносини й процеси, на які спрямовані безпекові впливи, тоді як предмет охоплює конкретизовані типи загроз та пов'язані з ними чинники, умови й ресурси, що визначають способи їх попередження та нейтралізації.

Слід зазначити, що О. О. Тихомиров запропонував підходити до забезпечення інформаційної безпеки як до «специфічного виду діяльності, у якій провідну роль відіграє держава». При цьому сутність державного забезпечення, на його думку, доцільно розуміти «як систему державних гарантій в інформаційній сфері, безпосередньо чи опосередковано закріплених у фундаментальних нормативно-правових актах, що регулюють інформаційні суспільні відносини» [87, с. 196].

Своє бачення розуміння вказаної категорії мають ряд дослідників: В. А. Ліпкан, В. М. Желіховський та Ю. Є. Максименко, спираючись на практико-орієнтований підхід, тлумачать забезпечення інформаційної безпеки держави як «результат свідомої й цілеспрямованої діяльності органів державного управління, спрямованої на недопущення порушення їхнього належного функціонування під впливом інформаційних загроз і небезпек» [56, с. 280].

Водночас важливою є позиція Т. С. Перун, згідно з якою «забезпечення інформаційної безпеки слід розглядати як складний соціально-правовий механізм формування та реалізації державної політики, зорієнтованої на створення й підтримання належного рівня захищеності об'єктів безпеки шляхом упровадження нормативно-правових, організаційних, управлінських та інших заходів, у тому числі таких, що відповідають характеру загроз життєво важливим інтересам особи, суспільства й держави в інформаційній сфері» [75, с. 268].

Спираючись на підхід В. А. Ліпкана, Ю. Є. Максименка та В. М. Желіховського, «систему забезпечення інформаційної безпеки доцільно

визначати як сукупність інформаційно-аналітичних, теоретико-методологічних, адміністративно-правових, організаційно-управлінських, спеціальних та інших заходів, спрямованих на забезпечення стійкого розвитку об’єктів інформаційної безпеки, а також інфраструктури її забезпечення» [56, с. 158]. Таке розуміння акцентує функціонально-діяльнісну природу системи, тобто її інструментарій і спрямованість на досягнення результату.

Натомість А. Ю. Нашинець-Наумова розкриває систему забезпечення безпеки через структурний підхід, визначаючи її як «внутрішню структуру, впорядковану сукупність, єдність і взаємозв’язок її елементів» [64, с. 31]. У сукупності ці підходи дають підстави трактувати систему забезпечення ІБ як сукупність взаємопов’язаних елементів і як комплекс заходів, що реалізуються для підтримання стійкості відповідних об’єктів та інфраструктури.

Отже, систему забезпечення інформаційної безпеки слід розуміти як відносно самостійну цілісність, що охоплює сукупність взаємопов’язаних елементів і функціонує у взаємодії із зовнішнім середовищем. Натомість механізм характеризує внутрішню організацію цієї системи, тобто набір інструментів, засобів і процедур, через які реалізуються її цілі та досягається заданий рівень захищеності.

Різноманіття наукових підходів породжує множинність моделей механізму її забезпечення. У цьому контексті інформаційну безпеку доречно визначити як інтегрований комплекс нормативних, організаційних, фінансових, інформаційно-технічних і соціальних засобів, з допомогою яких відбувається попередження, локалізація та нейтралізація актуальних і потенційних загроз інформації та інформаційним системам. Важливо підкреслити, що зазначений механізм не зводиться до технічних заходів запобігання несанкціонованому доступу чи втручанню в інформаційні ресурси. Його зміст охоплює також формування та впровадження стратегій управління ризиками, розвиток культури безпечної поведінки користувачів, а також удосконалення нормативно-правового регулювання відповідних відносин [28; 95].

Таким чином, сучасні процеси цифровізації та глобалізації формують якісно нове середовище ризиків, у якому інформаційний простір набуває ознак сфери міждержавної конкуренції та цілеспрямованих деструктивних впливів. У цих умовах інформаційна безпека концептуалізується не лише як стан захищеності інформаційної сфери, а як динамічний управлінсько-правовий процес мінімізації загроз і ризиків, пов'язаний із підтриманням соціальної довіри, стійкості та ціннісних засад розвитку. Аналіз доктринальних підходів засвідчує домінування інтегрованого розуміння інформаційної безпеки як сукупність правових, організаційних, технічних і соціальних компонентів, що забезпечують режим охорони національних інтересів та реалізацію інформаційного суверенітету. Відповідно, засади інформаційної безпеки постають як цілеспрямована діяльність держави й інших суб'єктів, інституційно оформлена у вигляді системи та механізму, які містять інструменти превенції, реагування і розвитку резильєнтності. З огляду на це подальший аналіз має бути зорієнтований на конкретизацію елементів системи, їх функцій та критеріїв ефективності в умовах гібридних загроз.

1.2. Інформаційна безпека в структурі національної безпеки України: принципи та функції

Розгляд концептуальних засад інформаційної безпеки потребує визначення її місця, принципів і функцій у системі державної безпеки України. Передумовою такого аналізу є уточнення змісту категорії «безпека», яка в етимологічному та філософському вимірах постає як необхідна умова стабільного існування й розвитку суспільства, держави та особи. У цьому контексті інформаційна безпека може бути інтерпретована як конкретизація загальної ідеї безпеки у сфері інформаційних відносин, де об'єктом захисту виступають інформаційні ресурси, процеси та інфраструктура, а також пов'язані з ними права й законні інтереси суб'єктів.

Збройна агресія Російської Федерації проти України, що супроводжується системним і масштабним інформаційним впливом, зумовила необхідність

перегляду національних уявлень і підходів до безпеки. З початком повномасштабної фази війни інформаційний простір остаточно утвердився як сфера застосування ідеологічної зброї, що істотно посилило актуальність зазначеної проблематики. Унаслідок цього інформаційна безпека стала одним із пріоритетних напрямів державної політики та предмет інтенсивних наукових досліджень.

Науковці визначають безпеку у межах різних методологічних підходів. Так, І. В. Пивовар та С. П. Драчук інтерпретують її як «динамічний процес і водночас як фундаментальну потребу», підкреслюючи, що безпека виступає цінністю, критерієм суспільного розвитку та методологією оцінки рівня захищеності соціальної системи [77, с. 80]. Інший підхід репрезентує В. Пасічник, який розуміє безпеку як «певний стан суспільних відносин – стан захищеності ключових цінностей та інтересів від загроз, за якого гарантуються оптимальні умови життєдіяльності, розвитку та самореалізації особи й соціальних спільнот» [74, с. 68]. У підсумку безпека постає як спроможність держави й суспільства мінімізувати загрози національним інтересам, особливо в інформаційному вимірі.

Узагальнення наведених позицій дає підстави стверджувати, що центральним у всіх підходах залишається уявлення про безпеку як про стан захищеності відповідних суб’єктів, тоді як філософський вимір акцентує: «безпека проявляється у збереженні й охороні суспільно визнаних цінностей, ідей та норм» [55].

У межах такого підходу інформаційна безпека набуває значення специфічної форми забезпечення захищеності. Зокрема, Л. Кочубей пов’язує її з «можливістю реалізації конституційних прав людини й суспільства на отримання, створення та поширення інформації» [46, с. 222]. Натомість Б. А. Кормич акцентує увагу на «захищеності правових норм, які регулюють та забезпечують конституційно закріплені умови існування й розвитку людини» [44, с. 267]. На думку Л. С. Харченко, Н. А. Ліпкана та О. В. Логінової, інформаційну безпеку слід розглядати як «складову державної безпеки, що

здійснюється державними й недержавними інституціями з метою забезпечня суверенітету України» [88, с. 75]. Різноспрямованість цих підходів свідчить про наявність як теоретичних, так і практичних труднощів у визначенні походження поняття ІБ.

У більш ширшому ракурсі інформаційну безпеку слід розглядати як концептуально-нормативну основу функціонування національної інформаційної системи: вона визначає рамки реалізації права особи на інформацію та задає інструменти охорони національних інтересів в інформаційній сфері. У цьому сенсі К. Захарченко пов’язує ІБ з «підтриманням національно-культурного розвитку спільноти й захистом державного суверенітету», підкреслюючи роль державної інформаційної політики та законодавчих гарантій інформаційної свободи і доступу громадян до суспільно значущої інформації [40, с. 11].

Нормативне закріплення відповідного підходу містить «Стратегія інформаційної безпеки України, затверджена Указом Президента України від 28 грудня 2021 року № 685/2021» [17]. У Стратегії, інформаційну безпеку визначено як «складову національної безпеки, що описує стан захищеності інтересів держави та громадян, за якого належно гарантуються конституційні права, підтримується доступ до достовірної й об’єктивної інформації та забезпечується дієва протидія негативним інформаційним впливам (зокрема скоординованій дезінформації й пропаганді), а також порушенням режимів допуску до інформації з обмеженим доступом» [17].

У підсумку інформаційну безпеку доцільно трактувати як складову національної безпеки, що відображає рівень гарантованості інтересів ключових учасників інформаційних відносин у межах інформаційної сфери. Досягнення такого рівня забезпечується узгодженим застосуванням правових, організаційних та інформаційно-технічних інструментів захисту, які реалізуються уповноваженими органами влади у взаємодії з громадянським суспільством в межах відповідних інформаційних процесів [17; 15].

Окремого теоретичного опрацювання потребує проблема принципів інформаційної безпеки, оскільки саме вони фіксують ключові орієнтири побудови відповідної системи.

Принципи інформаційної безпеки слід формулювати на основі чинного законодавства та загальних засад правового регулювання інформаційних відносин. Водночас у доктринальному вимірі до базових універсальних принципів можна віднести:

– принцип усвідомленої добровільності;

– принцип конфіденційності, що передбачає належний захист інформації;

– принцип обґрунтованості захисту інформації, за яким запроваджувані заходи мають відповідати реальному рівню загроз і не бути надмірними;

– принцип своєчасності, орієнтований на оперативне реагування на ризики й загрози;

– принцип прогнозування, пов’язаний із завчасним виявленням потенційних загроз та розробленням превентивних заходів [25, с. 130–132].

Проте у чинній «Стратегії» [17] принципи інформаційної безпеки як самостійна категорія прямо не визначені, що слід розглядати як істотну прогалину цього документа. Відсутність чіткого переліку принципів ускладнює формування єдиних стандартів практичної діяльності та уніфікацію безпекових підходів в інформаційній сфері.

Узагальнюючи викладене, можна запропонувати кілька положень. По-перше, принципи інформаційної безпеки доцільно аналізувати крізь призму діяльності, тобто як орієнтири спеціалізованої активності уповноважених суб’єктів: саме цілеспрямовані дії державних і недержавних інституцій формують реальний рівень захищеності національних інтересів в інформаційній сфері. По-друге, зміст принципів інформаційної безпеки невід’ємно пов’язаний з ідеологічними засадами інформаційної діяльності: вони визначають ціннісний

вектор правового регулювання процесів задоволення інформаційних потреб, окреслюють межі допустимого втручання та встановлюють стандарти захисту. По-третє, зведення принципів виключно до декларативних положень, що описують бажаний стан інформаційної безпеки, істотно обмежує їхній функціональний потенціал. Лише в межах діяльнісного, «забезпечувального» підходу повною мірою розкривається їхня соціальна спрямованість, цілісність і роль у формуванні ефективної системи захисту [57].

Принципи інформаційної безпеки мають відносно сталий характер, оскільки фіксують фундаментальні світоглядні та правові орієнтири безпекової діяльності, які не залежать від ситуативних коливань конкретних загроз. Натомість динамічним компонентом виступає система конкретних заходів та організаційна структура інституційного механізму: їхній зміст, інструментарій і форми діяльності можуть удосконалюватися й адаптуватися до змін інформаційного простору та появи нових загроз [71, с. 74].

Зазвичай, досліджують функції інформаційної безпеки нерідко у взаємозв’язку з функціями національної безпеки як більш загальної категорії. Зокрема, О. Джураєва наголошує, що «будь-яка загроза, спрямована проти суспільства, автоматично набуває характеру загрози національній безпеці», що дозволяє подолати уявлення про виключно військовий або силовий характер національної безпеки [36, с. 9]. Слід зазначити, що забезпечення національної безпеки є однією з основоположних функцій держави, зміст якої полягає у створенні умов захищеності різних об’єктів безпеки за наявності негативних тенденцій або формування потенційних чи реальних загроз національним інтересам [49, с. 65].

З огляду на співвідношення національної та інформаційної безпеки до ключових завдань держави слід віднести:

– забезпечення державного суверенітету та територіальної цілісності;

– гарантування сталого розвитку громадянського суспільства і держави, підвищення рівня та якості життя населення;

– інтеграцію України до європейського політичного, безпекового й правового простору [8].

Разом із тим функції інформаційної безпеки не можуть бути повністю ототожнені з функціями національної безпеки. Їх доцільно аналізувати як відносно самостійні елементи єдиної системи з урахуванням притаманної їм дворівневої природи.

Зокрема, пропонуємо виділити такі функції інформаційної безпеки: «формування та підтримання діяльності державних і недержавних інституцій у сфері захисту інформації; цілеспрямований вплив суб'єктів управління на джерела та канали загроз; визначення, ієрархізація й захист інтересів органів публічної влади в інформаційній сфері; розвиток міжнародного співробітництва щодо захисту національних інтересів; розбудова нормативно-правового забезпечення інформаційних відносин» [90, с. 138].

Щодо структурної організації національної безпеки О. Андрєєва підкреслює, що виокремлення її складових було зумовлено загостренням глобальних проблем у другій половині XX ст., появою якісно нових загроз, пов'язаних із розвитком сучасних комунікаційних технологій, а також необхідністю гарантування реалізації конституційних прав і свобод людини у сфері доступу до інформації, її отримання, зберігання й обміну [23, с. 136].

Таким чином, окремі компоненти національної безпеки виокремлюються залежно від специфіки загроз. Схожого підходу дотримується О. Мотайло, який характеризує національну безпеку як «складний, системний феномен, що постає у вигляді сукупності взаємопов'язаних елементів та охоплює комплекс концептуальних положень, соціально-політичних та правових інститутів, а також визначений набір засобів, методів і форм діяльності, спрямованих на протидію загрозам» [62, с. 292].

Водночас Л. Т. Рябовол наголошує, що центральною категорією є мета функціонування відповідної системи, у якій мають бути збалансовані як державні та і громадські інтереси [82, с. 29]. На думку дослідниці, визначальною ознакою такої системи є саме стан безпеки, тоді як забезпечення безпеки

можливе за умови збереження достатнього рівня стійкості до впливу негативних чинників, підтримання внутрішніх зв’язків між її елементами та здатності ефективно функціонувати для реалізації поставлених цілей [82, с. 29].

Інформаційну безпеку доцільно розглядати як базову частину національної безпеки. Зазначена позиція ґрунтується на тому, що інформація як соціально значущий ресурс впливає на ключові процеси функціонування держави й суспільства — від сфери публічного управління та оборони до економіки, культури й повсякденних комунікативних практик.

І. Р. Боднар виокремлює три ключові чинники, що зумовлюють необхідність належного функціонування ІБ:

– необхідність гарантування національної безпеки загалом;

– наявність специфічних загроз інформаційній сфері, здатних завдати істотної шкоди національним інтересам;

– можливість цілеспрямованого впливу інформації на свідомість і поведінку людей [28, с. 68–73].

У цьому контексті «інформаційна політика держави задає базові напрями діяльності органів влади в інформаційному секторі, а її зміст визначається національними інтересами держави, суспільства та особи» [45, с. 70]. Відтак інформаційний вимір національної безпеки спрямований на превенцію та нейтралізацію загроз через координацію і спрямування діяльності компетентних органів.

На нормативному рівні інформаційна складова відображена у Законі України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII [8]. Водночас Закон не містить розгорнутого переліку та змістовної характеристики концептуальних засад національної та інформаційної безпеки, що слід розглядати як прогалину загальносистемного рівня.

Натомість у стратегічних нормативно-правових документах інформаційний вимір національної безпеки конкретизується через систему пріоритетних цілей і завдань, яким відповідає визначений комплекс заходів. Так, у «Стратегії

національної безпеки України» [15] зазначено пріоритетні завдання, безпосередньо пов’язані з інформаційною сферою, зокрема:

- активну протидію кібератакам та іншій деструктивній пропаганді;
- забезпечення отримання повної, достовірної й своєчасної інформації;
- розвиток конкурентного середовища у медіасфері;
- гарантування кіберстійкості та кібербезпеки інформаційної інфраструктури;
- стимулювання інновацій і впровадження новітніх технологій, насамперед в інформаційній і телекомунікаційній сферах [15].

Особливе місце в системі стратегічних документів посідає «Стратегія інформаційної безпеки України». У ній інформаційну складову національної безпеки визначено як самостійний структурний елемент і наведено її дефініцію [17]. Важливо, що у «Стратегії інформаційна безпека» [17] розглядається також як функція держави, що полягає у:

- забезпеченні належного рівня захищеності національного інформаційного простору;
- підтриманні соціальної та політичної стабільності із застосуванням інформаційних засобів і механізмів впливу;
- гарантуванні прав кожного громадянина в інформаційній сфері [17].

Зазначимо, що , «інформаційна безпека являє собою незалежний компонент політики національної безпеки та має визначальне значення для збереження суверенітету та незалежності держави. Інформаційна компонента має виразний інтегруючий характер, оскільки вона є необхідною передумовою реалізації багатьох напрямів державної політики. Водночас інформаційні методи й технології активно використовуються в політичній, зовнішньополітичній та інших сферах як інструменти впливу, що додатково підкреслює пріоритетність інформаційної сфери при розв’язанні комплексу безпекових завдань» [67, с. 150].

Зміст інформаційної безпеки визначається необхідністю реагування на різноманітні за природою та походженням загрози. У цьому вимірі інформаційна

безпека об’єднує охоронні, регулятивні і контролюючі функції, реалізація яких передбачає виконання спеціально уповноваженими суб’єктами своїх повноважень. Тому інформаційну безпеку доцільно сприймати крізь призму специфічної діяльності суб’єктів різних рівнів, спрямованої на забезпечення національних інтересів в інформаційній сфері.

Підсумовуючі вказане зазначимо, що інформаційна безпека постає як комплексна, багаторівнева правова категорія, яка, з одного боку, є самостійною складовою національної безпеки, а з іншого — виконує інтегруючу функцію щодо інших аспектів національних інтересів держави, що мають визначальне значення для збереження її суверенітету.

Розмежування ідеологічно-цільового та організаційно-управлінського рівнів розуміння інформаційної безпеки дає змогу чіткіше окреслити її функціональне наповнення. На першому рівні інформаційна безпека відображає базові ціннісні орієнтири, цілі та принципи, на яких ґрунтується діяльність держави й суспільства в цій сфері. На другому рівні вона проявляється як специфічна сфера державного управління, що передбачає реалізацію охоронних, регулятивних і контрольних функцій, спрямованих на попередження, локалізацію та нейтралізацію загроз. Саме через діяльність уповноважених суб’єктів забезпечується досягнення належного стану захищеності національних інтересів.

Отже, поняття «безпека» фіксує стан захищеності та ціннісно-нормативні орієнтири розвитку соціальної системи, а інформаційна безпека постає як її конкретизація у сфері інформаційних відносин [74]. Доктринальні підходи демонструють багатоаспектність феномена ІБ: від інформаційних прав і охорони норм до забезпечення інформаційного суверенітету та протидії деструктивним впливам. Нормативна дефініція, підкреслює її статус як складової національної безпеки та орієнтує державну політику на захист суверенітету, демократичного ладу й інформаційних прав громадян. Функціонально інформаційна безпека реалізується через охоронні, регулятивні та контрольні механізми, а її

інтегруючий характер зумовлює потребу в узгодженості законодавчих і стратегічних рішень у межах єдиної системи національної безпеки.

