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

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему: «Трансформація інформаційної безпеки України в контексті європейської інтеграції»

Виконав:
студент 2 курсу, групи УМІБ-61
другого (магістерського) рівня вищої освіти,
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
ОПП «Міжнародна інформаційна безпека»
Михайловський Костянтин Сергійович
(прізвище, ім'я по батькові)

Керівник:
д.держ.упр, професор Солових В.П.
(науковий ступінь, вчене звання, прізвище, ім'я по батькові)

Рецензент:
д.і.н., професор Лиман Сергій Іванович
(науковий ступінь, вчене звання, прізвище, ім'я по батькові)

ХАРКІВ – 2025 рік

Харківський національний університет імені В. Н. Каразіна

ННІ «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Кафедра міжнародних відносин
Спеціальність 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
Освітньо-професійна програма «Міжнародна інформаційна безпека»
Рівень вищої освіти: другий (магістерський)

ЗАТВЕРДЖУЮ

Завідувач кафедри

Підпис

Наталія ВІННИКОВА
ініціали, прізвище

«2» червня 2025року

(зі змінами від 10.09.2025, 06.10.2025)

ЗАВДАННЯ

на кваліфікаційну роботу магістра

Михайловського Костянтина Сергійовича

(прізвище, ім'я та по батькові)

1. Тема роботи «Трансформація інформаційної безпеки України в контексті європейської інтеграції»
керівник роботи Солових Віталій Павлович, д.держ.упр., професор
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом по університету «02» червня 2025 року № 4001-5/1324 (зі змінами від «10» вересня 2025 року № 4001-5/3049; «6» жовтня 2025 року № 4001-5/3656.
2. Строк подання здобувачем вищої освіти роботи 21 листопада 2025 р.
3. Перелік питань, які потрібно розробити:
надати характеристику сутності інформаційної безпеки та її ролі в системі національної й міжнародної безпеки; з'ясувати теоретичні підходи щодо інформаційної безпеки в умовах європейської інтеграції; визначити нормативно-правові та стратегічні засади функціонування системи інформаційної безпеки України; розкрити інституційну систему забезпечення інформаційної безпеки України та виявити ключові проблеми координації між її складовими; виявити сучасні виклики та загрози інформаційній безпеці України в контексті зовнішніх і внутрішніх факторів; визначити пріоритетні інституційні та технологічні напрями трансформації системи інформаційної безпеки України в умовах європейської інтеграції.

4. План роботи

№ з/п	Назви етапів роботи	Строк виконання етапів
1	Вибір здобувачем теми КРМ і подання заяви на кафедру; затвердження теми та призначення наукового керівника; складання та затвердження індивідуального завдання на виконання КРМ	12.05.2025-30.06.2025
2	Підготовка вступу і розділу 1 КРМ	22.09.2025-30.09.2025
3	Підготовка розділу 2 КРМ	01.10.2025-15.10.2025
4	Підготовка розділу 3 КРМ	16.10.2025-31.10.2025
5	Підготовка висновків і переліку використаних джерел	03.11.2025-14.11.2025
6	Подання здобувачем завершеної КРМ науковому керівнику для перевірки та оформлення відгуку	17.11.2025-21.11.2025
7	Попередній розгляд КРМ на комісії від кафедри	24.11.2025-28.11.2025
8	Доопрацювання роботи, прийняття кафедрою рішення про допуск роботи до захисту в ЕК, оформлення та зовнішнє рецензування	01.12.2025-05.12.2025
9	Підготовка до захисту та захист КРМ в ЕК і присвоєння випускникам кваліфікації	08.12.2025-24.12.2025

5. Дата видачі завдання: 02 червня 2025 року (10.09.2025; 06.10.2025)

Студент Костянтин МИХАЙЛОВСЬКИЙ

(підпис) (ініціали, прізвище)

Керівник роботи Віталій СОЛОВИХ

(підпис) (ініціали, прізвище)

ЗМІСТ

ВСТУП

Актуальність дослідження визначається тим, що інформаційна безпека набула ключового значення для підтримання державного суверенітету України в умовах глибоких змін глобального й регіонального безпекового порядку. Сучасна система міжнародних відносин засвідчує стрімке посилення впливу інформаційного виміру на політичні, економічні та військові процеси, а конфлікти дедалі більше супроводжуються боротьбою у медіа- та кіберпросторі. Це особливо наочно проявилося під час російської збройної агресії проти України. Гібридна війна, розпочата росією у 2014 році й трансформована у повномасштабне вторгнення в лютому 2022 року, продемонструвала, що інформаційний компонент є одним із визначальних у сучасних конфліктах: інформаційні операції, кампанії дезінформації та кібератаки стали складовими агресивної стратегії на рівні з використанням традиційних військових засобів.

Ступінь наукової розробленості проблеми свідчить про зростаючий інтерес дослідників до питань інформаційної безпеки в умовах глобальних трансформацій та європейської інтеграції, водночас виявляє певні прогалини у вивченні специфіки української ситуації. Теоретичні основи дослідження інформаційної безпеки закладені у працях таких українських науковців як В. Горбулін, який комплексно проаналізував феномен гібридної війни та роль інформаційного компонента у російській агресії проти України. Д. Дубов та М. Ожеван розробили концептуальні підходи до аналізу інформаційної безпеки та стратегічних комунікацій у системі національної безпеки. Г. Почепцов дослідив механізми сучасних інформаційних війн та специфіку інформаційного протиборства у цифрову епоху. О. Золотар проаналізувала еволюцію законодавства України у сфері інформаційної безпеки та виклики його адаптації до сучасних загроз.

Серед зарубіжних дослідників варто відзначити напрацювання фахівців NATO StratCom Centre of Excellence, які систематично документують російські дезінформаційні кампанії та аналізують ефективність різних інструментів протидії. Європейські дослідники, зокрема аналітики Європейської комісії та ENISA, розробили концептуальні підходи до забезпечення кібербезпеки та

протидії дезінформації, що втілені у європейських регуляторних актах. Водночас слід зазначити, що більшість досліджень або фокусуються на загальних питаннях інформаційної безпеки без достатньої уваги до специфіки європейської інтеграції, або розглядають європейський досвід без його зіставлення з українським контекстом. Попри значний науковий інтерес до проблематики інформаційної безпеки, низка аспектів і досі залишається недостатньо опрацьованою. Зокрема, потребують глибшого аналізу практичні механізми адаптації української системи інформаційної безпеки до європейських нормативів у воєнних умовах, потенціал взаємного обміну знаннями та технологічними рішеннями між Україною та Європейським Союзом, а також можливості й перспективи залучення України до європейських програм і ініціатив у цій сфері. Наявність таких наукових прогалин підтверджує об'єктивну необхідність та вагомість проведення даного дослідження.

Мета дослідження полягає у визначенні концептуальних засад, механізмів та пріоритетних напрямів трансформації системи інформаційної безпеки України в умовах європейської інтеграції з урахуванням сучасних викликів та загроз.

Для досягнення поставленої мети необхідно розв'язати **такі завдання**:

– надати характеристику сутності інформаційної безпеки та її ролі в системі національної й міжнародної безпеки;

– з'ясувати теоретичні підходи щодо інформаційної безпеки в умовах європейської інтеграції;

– визначити нормативно-правові та стратегічні засади функціонування системи інформаційної безпеки України;

– розкрити інституційну систему забезпечення інформаційної безпеки України та виявити ключові проблеми координації між її складовими;

– виявити сучасні виклики та загрози інформаційній безпеці України в контексті зовнішніх і внутрішніх факторів;

– визначити пріоритетні інституційні та технологічні напрями трансформації системи інформаційної безпеки України в умовах європейської інтеграції.

Об’єктом дослідження є система забезпечення інформаційної безпеки України в контексті європейської інтеграції.

Предметом дослідження є трансформація системи інформаційної безпеки України під впливом європейських інтеграційних процесів.

Методи дослідження ґрунтується на комплексному застосуванні різноманітних наукових підходів, що дозволяють розкрити багатовимірність та складність процесів трансформації інформаційної безпеки. Системний підхід дає змогу розглядати інформаційну безпеку як складну систему взаємопов’язаних елементів та аналізувати механізми її інтеграції до ширшої європейської системи безпеки. Інституційний підхід забезпечує можливість аналізу процесів інституційних змін, механізмів трансферу європейських інституцій на національний рівень, факторів успішності адаптації. Комунікативний підхід дозволяє розкрити роль стратегічних комунікацій як інструменту забезпечення інформаційної стійкості та протидії дезінформації. Конструктивістський підхід виявляє значення дискурсів, ідентичностей та цінностей у формуванні політики інформаційної безпеки. Дослідження також спирається на теорії європейської інтеграції, зокрема неофункціоналізм для розуміння механізмів поступового поглиблення інтеграції через spillover effect, та концепцію європеїзації для аналізу процесів адаптації національних систем до європейських стандартів. Компаративний підхід застосовується для порівняння українського та європейського досвіду забезпечення інформаційної безпеки, виявлення спільних рис та відмінностей, можливостей взаємного навчання.

Інформаційна база дослідження включає широкий спектр джерел різного типу. Нормативно-правову основу становлять Конституція України, закони України про національну безпеку, про основні засади забезпечення кібербезпеки, про інформацію, про захист персональних даних, стратегічні документи у сфері національної безпеки та інформаційної безпеки України. Важливе значення мають документи Європейського Союзу, зокрема Загальний регламент захисту даних, Директива NIS2 про кібербезпеку, Акт про цифрові послуги, Кодекс практик щодо дезінформації, стратегії ЄС у сфері кібербезпеки та протидії дезінформації, програма Digital Europe. Аналітичну базу дослідження

становлять звіти та доповіді міжнародних організацій, зокрема НАТО, ОБСЄ, Ради Європи, аналітичні матеріали East StratCom Task Force, ENISA, NATO StratCom Centre of Excellence. Наукову основу формують монографії, наукові статті, матеріали конференцій українських та зарубіжних дослідників, опубліковані переважно у період 2020-2025 років. Емпіричну базу доповнюють офіційні веб-ресурси інституцій Європейського Союзу, органів державної влади України, міжнародних організацій, що надають оперативну інформацію про події, рішення, ініціативи у сфері інформаційної безпеки.

Практичне значення отриманих результатів полягає в тому, що вони можуть бути використані органами державної влади України під час розроблення та реалізації політики у сфері інформаційної безпеки в контексті євроінтеграційного курсу держави. Напрацьовані у дослідженні висновки є релевантними для Ради національної безпеки і оборони України у процесі підготовки стратегічних документів із питань національної безпеки та координації діяльності інституцій, відповідальних за інформаційну безпеку. Державна служба спеціального зв'язку та захисту інформації України може застосувати результати роботи для планування заходів із підвищення кіберзахисту об'єктів критичної інфраструктури та впровадження європейських стандартів у сфері кібербезпеки. Міністерство культури та інформаційної політики України здатне використати запропоновані рекомендації для удосконалення стратегічних комунікацій і протидії дезінформаційним операціям. Крім того, Міністерство закордонних справ України може враховувати отримані напрацювання під час координації міжнародної взаємодії у сфері інформаційної безпеки та представлення інтересів України в інституціях Європейського Союзу.

Матеріали дослідження можуть бути використані у навчальному процесі при викладанні дисциплін з національної безпеки, європейської інтеграції, міжнародних відносин, політичного аналізу у вищих навчальних закладах України. Концептуальні висновки та практичні рекомендації дослідження сприяють гармонізації української системи інформаційної безпеки з європейськими стандартами, що є важливим елементом виконання Угоди про

асоціацію між Україною та ЄС та підготовки до майбутнього членства України в Європейському Союзі. Аналіз унікального українського досвіду протидії гібридним загрозам може бути корисним для європейських партнерів у посиленні власної інформаційної стійкості, що сприяє перетворенню України з реципієнта на донора безпеки для Європи.

Апробація результатів дослідження. Результати дослідження були представлені автором на всеукраїнському науково-практичному круглому столі «Стратегічні напрями зовнішньої політики та дипломатії країн світу» (м. Харків, листопад 2025 р.), для участі в якому було підготовлено тези за відповідною тематикою «Трансформація інформаційної безпеки України в умовах європейської інтеграції та гібридної війни».

Структура роботи зумовлена логікою дослідження та необхідністю послідовного розкриття поставлених завдань. Кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел, який налічує 74 найменування. Загальний обсяг роботи становить 108 сторінок, з яких основного тексту – 101 сторінка.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ В УМОВАХ ЄВРОПЕЙСЬКОЇ ІНТЕГРАЦІЇ

1.1. Сутність поняття «інформаційна безпека» в системі національної та міжнародної безпеки

Усвідомлення природи інформаційної безпеки як ключового елементу національної безпекової системи є відправною точкою для аналізу тих трансформацій, що відбуваються у цій сфері в процесі європейської інтеграції України. Чітке теоретичне окреслення змісту поняття «інформаційна безпека» та визначення її ролі у структурі національної й міжнародної безпеки слугує необхідною аналітичною основою для подальшого вивчення інституційних механізмів, нормативно-правових засад і практик захисту інформаційного простору держави. Значущість цієї тематики особливо зростає в умовах посилення гібридних загроз, ескалації інформаційних протиборств та потреби узгодження українського правового поля із стандартами Європейського Союзу.