1.3. Внутрішні, зовнішні та гібридні загрози інформаційній безпеці МВС України: класифікація й прояви

Сучасний інформаційний простір трансформувався під впливом технологічних змін, що охопили всі сфери життя суспільства. Глобальна цифровізація, активне поширення соціальних мереж, Інтернету та технологій штучного інтелекту істотно змінили способи передавання й сприйняття інформації. З одного боку, зазначені процеси демократизували доступ до знань, сприяли підвищенню інформованості громадян і інтеграції суспільства у глобальні комунікативні мережі. З іншого боку, вони породили новий тип вразливостей, які становлять суттєві ризики для державної безпеки.

Огляд наукових джерел свідчить, що навіть у межах загальної теорії національної безпеки відсутній єдиний усталений підхід до тлумачення категорій «внутрішні», «зовнішні» та «гібридні» загрози [68; 31; 32]. У зв’язку з цим надалі під «внутрішніми загрозами» пропонується розуміти сукупність факторів і подій, що виникають та реалізуються всередині держави, деструктивно впливають на інформаційну систему й створюють небезпеку для інтересів держави та суспільства [31]. Відповідно, «зовнішні загрози» доцільно визначати як сукупність факторів і подій, що мають джерело на глобальному або наднаціональному рівні, однак проявляються в національному інформаційному просторі та спричиняють негативний вплив на інформаційну систему й інтереси держави та суспільства [68].

Загрози змішаного характеру, тобто гібридні загрози, поєднують зовнішні впливи з використанням внутрішніх вразливостей. Ворог одночасно застосовує воєнні засоби, інформаційно-психологічні операції, кібератаки та економічний тиск для досягнення своїх цілей. Гібридна загроза проявляється тоді, коли зовнішній противник використовує внутрішніх агентів або проблеми всередині країни для її дестабілізації [91]. Прикладом є використання підконтрольних

медіаресурсів і проросійських політичних акторів для поширення дезінформації. Протидія гібридним загрозам ускладнюється необхідністю одночасної роботи із зовнішнім противником і з внутрішніми чинниками, які він експлуатує [37]. Події останніх років засвідчують, що внутрішні соціальні конфлікти та протестні прояви за наявності інформаційного «підживлення» можуть набувати ознак інструменталізації та ставати елементом гібридної агресії [91; 74].

У науковій літературі послідовно наголошується, що суттєвий ризик для інформаційної безпеки становить чинний стан нормативно-правового регулювання інформаційних відносин. В. Я. Настюк виокремлює низку базових проблем, зокрема:

– «значний масив нормативно-правових актів, що регулюють інформаційні відносини, ускладнює їх пошук, системний аналіз і узгоджене практичне застосування;

– відсутність чітко визначеної та юридично закріпленої ієрархії таких актів призводить до різного тлумачення норм і суперечностей у правозастосуванні;

– у різних нормативно-правових актах використовуються терміни, які є нечіткими, некоректними або позбавленими однозначного змістового наповнення» [63, с. 28].

Отже, відповідна загроза має переважно нормативно-правову природу і прямо пов’язана з недоліками нормотворчої діяльності органів влади. Це зумовлено тим, що інформаційне законодавство охоплює надзвичайно широкий спектр типів інформаційної діяльності, що істотно ускладнює його кодифікацію та внутрішню узгодженість. Виявлені недоліки демонструють також залежність стану інформаційного законодавства від інших чинників, які визначають цілісність і послідовність державної політики.

Слід зазначити, що «Стратегія інформаційної безпеки України» [17] окреслила низку системних проблем державного управління в підвідомчій сфері, серед них доцільно виокремити: застарілість механізмів інформаційних

відносин, викликам і загрозам сучасності; низькі стандарти медіа; втручання в діяльність журналістів та засобів масової інформації [17]. Зазначені проблеми передусім обмежують можливості органів державної влади щодо попередження та протидії інформаційній агресії, а також стримують формування цілісної системи спеціалізованих суб'єктів інформаційної безпеки.

Не менш значущою є проблема недостатньої медіаграмотності населення й окремої особи, яка демонструє, що в центрі системи інформаційної безпеки перебувають громадяни як провідні суб'єкти інформаційних правовідносин. О. Литвиненко слушно зазначає, що за сучасних умов «інформаційна безпека держави й громадянина стає визначальним чинником захисту національних та особистих інтересів» [54, с. 262]. Джерело цієї загрози пов'язане зі сферою сприйняття людиною навколишньої дійсності та ґрунтується на її світоглядних орієнтирах, що значною мірою формуються під впливом державної інформаційної й освітньої політики. «Медіаграмотність не виникає стихійно: вона формується через медіаосвіту» [69, с. 113].

Своєю чергою О. Пархоменко-Куцевіл підкреслює, що «медіаманіпуляція масовою свідомістю базується насамперед на впливах на способи сприйняття інформації» [73, с. 180]. У цьому ракурсі медіаграмотність постає як спосіб, що дозволяє боротись з маніпулятивними технологіями і водночас долучатися до процесу підтримки ІБ. Доцільно виділити такі компоненти медіаграмотності як критичне мислення, здатність орієнтуватися в медіапросторі, свідоме медіаспоживання та базові навички медіапошуку» [54, с. 180]. Отже, ризики посилюються там, де слабкість державної політики поєднується з прагненням окремих суб'єктів (у тому числі іноземних держав) спрямовано впливати на суспільну думку за допомогою інформаційних ресурсів. Негативний вплив низького рівня медіаграмотності проявляється, зокрема, в ускладненні протидії деструктивним інформаційним впливам, оскільки громадяни не мають стійких «фільтрів» оцінювання отримуваної інформації; це підвищує результативність дезінформації та інформаційного тероризму.

Недостатній рівень розвитку механізмів захисту інформації має загальнодержавний вимір, оскільки безпосередньо впливає на стан державної безпеки. О. Резнікова виокремлює низку проблем у системі національної безпеки, а саме: «непослідовність і суперечливість…», «відсутність злагодженої системи управління ризиками», «проблеми координації…», «розбалансованість функціонування… систем реагування» [81, с. 439]. Поява цієї загрози значною мірою пов'язана з рівнем науково-технічного розвитку держави, від якого залежить захищеність інформаційно-телекомунікаційних систем, мереж і баз даних. У доктрині окреслюються такі прогалини в механізмах захисту інформації: «нечітке визначення прав та обов'язків суб'єктів», «недостатня правова врегульованість інституційної взаємодії» [79, с. 9].

Недосконаліть системи стратегічних комунікацій свідчить про те, що безпекова політика у інформаційній сфері має інтегрований характер і потребує скоординованих дій суб'єктів із різним правовим статусом та обсягом повноважень. В свою чергу стратегічні комунікації розглядаються як цілісний механізм регулювання інформаційної сфери, орієнтований, зокрема, на збереження національної культури та ідентичності [80, с. 32]. А. М. Благодарний та О. О. Кононець підкреслюють, що ефективна протидія інформаційній агресії можлива лише за умови інтегрованої взаємодії всіх інструментів держави із залученням громадянського суспільства; водночас для України однією з ключових проблем лишається недосконаліть системи стратегічних комунікацій [27, с. 5]. Відповідна загроза зумовлена слабкістю організаційно-правового механізму, який не забезпечує належних форм координації, взаємодії та партнерства між основними суб'єктами.

Зазначені ризики пов'язані також із категорією «інформаційна потреба», яка має світоглядний і когнітивний виміри. Я. В. Галета виокремлює умови формування інформаційних потреб у суспільстві: «недостатній методологічний інструментарій», «суперечність між уже наявними знаннями та новими відомостями», «розрив між теоретичними положеннями й реальною практикою» [34, с. 41]. Отже, потреба в інформації постає як закономірна реакція суб'єкта на

прагнення осягнути об’єктивну дійсність, тоді як обмеження доступу є наслідком недосконалості механізмів, сформованих як на загальнодержавному, так і на місцевому рівнях; саме місцевий рівень нерідко виявляється простором найгостріших проблем із доступом до інформації. Вплив цієї загрози проявляється, зокрема, в тому, що: «гальмується розвиток національної інформаційної системи…», «формується недовіра до держави…», «зростає імовірність звернення до нелегальних способів задоволення інформаційних потреб» [72].

Окремий блок становлять загрози, пов’язані з інформаційним тероризмом і дезінформаційними кампаніями. І. В. Яковюк та Є. М. Білоусов обґрунтовано вказують, що збройна агресія РФ проти України має глобальні наслідки й формує нову конфігурацію міжнародної напруженості; на початкових етапах агресивні дії можуть мати переважно неконвенційний характер, унаслідок чого особливо швидко поширюються популістські настрої, спрямовані на «розкладання» ліберальної демократії зсередини [91, с. 11]. Б. Д. Леонов і С. Я. Лихова характеризують інформаційний тероризм як «різновид деструктивного впливу» і виокремлюють психологічний та технічний різновиди [50, с. 174]. Специфічна небезпека інформаційного тероризму полягає у відсутності просторових меж: атаки можуть здійснюватися практично з будь-якої точки світу. Додатковий ризик зумовлений складністю ідентифікації виконавців, оскільки кібератаки нерідко реалізуються опосередковано — через розгалужені мережеві конфігурації та проміжні технічні засоби [50, с. 12]. Наслідки проявляються у: «дестабілізації…», «послабленні або втраті контролю над інформаційними ресурсами», «незаконному поширенні відомостей» [24].

Загроза, пов’язана з відсутністю контролю за змістом інформації в глобальних мережах, безпосередньо стосується завдань безпеки в інтернет-середовищі. Н. В. Лесько та М. Р. Малець звертають увагу на те, що Інтернет нівелює географічні кордони й ускладнює правове регулювання; додаткові проблеми спричиняють технічні особливості функціонування мережі, які не дозволяють застосувати традиційні механізми державного контролю [51, с. 189].

Як підкреслює І. А. Коваленко, особливо загострюється проблема захисту авторського права та суміжних прав в інтернеті через відсутність уніфікованого підходу, а законодавче регулювання не встигає за темпами розвитку інтернет-середовища [42, с. 54]. Основні наслідки неконтрольованого контенту можна узагальнити так: негативний вплив на свідомість населення через маніпулятивний або заборонений контент; незаконне використання чи поширення персональних даних; систематичні порушення авторського права та суміжних прав.

О. Ю. Буров наголошує, що «міжнародна кіберзлочинність істотно підриває національну безпеку…» через організованість і фінансування діяльності, вразливість онлайн-сервісів та формування ринку «програмних вразливостей» [32, с. 42]. Процеси цифровізації посилюють ці ризики й зумовлюють потребу держави в системному удосконаленні механізмів захисту. У «Стратегії кібербезпеки» [16] окреслено такі загрози, зокрема: гібридну агресію РФ у кіберпросторі кіберзлочинність, кібератаки, кібершпигунство, кібертероризм [16]. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII [11] конкретизує права людини, суспільство, державу, національні інтереси, критичну інфраструктуру як коло об’єктів кіберзахисту [11]. Вплив кіберзлочинності проявляється у: «посяганні на національні інтереси», «створенні загроз іншим складовим національної безпеки», «порушенні стабільного функціонування державних систем» [37].

Можливість реалізації масштабних дезінформаційних кампаній значною мірою зумовлена відсутністю ефективних міжнародно-правових механізмів заборони використання інформаційної зброї та демілітаризації глобального інформаційного простору. Додатковий рівень небезпеки полягає в можливості прихованого дистанційного впливу на критично важливі елементи інфраструктури (енергетика, транспорт, зв’язок, фінансовий сектор тощо) [76, с. 135]. Як процес цілеспрямованого створення й поширення неправдивої інформації, дезінформація зумовлює наслідки у вигляді: формування поведінки,

що суперечить конституційним засадам; обмеження права на доступ до достовірної інформації; дискредитації державної політики [60].

Особливу небезпеку становлять гібридні загрози, адже вони часто мають розмитий характер, їх складно ідентифікувати та своєчасно застосувати заходи протидії. Зокрема, пропагандистські наративи можуть поширюватися через формально легальні медіаресурси. Це вимагає постійного розвитку систем раннього виявлення та розвідки в сфері інформації, а також стійкої взаємодії правоохоронних органів і громадянського суспільства.

З огляду на динамічний характер загроз, класифікація та перелік конкретних викликів постійно оновлюються. Наведений перелік зовнішніх загроз не є вичерпним; він відображає спробу систематизувати найбільш актуальні виклики для інформаційної безпеки держави. В умовах стрімких трансформацій інформаційного простору виникають нові загрози, однак із високою ймовірністю вони матимуть похідний характер від уже окреслених, комбінуючи їхні елементи та посилюючи кумулятивний ефект.

Отже, загрози інформаційній безпеці України мають різну природу, але часто є взаємопов’язаними. Внутрішні вразливості національного інформаційного простору нерідко стають «точками входу» для зовнішнього впливу, що підсилює гібридний характер сучасної агресії та актуалізує потребу комплексної державної політики превенції й стійкості.

Таким чином, трансформація інформаційного простору під впливом цифровізації та технологій спричинила одночасне зростання можливостей комунікації й накопичення системних ризиків для національної безпеки. Запропонована диференціація загроз на внутрішні, зовнішні та гібридні дозволяє методологічно впорядкувати аналіз, проте реальна динаміка загроз демонструє їх взаємопроникнення й кумулятивний ефект. Ключовими внутрішніми чинниками вразливості виступають недоліки нормативно-правового регулювання, слабкість стратегічних комунікацій, дефіцит медіаграмотності та нерівномірність доступу до інформації. Зовнішній контур загроз визначається архітектурою глобальних мереж, міжнародною кіберзлочинністю,

інформаційним тероризмом і масштабними дезінформаційними кампаніями, які здатні вражати критичну інфраструктуру й суспільну стійкість. Отже, ефективна протидія потребує інтегрованого підходу, що поєднує правові, організаційні, технічні та соціально-освітні інструменти й орієнтується на раннє виявлення, превенцію та підвищення резильєнтності.

Висновки до розділу 1

Проведений теоретико-методологічний аналіз засвідчив, що інформаційна безпека в сучасних умовах має міждисциплінарну природу й не може бути зведена ані до суто технічного захисту інформації, ані до вузького правового режиму охорони інформаційних ресурсів. Вона постає як комплексна категорія національної безпеки, що відображає рівень стійкості інформаційного середовища, здатність держави й суспільства протидіяти деструктивним впливам та забезпечувати належні умови реалізації конституційних інформаційних прав. У межах такого підходу ключового значення набуває поєднання правового, організаційно-управлінського, інформаційно-технічного та соціально-освітнього компонентів, які спільно формують «архітектуру» захисту національного інформаційного простору.

Розкриття категорії «безпека» у філософсько-аксіологічному вимірі дало змогу обґрунтувати, що безпека є не лише станом захищеності, а й ціннісно-нормативним орієнтиром розвитку соціальної системи. Ця теза має принципове значення для інформаційної сфери, оскільки цифрова трансформація змінює структуру суспільних цінностей, моделі довіри, канали комунікації та поведінкові практики. Відтак інформаційна безпека повинна розглядатися як інструмент збереження й відтворення суспільно значущих цінностей і норм, а також як засіб підтримання соціальної стійкості в умовах інтенсивного інформаційного впливу. Такі засади як «інформаційний суверенітет» і «резильєнтність» набувають статусу стратегічних критеріїв розбудови державної політики, адже вони орієнтують її на превенцію, адаптивність і довгострокову здатність до відновлення після криз.

Узагальнення доктринальних підходів до визначення інформаційної безпеки показало наявність різних акцентів: захист державних інтересів і суверенітету; режим охорони правил функціонування інформаційних процесів; управління ризиками суб'єктами влади та інститутами суспільства; нормування правових, організаційних і технічних заходів у межах інформаційного права. Разом із тим ці підходи взаємно доповнюють один одного та дозволяють стверджувати, що домінантним у сучасному науковому дискурсі є інтегрований погляд на інформаційну безпеку як на поєднання: стану захищеності інформаційної сфери, системи взаємопов'язаних елементів інституційної та нормативної організації, механізму процедур і інструментів, через які забезпечується попередження, локалізація та нейтралізація загроз.

Важливим результатом є уточнення діяльнісної логіки через категорію «забезпечення». Встановлено, що забезпечення ІБ слід трактувати як організований процес досягнення визначеного рівня захищеності, який включає управління ризиками, стратегічне планування, координацію суб'єктів, а також розвиток культури безпечної інформаційної поведінки. Відповідно, «система засад ІБ» описує структуровану цілісність взаємопов'язаних елементів і заходів, тоді як «механізм забезпечення» відображає внутрішню організацію інструментів, засобів і процедур їх реалізації. Така диференціація має методологічну цінність, оскільки дозволяє переходити від загальних дефініцій до аналізу практичної дієздатності державної політики й інституційних рішень.

У межах розгляду місця інформаційної безпеки в системі національної безпеки України обґрунтовано, що вона виконує подвійну роль: по-перше, як самостійний структурний елемент національної безпеки; по-друге, як інтегруюча основа, без якої істотно ускладнюється реалізація інших безпекових компонентів (державної, оборонної, економічної, суспільної тощо). Нормативне визначення, задає комплексний орієнтир: захист суверенітету й територіальної цілісності, демократичного конституційного ладу, гарантування інформаційних прав, забезпечення доступу до достовірної інформації та протидія дезінформації, пропаганді й порушенням режимів охорони інформації з обмеженим доступом.

Водночас виявлено, що стратегічна нормативна база має прогалини методологічного рівня, зокрема відсутність у Стратегії чітко визначеного переліку принципів інформаційної безпеки як самостійної категорії. Це ускладнює уніфікацію практик, стандартизацію управлінських рішень, а також формування прозорих критеріїв результативності та відповідальності суб'єктів.

Окремо встановлено, що сучасний інформаційний простір, сформований цифровізацією, соціальними мережами, глобальними комунікаційними платформами та генеративним штучним інтелектом, суттєво змінює «ландшафт» загроз. Запропонована типологія загроз (внутрішні, зовнішні, гібридні) є методологічно виправданою, однак практична реальність демонструє їх взаємопроникнення. Внутрішній контур вразливостей містить проблеми нормативно-правового регулювання, управлінські дисфункції, недостатність механізмів стратегічних комунікацій, дефіцит медіаграмотності населення й нерівномірність доступу до інформації. Зовнішній контур загроз пов'язаний із архітектурою глобальних мереж, міжнародною кіберзлочинністю, кібершпигунством, інформаційним тероризмом, поширенням контенту й масштабними дезінформаційними кампаніями, включно з потенційним впливом на критичну інфраструктуру. Гібридні загрози є найбільш складними для ранньої ідентифікації, оскільки поєднують зовнішній тиск із використанням внутрішніх слабких місць; це висуває вимоги до систем раннього виявлення, координації, розвідки та контррозвідки в інформаційному середовищі, а також до партнерства держави з громадянським суспільством.

Узагальнюючи, можна констатувати, що інформаційна безпека потребує розгляду як адаптивної, багаторівневої системи, зорієнтованої на захист національних інтересів і забезпечення прав людини в умовах технологічної й ціннісної трансформації. Теоретичні висновки розділу формують методологічне підґрунтя для визначення суб'єктів інформаційної безпеки, їх компетенції та моделей координації; конкретизації інструментів і механізмів державної політики та обґрунтування критеріїв ефективності та стійкості національної інформаційної системи.