Наукова розробленість питання інформаційної безпеки характеризується багатовимірністю підходів та різноманітністю концептуальних інтерпретацій. Вагомий внесок у дослідження теоретичних засад інформаційної безпеки зробили українські науковці, зокрема В. Горбулін, який розглядав інформаційну безпеку як стратегічний пріоритет державної політики у сфері національної безпеки [6, с. 45]. О. Довгань акцентував увагу на інституційних аспектах забезпечення інформаційної безпеки та необхідності формування комплексної системи протидії інформаційним загрозам [8, с. 67]. Д. Дубов досліджував еволюцію концепції інформаційної безпеки у контексті глобальних трансформацій інформаційного простору та появи нових викликів у цифрову епоху [10, с. 112]. Серед європейських дослідників варто відзначити напрацювання щодо аналізу стратегічних комунікацій як інструменту забезпечення інформаційної стійкості демократичних держав [25, с. 34], та розробку концепції «м’якої сили» та інформаційного впливу у міжнародних відносинах. Водночас варто підкреслити, що швидка еволюція інформаційних технологій, зміна типології сучасних загроз та активізація євроінтеграційних процесів в Україні обумовлюють потребу у постійному оновленні

концептуальних підходів до інформаційної безпеки та їх адаптації до нових умов функціонування безпекового середовища.

Концепція інформаційної безпеки пройшла тривалий шлях еволюції від вузького трактування як захисту державних секретів до широкого розуміння як комплексної системи забезпечення стійкості інформаційного простору держави та суспільства. На початковому етапі розвитку теорії інформаційної безпеки, що припадає на період холодної війни, домінував державоцентричний підхід, за якого інформаційна безпека ототожнювалася передусім із захистом класифікованої інформації та протидією іноземній розвідці. Проте стрімкий розвиток інформаційно-комунікаційних технологій, формування глобального інформаційного простору та поява нових загроз зумовили необхідність розширення змісту цього поняття. У сучасній науковій літературі спостерігається багатоваріантність підходів до трактування інформаційної безпеки, що відображає складність та багатоаспектність цього явища.

Аналіз наукової літератури дає змогу виокремити декілька ключових підходів до трактування поняття інформаційної безпеки. Перший підхід зосереджує увагу на технічній складовій захисту, тобто на забезпеченні недоторканності інформації та інформаційних систем від несанкціонованого доступу, неправомірного використання, розголошення, пошкодження чи модифікації. У межах цього розуміння інформаційна безпека постає як стан захищеності інформаційних ресурсів, інфраструктури та технологій від внутрішніх і зовнішніх загроз [29, с. 78]. Другий підхід пропонує ширше трактування, розглядаючи інформаційну безпеку як захищеність національних інтересів у інформаційній сфері, що ґрунтуються на збалансованості потреб особи, суспільства й держави. Ця позиція відображена, зокрема, у Законі України «Про основні засади забезпечення кібербезпеки України», де кібербезпека визначається як забезпечення життєво важливих інтересів громадян, суспільства та держави під час функціонування у кіберпросторі [37]. Третій підхід робить акцент на інформаційному суверенітеті держави, її здатності вибудовувати власний інформаційний простір, ефективно протидіяти деструктивним інформаційним впливам та підтримувати стійкість суспільства до інформаційних

загроз.

У процесі трансформації системи інформаційної безпеки України особливе значення має підхід, закріплений у Доктрині інформаційної безпеки України. Згідно з цим документом, інформаційна безпека розглядається як елемент національної безпеки та визначається станом захищеності національних інтересів у інформаційній сфері, що ґрунтуються на збалансованих інтересах особи, суспільства й держави [42, с. 2]. Таке визначення підкреслює багатовимірність цього явища та необхідність врахування потреб різних суб'єктів безпекових відносин. Водночас зазначений підхід потребує подальшого змістового уточнення, оскільки формулювання «стан захищеності національних інтересів» залишається доволі узагальненим і потребує визначення конкретних індикаторів, критеріїв та методів оцінювання.

Структура інформаційної безпеки характеризується складністю та багатоелементністю. Аналіз наукових джерел та нормативно-правових документів дозволяє виокремити кілька основних компонентів інформаційної безпеки держави. По-перше, це безпека інформації, що передбачає захист даних від несанкціонованого доступу, витоку, модифікації чи знищення. Цей компонент охоплює забезпечення конфіденційності, цілісності та доступності інформації, що становить тріаду класичних принципів інформаційної безпеки [10, с. 156]. По-друге, безпека інформаційної інфраструктури, що включає захист технічних засобів обробки, зберігання та передачі інформації, інформаційних систем та мереж від кіберзагроз, фізичних пошкоджень та інших деструктивних впливів. По-третє, безпека інформаційного простору, що передбачає формування безпечного, надійного та стійкого інформаційного середовища, протидію поширенню дезінформації, пропаганди, деструктивного контенту. По-четверте, інформаційна стійкість суспільства, що означає здатність громадян критично оцінювати інформацію, протидіяти інформаційним маніпуляціям та зберігати національну ідентичність в умовах інформаційної експансії.

Місце інформаційної безпеки у системі національної безпеки визначається її наскрізним характером та взаємозв'язком з іншими складовими безпеки держави. Інформаційна безпека тісно пов'язана з політичною безпекою, оскільки

інформаційні впливи можуть використовуватися для дестабілізації політичної системи, підриву легітимності владних інституцій, втручання у виборчі процеси [8, с. 203]. Взаємозв'язок із економічною безпекою проявляється через захист економічної інформації, забезпечення безпеки фінансових систем, протидію економічному шпигунству. Зв'язок з обороною та військовою безпекою виявляється у функціонуванні систем військового управління, розвідки та спостереження, що критично залежать від захищеності інформаційних систем. Соціальна безпека також має інформаційний вимір, адже дезінформація може посилювати соціальні конфлікти, провокувати ксенофобію та розкол суспільства.

На міжнародному рівні інформаційна безпека посідає провідне місце серед напрямів співробітництва держав і діяльності міжнародних інституцій. Організація Об'єднаних Націй приділяє значну увагу цій проблематиці, зокрема через роботу Групи урядових експертів, яка аналізує вплив розвитку інформаційних і телекомунікаційних технологій на міжнародну безпеку та виробляє рекомендації для держав. Європейський Союз сформував комплексну політику у сфері інформаційної безпеки та протидії дезінформації, що охоплює створення спеціалізованих структур, ухвалення нормативно-правових актів у галузі цифрової та кібербезпеки, а також упровадження освітніх програм з медіаграмотності. У рамках НАТО інформаційна безпека розглядається як важливий елемент колективної оборони, а Альянс активно розвиває інструменти стратегічних комунікацій та механізми протидії гібридним загрозам.

Важливим аналітичним напрямом є осмислення інформаційної безпеки в європейському вимірі, оскільки саме від цього залежить ефективність адаптації української системи до стандартів Європейського Союзу. Європейська модель інформаційної безпеки вирізняється орієнтацією на захист демократичних принципів, прав людини, свободи вираження поглядів і медійного плюралізму. У стратегічних документах ЄС поширеним є поняття «інформаційної стійкості» (information resilience), яке акцентує на здатності держави та суспільства протистояти деструктивним інформаційним впливам без шкоди для базових прав і свобод. Європейська стратегія з кібербезпеки визначає інформаційну безпеку

як комплекс технічних, правових, інституційних та освітніх заходів, спрямованих на створення безпечного, відкритого та захищеного цифрового середовища.