РОЗДІЛ ІІ

НОРМАТИВНО-ПРАВОВІ ТА ІНСТИТУЦІЙНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МВС УКРАЇНИ

2.1. Нормативно-правові засади забезпечення інформаційної безпеки МВС України

Законодавче регулювання інформаційної безпеки в Україні ґрунтується на системі нормативно-правових актів, які закріплюють вимоги та критерії захищеності інформаційної сфери, визначають комплекс загальних організаційно-методологічних заходів, а також регламентують створення й експлуатацію систем захисту інформації.

Нормативна база України у сфері інформаційної безпеки включає норми Конституції України, рамкові закони у сфері національної безпеки, спеціалізовані акти (зокрема щодо кібербезпеки та захисту інформації в інформаційно-телекомунікаційних системах), а також стратегічні документи, введені в дію актами Президента України на підставі рішень Ради національної безпеки і оборони України.

Ключовим нормативним орієнтиром виступає Конституція України [1] (ухвалена 28 червня 1996 р.). Відповідно до статті 17 Конституції України забезпечення інформаційної безпеки належить до найважливіших функцій держави [1]. Це положення формує базову правову основу для подальшого розвитку галузевого законодавства та прийняття спеціалізованих актів у сфері інформаційної безпеки.

До базових законодавчих актів, що визначають концептуальні засади національної безпеки України, належить Закон України «Про національну безпеку України» (№ 2469-VIII від 21.06.2018 р.) [8]. Його значення полягає у встановленні принципів і цілей державної політики у сфері безпеки та оборони, розмежуванні повноважень суб’єктів сектору безпеки і оборони, а також у закріпленні підходів до стратегічного планування через систему стратегічних документів. Водночас Закон не деталізує перелік специфічних загроз в

інформаційній сфері та конкретні механізми їх нейтралізації; натомість він задає рамкові правові параметри, у межах яких пріоритети, ризики та інструменти реагування конкретизуються у відповідних стратегіях та підзаконних актах [8]. Таким чином, інформаційна безпека інституційно й нормативно позиціонується як складова системи національної безпеки, а практичні напрями її реалізації визначаються через документи стратегічного рівня та регуляторні рішення.

Важливе місце в системі спеціального законодавства посідає Закон України «Про основні засади забезпечення кібербезпеки України» (№ 2163-VIII від 05.10.2017 р.) [11], який закріпив інституційні та організаційні основи національної системи кібербезпеки. Цим Законом визначено коло суб'єктів відповідної системи та їх функції, встановлено повноваження державних органів у сфері запобігання, виявлення й нейтралізації кіберзагроз, а також окреслено координаційну роль Ради національної безпеки і оборони України у сфері кібербезпеки. Хоча Закон регулює насамперед кібербезпековий сегмент, його практична імплементація має безпосереднє значення для інформаційної безпеки загалом, оскільки стійкість інформаційного простору прямо залежить від надійності цифрової інфраструктури та захищеності інформаційно-комунікаційних систем [11].

Не менш важливим є Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» (№ 80/94-ВР від 05.07.1994 р.) [7], який закріплює організаційно-правові засади охорони інформації в інформаційно-телекомунікаційних (автоматизованих) системах. Закон установлює загальні вимоги до комплексного захисту інформації, зокрема визначає підходи до технічного та криптографічного захисту з метою запобігання несанкціонованому доступу, модифікації, блокуванню або іншим формам неправомірного впливу на інформацію [7].

Стратегічний рівень державної політики у цій сфері конкретизується актами Президента України, якими вводяться в дію рішення Ради національної безпеки і оборони України. Зокрема, Указ Президента України, яким введено в дію рішення РНБО від 14 травня 2021 року «Про Стратегію кібербезпеки України»

[16] (№ 447/2021 від 26.08.2021 р.), визначає пріоритети національних інтересів у сфері кібербезпеки, окреслює спектр актуальних і потенційних кіберзагроз, а також формулює цілі й завдання забезпечення кібербезпеки, спрямовані на створення умов безпечного функціонування кіберпростору та його використання в інтересах особи, суспільства і держави [16]. Аналогічно, Указ Президента України, яким введено в дію рішення РНБО від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки України» [17] (№ 685/2021 від 28.12.2021 р.), визначає ключові виклики та загрози національній безпеці в інформаційній сфері, встановлює стратегічні цілі й завдання протидії таким загрозам, а також підкреслює необхідність одночасного гарантування прав людини на інформацію та належного захисту персональних даних [17].

З огляду на складність предмета регулювання, нормативно-правову базу у сфері інформаційної безпеки доцільно викладати за функціонально-логічним принципом «від загального до спеціального» та «від правових гарантій — до інституційно-інфраструктурних механізмів реалізації». Наступним блоком визначаються правові засади захисту приватності та персональних даних як необхідної умови довіри до інформаційних систем і стійкості суспільства. Завершує аналіз законодавство, спрямоване на інформатизацію та розвиток інформаційної інфраструктури, яке створює організаційні й технологічні передумови практичного виконання вимог інформаційної безпеки.

Закон України «Про інформацію»[5] (№ 2657-XII від 02.10.1992 р.) визначає загальні засади регулювання суспільних інформаційних відносин, закріплює права громадян на інформацію та встановлює обов’язки суб’єктів інформаційної діяльності. Його нормативне значення полягає в окресленні поняття інформації, її видів, режимів доступу та принципів інформаційної діяльності. Хоча Закон передусім спрямований на гарантування свободи слова й базових прав у інформаційній сфері, він одночасно формує правову рамку для забезпечення інформаційної безпеки через визначення законних меж доступу, підстав обмеження інформації та захисту охоронюваних законом інтересів в інформаційному просторі [5].

Закон України «Про медіа» [6] (№ 2849-IX від 31.03.2023 р.) установлює правові засади функціонування медіасфери та спрямований на реалізацію свободи вираження поглядів і права на отримання достовірної та різнобічної інформації, забезпечення плюралізму, а також захист національних інтересів і прав користувачів медіасервісів. Важливим елементом є визначення правового статусу, порядку формування та повноважень Національної ради України з питань телебачення і радіомовлення як ключового регулятора у сфері медіа, діяльність якого має значення для підтримання стійкості інформаційного середовища [6].

Закон України «Про доступ до публічної інформації» [3] (№ 2939-VI від 13.01.2011 р.) установлює порядок реалізації та гарантії права кожного на доступ до інформації, що перебуває у володінні суб'єктів владних повноважень та інших розпорядників, а також визначає підходи до доступу до інформації, що становить суспільний інтерес. У вимірі інформаційної безпеки цей Закон забезпечує процесуальні стандарти прозорості, підзвітності та передбачуваності інформаційної діяльності публічної влади [3].

Закон України «Про захист персональних даних» [4] (№ 2297-VI від 01.06.2010 р.) регулює правовідносини у сфері обробки та захисту персональних даних і спрямований на охорону основоположних прав і свобод людини, насамперед права на приватність. Закон поширюється як на обробку персональних даних із застосуванням автоматизованих засобів, так і на обробку в неавтоматизованих масивах (картотеках), що є необхідною умовою довіри до інформаційних систем і безпечного функціонування цифрових сервісів [4].

Закон України «Про Національну програму інформатизації» [10] (№ 2807-IX від 01.12.2022 р.) визначає правові засади формування та виконання Національної програми інформатизації [10]. Його практичне значення полягає у створенні організаційних та програмних умов розвитку інформаційної інфраструктури держави й інформатизації суспільства. У контексті інформаційної безпеки реалізація Програми пов'язана з розвитком національних

інформаційних ресурсів, упровадженням вимог до захищеності інформаційних систем і підтримкою заходів технічного захисту інформації.

Незважаючи на вдосконалення законодавства, на практиці зберігаються проблеми дієвого правозастосування у сфері інформаційної безпеки. По-перше, динамічний розвиток інформаційного простору випереджає нормотворення, унаслідок чого низка сучасних явищ не має однозначної правової кваліфікації; це ускладнює притягнення винних осіб до відповідальності та актуалізує потребу законодавчого врегулювання нових різновидів інформаційних правопорушень. По-друге, складним є дотримання балансу між державними безпековими потребами та свободою вираження поглядів: посилення обмежувальних заходів в умовах воєнного стану, включно з рішеннями щодо діяльності окремих медіа, потребує чітких критеріїв необхідності, пропорційності та процедурних гарантій дотримання конституційних прав. По-третє, правозастосування об’єктивно ускладнюється умовами війни (тимчасова окупація частини територій, масове переміщення населення, руйнування інфраструктури), що обмежує інституційну спроможність органів публічної влади та правоохоронної системи.

Окрему групу нормативних актів становлять стратегічні та доктринальні документи у сфері інформаційної безпеки, які окреслюють довгострокові цілі, пріоритети та завдання, враховують актуальні загрози й конкретизують державну політику безпеки. «Доктрина інформаційної безпеки України» [18] була затверджена Указом Президента України № 47/2017 від 25 лютого 2017 р., яким введено в дію відповідне рішення РНБО. Доктрина фіксувала факт інформаційної агресії з боку Російської Федерації та визначала напрями державної політики з протидії загрозам, зокрема щодо захисту інформаційного суверенітету, розвитку національного інформаційного простору, посилення кіберзахисту, протидії пропаганді, дезінформації й інформаційно-психологічним операціям [18]. Водночас у 2021 р. у межах оновлення стратегічного регулювання статтю 2 Указу № 47/2017 (якою затверджувалася Доктрина) було визнано такою, що втратила чинність, у зв’язку із затвердженням Стратегії інформаційної безпеки [17].

Стратегія національної безпеки України, схвалена рішенням РНБО та введена в дію Указом Президента України № 392/2020 від 14.09.2020 р., віднесла інформаційну та кібербезпеку до ключових пріоритетів державної політики [15]. Документ орієнтує державу на нарощування спроможностей протидії гібридним загрозам, розвиток національної системи кібербезпеки, посилення координації між суб'єктами сектору безпеки і оборони та правоохоронними органами, а також на протидію спеціальним інформаційним операціям, кібератакам і пропаганді [47, с. 136–146]. Отже, стратегічний рівень інституційно інтегрує інформаційну безпеку в систему національної безпеки, визначаючи її як чинник загальної стійкості держави.

Стратегія інформаційної безпеки України, затверджена Указом Президента України № 685/2021 від 28 грудня 2021 р. та введена в дію рішенням РНБО від 15 жовтня 2021 р., визначає актуальні виклики та загрози національній безпеці в інформаційній сфері, формулює стратегічні цілі й завдання протидії таким загрозам, а також акцентує на захисті прав осіб на інформацію і персональних даних; реалізацію Стратегії визначено на період до 2025 року [17]. Стратегія конкретизує пріоритетні напрями державної політики, зокрема: протидію дезінформації та інформаційним операціям; удосконалення регулювання інформаційних відносин і медіасфери; підвищення рівня медіакультури та медіаграмотності; посилення міжнародної присутності та позитивного іміджу України у світових інформаційних ресурсах; а також узгодження з кібербезпековим контуром через розмежування предметів регулювання зі Стратегією кібербезпеки [17; 47, с. 136–146]. Важливим системоутворюючим блоком є розвиток стратегічних комунікацій і міжвідомча координація: документ фіксує проблеми несформованості дієвого механізму координації, визначає координаційну роль РНБО та передбачає реалізацію на основі плану заходів Кабінету Міністрів України із залученням інститутів громадянського суспільства [17].

«Стратегія кібербезпеки України» (Указ Президента України від 26.08.2021 № 447/2021) конкретизує положення Стратегії національної безпеки України у

кібервимірі та визначає пріоритети розбудови національної системи кібербезпеки на довгострокову перспективу [16]. У документі акцентовано на підвищенні захищеності критичної інформаційної інфраструктури, створенні дієвих механізмів реагування на кіберінциденти та розвитку міжнародної співпраці у сфері кібербезпеки, розглядаючи кіберстійкість як технологічну передумову безпеки інформаційного простору [16].

Отже, законодавче забезпечення інформаційної безпеки України має багаторівневий характер і включає конституційні засади, рамкові акти у сфері національної безпеки, спеціалізоване законодавство (кібербезпека, захист інформації в ІТС), а також стратегічні документи, що конкретизують цілі, пріоритети й інструменти державної політики. Сукупність галузевих законів («Про інформацію», «Про медіа», «Про доступ до публічної інформації», «Про захист персональних даних», «Про Національну програму інформатизації») формує правові режими доступу, прозорості, приватності та розвитку інфраструктури, без яких неможлива стійкість інформаційного простору [56; 34; 10]. Водночас ефективність цієї нормативної системи обмежується розривом між темпами технологічних змін і нормотворенням, проблемами правової визначеності для нових форм інформаційних правопорушень, а також складністю забезпечення балансу між безпековими обмеженнями та конституційними правами в умовах воєнного стану. Таким чином, пріоритетом виступає не лише подальше вдосконалення законодавства, а й підвищення інституційної спроможності його реалізації — через уніфікацію підходів, процедурні гарантії, міжвідомчу координацію та стабільні механізми стратегічних комунікацій.

2.2. Засади функціонування інституційної система інформаційної безпеки МВС України

Інформаційна безпека в науковому розумінні має подвійний характер. З одного боку, вона постає як стан захищеності національного інформаційного простору, за якого деструктивні інформаційні впливи не завдають істотної

шкоди життєво важливим інтересам держави. З іншого боку, ІБ є системою організаційно-правових, інституційних, технологічних і комунікаційних заходів, що здійснюються уповноваженими суб'єктами з метою запобігання, виявлення, нейтралізації загроз.

Як засвідчує та демонструє практика останніх років, загрози інформаційного виміру уражають не тільки цифрові дані та мережі, а й державне управління, функціонування критичних сфер, моральний стан громадян, а також міжнародну суб'єктність держави. Відповідно, інституційна система забезпечення інформаційної безпеки має розглядатися не як сукупність розрізнених органів, а як єдина багаторівнева система, де правове регулювання, компетенції, координація взаємодії між ними та ресурсне забезпечення спрямовані на досягнення спільного результату.

Отже методологічний аналіз інституційної системи доцільно розглядати на основі трьох принципів:

1. системності (взаємозв'язок суб'єктів і процедур, наявність напрямів та меж діяльності);
2. функціональної диференціації (розмежування ролей стратегічного керівництва, регуляторного механізму, оборони, правоохоронної діяльності та комунікації);
3. результативності (орієнтація на вимірювані рівня вразливостей, скорочення часу реагування, підвищення стійкості інформаційного простору).

Зазначимо, що доцільно, перш ніж почати аналіз суб'єктів, окреслити цінності, ресурси, процеси та середовища, у межах яких формуються інформаційні ризики та загрози й які потребують захисту інституційними, правовими та технологічними засобами, тобто об'єктів сфери ІБ. Зазначений підхід дозволить уникнути редукції інформаційної безпеки до кіберзахисту та забезпечить теоретико-методологічну єдність технічних і соціальних вимірів інформаційного сектору.

У межах класифікації доцільно виокремити чотири групи об’єктів, які охоплюють як технічні, так і соціально-комунікаційні компоненти простору інформаційної безпеки.

Перша група охоплює критичну інформаційну інфраструктуру, що об’єднує галузі та сервіси, від функціонування яких залежить життєдіяльність держави і суспільства (енергетика, транспорт, зв’язок, фінансові сервіси, охорона здоров’я і теплопостачання, урядовий зв’язок та ін). Важливою складовою виступають інформаційно-комунікаційні системи управління технологічними процесами, а також підсистеми SCADA/ICS, які забезпечують керування виробничими й інфраструктурними контурами. Типовий профіль загроз для цього класу визначається поєднанням кібервпливів і техніко-інформаційних диверсій: атаки на технологічні мережі, компрометація ланцюгів постачання, шкідливе програмне забезпечення, цілеспрямоване руйнування або деградація вузлів управління [8; 11; 17].

Наступна група це державні інформаційні ресурси, що включають державні реєстри, бази даних, інформаційні системи органів влади, а також цифрові сервіси. На відміну від критичної інфраструктури, де первинною є фізична безперервність сервісів, тут центральним є поєднання технологічної надійності з легітимністю та довірою до державних цифрових платформ. Загрози включають несанкціонований доступ, витоки даних, підміну або модифікацію інформації, зупинку сервісів, а також дискредитаційні операції навколо державних платформ [3; 4; 7].

Третя група, це персональні дані та приватність, яка охоплює масиви персональних даних у державному й приватному секторах, а також відомості, здатні бути використаними для шантажу, переслідування, соціальної інженерії та інших форм цілеспрямованого впливу на особу. Цей сегмент є одночасно правовим і технологічним: він пов’язує режим приватності, вимоги законності обробки та практики кіберзахисту даних. Типовими загрозами є витоки, незаконна обробка, фішинг, шахрайство, доксинг, профілювання, зловживання

доступом та інші форми порушення принципу захисту персональних даних [32; 59].

Остання, п’ята група це інформаційний простір і публічні комунікації, що охоплює медіасередовище, соціальні мережі та месенджери, а також зовнішній інформаційний контур — іноземні аудиторії, міжнародні платформи та канали стратегічних комунікацій. Його специфіка полягає в домінуванні нематеріальних параметрів: довіра, легітимність, наративи, суспільна єдність, міжнародна репутація. Типові загрози включають пропаганду, фейки, керовані кампанії впливу, поляризацію, підрив довіри до інститутів, дискредитацію та форми інформаційного терору[21; 22].

Підсумовуючі раніше вказане, слід зазначити, що запропонована класифікація демонструє, що об’єкти інформаційної безпеки формують єдиний взаємопов’язаний комплекс, у якому технічні елементи функціонально поєднані із соціальними. Це створює методологічну основу для подальшого аналізу, узгодження компетенцій, виявлення прогалин та проєктування механізмів підвищення стійкості інформаційного простору України.

Суб’єктами забезпечення інформаційної безпеки є державні та недержавні інституції, а також громадяни й їхні об’єднання, які в межах установлених законом повноважень або через усталену суспільну практику впливають на стан захищеності національного інформаційного простору. У теоретико-методологічному вимірі йдеться про багатофакторну систему, де безпековий компонент є похідним від взаємодії різних інституційних груп, що мають відмінні ресурси, інструменти та сфери відповідальності. Відповідно, аналіз суб’єктного складу доцільно будувати на двох взаємодоповнювальних підходах: секторному і функціонально-управлінському. Поєднання цих підходів дає змогу визначити конкретні органи, що забезпечують інформаційну безпеку і розподіл їх функцій. Виокремимо три ключові сектори: державний, громадянський або суспільний та приватний сектори.

Державний сектор охоплює органи стратегічного керівництва, виконавчої влади, спеціальні служби, оборонні та правоохоронні структури, регуляторів і

наглядові інституції. Його системна роль полягає у формуванні політики та правових режимів, розподілі ресурсів, організації координації і застосуванні примусових інструментів у межах законності та принципу пропорційності. Саме держава задає нормативні “правила гри”, визначає пріоритети, встановлює вимоги до суб’єктів, створює інституційні механізми реагування на загрози та забезпечує відповідальність за порушення[8].

Громадянське суспільство виконує функції соціальної резильєнтності та демократичної підзвітності. Воно підсилює інформаційну безпеку через моніторинг інформаційних впливів, просвіту і розвиток медіаграмотності, незалежну експертизу управлінських рішень, а також через формування механізмів суспільної довіри до державної політики. У цьому секторі безпека проявляється як здатність суспільства зберігати раціональність, солідарність і стійкість до маніпуляцій, а також як здатність демократичних інститутів підтримувати легітимність і підзвітність безпекових рішень. Приватний сектор (оператори зв’язку, ІТ-компанії, власники й оператори інфраструктури, банки та платіжні системи, платформи і провайдери цифрових послуг) забезпечує значну частину операційної спроможності інформаційної безпеки, оскільки критичні сегменти цифрових ресурсів, каналів комунікації і сервісів функціонують у приватному або змішаному середовищі. Практично це означає, що приватний сектор є не лише об’єктом регулювання, а й повноправним суб’єктом виконання вимог безпеки та носієм ключових технологічних компетентностей: від архітектури захищених сервісів до інцидент-менеджменту і відновлення [33; 34].