Порівняльний аналіз українського та європейського підходів до забезпечення інформаційної безпеки засвідчує наявність як схожих положень, так і суттєвих відмінностей. До спільних рис належить трактування інформаційної безпеки як комплексної системи заходів, багаторівнева та багатосуб'єктна відповідальність за її підтримання, а також розуміння необхідності забезпечення балансу між безпекою та свободою доступу до інформації**.** Водночас у європейському дискурсі важливе значення надається нормативно-правовим механізмам захисту персональних даних. Разом із тим український підхід історично тяжів до державоцентричної моделі, тоді як у європейській практиці домінує орієнтація на права людини, розвиток громадянського суспільства та мінімізацію надмірного державного втручання. У процесі європейської інтеграції України простежується поступове наближення цих концептуальних підходів, що відображено, зокрема, у новій редакції Стратегії інформаційної безпеки України, ухваленій у 2021 році [41]. У документі інформаційна безпека трактується як стан захищеності життєво важливих інтересів громадянина, суспільства та держави, за якого унеможливлюється заподіяння шкоди внаслідок неповної, недостовірної чи несвоєчасної інформації, негативного інформаційного впливу, порушень цілісності, конфіденційності чи доступності інформації, а також негативних наслідків використання інформаційних технологій.

Ключовим елементом розуміння природи інформаційної безпеки є визначення її основних об'єктів та суб'єктів. До об'єктів інформаційної безпеки належать національні інтереси в інформаційній сфері, інформаційні ресурси та інфраструктура, інформаційний простір держави, а також права і свободи людини й громадянина у сфері інформаційних відносин. Суб'єктами, відповідальними за забезпечення інформаційної безпеки, виступають держава в особі органів законодавчої, виконавчої і судової влади, органи місцевого самоврядування, інститути громадянського суспільства, суб'єкти

господарювання та окремі громадяни [12, с. 134]. Така багатосуб'єктність відображає складність і багатовимірність системи інформаційної безпеки, підкреслюючи необхідність координації діяльності різних акторів та належного розподілу відповідальності між ними.

Методологічно важливим аспектом є визначення ключових функцій інформаційної безпеки. Захисна функція передбачає протидію інформаційним загрозам і захист інформаційних ресурсів та інфраструктури від несанкціонованих впливів. Превентивна функція пов'язана з раннім виявленням потенційних ризиків та недопущенням інформаційних криз чи конфліктів. Регулятивна функція реалізується через формування системи правових норм, стандартів і процедур, що регулюють діяльність у сфері інформаційної безпеки. Освітня функція спрямована на підвищення інформаційної культури та медіаграмотності населення, розвиток критичного мислення і навичок безпечного користування інформаційним простором [30, с. 89]. Координаційна функція забезпечує узгодження дій різних учасників системи інформаційної безпеки і сприяє міжвідомчій та міжнародній взаємодії у цій сфері.

Принципи забезпечення інформаційної безпеки формують нормативно-правову основу функціонування національної системи захисту інформаційного простору. До ключових принципів належать: принцип законності, який вимагає, щоб діяльність у сфері інформаційної безпеки здійснювалася виключно відповідно до чинного законодавства; забезпечення збалансованості інтересів особи, суспільства й держави; гарантування свободи доступу, використання, поширення та зберігання інформації; вимога достовірності та повноти інформаційних повідомлень; підтримання різноманіття джерел інформації та медіаплюралізму; комплексний підхід до організації системи інформаційної безпеки; пріоритет захисту прав і свобод людини; а також розвиток міжнародного співробітництва у цій сфері [18, с. 167].

Сучасне трактування інформаційної безпеки передбачає врахування нових типів загроз, що виникли внаслідок цифрової трансформації суспільства. Стрімке поширення соціальних мереж, використання штучного інтелекту для створення дипфейків, розвиток автоматизованих інструментів поширення

дезінформації, застосування великих даних для цілеспрямованого інформаційного впливу – усе це формує нові, більш складні виміри інформаційної безпеки. Пандемія COVID-19 виявила вразливість сучасних суспільств до інфодемії – масштабного поширення неправдивої або маніпулятивної інформації, що здатна завдавати суттєвої шкоди громадському здоров'ю та соціальній стабільності. Російська агресія проти України, розпочата у 2014 році та розширена до повномасштабного вторгнення у 2022 році, продемонструвала нові форми гібридної війни, у яких інформаційний компонент відіграє ключову роль у підриві обороноздатності, соціальної єдності та стійкості держави-жертви [6, с. 234].

Теоретичне осмислення інформаційної безпеки вимагає врахування діалектичного співвідношення між безпекою та свободою інформації. Забезпечення інформаційної безпеки не може слугувати підставою для надмірного чи необґрунтованого обмеження свободи вираження поглядів, доступу до інформації або діяльності засобів масової інформації. Пошук оптимального балансу між цими двома цінностями є одним із ключових завдань демократичної держави в межах її інформаційної політики. Європейська практика засвідчує, що ефективне забезпечення інформаційної безпеки можливе за умови дотримання високих стандартів прав людини – завдяки прозорості діяльності відповідних інституцій, наявності судового контролю та активній участі громадянського суспільства у моніторингу й оцінюванні інформаційної політики.

Інтеграція України до європейського безпекового простору передбачає адаптацію національної концепції інформаційної безпеки до норм і принципів Європейського Союзу. Це означає посилення уваги до захисту прав людини в інформаційній сфері, розвиток механізмів громадського контролю, підвищення прозорості діяльності органів державної влади та впровадження принципів відкритого врядування. Водночас українська модель інформаційної безпеки має враховувати особливості безпекової ситуації, у якій перебуває держава, зокрема триваючу збройну агресію Російської Федерації та системний характер інформаційних атак [9, с. 156]. Узгодження національного законодавства з

правом ЄС у сферах інформаційної безпеки, кібербезпеки та захисту персональних даних є важливою складовою виконання Угоди про асоціацію між Україною та ЄС і створює правові умови для подальшого поглиблення інтеграційних процесів [47].

Отже, інформаційна безпека постає як складний і багатовимірний феномен, що охоплює захист інформації, інформаційних систем та інформаційного простору держави від широкого спектра внутрішніх і зовнішніх загроз за умов дотримання балансу інтересів особи, суспільства й держави. Еволюція концепції інформаційної безпеки віддзеркалює стрімкий розвиток інформаційно-комунікаційних технологій, появу нових типів загроз і трансформацію підходів до забезпечення національної безпеки в умовах глобалізованого середовища. Інформаційна безпека займає особливе місце у системі національної та міжнародної безпеки завдяки своєму інтегративному характеру й тісному взаємозв'язку з іншими складовими безпекової політики держави, а також з огляду на зростання ролі інформаційного чинника у сучасних міжнародних відносинах.