Аспекти секторного рівня полягають в тому, що інформаційна безпека за своєю природою не може бути забезпечена виключно державою. Її результативність визначається не стільки ієрархією органів управління, скільки якістю механізмів взаємодії та партнерства. Що випливають із здатності держави інституціоналізувати взаємодію з бізнесом і громадянським суспільством через стандарти обміну даними, протоколи реагування, спільні навчання та прозорі режими кризових комунікацій [44; 40]. Натомість функціонально-управлінський аспект класифікації виокремлює:

Стратегічний напрям – Президент України та Рада національної безпеки та оборони України (РНБО) задають стратегічні пріоритети, визначають межі допустимих інструментів протидії загрозам, забезпечують ухвалення політико-управлінських рішень щодо системних ризиків для національної безпеки та оборони. На цьому рівні встановлюється межі, критичності і першочерговості загроз є та інструменти як можуть застосовуватися правомірно та пропорційно. В інституційній структурі цього напрямку функціонує Національний координаційний центр кібербезпеки (НКЦК) як міжвідомчий координаційний орган у кіберсфері, цілями якого є синхронізація позицій суб'єктів сектору безпеки і оборони, підтримка узгоджених процедур реагування, підготовка пропозицій щодо кризових режимів і розвиток національних спроможностей [13; 14; 17].

Управлінський напрям забезпечує операціоналізацію стратегічних рішень, перетворюючи їх на політики, програми та процедури. Кабінет Міністрів України реалізує державну політику через затвердження підзаконних актів, планів і стандартів, організацію ресурсів (кадрових, фінансових, технологічних), координацію міністерств і відомств, формування державних програм та механізмів моніторингу виконання. Саме на цьому рівні стратегічні орієнтири набувають форми конкретних виконавців, бюджетних рішень, процедур взаємодії та індикаторів результативності. Від ефективності управлінського контуру залежить, чи перетвориться інформаційна безпека на практику повсякденного державного управління, а не залишиться сукупністю декларацій [46].

Спеціальний безпековий (контррозвідувальний) напрям зорієнтований на загрози, що мають характер цілеспрямованих спеціальних операцій противника та посягають на основи державності. СБУ здійснює виявлення і нейтралізацію загроз державній безпеці в інформаційній сфері, забезпечує контррозвідувальний захист інформаційних об'єктів і процесів управління, протидіє підривній діяльності, охороняє режими державної таємниці та реагує на інциденти з ознаками диверсії чи шпигунства. У системі інформаційної безпеки

цей контур функціонує на межі інформаційного та силового вимірів, де кібератака або інформаційна кампанія розглядається як елемент ширшої стратегії агресора. Звідси випливає методологічна вимога: контррозвідка має доповнювати інші контури, а не дублювати їх, що передбачає чіткі інтерфейси взаємодії з технічним реагуванням і процесуальним розслідуванням [12; 8].

Техніко-регуляторний інапрям формує технологічний каркас інформаційної безпеки державного сегмента та критичної інфраструктури. Державна служба спеціального зв'язку та захисту інформації України Держспецзв’язку забезпечує криптографічний і технічний захист інформації, урядовий зв’язок, розвиток вимог і стандартів кіберзахисту; CERT-UA здійснює моніторинг, попередження, методичний супровід і координацію реагування на кіберінциденти. У науковій інтерпретації він поєднує нормативно-технічну стандартизацію та оперативну керованість інцидентів. Саме тут закладаються передумови переходу від реактивної логіки до системного управління ризиками та інституційного навчання [2; 10; 11].

Напрям цифровізації держави, кібергігієни та компетентностей забезпечує інтеграцію безпеки в цифрову трансформацію. Міністерство цифрової трансформації України впливає на інформаційну безпеку через розвиток цифрової інфраструктури й електронних сервісів, формування політик цифрової грамотності та кібергігієни, взаємодію з IT-галуззю та міжнародними партнерами, а також запровадження практик безпеки у життєвому циклі цифрових продуктів. Науково принциповим є те, що безпека в цьому контурі має бути “вбудованою властивістю” цифрових сервісів, а не зовнішнім контролем після впровадження. Така логіка зменшує структурні вразливості, підвищує довіру до е-урядування і знижує витрати на виправлення помилок у перспективі [5].

Оборонний напрям охоплює кібероборону військових систем та інформаційно-психологічний захист у секторі оборони. МОУ та ЗСУ забезпечують захист мереж зв’язку і управління, розвиток підрозділів кіберзахисту та інформаційних операцій, підтримку стратегічних комунікацій

оборони, протидію пропаганді і зміцнення морально-психологічної стійкості. Його особливість полягає у спеціальних режимах секретності та оперативності; водночас оборонний сегмент потребує сумісності з національною системою реагування, оскільки сучасні загрози “перетікають” між цивільним і військовим середовищем через взаємозалежність інфраструктури та цифрових ресурсів [16; 8].

Правоохоронний напрям забезпечує процесуальне реагування і реалізацію кримінально-правових механізмів захисту інформаційної сфери. МВС і Національна поліція, зокрема кіберполіція, розслідують кіберзлочини, працюють із цифровими доказами, формують доказову базу та взаємодіють із технічними командами реагування і спеціальними службами. Системна функція цього контуру полягає в тому, щоб завершити цикл реагування — перетворити технічний інцидент на юридично значущий результат, який створює ефект стримування, підвищує невідворотність відповідальності та зменшує мотивацію повторних атак [8; 11; 9].

Регуляторно-комунікаційний і секторний напрями охоплюють органи, що формують інформаційну політику, здійснюють медіарегулювання та нагляд, забезпечують правові режими захисту даних і інформаційних ресурсів, а також секторних регуляторів (зокрема у фінансовій сфері), які встановлюють вимоги кіберстійкості для піднаглядних установ. Окремо парламент визначає законодавчу рамку та здійснює контроль, окреслюючи легітимні межі державного втручання в інформаційну сферу. У науковому сенсі цей блок виконує дві критичні функції: нормативне впорядкування інформаційного простору (правила, стандарти, нагляд) і підтримання довіри через правові гарантії та демократичну підзвітність, без яких неможлива стійкість інформаційної політики [1; 8].

Отже вказані моделі в сукупності показують, що суб’єктний склад забезпечення інформаційної безпеки України є розгалуженим і взаємозалежним. Результативність системи визначається не кількістю інституцій, а узгодженістю їхніх компетенцій, наявністю стандартизованих процедур взаємодії та стійких

механізмів координації, які охоплюють повний цикл безпеки — від попередження до інституційного навчання. Звідси випливають ключові умови підвищення ефективності: чітке розмежування відповідальності й визначення напрямів реагування, інституціоналізація партнерства з приватним сектором і громадянським суспільством, а також баланс між безпекою та правами людини через прозорі, пропорційні й підзвітні механізми державної політики.

Сучасна архітектура механізму інформаційної безпеки має об'єктивно багатоаспектний характер і, відповідно, залежить від недержавних суб'єктів також. Це зумовлено тим, що значна частина критично важливих компонентів цифрового середовища — телекомунікаційні мережі, дата-центри, хмарні платформи, програмні продукти, соціальні медіа, інструменти електронної комерції, а також великі масиви даних — перебуває у приватній власності або експлуатується недержавними організаціями. За таких умов недержавний напрям не може розглядатися як факультативний ресурс чи "допоміжна" ланка державної системи він навпаки, є функціонально необхідним елементом національної моделі безпеки, без якого неможливі ані інфраструктурна стійкість, ані ефективне реагування на інциденти, ані підтримання суспільної довіри в умовах інформаційного протиборства [100].

Водночас внесок недержавних суб'єктів доцільно аналізувати диференційовано, розрізняючи приватний сектор і громадянське суспільство, оскільки вони підсилюють інформаційну безпеку через різні механізми. Приватний сектор забезпечує переважно технологічні, організаційні та ресурсні спроможності, формуючи операційну "матеріальну базу" стійкості цифрового середовища. Натомість громадянське суспільство діє передусім у когнітивно-комунікаційному вимірі, посилюючи соціальну резильєнтність, забезпечуючи незалежний контроль і сприяючи демократичній підзвітності державної політики [44].

У системі інформаційної безпеки приватний сектор виконує сукупність системних функцій, які доцільно інтерпретувати як три взаємопов'язані напрями. По-перше, інфраструктурно-стабілізаційний, адже оператори мереж і

цифрових сервісів забезпечують технічну стійкість середовища: безперервність зв'язку, резервування критичних елементів, розподіленість ресурсів, захист від атак на доступність, підтримання працездатності ключових сервісів у кризових режимах. По-друге, технологічно-експертний: провайдери, ІТ-компанії, інтегратори та постачальники рішень у сфері кібербезпеки впроваджують засоби моніторингу та аналізу подій безпеки, управління ідентичностями та доступом, захисту кінцевих пристроїв, безпеки хмарних середовищ, криптографічні механізми, а також підтримують відновлення після інцидентів. По-третє, приватний сектор виконує операційно-ризиковий напрям через підприємства критичних галузей: оператори критичної інфраструктури є безпосередніми носіями кіберризику, оскільки інцидент у їхніх інформаційно-комунікаційних системах здатен трансформуватися у каскадні відмови в економіці, соціальній сфері та безперервності управління. Саме тому вони виступають ключовими виконавцями вимог безпеки на практиці: здійснюють управління вразливостями, аудит, сегментацію мереж, інцидент-менеджмент, тестування планів безперервності, підготовку персоналу та відпрацювання сценаріїв реагування. Узагальнено, приватний сектор не обмежується виконавчими функціями, а фактично формує значну частину операційної спроможності держави у цифровому середовищі — особливо там, де державні ресурси об'єктивно обмежені або де інфраструктура належить приватним власникам [8; 17].

Паралельно громадянське суспільство посилює інформаційну безпеку через механізми соціальної стійкості та демократичної легітимності. Його внесок доцільно описувати через чотири ключові функції. Передусім це моніторинг і викриття дезінформації: фактчекінгові ініціативи, медіаспостерігачі та аналітичні осередки виявляють кампанії маніпуляції, фіксують ворожі наративи, здійснюють публічне спростування і формують доказову базу щодо джерел та механізмів поширення деструктивного контенту, тим самим знижуючи "швидкість розповсюдження" фейків та підвищуючи поріг довіри до неперевірених повідомлень. Друга функція — розвиток медіаграмотності та інформаційної культури: освітні програми, тренінги і просвітницькі кампанії

формують навички критичного мислення, розпізнавання маніпуляцій і безпечної поведінки у цифровому середовищі. В умовах, коли людський фактор залишається однією з ключових вразливостей, ця діяльність має безпосередню безпекову цінність. Третя функція — експертно-аналітичний контроль і формування пропозицій для політики: аналітичні центри та професійні спільноти забезпечують незалежну оцінку державних рішень, пропонують зміни до нормативної бази, стандартизації та інституційної архітектури, виконуючи роль механізму “зворотного зв’язку” для державного управління. Нарешті, громадянське суспільство виконує функцію легітимації рішень через прозорість і підзвітність, оскільки публічні дискусії, експертна критика та громадський контроль зменшують ризик зловживань у сфері інформаційної політики, підтримують дотримання прав і свобод і, як наслідок, зберігають довіру до державних інституцій. Соціальна прийнятність безпекових заходів є необхідною умовою їх тривалої ефективності: навіть технічно коректні рішення можуть призвести до втратити результативність [4; 16].

Водночас результативність недержавного контуру визначається не самим фактом наявності приватних і громадських акторів, а якістю їх інтеграції в національну систему. Центральним механізмом виступає публічно-приватне партнерство, доповнене стійкими “режимами довіри”, що знімають бар’єри для взаємодії як у кризових ситуаціях, так і в повсякденному управлінні ризиками. До базових умов такої інтеграції належать стандартизований обмін інформацією про інциденти та загрози (узгоджені формати повідомлень, визначені канали й часові рамки), правові гарантії конфіденційності технічної інформації (щоб компанії могли передавати дані без ризику непропорційних репутаційних або правових втрат за умови дотримання закону), спільні навчання та відпрацювання сценаріїв, узгоджені протоколи кризових комунікацій і чітке розмежування відповідальності між державою та недержавними учасниками. Саме ці умови перетворюють участь недержавних акторів на системну властивість, а не на сукупність ситуативних взаємодій [17].

Відповідно, успішність національної моделі визначається тим, наскільки держава спроможна інституціоналізувати партнерства, забезпечити взаємну довіру, стандартизацію взаємодії та баланс між безпековими потребами і демократичними гарантіями. Разом із тим, навіть за наявності розвиненої мережі інституцій та активної участі недержавних суб'єктів система може зберігати структурні обмеження, пов'язані з координацією, ресурсною асиметрією та фрагментацією правових режимів. У науковому трактуванні ці обмеження слід розуміти не як "дефекти окремих органів", а як системні дисфункції взаємодії на стиках компетенцій, ресурсів і правових процедур, коли формально наявні інститути та норми не завжди трансформуються у стабільні процеси запобігання, реагування та відновлення.

Проведений аналіз дає підстави стверджувати, що інституційне забезпечення інформаційної безпеки України еволюціонувало у цілісну багаторівневу систему, яка поєднує різні типи державних і недержавних спроможностей та відображає сучасну природу інформаційних загроз. Її архітектура функціонує як інтегрований механізм, у якому стратегічне керівництво визначає пріоритети та режими реагування; урядовий рівень забезпечує розроблення й реалізацію політик через нормативні акти, програми і ресурси; спеціальні служби реалізують контррозвідувальні та безпекові функції; техніко-регуляторний кіберконтур формує стандарти, вимоги та інфраструктуру реагування; оборонний сегмент забезпечує кібероборону і інформаційно-психологічний захист у військовій сфері; правоохоронний блок гарантує процесуальне реагування та притягнення винних до відповідальності; регуляторно-комунікаційні інструменти підтримують порядок у медіасфері та забезпечують публічні комунікації; а недержавні актори (приватний сектор, медіа, громадянське суспільство, експертне середовище) підсилюють як технологічну стійкість, так і соціальну резильєнтність [8; 17; 44].

Отже, інституційна система забезпечення інформаційної безпеки України може бути охарактеризована як динамічна, багатокомпонентна і мультиакторна модель, яка вже довела свою життєздатність у надзвичайно високому рівні

загроз. Її подальше вдосконалення має ґрунтуватися на переході від переважно реактивної логіки до логіки проактивного управління ризиками, де ключовими стають стандартизація, інтероперабельність, партнерства, розвиток людського капіталу та інституційна підзвітність. Саме така траєкторія забезпечує не лише зниження поточних вразливостей, а й формування стратегічної резильєнтності держави в умовах тривалого інформаційного протиборства.

2.3. Інформаційна стійкість і державна політика у контексті інституційної взаємодії

Інформаційна стійкість, як одна з концептуальних засад інформаційної безпеки, набуває критичного значення в умовах впливу сучасних гібридних загроз, зумовлених збройною агресією проти України. Держава та суспільство змушені реагувати на масив дезінформації, спроби впливу на свідомість громадян та інші форми інформаційних атак. Відтак особливої актуальності набуває розуміння того, яким чином органи публічної влади й інституції громадянського суспільства можуть спільно протидіяти зазначеним викликам. Визначення та впровадження результативних механізмів взаємодії є необхідною передумовою підвищення інформаційної стійкості суспільства й збереження національної безпеки.

Поділяємо підхід І. В. Мельник, яка визначає інформаційну стійкість як здатність суспільства, державних інститутів та окремих громадян адаптуватися і відновлюватися після впливу новітніх викликів [59, с. 13]. У прикладному вимірі йдеться про здатність протистояти маніпулятивним інформаційним технологіям, зберігати критичне ставлення до отримуваних повідомлень та підтримувати функціонування ключових соціальних інститутів у кризових умовах.

У науковій літературі інформаційна стійкість також трактується як результат реалізації безпекових стратегій, спрямованих на забезпечення стабільності та розвитку суспільства з урахуванням впливу інформації на свідомість і ціннісні орієнтації людей [59, с. 69]. У цьому контексті інформаційна стійкість передбачає не лише захист від агресивних інформаційних дій, а й

формування смислових рамок та поширення достовірної інформації, співвіднесеної з національними цінностями [59, с. 69]. Таким чином інформаційна стійкість, інтегрує класичні елементи інформаційної безпеки з інструментами суспільної резильєнтності, зокрема розвитком медіаграмотності, критичного мислення та довіри до незалежних і верифікованих джерел.

Загалом державні інституції зорієнтовані на захист інформаційного простору України та розбудову системи стримування інформаційних атак обґрунтовано виступають гарантом безпеки в інформаційному просторі, особливо на локальному рівні; тому до процесу посилення інформаційної стійкості залучається громадський сектор як важливий партнер публічної влади [33, с. 45–59]. Є. В. Вознюк зазначає, що вагому роль у підтримці інформаційної стійкості відіграють некомерційні організації, волонтерські проєкти, незалежні медіа та експертні центри, які нерідко компенсують дефіцит державних ресурсів у протидії інформаційним загрозам [33, с. 45–59].

Тому доцільно зауважити, що громадське суспільство виконує функцію союзника держави в секторі інформаційної безпеки, адже недержавні інституції швидко реагують на нові загрози, здійснюють суспільний контроль за діями влади, поширюють просвітницькі матеріали та формують альтернативний дискурс у публічному просторі [33, с. 49–59]. Разом із тим ефективність такого партнерства залежить від якості інституційно оформлених шляхів координації та взаємної діяльності.

Взаємодія державних інституцій із представниками громадянського суспільства реалізується через інституціоналізовані консультації, спільні робочі групи, публічні обговорення проєктів стратегічних документів, а також освітньо-дискусійні платформи [58]. Практика функціонування громадських рад при органах виконавчої влади, зокрема у сфері гуманітарної та інформаційної політики, нормативно оформлюється відповідними актами [20]. У прикладному вимірі такі інструменти дозволяють залучати громадськість і медіа до вироблення рекомендацій щодо протидії дезінформації, розбудови антикризових контурів і розвитку стратегічних комунікацій.

У компаративному вимірі доцільно врахувати модель США, що інституціоналізує координацію держави, бізнесу та експертних спільнот у кіберпросторі через механізм Joint Cyber Defense Collaborative (JCDC) [102]. Її логіка полягає у переході від фрагментарних контактів і реактивної підтримки до операційної співпраці в режимі колективної кібероборони: партнери спільно формують ситуаційну обізнаність, узгоджують пріоритети захисту та координують дії у відповідь на активні кампанії противника. Водночас у літературі підкреслюється, що ефективність такого підходу залежить від чіткості процедур координації, визначеності функцій та стандартів комунікації. Нормативне оформлення JCDC концептуалізується як програма підтримки публічно-приватного партнерства для колективних операцій кіберзахисту, оперативного обміну інформацією, узгодженого планування дій (від виявлення й запобігання до реагування, відновлення та підвищення кваліфікації), а також функціонування консультативних форматів партнерів [102].

В українському контексті адаптивним аналогом може виступати постійна міжсекторальна платформа за координаційної ролі Національного координаційного центру кібербезпеки [14] та з операційним ядром на базі CERT-UA [93]. М’яка імплементація підходу JCDC означала б закріплення регулярних спільних процедур (обмін попередженнями, спільні аналітичні продукти, узгодження пріоритетів реагування), визначення стандартів участі для критичної інфраструктури, фактчекінгових і аналітичних неурядових організацій, а також запуск сценарно-планувальних форматів для синхронізації комунікацій і технічного реагування.

Як приклад публічно-комунікаційної форми взаємодії доцільно навести Kyiv StratCom Forum [95] — дискусійну платформу, започатковану Центром стратегічних комунікацій. Такі заходи можуть виконувати роль «інтерфейсу координації» між державою і суспільством: підвищувати узгодженість наративів і практик реагування, посилювати горизонтальні зв’язки між інституціями та сприяти накопиченню і поширенню практичного досвіду протидії дезінформації [95].

Ефективність національної системи інформаційної безпеки визначається не стільки кількістю залучених інституцій, скільки якістю їхньої взаємодії та здатністю діяти як єдина мережа управління ризиками. З огляду на багатоаспектний характер інформаційної сфери, координація не може бути побудована виключно як адміністративна “вертикаль”. Методологічно обґрунтованою є вертикально-горизонтальна модель, яка одночасно забезпечує: стратегічне визначення цілей і підзвітність; міжвідомчу синхронізацію в операційних процесах; інтеграцію недержавних акторів у контури запобігання та реагування.

Вертикальний вимір координації забезпечує послідовність політики та перетворення стратегічних пріоритетів на стандарти, процедури й практику. У межах цієї логіки система вибудовується за принципом “стратегія, управління, виконання”:

– Стратегічний рівень задає рамку національних інтересів і критичності: які об’єкти є пріоритетними, які загрози мають системний характер, які інструменти протидії допустимі з погляду пропорційності та законності. Саме тут формується політична відповідь на комплексні ризики (кібератаки, інформаційні операції, втручання у процеси управління, підрив довіри).

– Урядовий рівень здійснює операціоналізацію стратегічних рішень: затверджує підзаконні акти, плани, вимоги та стандарти; розподіляє ресурси; організовує виконання через міністерства й відомства; формує механізми моніторингу та оцінювання результативності.

– Виконавчий/об’єктовий рівень охоплює реалізацію політик у конкретних органах влади, а також у системах операторів критичної інфраструктури та цифрових сервісів. На цьому рівні стратегія “матеріалізується” у технічних і організаційних практиках: управління вразливостями, аудит, контроль доступу, резервування, інцидент-менеджмент, навчання персоналу, плани безперервності та відновлення.

Ключова вимога до вертикальної координації — керованість повного циклу: щоб рішення верхнього рівня мали визначених виконавців, метрики, строки, бюджетні механізми та канали зворотного зв'язку. Без цього система ризикує залишатися нормативно насиченою, але процесно слабкою.

Горизонтальний вимір координації є критичним у ситуаціях, де загроза не "належить" одному органу, а перетинає компетенції кількох контурів. Йдеться насамперед про взаємодію СБУ, Держспецзв'язку та CERT-UA, Національної поліції (кіберполіції), МОУ та ЗСУ і профільних органів виконавчої влади. У сучасних умовах саме горизонтальна синхронізація визначає швидкість і якість реагування, а також здатність формувати узгоджену ситуаційну обізнаність.
Горизонтальна координація спирається на три групи інструментів:

– єдині протоколи та реагування: стандартизовані сценарії дій для типових інцидентів (атаки на доступність, компрометація облікових записів, ураження ланцюга постачання, витік даних, інциденти на об'єктах критичної інфраструктури). протоколи мають описувати не лише технічні кроки, а й управлінські рішення: хто є "ведучим інциденту", які критерії ескалації, хто ухвалює рішення щодо публічних повідомлень, як узгоджується режимність і доступ до матеріалів.

– обмін даними: сумісні формати й канали передачі інформації про загрози, індикатори компрометації, вразливості та хід реагування. для системи принципово важливо зменшувати "відомчі силоси" і забезпечувати швидкий перехід від фрагментів даних до узгодженої картини ризиків.

– розмежування зон відповідальності та інтерфейси взаємодії: особливо на стику трьох логік — технічного реагування, контррозвідувального виміру й процесуального розслідування. без формалізованої моделі "ведення інциденту" виникають конфлікти пріоритетів, паралельні дії та розмивання відповідальності за кінцевий результат.

Отже, горизонтальна координація — це не “паралель” до вертикалі, а механізм, який робить систему функціонально цілісною в умовах міжсекторних і міжвідомчих загроз.

Зазначимо, що координація в інформаційній безпеці охоплює щонайменше три взаємопов’язані контури, які утворюють мінімально необхідний цикл управління:

– запобігання: розроблення і впровадження стандартів, управління ризиками, аудит, підготовка персоналу, навчання та кібергігієна, тестування планів безперервності. Це контур, який перетворює безпеку на регулярну управлінську функцію, а не на реакцію “після інциденту”.

– реагування: виявлення інцидентів, технічна локалізація, мінімізація наслідків, кризове управління та координація комунікацій. Його результативність визначається швидкістю ескалації, узгодженістю рішень і здатністю відновлювати критичні сервіси в контрольованому режимі.

– притягнення до відповідальності: розслідування, збирання та збереження цифрових доказів, процесуальне супроводження, кримінально-правова реакція. Цей контур завершує цикл, забезпечуючи превентивний ефект стримування та відновлення справедливості.

Вказаний цикл доцільно доповнювати четвертим елементом — напрямом відновлення та інституційного навчання, тобто післяінцидентний аналіз, оновлення стандартів і протоколів, корекція моделей загроз, підвищення зрілості процесів. Саме він забезпечує еволюцію системи й зменшує повторюваність інцидентів.

Окремий вимір становить взаємодія з недержавними учасниками — операторами інфраструктури, ІТ-компаніями, фінансовим сектором, провайдерами цифрових послуг, а також громадськими ініціативами та експертним середовищем. З огляду на те, що значна частина мереж, платформ і даних перебуває у приватному або змішаному середовищі, координація з недержавними акторами є не допоміжною, а системоутворюючою.

Критичними стають так звані режими довіри, які дозволяють співпрацю масштабовано й без втрати легітимності:

– обмін індикаторами компрометації та технічними даними на стандартизованих засадах і в визначені часові рамки;

– правові гарантії конфіденційності технічної інформації (щоб участь у реагуванні не перетворювалася на непропорційні репутаційні чи правові ризики для операторів за умови добросовісної поведінки);

– спільні навчання і відпрацювання сценаріїв із залученням ключових секторів;

– узгоджені кризові комунікації, які запобігають паніці, підриву довіри й експлуатації інцидентів противником у когнітивному вимірі;

– чітке розмежування відповідальності, щоб партнерство не деградувало у перекладання функцій або ризиків.

Таким чином, координація суб’єктів забезпечення інформаційної безпеки має будуватися як комбінована вертикально-горизонтальна модель, у межах якої стратегічна вертикаль забезпечує єдність цілей і ресурсне підкріплення політики, а горизонтальні механізми — міжвідомчу керованість інцидентами у реальному часі. Функціонально така координація повинна покривати контури запобігання, реагування, притягнення до відповідальності та інституційного навчання. Окремою умовою стійкості є інституціоналізована інтеграція недержавних акторів через правові, технічні й організаційні механізми довіри та партнерства. Саме поєднання цих елементів формує керовану й результативну архітектуру інформаційної безпеки, здатну діяти в умовах гібридних загроз і високої динаміки цифрового середовища.

Отже, інформаційна стійкість у воєнних умовах постає як інтегральна здатність держави, суспільства й громадян одночасно протидіяти дезінформації, підтримувати довіру до верифікованих джерел та забезпечувати безперервність функціонування ключових інститутів. Її досягнення неможливе виключно державними засобами: необхідним є партнерство з громадянським суспільством,

яке виконує компенсаторні, контрольні та просвітницькі функції. Найперспективнішим напрямом розвитку є інституціоналізація стандартних процедур координації (за аналогією до JCDC), посилення ролі НКЦК і CERT-UA в операційній взаємодії, розвиток стратегічних комунікаційних платформ, а також системна медіаосвіта. Водночас воєнні обмеження, дефіцит локальної спроможності та звуження ресурсної бази громадського сектору потребують цільових рішень — від підтримки каналів діалогу до ресурсного забезпечення партнерських мереж і підвищення комунікаційної компетентності публічної влади.

Висновки до розділу 2

Підсумовуючи, доцільно узагальнити результати аналізу за трьома взаємопов'язаними контурами — нормативним, інституційним та партнерства — які в сукупності формують цілісну архітектуру забезпечення інформаційної безпеки України.

Нормативний контур забезпечує базові правові рамки функціонування інформаційної сфери та визначає легітимні межі захисту національних інтересів. Конституційні приписи, передусім положення про ІБ задають фундамент для галузевого законодавства, а рамкові закони формують загальні принципи, визначають суб'єктів і ключові напрями державної політики, однак значною мірою делегують конкретизацію загроз і практичних інструментів стратегічним та підзаконним актам. Профільні нормативні масиви забезпечують баланс між гарантіями прав людини та безпековими потребами, створюючи юридичні режими доступу, обмежень і відповідальності, а також підвалини довіри до інформаційних систем. Водночас визначальними залишаються проблеми правозастосування: динаміка технологічних змін і гібридних практик агресора випереджає темпи регуляторної адаптації; складним є підтримання пропорційності між безпековими обмеженнями та свободою слова; воєнні умови об'єктивно ускладнюють реалізацію процедур контролю й відповідальності. Отже, ефективність нормативного контуру залежить від внутрішньої

узгодженості правового масиву, точності дефініцій, усунення прогалин та спроможності держави забезпечувати виконання стратегічних рішень через дієві підзаконні механізми.

Інституційна система забезпечення інформаційної безпеки України може бути охарактеризована як динамічна, багатокомпонентна модель, яка вже довела свою життєздатність у надзвичайно високому рівні загроз. Її подальше вдосконалення має ґрунтуватися на умовах, де ключовими стають стандартизація партнерства, розвиток людського капіталу та інституційна підзвітність забезпечує не лише зниження поточних вразливостей, а й формування стратегічної резильєнтності держави в умовах тривалого інформаційного протиборства.

Інформаційна стійкість у воєнно-гібридному середовищі постає як комплексна здатність суспільства, інститутів і громадян адаптуватися, зберігати критичність до інформації та відновлюватися після деструктивних впливів. У цьому сенсі держава не може бути єдиним гарантом стійкості, особливо на локальному рівні; необхідною умовою виступає кооперація з громадянським суспільством (НУО, волонтерські ініціативи, незалежні медіа, експертні центри), яке забезпечує моніторинг, фактчекінг, просвітництво, суспільний контроль і вироблення альтернативних аналітичних продуктів. Практичні формати партнерства включають консультації, робочі групи, громадські ради, стратегічно-комунікаційні платформи та спільні освітні кампанії з медіаграмотності. Водночас наявні системні бар’єри: воєнні режимні обмеження та зниження регулярності комунікації, дефіцит спроможностей на місцевому рівні, зменшення ресурсної бази громадського сектору в громадах. Тому необхідним є перехід від ситуативних контактів до інституціоналізованої, стандартизованої взаємодії з чіткими правилами участі, прогнозованими процедурами обміну інформацією, сценарним плануванням і підтримкою сталих мереж партнерств. У компаративному вимірі продуктивним орієнтиром є моделі операційної міжсекторальної координації на кшталт JCDC, адаптація яких може бути реалізована через розвиток постійної платформи взаємодії за

координаційної ролі НКЦК та операційного ядра CERT-UA з відповідним інституційним забезпеченням.

Отже, ефективна інформаційна безпека України формується лише за умови синхронізації трьох контурів: нормативного (який задає правові режими та гарантії), інституційного (який забезпечує координацію і виконання спеціалізованих функцій) та суспільної стійкості і партнерств (який нарощує резильєнтність через участь громадянського сектору й медіаосвіту). Стратегічним результатом такої синергії має стати перехід до системної, превентивної моделі: з чіткими правилами правозастосування, узгодженими механізмами управління ризиками, міжвідомчою координацією у протидії інформаційним і кібернетичним загрозам.

РОЗДІЛ ІІІ

ШЛЯХИ УДОСКОНАЛЕННЯ ОСНОВНИХ ЗАСАД ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МВС УКРАЇНИ

3.1. Медіаграмотність і культура інформаційної гігієни як безпекові засади інформаційного простору

Повномасштабна війна засвідчила, що інформаційний простір фактично набув ознак повноцінного «театру» протиборства, а забезпечення його стійкості та захищеності стало одним із ключових пріоритетів безпеки держави.

Одночасно курс України на євроінтеграцію зумовлює необхідність гармонізації засад національної системи інформаційної безпеки з правовими вимогами Європейського Союзу, зокрема Директиви (EU) 2022/2555 (NIS2). Вона встановлює вимоги до кібербезпеки, поширюється на сектори енергетики, транспорту, охорони здоров'я та державного управління, а також запроваджує посилені наглядові механізми й стандартизовані санкції для держав-членів [97]. Практичний аналіз забезпечення кібербезпеки, підвищення культури інформаційної безпеки й медіаграмотності населення, а також узагальнення уроків, здобутих у ході повномасштабної війни, набуває особливого значення [17].

З огляду на це доцільним є предметний аналіз інформаційного простору та його стійкості у кібернетичному (технологічному) вимірі. Практика війни демонструє, що протиборство в інформаційному середовищі має співрозмірне значення з веденням бойових дій у фізичному просторі, оскільки безпосередньо впливає на здатність держави, суспільства та сектору безпеки бути дієздатними в умовах кризових загроз. Стійкість інформаційного простору визначається, з одного боку, рівнем кібербезпеки (спроможністю захищати технічну інфраструктуру, інформаційно-комунікаційні мережі та дані), а з іншого — станом інформаційної безпеки у широкому розумінні, що охоплює протидію дезінформації й пропаганді та захист населення від маніпулятивних впливів [17]. За останні роки Україна накопичила унікальний досвід в обох напрямах,

поєднавши болючі уроки з прикладами результативної протидії. Це зумовлює потребу системного аналізу практик і інструментів підвищення стійкості держави та суспільства на основі конкретних механізмів реагування, а також окреслення пріоритетних напрямів удосконалення наявних систем.

З 2014 року проти України здійснюються безпрецедентні масовані кібератаки на державні органи, банківський сектор, енергетику, телекомунікаційні мережі тощо. За різними оцінками, ці операції були спрямовані на підрив системи інформаційної безпеки, ураження критичної інфраструктури та обмеження доступу населення до достовірної інформації [96]. Характерною ознакою таких дій стало поєднання ракетних ударів по об’єктах інфраструктури з паралельними атаками на їхні інформаційні системи [43]. Упродовж першого року повномасштабного вторгнення фіксувалися сотні серйозних інцидентів, що мали критичний вплив на функціонування органів влади та повсякденне життя громадян [96]. Показовим прикладом стала кібератака 28 березня 2022 року на одного з найбільших провайдерів фіксованого зв’язку в Україні — «Укртелеком», унаслідок якої доступність мережі тимчасово знизилася до незначної частки від довоєнного рівня [92]. Іншим резонансним випадком стала спроба ураження програмних компонентів енергетичного сектору шляхом упровадження шкідливого програмного забезпечення в мережі операторів розподілу електроенергії з метою спричинення масштабних відключень.

Зазначені інциденти вдалося нейтралізувати завдяки високому рівню готовності українських кіберзахисників, скоординованим діям державних органів та підтримці міжнародних партнерів [93]. Успіх у протистоянні загрозам значною мірою забезпечувався попередніми інвестиціями у розвиток кібербезпеки та налагодженою взаємодією між суб’єктами забезпечення інформаційної й кібербезпеки. Критичну роль відіграли команди реагування на цифрові інциденти, зокрема CERT-UA [93]. Важливим чинником стало також залучення волонтерської спільноти, передусім неформального об’єднання «IT-армія України», ініційованого Міністерством цифрової трансформації у 2022

році для здійснення операцій у кіберпросторі проти ворожих цифрових ресурсів [94]. Хоча правовий статус таких практик є предметом фахової дискусії, вони стали помітним елементом сучасної практики кібервійни.

Не менш важливим компонентом стійкості є захист критичної інформаційної інфраструктури, до якої належать системи зв'язку, енергомережі, транспортні та фінансові системи — об'єкти, від безперебійного функціонування яких залежить життєдіяльність країни [16]. Повномасштабна війна висвітлила нагальну потребу комплексного захисту цих систем як від кібератак, так і від фізичних (кінетичних) загроз.

Підвищення та вдосконалення рівня кіберстійкості передбачає реалізацію комплексу взаємопов'язаних заходів, серед яких:

– багатоетапний кіберзахист: побудова багатошарової системи захисту для органів державної влади, державних електронних реєстрів і критичних баз даних; запровадження безперервного моніторингу та аудиту безпеки, багатофакторної автентифікації, сучасних криптографічних механізмів і резервного копіювання даних [93];

– оперативне реагування та відновлення: розроблення процедур ізоляції/відключення уражених сегментів мережі з метою локалізації атаки, а також регламентів швидкого відновлення критичних функцій і сервісів (планування безперервності та аварійного відновлення);

– партнерство з приватним сектором: системна взаємодія держави з IT-компаніями, інтернет-провайдерами та операторами зв'язку для обміну технічною інформацією про інциденти й стан мереж, відновлення телекомунікацій на постраждалих та деокупованих територіях, а також забезпечення каналів зв'язку для потреб сектору безпеки [22].

Стратегічно важливою є орієнтація України на імплементацію вимог Директиви (EU) 2022/2555 (NIS2), яка підвищує загальноєвропейські стандарти кібербезпеки через ширше охоплення секторів, вимоги до управління ризиками та звітності (повідомлення про значні інциденти, та через акцент на безпеці

ланцюгів постачання і координаційних спроможностях держав щодо реагування [97].

Ключовим компонентом стійкості інформаційного простору став захист суспільства від ворожих інформаційно-психологічних впливів. Протидія цим загрозам стала завданням не лише державного сектору, а й громадянського суспільства та медіаспільноти, що зумовило формування багаторівневого підходу до нейтралізації дезінформації [94].

По-перше, було розгорнуто механізми оперативного інформування та превентивної комунікації щодо типових маніпулятивних наративів і потенційних фейків ще до їх масового поширення. Важливу роль у цьому відіграє централізована система державних комунікацій з реагування на інформаційні атаки, до якої, зокрема, залучено Центр протидії дезінформації та суб'єктів сектору безпеки [21].

По-друге, було посилено протидію ворожій пропаганді в медіапросторі. Ще до початку повномасштабної війни РНБО стала ініціатором застосування персональних санкцій щодо окремих інформаційних ресурсів, які поширювали проросійські наративи, спрямовані на дестабілізацію внутрішньополітичної ситуації [21].

По-третє, розвивалася система фактчекінгу як на урядовому, так і на громадському рівнях: Центр протидії дезінформації регулярно оприлюднює огляди фейків та їх спростування, тоді як громадські ініціативи й спеціалізовані платформи системно виявляють маніпулятивні матеріали, уточнюють контекст і відновлюють фактичну картину подій, підвищуючи загальну інформаційну стійкість суспільства [21].

Водночас не менш важливою передумовою довгострокової стійкості держави є високий рівень культури інформаційної безпеки серед населення. Вона охоплює обізнаність громадян щодо інформаційних ризиків, сформовані навички критичного мислення й медіаграмотності, а також систему цінностей та установок, що знижують вразливість до маніпулятивного впливу [22]. Для України, яка протистоїть інтенсивним інформаційно-психологічним операціям і

пропаганді держави-агресора, формування такої культури має стратегічне значення.