Порівняння українського та європейського підходів демонструє тенденцію до їх поступового зближення в контексті євроінтеграційних процесів, що створює міцну концептуальну основу для подальшого дослідження інституційних механізмів, нормативно-правових засад та практичних інструментів забезпечення інформаційної безпеки. Сформульовані узагальнення закладають необхідний теоретичний фундамент для аналізу сучасних підходів до дослідження інформаційної безпеки у європейському інтеграційному вимірі, який стане предметом розгляду в наступному параграфі.

1.2. Теоретичні підходи до аналізу інформаційної безпеки в контексті європейських інтеграційних процесів

Визначення сутності та структурних елементів інформаційної безпеки, здійснене у попередньому параграфі, створює необхідну основу для подальшого розгляду методологічних засад дослідження цього явища в умовах європейської

інтеграції України. Теоретичне осмислення інформаційної безпеки вимагає застосування різних методологічних підходів, які дають змогу всебічно розкрити складність і багатовимірний характер трансформацій національної системи інформаційної безпеки під впливом інтеграційних процесів. Методологічний інструментарій аналізу інформаційної безпеки в європейському інтеграційному контексті включає системний, інституційний, комунікативний та конструктивістський підходи, кожен з яких акцентує на окремих вимірах цього феномену й дозволяє виявити закономірності адаптації національних безпекових механізмів до наднаціональних стандартів та практик.

Методологічні аспекти дослідження інформаційної безпеки у контексті європейських інтеграційних процесів дедалі частіше опиняються у центрі наукового інтересу дослідників як в Україні, так і за її межами. Вагомий внесок у розробку теоретико-методологічних засад аналізу інформаційної безпеки зробив Д. Дубов, який обґрунтував необхідність застосування міждисциплінарного підходу до вивчення інформаційної безпеки, що інтегрує здобутки політології, соціології, інформатики та правознавства [10, с. 89]. М. Ожеван досліджував комунікативні аспекти інформаційної безпеки та розробив концептуальну модель аналізу стратегічних комунікацій у системі забезпечення національної безпеки [25, с. 134]. Г. Почепцов запропонував дискурсивний підхід до аналізу інформаційних операцій та інформаційних війн, що дозволяє виявити механізми конструювання реальності через інформаційні впливи [30, с. 56]. Серед дослідників варто відзначити також напрацювання щодо застосування конструктивістської методології до аналізу формування європейської ідентичності та ролі комунікації у процесах європейської інтеграції, а також розробку теорії сек'юритизації, яка пояснює механізми перетворення певних питань на проблеми безпеки через дискурсивні практики. Водночас слід зазначити, що специфіка дослідження інформаційної безпеки саме в контексті європейської інтеграції України залишається недостатньо розробленою, що зумовлює необхідність подальшого методологічного пошуку та адаптації існуючих теоретичних підходів до аналізу трансформаційних процесів у цій сфері.

Системний підхід до аналізу інформаційної безпеки розглядає її як складну соціотехнічну систему, що складається з взаємопов'язаних елементів, між якими існують стійкі зв'язки та відносини. Застосування системної методології дозволяє виявити структуру системи інформаційної безпеки, ієрархію її компонентів, механізми взаємодії між різними підсистемами, а також закономірності функціонування системи як цілісності [29, с. 167]. У контексті європейської інтеграції системний підхід дає змогу проаналізувати процеси інтеграції національної системи інформаційної безпеки України до більш широкої європейської системи безпеки, виявити адаптаційні механізми та визначити елементи національної системи, що зазнають найбільших трансформацій під впливом європеїзації.

Основними елементами системи інформаційної безпеки, що підлягають аналізу з позицій системного підходу, є суб'єкти забезпечення інформаційної безпеки, об'єкти захисту, загрози та виклики, механізми та інструменти протидії загрозам, нормативно-правова база, ресурсне забезпечення. Системний аналіз передбачає розгляд не лише окремих компонентів, а й характеру зв'язків між ними, що особливо важливо для розуміння процесів європейської інтеграції. Європеїзація системи інформаційної безпеки означає не просте запозичення окремих елементів європейської моделі, а системну трансформацію, що охоплює всі рівні та компоненти національної системи. Прикметно, що системний підхід дозволяє виявити синергетичні ефекти від взаємодії різних елементів системи, а також виявити можливі дисфункції та протиріччя, що виникають у процесі адаптації національної системи до європейських стандартів.

Опис системного підходу до аналізу інформаційної безпеки потребує врахування концепції відкритих систем, у межах якої національна система інформаційної безпеки розглядається як така, що перебуває у безперервній взаємодії із зовнішнім середовищем, здійснюючи з ним обмін інформацією, ресурсами, нормативними моделями та практиками. Інтеграція до європейського безпекового простору означає розширення меж національної системи, встановлення нових зв'язків з європейськими інституціями, гармонізацію національних процедур з європейськими стандартами. Системний підхід

дозволяє аналізувати динаміку цих процесів, виявляти фактори, що сприяють або перешкоджають інтеграції, прогнозувати можливі наслідки системних трансформацій для національної безпеки.

Інституційний підхід до дослідження інформаційної безпеки зосереджується на значенні формальних і неформальних інституцій у забезпеченні захисту національного інформаційного простору. Інституції в цьому контексті розглядаються як усталені «правила гри», що структурують взаємодію суб'єктів у сфері інформаційної безпеки, визначають їхні повноваження та обов'язки, а також формують систему стимулів і обмежень, які впливають на їхню поведінку [21, с. 112]. Застосування інституційного підходу до дослідження трансформації інформаційної безпеки України в контексті європейської інтеграції передбачає аналіз процесів інституційних змін, механізмів трансферу інституцій з європейського рівня на національний, факторів, що визначають успішність інституційної адаптації.

Інституційний аналіз охоплює вивчення як формальних інституцій, до яких належать законодавчі акти, стратегії, концепції, організаційні структури державних органів, так і неформальних інституцій, таких як усталені практики, норми професійної етики, традиції міжвідомчої співпраці. У контексті європейської інтеграції особливої ваги набуває дослідження процесів гармонізації національного законодавства з правом Європейського Союзу, впровадження європейських директив і регламентів, а також адаптації національних інституційних механізмів до вимог acquis ЄС. Важливо відзначити, що інституційні зміни не є автоматичними або механічними, вони залежать від багатьох факторів, включаючи політичну волю, ресурсне забезпечення, професійні компетенції, соціокультурний контекст.

Концепція європеїзації, що активно використовується в дослідженнях процесів трансформації національних систем під впливом інтеграції до Європейського Союзу, становить важливий елемент інституційного підходу. Європеїзація розуміється як процес формування, поширення та закріплення на інституційному рівні формальних і неформальних норм, процедур, політичних парадигм, моделей поведінки та способів організації діяльності, що спочатку

визначаються та консолідуються у процесі формування політики ЄС, а потім інкорпоруються у логіку національного дискурсу, ідентичностей, політичних структур та публічної політики. Аналіз європеїзації системи інформаційної безпеки України дозволяє виявити напрями, темпи та глибину інституційних трансформацій, визначити фактори успішності або неуспішності адаптаційних процесів, оцінити ступінь відповідності національної системи європейським стандартам.