Вагоме місце у підвищенні медіаграмотності посідають державні ініціативи в освітній сфері. Усвідомлення значущості медіаграмотності та інформаційної культури інституційно формувалося ще до повномасштабного вторгнення, зокрема через ухвалення Концепції впровадження медіаосвіти в Україні та відповідні управлінські рішення у сфері освіти. Останніми роками ця політика отримала додатковий імпульс у вигляді спеціальних програм і стратегічних документів, у яких наголошується на необхідності формування відповідних компетентностей «з дитинства», тобто шляхом інтеграції їх до освітніх програм різних рівнів [43].

У загальній середній освіті елементи медіаграмотності доцільно інтегрувати у громадянську освіту, українську мову і літературу, історію та інші дисципліни. У закладах вищої освіти розвиваються освітні програми й спеціалізації, пов’язані з інформаційною та кібербезпекою, стратегічними комунікаціями й цифровою культурою. Для державних службовців реалізуються програми підвищення кваліфікації з питань стратегічних комунікацій, кібергігієни та протидії дезінформації [22]. У сукупності ці практики формують контури системи неперервної освіти у сфері інформаційної безпеки.

Значну роль у формуванні культури інформаційної безпеки відіграє громадянське суспільство, оскільки вона включає не лише вміння розпізнавати фейки, а й відповідальне ставлення до споживання та поширення інформації. Українське суспільство в перші місяці повномасштабної війни продемонструвало високий рівень самообмеження щодо публікації потенційно чутливої інформації та готовність дотримуватися принципів інформаційної гігієни. Держава через стратегічні комунікації закріплювала ці установки, поєднуючи їх із глобальною інформаційною кампанією на підтримку України [43].

Отже, підвищення стійкості інформаційного простору України в умовах війни забезпечується синергією заходів кіберзахисту та протидії пропаганді.

Значну роль відіграє міжнародна підтримка: обмін інформацією про загрози із союзниками, надання технічних ресурсів, спільні ініціативи в межах ЄС і НАТО, а також консолідація зусиль для протидії глобальним дезінформаційним кампаніям [93].

Водночас війна оголила низку структурних проблем, що потребують подальшого розв'язання. До пріоритетних завдань належать:

– розвиток власних кіберспроможностей, зокрема створення повноцінних кібервійськ у структурі Сил оборони відповідно до стратегічних документів [16];

– упровадження сучасних стандартів захисту критичної інфраструктури з орієнтацією на вимоги NIS2 та суміжних актів ЄС [97];

– удосконалення законодавства щодо відповідальності за інформаційні злочини й кіберзлочини, а також запровадження державної системи оцінювання ефективності заходів кібербезпеки та інформаційної безпеки (індикаторів стійкості);

– підтримка та інституціоналізація громадських ініціатив у сфері фактчекінгу, медіаграмотності й розвитку культури безпеки [4322].

Стійкість інформаційного простору України у воєнний період має комплексну природу і формується на перетині технологічних, організаційних та соціокультурних чинників. Практика війни підтвердила, що ефективний кіберзахист критичної інфраструктури (через багаторівневі моделі безпеки, безперервний моніторинг, готовність до відновлення та державно-приватну взаємодію) є необхідною, але недостатньою умовою загальної захищеності. Не менш визначальними виступають інституційні механізми протидії дезінформації (превентивні комунікації, санкційні інструменти, багаторівневий фактчекінг) та розвиток культури інформаційної безпеки населення, що включає медіаграмотність, критичне мислення й відповідальні практики інформаційної поведінки.

Подальше посилення стійкості потребує системної інституціоналізації здобутих воєнних практик: розвитку національних кіберспроможностей і кібервійськ, інтеграції стандартів захисту інфраструктури відповідно до NIS2,

удосконалення правових механізмів відповідальності та впровадження вимірюваних метрик ефективності державної політики. У сукупності ці кроки забезпечують перехід від реагування на інциденти до зрілої моделі управління ризиками, сумісної з європейським безпековим середовищем і здатної підтримувати довгострокову резильєнтність держави та суспільства.

3.2. Удосконалення державного механізму забезпечення інформаційної безпеки МВС України в умовах цифрової трансформації

В умовах прискореного розвитку інформаційних технологій і поглиблення цифрової трансформації суспільства забезпечення інформаційної безпеки набуває статусу одного з пріоритетних напрямів державної політики. Інформаційні ресурси й комунікаційні мережі дедалі більшою мірою визначають результативність економічних процесів, ефективність публічного управління та інтенсивність соціальної взаємодії, що об’єктивно підвищує залежність держави і суспільства від стійкості цифрових сервісів. За цих умов зростає вразливість інформаційних систем до багаторівневих загроз (кібернетичних, організаційних, інформаційно-психологічних), а також ризики порушення безперервності функціонування критичної інформаційної інфраструктури. Це зумовлює необхідність розроблення і впровадження комплексних організаційно-правових та технологічних механізмів захисту, спрямованих на попередження інцидентів, мінімізацію їх наслідків і відновлення критично важливих систем.

Для України, яка інтенсивно інтегрується у глобальний інформаційний простір, проблематика інформаційної безпеки є стратегічно значущою. Держава має не лише адаптуватися до динамічних змін цифрового середовища, а й забезпечувати проактивний захист національних інтересів. Реалізація такої політики передбачає комплексний підхід, що охоплює: 1) удосконалення нормативно-правового регулювання; 2) підвищення рівня професійної підготовки кадрів; 3) розвиток технологічних спроможностей; 4) посилення міжвідомчої координації та узгодженості управлінських рішень. У цьому контексті розроблення рекомендацій щодо удосконалення державного

механізму інформаційної безпеки є актуальним науково-практичним завданням, оскільки сприяє зміцненню міжнародної суб’єктності держави, сталому розвитку суспільства та формуванню надійної системи протидії загрозам.

Засади інформаційної безпеки слід розглядати у двох взаємопов’язаних вимірах: по-перше, як здатність держави захищати національні інтереси (у тому числі економічні) від внутрішніх і зовнішніх загроз; по-друге, як спроможність суспільства та інституцій забезпечувати безперервність і відновлюваність базових процесів життєдіяльності за умов інформаційних впливів та технологічних ризиків. Високий рівень інформаційної безпеки є необхідною передумовою сучасного соціально-економічного розвитку, оскільки гарантує стабільність цифрових сервісів, прогнозованість управлінських рішень і сталість суспільних комунікацій.

Результативність нормативно-правового регулювання у цій сфері має поєднуватися з належним інституційним і процедурним забезпеченням: доступом до релевантних інформаційних ресурсів, їх якісною обробкою та використанням у процесі ухвалення рішень. Сукупно це становить основу як підтримання інформаційної безпеки, так і реалізації послідовної державної політики у відповідній сфері.

Наукові джерела фіксують наявність суттєвих недоліків у нормативній базі інформаційної безпеки. Так, О. Ю. Борисов зазначає, що «нормативно-правова база наразі не створена в належному, придатному до функціонування вигляді, внаслідок цього конкретні функції органів влади у сфері інформаційної безпеки фактично не визначені, а система їх формування часто змінюється» [29, с. 115]. Ця позиція вказує на проблему фрагментарності регулювання та невизначеності компетенцій, що знижує керованість системи й ускладнює практичну реалізацію політики.

С. О. Лисенко обґрунтовує необхідність конституційних засад як нормативного підґрунтя легітимного регулювання інформаційної безпеки, наголошуючи, що «вплив сучасних реалій на систему управління забезпеченням інформаційної безпеки зумовлює формування конституційних засад як

нормативного підґрунтя її легітимного регулювання» [52, с. 160]. Автор підкреслює, що систематизація норм має усувати надмірну процедурну складність та необґрунтовані бар’єри [52, с. 160], тобто сприяти підвищенню ефективності правозастосування.

У літературі також обстоюється підхід, за якого державна політика інформаційної безпеки повинна спиратися на методологічно вивірені та систематизовані розробки, інтегровані в єдину концепцію, де політика розглядається як цілісна сукупність цілей, інтересів і цінностей, а також стратегії й тактики, що реалізуються державою для регулювання процесів інформаційної взаємодії у ключових сферах життєдіяльності [75].

О. Довгань пов’язує успішну інтеграцію України до міжнародних інформаційних обмінів із концентрацією правової діяльності на пріоритетних напрямах, зокрема: формуванні системи правових актів для збереження і розвитку національних інформаційних ресурсів; адаптації законодавства до міжнародно-правових підходів; участі у міжнародній правотворчості; створенні правової основи міжнародної співпраці щодо протидії кібертероризму та іншим видам інформаційної злочинності [38, с. 69–70]. З цього випливає, що нормативне забезпечення має одночасно виконувати внутрішню (регулятивну) та зовнішню (інтеграційну) функції.

Відповідно до позиції О. І. Пугачова, ключовими векторами вдосконалення нормативного забезпечення є: гармонізація національного законодавства з міжнародними стандартами та розвиток співпраці з міжнародними організаціями й країнами-партнерами; ухвалення спеціалізованих актів щодо конкретних сегментів (кіберзахист критичної інфраструктури, протидія інформаційним операціям, захист ресурсів органів державної влади) із визначенням повноважень і відповідальності; посилення контролю й юридичної відповідальності, включно з ефективними санкціями [80]. Вказані напрями можуть бути розглянуті як «каркас» модернізації правових основ.

О. Солодка акцентує на значущості зміцнення організаційних основ забезпечення інформаційної безпеки, насамперед через координацію діяльності

суб’єктів у протидії інформаційній агресії та забезпеченні кібербезпеки, розвиток державно-приватного партнерства, запровадження демократичного контролю та удосконалення комунікаційної політики у взаєминах із суспільством [85, с. 40]. Отже, організаційний компонент охоплює не лише управлінську архітектуру, а й механізми легітимації, підзвітності та взаємодії.

Удосконалення організаційного забезпечення передбачає чітке визначення повноважень і відповідальності інституцій з метою усунення дублювання функцій і прогалин у компетенціях. До базових кроків доцільно віднести:

– створення дієвого механізму міжвідомчої координації та взаємодії спеціалізованих органів;

– належне ресурсне забезпечення та контроль за виконанням програм і планів дій;

– розвиток системи моніторингу інформаційного простору і наукового супроводу для своєчасного виявлення нових загроз та регулярного оновлення організаційних рішень.

Забезпечення кібернетичної безпеки є складовою організаційної основи інформаційної безпеки, тому кібербезпекова інфраструктура потребує системного зміцнення. Наголошується, що «підвищення кіберстійкості передбачає здатність усіх ключових суб’єктів своєчасно виявляти та ефективно реагувати на кібератаки, захищати критичну інформаційну інфраструктуру та підтримувати режим постійної готовності» [11]. Практичним наслідком цього підходу є потреба у впровадженні державної системи управління інцидентами та створенні ситуаційних центрів, які забезпечують централізований моніторинг і реагування.

Окремого значення набуває формування операційно-координаційного «шару» взаємодії, який забезпечує спільне планування та синхронізовані дії державних і недержавних учасників у режимі реальних інцидентів. У цьому аспекті показовою є модель США — JCDC, що розглядалася як відповідь на обмеження «добровільних» партнерств та як спроба перевести кооперацію у

площину узгоджених планів і спільних операційних дій [102]. Водночас незалежні оцінки міжвідомчої взаємодії вказують на необхідність процедурної визначеності й дисципліни координації, інакше співпраця залишається частково реалізованою [102]. Законодавча концепція JCDC формалізує його функції як підтримання стратегічних і операційних партнерств, розроблення планів кібероборони, збирання й поширення релевантної інформації, підготовку спільних аналітичних продуктів та створення Advisory Council для управління ініціативами й стандартами взаємодії [102]. Це дає підстави інтерпретувати JCDC як механізм операціоналізації державно-приватного партнерства.

Інформаційно-технологічний та соціально-освітній елементи (та іміджевий компонент) як взаємодоповнювальні контури безпеки

Методологічно обґрунтованою є позиція О. Солодкої про те, що інформаційна безпека має забезпечуватися не лише через нарощування технологічних можливостей, а й через її усвідомлення всіма суб'єктами інформаційних відносин; у зв'язку з цим актуалізуються питання інформаційної етики, приватності та захисту від маніпулятивних впливів [85, с. 42]. Такий підхід зумовлює розгляд забезпечення інформаційної безпеки як взаємодії щонайменше двох взаємодоповнювальних елементів: інформаційно-технологічного та соціально-освітнього.

Інформаційно-технологічний елемент охоплює сукупність технічних і організаційно-технічних спроможностей держави щодо захисту інформаційних систем і даних, підтримання безперервності функціонування та відновлюваності критично важливих сервісів, а також підвищення кіберстійкості інфраструктури в умовах кібератак і технологічних збоїв.

Соціально-освітній елемент спрямований на формування людського й інституційного потенціалу інформаційної безпеки: підвищення цифрової та медіаграмотності населення, підготовку і перепідготовку фахівців, розвиток освітньої й науково-методичної бази, закріплення практик відповідальної поведінки в інформаційному просторі (у тому числі щодо етики та приватності). Він забезпечує суспільну стійкість до інформаційно-психологічних впливів,

знижує вразливість до маніпуляцій і підсилює адаптивність у середовищі швидких технологічних змін.

Отже, ефективність державної політики у сфері інформаційної безпеки визначається синергією: технологічні засоби формують інфраструктурний контур захисту, тоді як освіта і культура безпеки забезпечують його результативність у практиці взаємодії держави, суспільства та особи. Додатково протидія дезінформації та інформаційним операціям має бути інтегрована зі стратегічними комунікаціями й формуванням позитивного міжнародного іміджу України як елементу інформаційної безпеки: рівень довіри всередині країни та міжнародної підтримки прямо впливає на стійкість до ворожих впливів, розширення співробітництва та залучення ресурсів розвитку.

Практичні напрями формування стійкості до дезінформації та підтримки якісного медіасередовища

Стійкість суспільства значною мірою визначається рівнем медіаграмотності, здатністю критично сприймати інформацію та протидіяти маніпуляціям, а також сформованістю культури кібергігієни. До проблем соціально-освітнього характеру доцільно віднести нерівномірний вплив якісних національних медіа, зокрема на місцевому рівні, а також ризики тиску й погроз на адресу журналістів і медіаактивістів у воєнних умовах. За відсутності паралельних заходів із просвіти громадян і підтримки незалежних медіа суспільство залишається вразливим до пропагандистських впливів.

Для формування суспільства, стійкого до дезінформації, необхідна комплексна стратегія, що орієнтована на довгострокове підвищення когнітивної та комунікаційної стійкості. До ключових практичних напрямів належать:

– масштабне підвищення медіаграмотності населення через наскрізні програми медіаосвіти та навчальні модулі для різних вікових і професійних груп;

– інституційна співпраця держави, медіа та громадського сектору для обміну даними про інформаційні кампанії, координації публічних роз’яснень і вироблення стандартів реагування;

– вдосконалення законодавства та розвиток саморегуляції медіа із збереженням балансу між протидією загрозам і гарантіями свободи вираження поглядів, підвищенням прозорості медіавласності та забезпеченням захисту журналістів.

Аналіз дає підстави стверджувати, що ІБ України є багатокомпонентною системою, у якій нормативно-правові, організаційні, інформаційно-технологічні та соціально-освітні елементи утворюють взаємопов'язаний комплекс. Нормативно-правове забезпечення має бути спрямоване на гармонізацію з міжнародними стандартами, розроблення спеціалізованих актів для окремих сегментів інформаційної сфери та на вдосконалення інструментів контролю й юридичної відповідальності. Організаційне забезпечення вимагає побудови дієвої координаційної архітектури, посилення міжвідомчої взаємодії, усунення дублювання функцій, формування операційно-координаційних механізмів реагування на інциденти та інтеграції державно-приватного партнерства. Інформаційно-технологічний контур потребує модернізації технічних рішень, розвитку і захисту критичної інформаційної інфраструктури, створення та посилення національних спроможностей реагування (CERT) та інтегрованих систем моніторингу. Соціально-освітній контур має забезпечити культуру безпеки, медіаграмотність, кадровий потенціал і науково-методичний супровід. У сукупності реалізація цих напрямів на засадах міжсекторальної взаємодії створює передумови для стійкої, адаптивної та результативної системи захисту національного інформаційного простору.

Отже засади ІБ постають як комплексна система, що вимагає одночасного посилення нормативно-правових, організаційних, технологічних і соціально-освітніх компонентів. Фрагментарність регулювання та нечіткість розподілу компетенцій знижують керованість системи і вимагають концептуальної систематизації норм, гармонізації з міжнародними підходами, уточнення відповідальності суб'єктів та підсилення механізмів контролю. Організаційний вимір має еволюціонувати від формальної координації до операційної взаємодії у реальних інцидентах, що передбачає розвинену інфраструктуру управління

інцидентами, ситуаційні центри та інструменти «операціоналізації» партнерств (зокрема за логікою платформ на кшталт JCDC). Технологічна стійкість критичної інфраструктури та національних кіберспроможностей повинна доповнюватися соціально-освітньою резильєнтністю: медіаграмотністю, культурою кібергігієни та підтримкою якісного медіасередовища. Додатковим підсилювальним чинником виступає позитивний міжнародний імідж України як елемент стратегічних комунікацій, що підвищує довіру та ресурсну підтримку, а отже — загальну стійкість держави в інформаційному протиборстві.

3.3. Інституційні засади забезпечення інформаційної безпеки: зарубіжний досвід та його релевантність для МВС України

Сучасна інформаційна безпека вийшла за межі охорони інформації у вузькому розумінні та трансформувалася у комплексну категорію національної стійкості. Йдеться про здатність держави, економіки й суспільства забезпечувати безперервність управління, сталість функціонування критичних сервісів і збереження суспільної довіри в умовах кібератак, деструктивних інформаційних операцій, маніпулятивних впливів у цифровому середовищі, компрометації ланцюгів постачання та технологічної залежності. Відповідно, зарубіжний досвід є цінним не лише як сукупність окремих заходів, а передусім як зразок інституційних і нормативних архітектур, які забезпечують керованість ризиків, координацію реагування та належну підзвітність суб’єктів у сфері безпеки.

Необхідність удосконалення нормативно-правової бази України та практик залучення громадськості у цій сфері зумовлюється сукупністю чинників, серед яких: гібридний характер сучасного інформаційного протиборства; розширення євроінтеграційного порядку денного та поглиблення інтеграції України до європейського інформаційного простору; високі темпи інформатизації й цифровізації соціальних процесів; потреба в результативній протидії дезінформаційним впливам і системному розвитку медіаграмотності громадян.

Зазначені фактори детермінують доцільність аналізу зарубіжного досвіду, який дозволяє:

– сформувати модель удосконалення засад інформаційної безпеки та можливості її імплементації в Україні (організаційні рішення, законодавчі моделі, механізми взаємодії суб'єктів);

– виявити типові закономірності ідентифікації, запобігання та протидії загрозам інформаційній безпеці на різних рівнях;

– уточнити роль і місце інформаційної безпеки та зв'язки відповідної системи в рамках національної безпеки, включно з її внутрішньою архітектонікою та способами концептуального відображення;

– виокремити етапи розвитку практик і проаналізувати чинники їх еволюції, а також зміни структурних елементів і принципів функціонування.

Охоплення наведених юрисдикцій забезпечує більш повну й збалансовану емпіричну базу, підвищує достовірність і прикладну цінність висновків для України. Тому, далі розглянемо досвід окремих держав у розрізі інституційних та нормативних механізмів.

Досвід США є одним із найбільш репрезентативних, зважаючи, зокрема, на системну підтримку України у протидії інформаційним загрозам у період повномасштабної війни. Як зазначає В. М. Брижко, в «американському науковому дискурсі теорія національної безпеки інституціоналізувалася в межах політології та включила окремий напрям забезпечення ІБ» [30, с. 34].