Комунікативний підхід до дослідження інформаційної безпеки фокусується на процесах комунікації, інформаційних потоках, механізмах формування та поширення дискурсів у сфері безпеки. Цей підхід виходить з розуміння інформаційного простору як комунікативного середовища, в якому відбувається обмін інформацією між різними акторами, формуються смисли та значення, конструюються уявлення про безпеку та загрози. Комунікативний підхід особливо релевантний для аналізу інформаційної безпеки, оскільки саме комунікаційні процеси становлять одночасно і об’єкт захисту, і канал загроз, і інструмент забезпечення безпеки.

Застосування комунікативного підходу до аналізу інформаційної безпеки в контексті європейської інтеграції передбачає розгляд стратегічних комунікацій як ключового інструменту забезпечення інформаційної стійкості держави та суспільства. Стратегічні комунікації трактується як узгоджене й ефективне застосування державою наявних комунікативних інструментів і ресурсів з метою підтримки реалізації політичних завдань та досягнення національних безпекових пріоритетів [25, с. 23]. Європейський Союз приділяє значну увагу розвитку стратегічних комунікацій як інструменту протидії дезінформації та зміцнення інформаційної стійкості. Створення East StratCom Task Force у структурі Європейської служби зовнішніх дій стало відповіддю на активізацію російських інформаційних кампаній, спрямованих на підрив єдності ЄС та дестабілізацію країн Східного партнерства.

Комунікативний підхід дозволяє проаналізувати механізми поширення дезінформації, виявити вразливості національного інформаційного простору, оцінити ефективність заходів протидії маніпулятивним впливам. Особлива увага

приділяється аналізу соціальних мереж як каналів комунікації, що можуть використовуватися як для легітимної взаємодії, так і для поширення деструктивного контенту, координації інформаційних атак, таргетованого впливу на певні цільові аудиторії. Розуміння механізмів функціонування сучасного медіаландшафту, особливостей споживання інформації різними соціальними групами, психологічних механізмів впливу інформації на свідомість є необхідною передумовою для розробки ефективної політики інформаційної безпеки.

Конструктивістський підхід до аналізу інформаційної безпеки виходить з розуміння безпеки не як об'єктивної реальності, а як соціального конструкту, що формується через дискурсивні практики та інтерсуб'єктивні смисли. Згідно з конструктивістською методологією, питання стають проблемами безпеки не через їхні об'єктивні характеристики, а через процес сек'юритизації, тобто дискурсивне конструювання певного явища як екзистенційної загрози, що потребує надзвичайних заходів. Застосування конструктивістського підходу до аналізу інформаційної безпеки дозволяє виявити механізми формування уявлень про інформаційні загрози, роль дискурсів безпеки у легітимації певних політичних рішень, вплив ідентичностей та цінностей на визначення пріоритетів інформаційної безпеки.

У контексті європейської інтеграції конструктивістський підхід дає можливість проаналізувати процеси формування спільного європейського дискурсу інформаційної безпеки, механізми узгодження національних та наднаціональних уявлень про загрози, роль ідентичності у визначенні безпекових пріоритетів. Прикметно, що європейський дискурс інформаційної безпеки характеризується акцентом на захисті демократичних цінностей, прав людини, верховенстві права, тоді як в деяких державах-членах традиційно домінували державоцентричні підходи до безпеки. Процес європейської інтеграції передбачає поступову конвергенцію національних дискурсів безпеки з європейським, що відбувається через механізми соціалізації, навчання, обміну досвідом, спільної діяльності у міжнародних форматах.

Особливого значення у сучасному дискурсі європейської інформаційної

безпеки набувають концепції інформаційного та цифрового суверенітету Європейського Союзу. Концепція цифрового суверенітету виникла як відповідь на зростаючу залежність Європи від цифрових технологій, що розробляються та контролюються іноземними, передусім американськими та китайськими, корпораціями. Цифровий суверенітет визначається як здатність Європейського Союзу діяти незалежно у цифровому просторі, контролювати критичні цифрові технології та інфраструктури, захищати власні цінності та інтереси у цифровій сфері.

Стратегія цифрового суверенітету ЄС охоплює декілька ключових напрямів. По-перше, це розвиток власних технологічних компетенцій та зменшення технологічної залежності від третіх країн. Європейська комісія ініціювала низку програм, спрямованих на підтримку європейських технологічних компаній, інвестиції у дослідження та розробки у сфері квантових технологій, штучного інтелекту, кібербезпеки, хмарних обчислень. По-друге, це встановлення жорстких регуляторних стандартів для цифрових платформ та послуг, що працюють на європейському ринку. Прийняття Акта про цифрові послуги та Акта про цифрові ринки у 2022 році стало важливим кроком у цьому напрямі, встановивши нові правила для великих онлайн-платформ щодо модерації контенту, захисту користувачів, протидії дезінформації.

По-третє, стратегія цифрового суверенітету передбачає захист європейських даних та створення власної цифрової інфраструктури. Загальний регламент про захист даних, що набрав чинності у 2018 році, встановив високі стандарти захисту персональних даних та обмежив можливості передачі даних європейських громадян за межі ЄС [6]. Ініціатива створення європейської хмарної інфраструктури Gaia-X покликана забезпечити європейським компаніям та державним установам доступ до надійних хмарних послуг, що відповідають європейським вимогам щодо безпеки, приватності та суверенітету даних. По-четверте, важливою складовою стратегії є забезпечення кібербезпеки критичних інфраструктур. Директива NIS2, прийнята у 2022 році, розширила коло суб’єктів, що підпадають під вимоги кібербезпеки, та посилила зобов’язання держав-членів щодо забезпечення захисту критичних інфраструктур.

Концепція інформаційного суверенітету тісно пов’язана з цифровим суверенітетом, але має ширше значення, охоплюючи не лише технологічні аспекти, а й культурні, політичні та ідентичнісні виміри інформаційного простору. Інформаційний суверенітет розуміється як здатність держави або інтеграційного об’єднання контролювати інформаційні потоки на власній території, формувати власний інформаційний порядок, захищати власні наративи та цінності від зовнішніх інформаційних впливів [22, с. 178]. У європейському контексті концепція інформаційного суверенітету виявляється у прагненні захистити європейську демократичну культуру, плюралізм медіа, верховенство права від авторитарних моделей управління інформацією, що просуваються деякими недемократичними режимами.

Водночас слід зазначити, що концепція суверенітету в інформаційній сфері є суперечливою та викликає дискусії як у науковому, так і у політичному середовищі. Критики вказують на ризики використання риторики інформаційного суверенітету для виправдання цензури, обмеження свободи слова, фрагментації глобального інформаційного простору. Існує напруження між прагненням захистити національний або регіональний інформаційний простір від деструктивних зовнішніх впливів та необхідністю забезпечити відкритість, свободу інформації, міжнародну співпрацю. Європейський підхід намагається знайти баланс між цими вимогами, акцентуючи на захисті демократичних цінностей та прав людини як меті забезпечення інформаційного суверенітету.