Практичний (інституційно-операційний) вимір американської моделі пов'язаний із механізмами оперативної координації держави з приватним сектором, зокрема через CISA Joint Cyber Defense Collaborative (JCDC), що передбачає спільне планування, обмін даними та координацію дій у відповідь на масштабні кампанії атак.

Нормативно-методичний вимір формують, з одного боку, Executive Order 14028 [98**Error! Reference source not found.**], спрямований на підвищення рівня кіберзахисту, а з іншого — рамкові інструменти управління ризиками на кшталт NIST Cybersecurity Framework 2.0 [99**Error! Reference source not found.**], який задає уніфіковану «мову» кіберризик-менеджменту та посилює управлінську функцію Govern як надбудову стратегічного керування.

О. В. Соснін вказує, що «практична політика США у сфері інформаційної безпеки зорієнтована на посилення позицій держави в глобальному інформаційному просторі й водночас поєднує інструменти лібералізації та державного регулювання із прагненням прямого контролю над інформаційними ресурсами, що створює внутрішню напругу між підходами» [86, с. 158]. У контексті України ключовою є не мета домінування, а технологія балансування: суперечність між лібералізацією та регулюванням може пом’якшуватися через чітке розмежування зон відповідальності держави та приватного сектору, а також через прозорі процедури й підзвітність.

Інституційний вимір американської моделі характеризується залученням громадянського суспільства та державно-приватного партнерства. Як зазначає І. О. Кириченко, «американська модель інтегрує громадянське суспільство та вибудовує державно-приватне партнерство, що об’єднує правоохоронні, військові, розвідувальні органи й громадськість» [41, с. 170]. Таке залучення підсилює спроможність системи своєчасно ідентифікувати загрози, координувати реагування та нейтралізувати їхні наслідки. Водночас, за спостереженням Ш. Бойна, «правоохоронним органам надаються повноваження щодо моніторингу загроз із забезпеченням секретності розслідувань, а судова практика виробляє способи узгодження завдань розслідування з гарантіями конфіденційності та приватної власності громадян» [101, с. 329]. Це ілюструє прагнення поєднати безпекову результативність із правовими гарантіями, насамперед у площині приватної власності та захисту персональних даних.

Узагальнення дозволяє виокремити пріоритетні напрями американської моделі:

– захист приватної власності та персональних даних. Зокрема, «США посилюють інституційний захист приватних даних і розглядають створення Федерального агентства із захисту даних… із правом накладення штрафів за незаконні практики обробки даних» [26, с. 48]. Для України практично значущим є перехід від переважно дорадчих механізмів до дієвих інструментів впливу на

порушників приватної власності приватної власності та підвищення підзвітності суб'єктів обробки даних;

– захист кіберпростору (кібербезпека). Стратегічні документи США акцентують захист критичної інфраструктури, зниження спроможностей джерел загроз, підвищення стійкості систем, інвестиції у перспективні технології та розвиток партнерств;

– міжнародна кооперація як відповідь на транснаціональність загроз і необхідна умова колективної безпеки [83, с. 96].

В умовах інтеграції України до європейського політико-правового простору актуалізується аналіз підходів ЄС та держав-членів до забезпечення реалізації засад інформаційної безпеки. Ю. Є. Максименко зазначає, що на рівні ЄС «інформаційна безпека часто звужується до інформаційно-технічного виміру, тоді як інформаційно-психологічна складова та компонент захисту прав і свобод людини залишаються периферійними…» [57, с. 112]. Водночас зазначена обставина частково компенсується тим, що значний обсяг предметного регулювання та практик реагування формується на рівні національного законодавства держав-членів.

До комплексу заходів ЄС у цій сфері відносять: «розвиток медіаграмотності; формування інструментів запобігання кіберзагроз; технічну та інноваційну підтримку у захисті інформації; міжнародну кооперацію; протидію кіберзлочинності; протидію ворожій пропаганді» [70, с. 119]. Такі заходи виконують рамкову та ціннісно-орієнтовну функцію, задаючи загальні пріоритети для політик держав-членів і сприяючи уніфікації базових підходів.

Характерною є також практика секторальної диференціації: виокремлення критично важливих сфер (зокрема енергетики) з подальшою конкретизацією профілів загроз і розробленням спеціалізованих механізмів попередження та реагування. З огляду на це доцільним є аналіз національних практик держав-членів ЄС, оскільки саме на національному рівні концентрується основний масив

правового регулювання та інституційних механізмів протидії інформаційним загрозам.

З урахуванням того, що рамкові підходи ЄС конкретизуються переважно на національному рівні, доцільно перейти до аналізу репрезентативних кейсів, які демонструють відмінні моделі організаційно-правового забезпечення інформаційної безпеки. У цьому контексті розглядається практика Польщі та Німеччини як держав-членів ЄС, а також Великої Британії як близької за стандартами та інституційною логікою, релевантної для України з погляду протидії гібридним і кіберзагрозам.

У Республіці Польща правові засади забезпечення інформаційної безпеки виходять з системи законодавчих актів, що визначають напрями інформаційної політики, стандарти функціонування інформаційно-комунікаційних сервісів, механізми регулювання інформаційної діяльності та питання ліцензування. Окремий пласт регулювання, за наявними дослідженнями, стосується умов здійснення інформаційної діяльності релігійними організаціями та розвитку ними власної інформаційної інфраструктури. Для протидії інформаційним загрозам Польща активно залучає громадянське суспільство: зокрема, «створено Центр аналізу пропаганди і дезінформації, який зосереджується на ідентифікації та протидії російській дезінформації у національному інформаційному просторі» [84, с. 515]. Практична цінність польського досвіду для України зумовлена близькістю безпекового контексту; прикладна перевага полягає в інституціоналізації участі громадськості, стандартизації інформаційних послуг і накопиченні практик протидії пропаганді.

У Федеративній Республіці Німеччина стратегічна модель інформаційної безпеки вибудовується через систему пріоритетів, що охоплює: «захист критично важливих інформаційних інфраструктур та інформаційно-телекомунікаційних систем; посилення безпеки державного управління; інституціалізацію координації; протидію кіберзлочинності; розвиток надійних технологій і кадрового потенціалу; а також захист персональних даних у процесах електронного обміну» [89, с. 35]. На наш погляд, цей підхід синтезує

національний та європейський рівні регулювання, що у сукупності сприяє належному рівню охорони національних інтересів [66, с. 380].

Велика Британія демонструє інноваційну модель, зорієнтовану на довгострокову перспективу та випереджальне управління ризиками. У країні сформовано систему розвитку й підтримки сектору інформаційної безпеки, здатну відповідати актуальним потребам національної безпеки. Її ядро становлять: «превенція майбутніх загроз і завчасне впровадження інноваційних технологій; підготовка кадрів; підтримка наукових досліджень; реалізація активної стратегії протидії загрозам в інформаційній сфері» [58, с. 30]. Така логіка є продуктивною, оскільки переносить акцент із реагування на інциденти на їх попередження, знижує ймовірність кризових сценаріїв та підвищує стійкість інформаційної системи держави.

Зазначений підхід конкретизується в урядових політиках щодо кіберстійкості державного сектору, де «пріоритетами визначаються: управління кіберризиками; підвищення захищеності; розбудова спроможностей виявлення та реагування; розвиток компетентностей; зменшення впливу кіберінцидентів та готовність до відновлення» [68, с. 35]. Виокремлення правового й організаційного компонентів є логічним, адже від кіберстійкості публічних інституцій безпосередньо залежать безперервність державного управління та ефективність реалізації державної політики в ключових сферах суспільного життя.

Конфігурація зарубіжних моделей безпеки в інформаційній сфері формується під впливом політико-правових та організаційно-технологічних характеристик кожної держави. До ключових чинників, що визначають відмінності моделей, доцільно віднести:

– рівень розвитку інформаційного суспільства (масштаби цифровізації та впровадження технологій захисту інформації);

– рівень інтеграції держави до наднаціональних структур і безпекових форматів;

– спосіб концептуального визначення інформаційної безпеки (її місце в архітектурі національної безпеки та внутрішня структура, зорієнтована на релевантні загрози);

– підхід до формалізації засад інформаційної безпеки (ступінь нормативного визначення рівнів, елементів і механізмів забезпечення);

– модель правового регулювання, що залежить від конституційно-правової доктрини та розуміння права на інформацію.

Отже, зарубіжний досвід є релевантним для України насамперед у частині:

– розбудови цілісного національного інформаційного простору;

– створення превентивних механізмів виявлення загроз та їх науково-методологічного обґрунтування;

– розвитку інструментів суспільно орієнтованого інформаційного врядування;

– інституційного посилення органів публічної влади, уповноважених на захист інформаційної сфери.

Окремого значення набуває міжнародна співпраця, яка домінує у політиці більшості технологічно розвинених держав, а також пошук збалансованої моделі поєднання ліберальних підходів із необхідним державним регулюванням. Водночас імплементація будь-яких практик має ґрунтуватися на попередній оцінці їх сумісності з національною правовою системою та здатності до адаптації з урахуванням інституційних, ресурсних і безпекових обмежень України.

Зарубіжні підходи до інформаційної безпеки демонструють еволюцію від охорони інформації до управління національною стійкістю, де ключовими стають керованість ризиків, операційна координація, підзвітність суб’єктів і інтеграція приватного сектору та громадянського суспільства. Американська модель репрезентує операціоналізацію державно-приватного партнерства (зокрема через JCDC) та стандартизацію управління кіберризиками, поєднану з пошуком балансу між безпекою і приватністю. Європейський Союз формує рамкові пріоритети (кіберстійкість, медіаграмотність, протидія пропаганді, міжнародна кооперація), які конкретизуються у національних системах держав-

членів. Польща, Німеччина та Велика Британія ілюструють різні конфігурації інституційної організації: від інституціоналізації громадської участі та протидії дезінформації до пріоритетизації захисту критичної інфраструктури й випереджального управління ризиками. Для України практично цінними є підходи, що забезпечують превентивність, координацію та інтегрованість політик, однак їх запровадження має здійснюватися через адаптацію до національної правової системи, ресурсних можливостей і актуального безпекового контексту, а не шляхом механічного запозичення.

Висновки до розділу 3

Інформаційна безпека України в умовах повномасштабної війни та прискореної цифрової трансформації має розглядатися не як вузький режим охорони даних, а як комплексна система національної стійкості, спрямована на забезпечення безперервності державного управління, стабільності критичних сервісів і збереження суспільної довіри за умов кібератак, інформаційно-психологічних операцій, дезінформаційних кампаній, ризиків компрометації ланцюгів постачання та технологічної залежності. Воєнна практика підтвердила «подвійну природу» стійкості інформаційного простору: з одного боку — це кіберстійкість інфраструктури (захист мереж, реєстрів, критичних систем, здатність виявляти інциденти, реагувати та відновлюватися), з іншого — суспільна резильєнтність (медіаграмотність, критичне мислення, інформаційна гігієна, довіра до інституцій). Відтак ефективність державної політики визначається саме синергією технологічних спроможностей і соціально-освітньої складової: жоден із контурів не є самодостатнім без іншого.

Отже, подальше зміцнення системи можливе лише за умов завершення переходу від фрагментарних заходів до керованої архітектури управління ризиками. У нормативному вимірі це означає систематизацію та модернізацію правового поля, уточнення компетенцій і відповідальності суб’єктів, запровадження спеціалізованих режимів для критичних сегментів (критична інфраструктура, державні інформаційні ресурси, протидія інформаційним

операціям), гармонізацію з європейськими підходами (зокрема логікою NIS2) та посилення контролю і правозастосування. В інституційному вимірі нагальною є еволюція від «координації на папері» до операційної взаємодії: розбудова державної системи управління інцидентами, ситуаційних центрів, регламентів безперервності та відновлення, а також інституціоналізація державно-приватного партнерства як постійного механізму спільного планування, обміну даними й реагування (з опорою на релевантні зарубіжні зразки на кшталт JCDC при усвідомленні їхніх умов ефективності). Важливим методологічним принципом є баланс безпекової результативності з правовими гарантіями — насамперед у площині приватності та захисту персональних даних, що забезпечує легітимність і довіру до політики.

У соціально-освітньому вимірі матеріали аргументують пріоритет системного розвитку медіаосвіти, цифрової компетентності та культури кібергігієни як інструментів довгострокового зниження вразливості до маніпуляцій. Протидія дезінформації має бути багаторівневою і поєднувати превентивні комунікації, фактчекінг, підтримку якісного медіасередовища, захист журналістів та сталі формати взаємодії держави, медіа й громадянського сектору. Окремо підкреслено, що державний імідж і стратегічні комунікації виконують функціональну роль у системі інформаційної безпеки, оскільки підсилюють внутрішню довіру й зовнішню підтримку, впливають на ресурсну спроможність держави та підвищують стійкість до ворожих наративів.

Загалом, узагальнення вказує на необхідність закріплення інтегрованої моделі політики: нормативний контур (правила й відповідальність), інституційний контур (координація та операційне управління), технологічний контур (кіберстійкість критичних систем), соціально-освітній та комунікаційний контур (резильєнтність суспільства і стратегічні комунікації), посилений міжнародною кооперацією. Практичним критерієм зрілості такої моделі має стати перехід до вимірюваності результатів через систему індикаторів стійкості (готовність, виявлення, реагування, відновлення; ефекти медіаосвітніх програм; результативність комунікацій), що забезпечить управління не деклараціями, а

доведеними показниками. Саме така синергійна, керована й адаптивна система створює реальні передумови для довгострокової стійкості України в умовах війни, гібридних загроз і швидких технологічних змін.

ВИСНОВКИ

У висновках кваліфікаційної роботи узагальнено результати дослідження концептуальних засад інформаційної безпеки МВС України та визначено їх місце у системі національної безпеки в умовах цифрової трансформації й гібридних загроз. На підставі аналізу теоретико-методологічних підходів, вітчизняного законодавчого регулювання та інституційної практики забезпечення інформаційної безпеки, обґрунтовано ключові дефінітивні ознаки досліджуваної категорії, її принципи, функції та механізми реалізації. Відповідно до чого сформульовано такі висновки та рекомендації:

Проведений теоретико-методологічний аналіз засвідчив, що інформаційна безпека в сучасних умовах має міждисциплінарну природу й не може бути зведена ані до суто технічного захисту інформації, ані до вузького правового режиму охорони інформаційних ресурсів. Вона постає як комплексна категорія національної безпеки, що відображає рівень стійкості інформаційного середовища, здатність держави й суспільства протидіяти деструктивним впливам та забезпечувати належні умови реалізації конституційних інформаційних прав. У межах такого підходу ключового значення набуває поєднання правового, організаційно-управлінського, інформаційно-технічного та соціально-освітнього компонентів, які спільно формують «архітектуру» захисту національного інформаційного простору.

Розкрито категорію «безпека», що дало змогу обґрунтувати, її не лише станом захищеності, а й ціннісно-нормативним орієнтиром розвитку соціальної системи. Ця теза має принципове значення для інформаційної сфери, оскільки цифрова трансформація змінює структуру суспільних цінностей, моделі довіри, канали комунікації та поведінкові практики. Відтак інформаційна безпека повинна розглядатися як інструмент збереження й відтворення суспільно значущих цінностей і норм, а також як засіб підтримання соціальної стійкості в умовах інтенсивного інформаційного впливу. У цьому контексті

«інформаційний суверенітет» і «стійкість» набувають статусу стратегічних критеріїв розбудови державної політики, адже вони орієнтують її на превенцію, адаптивність і довгострокову здатність до відновлення після криз.

Визначено межі положення інформаційної безпеки в системі національної безпеки України обґрунтовано, що вона виконує подвійну роль: по-перше, як самостійний структурний елемент національної безпеки; по-друге, як інтегруюча основа, без якої істотно ускладнюється реалізація інших безпекових компонентів. Нормативне визначення, задає комплексний орієнтир: захист суверенітету й територіальної цілісності, демократичного конституційного ладу, гарантування інформаційних прав, забезпечення доступу до достовірної інформації та протидія дезінформації, пропаганді й порушенням режимів охорони інформації.

Здійснено аналіз сучасної нормативно - правової сфери, яка забезпечує базові правові рамки функціонування інформаційної сфери та визначає легітимні межі захисту національних інтересів. Конституційні приписи, передусім положення про інформаційну безпеку як одну з найважливіших функцій держави, задають фундамент для галузевого законодавства. Рамкові закони у сфері національної безпеки, кібербезпеки та захисту інформації формують загальні принципи, визначають суб’єктів і ключові напрями державної політики, однак значною мірою делегують конкретизацію загроз і практичних інструментів стратегічним та підзаконним актам. Водночас визначальними залишаються проблеми правозастосування: динаміка технологічних змін і гібридних практик агресора випереджає темпи регуляторної адаптації; складним є підтримання пропорційності між безпековими обмеженнями та свободою слова; суспільні умови об’єктивно ускладнюють реалізацію процедур контролю й відповідальності. Отже, ефективність нормативного контуру залежить від внутрішньої узгодженості правового масиву, точності дефініцій, усунення прогалин та спроможності держави забезпечувати виконання стратегічних рішень через дієві підзаконні механізми.

Визначено інституційний механізм, що відображає організаційно-управлінську реалізацію нормативних приписів і стратегічних цілей. Система суб'єктів забезпечення інформаційної безпеки є багаторівневою: стратегічний рівень формує політичні пріоритети, нормативні рамки, контроль і координацію; галузево-операційний рівень виконує спеціалізовані завдання — від контррозвідки та протидії підривній діяльності до кіберзахисту, технічного й криптографічного захисту та розслідування кіберзлочинів. Разом із тим надмірна фрагментація компетенцій і неповнота нормативного визначення суб'єктного складу в окремих стратегічних документах створюють ризики розмиття відповідальності. Відтак ключовими напрямами розвитку інституційного контуру мають бути стандартизація координаційних процедур, уніфікація підходів до обміну даними, узгодження повноважень і формування наскрізного управління ризиками.

Наголошено, що сфера суспільної стійкості та партнерства доповнює державні механізми та відображає соціальний вимір інформаційної безпеки. Інформаційна стійкість постає як комплексна здатність суспільства, інститутів і громадян адаптуватися, зберігати критичність до інформації та відновлюватися після деструктивних впливів. У цьому сенсі держава не може бути єдиним гарантом стійкості, особливо на локальному рівні; необхідною умовою виступає кооперація з громадянським суспільством, яке забезпечує моніторинг, фактчекінг, просвітництво, суспільний контроль і вироблення альтернативних аналітичних продуктів. Практичні формати партнерства включають консультації, робочі групи, громадські ради, стратегічно-комунікаційні платформи та спільні освітні кампанії з медіаграмотності. Водночас наявні системні бар'єри: воєнні режимні обмеження та зниження регулярності комунікації, дефіцит спроможностей на місцевому рівні, зменшення ресурсної бази громадського сектору в громадах. Тому необхідним є перехід від ситуативних контактів до інституціоналізованої, стандартизованої взаємодії з чіткими правилами участі, прогнозованими процедурами обміну інформацією, сценарним плануванням і партнерською підтримкою. У компаративному вимірі

продуктивним орієнтиром є моделі операційної міжсекторальної координації на кшталт JCDC, адаптація яких в українських умовах може бути реалізована через розвиток платформи взаємодії та координації НКЦК та операційного ядра CERT-UA з відповідним інституційним забезпеченням.