Для України концепції цифрового та інформаційного суверенітету Європейського Союзу мають вагоме прикладне значення, оскільки задають стратегічні орієнтири модернізації та розвитку національної системи інформаційної безпеки в умовах євроінтеграційного поступу. Адаптація до європейських стандартів означає не просте копіювання європейських нормативних актів, а осмислене впровадження підходів, що базуються на принципах демократії, верховенства права, захисту прав людини. Це передбачає розвиток власних технологічних компетенцій у сфері кібербезпеки, захисту даних, стратегічних комунікацій, створення стійкого медіаландшафту,

підвищення медіаграмотності населення, зміцнення інституційної спроможності державних органів у сфері інформаційної безпеки.

Порівняльний аналіз європейського та українського підходів до інформаційної безпеки засвідчує наявність як спільних, так і відмінних характеристик. Серед спільних положень – визнання інформаційної безпеки стратегічним пріоритетом державної політики, розуміння необхідності комплексного підходу до захисту інформаційного простору, а також усвідомлення загроз, що походять від авторитарних режимів, які використовують інформаційні технології для підриву демократичних інституцій. Водночас відмінності проявляються у різних акцентах, пріоритезації ризиків та доборі інструментів реалізації політики. Українська модель інформаційної безпеки сформувалася в умовах тривалої та системної інформаційної агресії з боку Російської Федерації, що зумовило підвищену увагу до протидії дезінформаційним кампаніям, пропаганді та ворожим інформаційним операціям. Європейський підхід, натомість, ґрунтується на ширшому використанні механізмів саморегулювання, тісній взаємодії з інститутами громадянського суспільства та партнерстві з технологічними компаніями у сфері забезпечення інформаційної стійкості.

Гармонізація української системи інформаційної безпеки зі стандартами Європейського Союзу потребує одночасного врахування двох вимірів: збереження накопиченого досвіду протидії гібридним загрозам та інтеграції найкращих європейських практик у сферах регулювання цифрового середовища, захисту персональних даних, розвитку медіаграмотності та стратегічних комунікацій. Важливим напрямом у цьому процесі є активна участь України в європейських та євроатлантичних ініціативах у галузі інформаційної безпеки, зокрема в діяльності East StratCom Task Force, Центру передового досвіду НАТО зі стратегічних комунікацій, а також у програмах Horizon Europe, спрямованих на розвиток кібербезпеки та цифрових технологій. Залучення до цих ініціатив дає змогу не лише переймати передові європейські підходи, але й долучатися до формування спільного безпекового простору ЄС, роблячи власний внесок у протидію спільним викликам та загрозам.

Методологічний плюралізм у дослідженні інформаційної безпеки в умовах європейської інтеграції передбачає не протиставлення різних підходів, а їх взаємне доповнення та поєднання в єдину аналітичну конструкцію. Системний підхід дає змогу сформувати цілісне бачення трансформацій національної системи інформаційної безпеки та простежити структурні зв'язки між її ключовими компонентами. Інституційний підхід зосереджує увагу на механізмах інституційних змін, процесах запозичення, трансферу й адаптації європейських інституційних моделей на національному рівні. Комунікативний підхід акцентує на динаміці інформаційних потоків, особливостях стратегічних комунікацій та їх ролі у зміцненні інформаційної стійкості. Конструктивістський підхід дає можливість врахувати вплив ідей, дискурсів та ідентичностей на формування політики інформаційної безпеки. Поєднання цих підходів у єдиній методологічній рамці забезпечує комплексне й багатовимірне розуміння процесів трансформації системи інформаційної безпеки України в контексті євроінтеграційних процесів.

Отже, теоретичні підходи до аналізу інформаційної безпеки в умовах європейських інтеграційних процесів формують методологічний фундамент для комплексного дослідження трансформацій у цій сфері. Системний, інституційний, комунікативний та конструктивістський підходи дають змогу висвітлити різні виміри інформаційної безпеки, простежити механізми європеїзації національних систем та проаналізувати процеси становлення спільного європейського безпекового простору. Концепції цифрового й інформаційного суверенітету Європейського Союзу задають стратегічні орієнтири розвитку інформаційної безпеки в європейському контексті та визначають напрям подальшої адаптації української системи до стандартів ЄС. Сформульовані методологічні узагальнення створюють необхідну основу для подальшого аналізу нормативно-правових і стратегічних засад забезпечення інформаційної безпеки України, що стане предметом розгляду в наступному параграфі.

1.3. Нормативно-правові та стратегічні засади забезпечення інформаційної безпеки України

Аналіз теоретичних підходів до вивчення інформаційної безпеки, здійснений у попередньому параграфі, формує необхідне методологічне підґрунтя для переходу до розгляду нормативно-правових та стратегічних засад забезпечення інформаційної безпеки України. Перехід від теоретичної концептуалізації до вивчення практичних механізмів правового регулювання є логічно вмотивованим, оскільки саме нормативно-правова база визначає інституційну конфігурацію системи інформаційної безпеки, розподіл повноважень між суб'єктами її забезпечення, права та обов'язки різних акторів, а також процедури реагування на загрози. В умовах європейської інтеграції України особливої ваги набуває аналіз процесів гармонізації національного законодавства з правом Європейського Союзу, імплементації європейських стандартів у національну практику та адаптації стратегічних документів до підходів ЄС у сфері інформаційної безпеки.

Нормативно-правове регулювання інформаційної безпеки України є предметом активного дослідження вітчизняних учених і практиків. В. Ліпкан здійснив комплексний аналіз правових засад національної безпеки, приділивши окрему увагу її інформаційному компоненту [18, с. 234]. О. Золотар досліджувала еволюцію українського законодавства у сфері інформаційної безпеки та виокремила ключові тенденції його розвитку в умовах протидії гібридним загрозам [12, с. 156]. Д. Дубов проаналізував стратегічні документи в галузі інформаційної безпеки та підкреслив необхідність їх оновлення з огляду на нові виклики та євроінтеграційні процеси [9, с. 89]. І. Арістова розглядала конституційно-правові засади інформаційної безпеки, акцентуючи на проблематиці балансу між безпекою та свободою інформації [1, с. 201]. Водночас швидка еволюція законодавства, ухвалення нових стратегічних документів і поглиблення європейської інтеграції потребують постійного перегляду та оновлення аналізу нормативно-правових підвалин інформаційної безпеки України.