Уточнено прикладні орієнтири подальшого розвитку системи інформаційної безпеки, що зводяться до завершення переходу від фрагментарних заходів до керованої архітектури. У нормативному вимірі це означає систематизацію і модернізацію правового поля, уточнення компетенцій і відповідальності, запровадження спеціальних режимів для критичних сегментів, гармонізацію з європейськими підходами та посилення правозастосування. В інституційному вимірі — розвиток державної системи управління інцидентами, ситуаційних центрів, регламентів безперервності та відновлення, а також інституціоналізацію державно-приватного партнерства як постійного механізму спільного планування, обміну даними й реагування. Методологічним принципом має залишатися баланс безпекової ефективності з правовими гарантіями (насамперед приватності та захисту персональних даних), що є умовою легітимності й довіри. Критерієм результативності запропонованої моделі має стати інституційне впровадження системи індикаторів, що дасть змогу перейти з площини декларативних наративів у площину підтверджених показників, це дасть можливість порівнювати результати та корегувати завдання. Саме керована та адаптивна структура здатна створити практичні передумови для довгострокової безпекової стійкості України в умовах війни, гібридних впливів і прискорених технологічних трансформацій.

Рекомендовано на підставі результату дослідження, що інформаційна безпека України в умовах повномасштабної війни та прискореної цифрової трансформації має розглядатися не як вузький режим охорони даних, а як комплексна система національної стійкості, спрямована на забезпечення безперервності державного управління, стабільності критичних сервісів і збереження суспільної довіри за умов кібератак, інформаційно-психологічних операцій, дезінформаційних кампаній, ризиків компрометації ланцюгів

постачання та технологічної залежності. Практичний досвід підтвердив «подвійну природу» стійкості інформаційного простору: з одного боку — це кіберстійкість інфраструктури, з іншого — суспільна. Відтак ефективність державної політики визначається саме синергією технологічних спроможностей і соціально-освітньої складової: жоден із контурів не є самодостатнім без іншого.

Отже, ефективний комплекс інформаційної безпеки МВС України формується лише за умови синхронізації трьох рівнів: нормативного, інституційного та суспільної стійкості. Стратегічним результатом такої синергії має стати перехід до системної, превентивної моделі: з чіткими правилами правозастосування, узгодженими механізмами управління ризиками, міжвідомчою координацією та інституціолізованою співпрацею держави і суспільства у протидії інформаційним і кібернетичним загрозам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України : Закон України від 28.06.1996 р. № 254к/96-ВР. Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141.

2. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 р. № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text. (дата звернення: 03.11.2025)

3. Про доступ до публічної інформації : Закон України від 13.01.2011 р. № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text. (дата звернення: 03.11.2025)

4. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text. (дата звернення: 03.11.2025)

5. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/go/2657-12. (дата звернення: 03.11.2025)

6. Про медіа : Закон України від 13.12.2022 р. № 2849-IX. URL: https://zakon.rada.gov.ua/go/2849-20. (дата звернення: 03.11.2025)

7. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. URL: https://zakon.rada.gov.ua/go/80/94-вр. (дата звернення: 03.11.2025)

8. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/go/2469-19. (дата звернення: 26.11.2025)

9. Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII. URL: https://zakon.rada.gov.ua/go/580-19. (дата звернення: 26.11.2025)

10. Про Національну програму інформатизації : Закон України від 12.12.2022 р. № 2807-IX. URL: https://zakon.rada.gov.ua/go/2807-9. (дата звернення: 03.12.2025)

11. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/go/2163-19. (дата звернення: 26.11.2025)

12. Про Службу безпеки України : Закон України від 25.03.1992 р. № 2229-XII. URL: https://zakon.rada.gov.ua/go/2229-12. (дата звернення: 03.02.2020)

13. Про Раду національної безпеки і оборони України : Закон України від 05.03.1998 р. № 183/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text. (дата звернення: 26.11.2025)

14. Про Національний координаційний центр кібербезпеки : Указ Президента України від 07.06.2016 р. № 242/2016. URL: https://zakon.rada.gov.ua/go/242/2016. (дата звернення: 26.11.2025)

15. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14.09.2020 р. № 392/2020. URL: https://zakon.rada.gov.ua/go/392/2020. (дата звернення: 13.11.2025)

16. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/go/447/2021. (дата звернення: 03.10.2025)

17. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/go/685/2021. (дата звернення: 03.10.2025)

18. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 р. № 47/2017. URL: https://zakon.rada.gov.ua/go/47/2017. (дата звернення: 25.11.2025)

19. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки» : Указ

Президента України від 16.02.2022 р. № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text. (дата звернення: 25.11.2025)

20. «Про утворення Ради голів громадських рад при органах виконавчої влади». Постанова Кабінет міністрів України від 20.06.2012 р. № 658. URL. https://zakon.rada.gov.ua/laws/show/658-2012-%D0%BF#Text. (дата звернення: 03.12.2025)

21. Про створення Центру протидії дезінформації : Рішення Ради національної безпеки і оборони України від 11.03.2021 р. URL: https://zakon.rada.gov.ua/go/n0015525-21. (дата звернення: 03.12.2025)

22. Стратегія розвитку медіаграмотності в Україні на період до 2026 року : Наказ Міністерства культури та інформаційної політики України. № 377 від 24.05.2024 р. URL: https://mkip.gov.ua. (дата звернення: 03.11.2025)

23. Андрєєва О. Н. Специфіка інформаційної складової концепту національної безпеки держави. *European political and Law discourse*. 2015. Vol. 2. Issue 2. P. 135–140.

24. Андрусишин Ю. Я., Бараннік В. В. Інформаційний тероризм як сучасна загроза інформаційній безпеці людини, суспільства, держави. *Інформаційна безпека людини, суспільства, держави*. 2021. № 1. С. 6–15.

25. Баран М. В. Принципи правового регулювання інституту інформаційної безпеки. *Наук. вісник Ужгородського нац. ун-ту*. 2021. № 66. С. 129–134.

26. Белоусова Н. Б. Концептуальні засади інформаційної безпеки США за адміністрації Барака Обами. *Проблеми міжнародних відносин*. 2011. № 2. С. 40 – 53.

27. Благодарний А. М., Кононець О. О. Стратегічні комунікації у сфері національної безпеки і оборони України. *Young Scientist*. 2023. № 1 (113). 2023. С. 5–9

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

29. Борисов О. Ю. Нормативно-правова база забезпечення інформаційної безпеки України: сучасні проблеми та відправні точки їх вирішення. *Інформація і право*, № 4(35), 2020, С. 113–118.

30. Брижко В. М. До питання сучасної інформаційної політики. *Вісник Академії управління МВС*. 2009. № 2. С. 32–36.

31. Будник М. М., Тимофєєв Д. С. Внутрішні загрози інформаційної безпеки та заходи по їх мінімізації : URL: http://ir.nmu.org.ua/bitstream/handle/123456789/1666/7.pdf?sequence=1. (дата звернення: 01.11.2025).

32. Буров О. Ю. Кіберзлочинність як загроза інформаційному суспільству. *Теорія і практика інтелектуальної власності*. 2008. № 3. С. 39– 44.

33. Вознюк Є. В. Громадські об'єднання на захисті інформаційного простору України. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2021. № 3 (11). С. 49–59.

34. Галета Я. В. Роль інформаційних потреб у становленні особистості. *Наукові записки*. 2019. № 140. С. 39–43.

35. Громико І. О., Саханчук Т. І. Державна домінантність визначення інформаційної безпеки України в умовах протидії загрозам. *Право України*. 2008. № 8. С. 130-134.

36. Джураєва О. О. Теоретико-правовий аспект функції забезпечення національної безпеки сучасної держави. *Науковий вісник Міжнародного гуманітарного університету*. 2021 № 53. С. 8–11.

37. Дикий А., Савіцький В., Савчук С., Соха А. Світові тенденції кіберзлочинності та загрози інформаційній безпеці держав. *Society and Security*, (1(7), С. 63–74.

38. Довгань О. Д. Організація правового гарантування безпеки інформаційних обмінів у контексті глобалізації. *Правова інформатика*. 2013. № 4(40). С. 79-88.

39. Єсімов С. С. Шляхи удосконалення нормативно-правового регулювання у сфері інформаційної безпеки. *Наукові записки Львівського університету бізнесу та права*. 2013. Вип. 11. С. 73-76.

40. Захарченко К. В. Інституційний вимір інформаційної безпеки України: трансформаційні виклики, глобальні контексти, стратегічні орієнтири : автореф. дис. … д-ра політ. наук : 23.00.02. Львів. 2021. 34 с.

41. Кириченко І. О. Стратегічні імперативи національної інформаційної безпеки адміністрації Б. Клінтона. *Актуальні проблеми міжнародних відносин*. 2011. № 103. С. 165–171.

42. Коваленко І. А. Актуальні проблеми захисту й охорони прав інтелектуальної власності в мережі Інтернет в умовах глобалізації суспільства та сучасних технологій. *Вчені записки ТНУ імені В. І. Вернадського*. 2018. № 3. С. 52–55.

43. Концепція впровадження медіаосвіти в Україні: нова редакція. / Найдьонова Л. А., Слюсаревський М. М. Київ, 2016. 16 с. URL: http://mediaosvita.org.ua/book/kontseptsiya-vprovadzhennya-mediaosvity/ (дата звернення: 03.02.2020).

44. Кормич Б. А. Інформаційна безпека: організаційно-правові основи. К.: Кондор, 2004. 382 с.

45. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України : монографія. Одеса : Юридична література. 2003. 472 с.

46. Кочубей Л. О. Інформаційна безпека держави: інструменти захисту інформаційного простору : монографія. – Київ, 2018.

47. Красноступ Г. М. Нова Стратегія інформаційної безпеки: правова відповідь на сучасні виклики. *Інформація і право*. 2025. № 2(53). С. 136 – 146.

48. Кузнєцов О. П. Основні функції та принципи діяльності громадських рад органів державної влади та місцевого самоврядування. *Право та державне управління.* 2024. № 4. С. 608- 614.

49. Лемак О. В. Забезпечення національної безпеки як функція держави. *Науковий вісник Ужгородського національного університету*. 2016. № 38. С. 64–67.

50. Леонов Б. Д., Лихова С. Я. Інформаційний тероризм як загроза національній безпеці України. *Юридичний вісник*. 2021. № 2 (59). С. 170–176.

51. Лесько Н. В., Малець М. Р. Правова характеристика глобальної мережі Інтернет. *Юридичний науковий електронний журнал*. 2021. № 1. С. 186–189.

52. Лисенко С. О. Конституційні засади розуміння інформаційної безпеки. *Публічне урядування*. 2016. № 4. С. 154-161.

53. Лисенко, С.О., Полотнянко О. Концептуальні підходи до забезпечення інформаційної безпеки в Україні. *Вісник НААУ.* № 5 (111). 2025. С. 26-31.

54. Литвиненко О. В. Медіаграмотність громадян у контексті гібридних воєн: приклад України. *Young Scientist*. 2018. № 3 (55). С. 259–263.

55. Ліпкан В. А. Теорія національної безпеки : підручник. Київ : КНТ. 2009. 631 с.

56. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції. Київ : КНТ, 2006. 280 с.

57. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України: дис… канд. юр. наук: 12.00.01. Київ. 2007. 186 с.

58. Мацелик М. О., Санжарова Г. Ф., Санжаров В. А. Третя національна стратегія кібербезпеки Великої Британії: політика «на майбутнє» в динамічному технічному середовищі. *Юридичний науковий електронний журнал*. 2023. № 9. С. 28–30.

59. Мельник І. В. Інформаційна стійкість України: вибір трендів масової культури та їх вплив на суспільну свідомість і стратегії державного управління. *Механізми публічного управління*. 2021. № 2. С. 69–73.

60. Мельнік Ю. П. Вплив дезінформації на державну інформаційну політику: вітчизняний та зарубіжний досвід. *«Філософія та політологія в контексті сучасної культури».* 2023. Т. 15, № 2. С. 114-119.

61. Мороз Н. С. Сутність інформації в контексті загальних принципів інформаційної безпеки. *Вісник Національного університету «Львівська політехніка». Юридичні науки*. 2016. № 845. С. 137-142.

62. Мотайло О. В. Основні концептуальні підходи до сутності поняття «національна безпека». *Право та державне управління*. 2019. № 4. С. 286– 293.

63. Настюк В. Я. Формування системи інформаційного законодавства в Україні. *Інформація і право*. 2011. № 2 (2). С. 27–31.

64. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання : монографія. Київ : Гельветика, 2017. 168 с.

65. Недохлєбов І. І. Інформаційна безпека України в умовах сучасних загроз: організаційно-правові аспекти : дис. ... канд. юрид. наук : 12.00.07. Запоріжжя, 2024. 239 с.

66. Недохлєбов І. І. Забезпечення інформаційної безпеки на рівні ЄС та окремих держав-членів. Теоретичні та практичні проблеми реалізації норм права: матеріали IX Міжнародної науково-практичної конференції, м.Кременчук, 22–23 грудня 2023 р. Львів – Торунь : Liha-Pres, 2023. С. 378–381.

67. Недохлєбов І. І. Інформаційна безпека в структурі національної безпеки України. Development trends in legal science and education of Ukraine in the context of European integration: proceeding of the international scientific conference, Częstochowa, November 1–2, 2023. Riga: Publishing House “Baltija Publishing”, 2023. P.148–152.

68. Недохлєбов І. І. Теоретико-правовий аналіз зовнішніх загроз інформаційній безпеці України. *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція*. 2023. № 64. С. 18-21.

69. Нітченко Г. М., Ховрич М. О. Теоретичний аналіз проблеми медіаграмотності молоді. *Педагогічні науки*. 2018. № 151. С. 112–115.

70. Олефір І. В. Особливості забезпечення інформаційної безпеки у провідних країнах. *Регіональні студії*. 2018. № 12. С. 118–121.

71. Олійник О. В. Принципи забезпечення інформаційної безпеки України. *Юридичний вісник*. 2016. № 4 (41). С. 72–78.

72. Основи управління інформаційною безпекою: навч. посібник / А. М. Гребенюк, Л. В. Рибальченко. Дніпро : Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.

73. Пархоменко-Куцевіл О. І. Проблеми забезпечення інформаційної безпеки під час здійснення військових операцій та бойових дій. *Публічне управління і адміністрування в Україні*. 2022. № 8. С. 177–181.

74. Пасічник В. Філософська категорія безпека як основа нової парадигми державного управління національною безпекою. *Демократичне врядування.* 2011. № 7. С. 57–70.

75. Перун Т. С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні : дис. ... канд. юрид. наук : 12.00.07. Львів. 2019. 268 с.

76. Перун Т. С. Забезпечення інформаційної безпеки в зоні бойового конфлікту. *Актуальні проблеми держави і права*. 2020. № 5. С. 131–138.

77. Пивовар В., Драчук С. Філософські проблеми безпеки як методологічна основа забезпечення безпеки фондового ринку. *Правова інформатика.* 2007. № 2 (4). С. 77–82.

78. Предборський В. А. Економічна безпека держави : монографія. Київ. Кондор. 2005. 391 с.

79. Прокофьєв М. І., Хорошко В. О. Проблеми захисту інформації в Україні. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2015. № 2 (30). С. 9–14.

80. Пугачов О. І. Удосконалення державних механізмів забезпечення інформаційної безпеки України : дис ... док. філ.. : 25.00.01 Київ, 2025. 238 с.

81. Резнікова О. О. Національна стійкість в умовах мінливого безпекового середовища : монографія. Київ. НІСД. 2022. 532 с.

82. Рябовол Л. Т. Національна безпека України: структурно функціональний аналіз. *Вісник Університету імені Альфреда Нобеля*. 2020. № 1. С. 25–30.

83. Саранча В. І., Шабуніна В. В., Тур О. М. Управління інформаційною безпекою: американський досвід. *Бібліотекознавство. Документознавство. Інформологія*. 2023. № 3. С. 89–98.

84. Сливка М. М., Лук'янова Г. Ю. Правове забезпечення інформаційної безпеки : досвід країн Європейського Союзу. *Юридичний науковий електронний журнал*. 2021. № 11. С. 514–516.

85. Солодка О. М. Пріоритети удосконалення інформаційної безпеки України. *Інформація і право*. 2015. № 3. С. 36-42.

86. Соснін О. В. Державна політика в галузі управління інформаційним ресурсом України : дис. … д-ра політ. Наук : 23.00.02. Одеса. 2005. 264 с.

87. Тихомиров О. О. Забезпечення інформаційної безпеки як функція сучасної держави : монографія. заг. ред. Р. А. Калюжний. Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. 196 с.

88. Харченко Л. С., Ліпкан В. А., Логінов О. В. Інформаційна безпека України : глосарій. заг. ред. Р. А. Калюжний. Київ : «Текст», 2004. 134 с.

89. Чернухін І. О. Досвід Федеративної Республіки Німеччини в побудові системи захисту інфраструктури від кібернетичних загроз. *Інформаційна безпека людини, суспільства, держави*. 2014. № 1. С. 27-43.

90. Яковлєв П. О. Функції державного регулювання у сфері забезпечення інформаційної безпеки в Україні. *Часопис Київського університету права.* 2020. № 1. С. 155–159.

91. Яковюк І. В., Білоусов Є. М. Національна безпека України в умовах нових викликів європейській та євроатлантичній солідарності : монографія. Харків : «ФО-П Рубан В. В.». 2022. 148 с.

92. «Укртелеком» зазнав потужної кібератаки. MediaSapiens. [Електронний ресурс]. 29.03.2022.

URL: https://ms.detector.media/kiberbezpeka/post/29252/2022-03-29-ukrtelekom-zaznav-potuzhnoi-kiberataky. (дата звернення: 15.10.2025).

93. CERT-UA Урядова команда реагування на комп'ютерні надзвичайні події України. Державна служба спеціального зв'язку та захисту інформації України. [Електронний ресурс] URL: https://cert.gov.ua. (дата звернення: 18.10.2025).

94. Індекс медіаграмотності українців: 2020 – 2022 : аналітичний звіт. ГО «Детектор медіа». Київ, 2023. [Електронний ресурс]. URL: https://detector.media/infospace/article/210210/2023-04-18-indeks-mediagramotnosti-ukraintsiv-2020-2022-povna-versiya. (дата звернення: 15.10.2025).

95. Центр стратегічних комунікацій. [Електронний ресурс]. URL: https://spravdi.org/.(дата звернення: 20.10.2025).

96. Центр демократії та верховенства права. [Електронний ресурс]. URL. https://cedem.org.ua/direction-nezalezhni-media/mediyna-ta-info-gramotnist. (дата звернення: 15.10.2025).

97. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive) // Official Journal of the European Union. – 2022. – Vol. L 333. – P. 80–152.

98. Executive Order 14028—Improving the Nation's Cybersecurity. May 12, 2021. URL: https://www.govinfo.gov/link/cpd/executiveorder/14028. (дата звернення: 10.11.2025).

99. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Paper (CSWP) NIST CSWP 29. February 26, 2024. Gaithersburg, MD: NIST, 2024. 32 p. DOI: 10.6028/NIST.CSWP.29. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf. (дата звернення: 10.10.2025).

100. Ransomware: Federal Agencies Provide Useful Assistance but Can Improve Collaboration: report to congressional addressees (GAO-22-104767). Washington: U.S. Government Accountability Office, 2022. URL: https://www.gao.gov/assets/gao-22-104767.pdf. (дата звернення: 10.11.2025).

101. Shawn Marie Boyne Data Protection in the United States. The American journal of comparative law. 2018. Vol. 66. P. 299–343.

102. Joint Cyber Defense Collaborative Act: H.R. 9768 (118th Congress, 2d Session), introduced Sept. 24, 2024: text. Congress.gov. URL: https://www.congress.gov/bill/118th-congress/house-bill/9768/text. (дата звернення: 10.11.2025).