Конституційні засади інформаційної безпеки України закріплені у

Конституції України, яка гарантує кожному право на свободу думки й слова, вільне висловлення поглядів і переконань, а також право збирати, зберігати, використовувати та поширювати інформацію будь-якими законними способами [14, ст. 34]. Водночас Основний Закон передбачає можливість обмеження цих прав у випадках, визначених законом, зокрема в інтересах національної безпеки, територіальної цілісності та громадського порядку. Таке конституційне врегулювання співвідношення свободи інформації та безпекових потреб держави формує правову основу для подальшого розвитку законодавства у сфері інформаційної безпеки. Важливо підкреслити, що положення Конституції України щодо інформаційних прав і свобод відповідають міжнародним стандартам, закріпленим у Загальній декларації прав людини, Міжнародному пакті про громадянські і політичні права та Європейській конвенції з прав людини.

Базовим законодавчим документом, який визначає правові та організаційні засади захисту життєво важливих інтересів людини, суспільства та держави від внутрішніх і зовнішніх загроз, є Закон України «Про національну безпеку України» 2018 року [36]. У ньому визначено систему суб'єктів забезпечення національної безпеки, їх повноваження, механізми взаємодії та процедури стратегічного планування у сфері безпеки й оборони. Інформаційна безпека в межах цього закону розглядається як одна з ключових складових національної безпеки, а державна політика спрямовується на її зміцнення та розвиток інформаційного суспільства. Важливо, що закон ухвалювався вже після початку російської агресії проти України і враховує практичний досвід протидії гібридним загрозам, включно з інформаційними операціями противника.

Спеціальним нормативно-правовим актом у сфері інформаційної безпеки є Закон України «Про основні засади забезпечення кібербезпеки України», прийнятий у 2017 році [37]. Він визначає правові й організаційні засади захисту життєво важливих інтересів особи, суспільства та держави в кіберпросторі, окреслює цілі та принципи державної політики у сфері кібербезпеки, встановлює повноваження органів влади, підприємств та установ, а також права й обов'язки громадян у цій сфері. Закон трактує кібербезпеку як стан захищеності життєво

важливих інтересів під час використання кіберпростору, що передбачає сталий розвиток інформаційного суспільства, стабільність цифрового комунікаційного середовища, а також своєчасне виявлення, запобігання й нейтралізацію реальних та потенційних загроз національній безпеці України.

Закон України про кібербезпеку визначає коло об'єктів кібербезпеки, до яких належать права та свободи людини і громадянина, суспільство й держава, а також національні інтереси України в кіберпросторі. У документі окреслено й широке коло суб'єктів, відповідальних за забезпечення кібербезпеки. До них віднесено Президента України, Раду національної безпеки і оборони України, Кабінет Міністрів України, органи виконавчої влади, Національний банк України, місцеві державні адміністрації, органи місцевого самоврядування, військові формування, правоохоронні органи спеціального призначення, розвідувальні структури, а також центральний орган виконавчої влади, уповноважений формувати й реалізовувати державну політику у сфері захисту державних інформаційних ресурсів та інформаційно-телекомунікаційних систем. Важливо, що закон закріплює необхідність координації діяльності усіх зазначених суб'єктів, яка здійснюється через функціонування Координаційного центру кібербезпеки при Раді національної безпеки і оборони України.

Однак слід зазначити, що імплементація Закону про кібербезпеку стикається з певними труднощами. Зокрема, станом на 2024 рік не всі передбачені законом підзаконні акти були прийняті, що ускладнює практичну реалізацію його норм. Координаційний центр кібербезпеки, створений у 2021 році, потребує подальшого зміцнення інституційної спроможності та ресурсного забезпечення. Водночас російська збройна агресія стала каталізатором активізації роботи у сфері кібербезпеки, що виявилося у прийнятті низки додаткових нормативних актів, посиленні координації між відповідними державними органами, залученні міжнародної технічної допомоги.

Важливим елементом правової системи забезпечення інформаційної безпеки є Закон України «Про інформацію», прийнятий ще у 1992 році та неодноразово змінюваний [35]. Цей закон регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту

інформації. Закон визначає основні принципи інформаційних відносин, види інформації за змістом, порядок доступу до інформації, відповідальність за порушення законодавства про інформацію. З урахуванням тривалого часу дії цього закону та значних змін в інформаційній сфері, що відбулися за минулі десятиліття, він потребує суттєвого оновлення та приведення у відповідність із сучасними реаліями цифрової епохи.

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» 1994 року визначає правові та організаційні засади забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [34]. Документ містить класифікацію таких систем за рівнями захищеності, встановлює вимоги до засобів технічного захисту інформації, регламентує процедури сертифікації відповідних засобів, а також окреслює права й обов'язки власників інформації та користувачів систем. Разом із тим, з огляду на стрімкий розвиток цифрових технологій, появу нових типів кіберзагроз та необхідність гармонізації з європейськими стандартами кібербезпеки, цей закон потребує подальшої актуалізації та модернізації.

Окремий сегмент законодавчого забезпечення інформаційної безпеки України становлять акти, що регулюють функціонування засобів масової інформації та медіапростору. Закон України «Про телебачення і радіомовлення» визначає правові засади діяльності телерадіоорганізацій, регламентує вимоги до змісту програм, встановлює обмеження щодо поширення пропагандистського та шкідливого контенту [43]. Закон України «Про друковані засоби масової інформації (пресу) в Україні» регулює діяльність друкованих медіа [32]. Важливою складовою протидії російській інформаційній агресії стало ухвалення законів, що обмежують розповсюдження продукції російської культурної індустрії та забороняють діяльність політичних партій і організацій, пов'язаних з державою-агресором. Попри дискусії щодо співвідношення таких заходів із гарантіями свободи слова, вони були визнані виправданими в умовах триваючої воєнної агресії.

Значну роль у правовому регулюванні інформаційної безпеки відіграють

підзаконні нормативно-правові акти: укази Президента України, постанови Кабінету Міністрів України, накази міністерств і відомств. Одними з ключових документів цього рівня є накази Адміністрації Державної служби спеціального зв'язку та захисту інформації України, якими затверджуються порядки, стандарти та вимоги у сферах кіберзахисту, технічного та криптографічного захисту інформації. Державна служба спеціального зв'язку та захисту інформації України виступає центральним органом виконавчої влади, відповідальним за формування та реалізацію державної політики у галузі кібербезпеки, захисту державних інформаційних ресурсів, технічного захисту інформації та телекомунікацій.

Стратегічні документи у сфері інформаційної безпеки визначають довгострокові пріоритети й напрями державної політики. Центральним з них є Стратегія національної безпеки України, затверджена Указом Президента України у 2020 році [39]. У документі окреслено актуальні загрози національній безпеці, серед яких окреме місце займають інформаційні загрози, дезінформаційні операції та кіберзагрози. Стратегія визначає ключові пріоритети державної політики у сфері безпеки, включно із забезпеченням інформаційної безпеки та інформаційного суверенітету України, розвитком стратегічних комунікацій, протидією дезінформації, посиленням кіберзахисту критичної інфраструктури.

Доктрина інформаційної безпеки України, ухвалена Указом Президента у 2017 році, виступає спеціалізованим стратегічним документом, який окреслює національні інтереси держави в інформаційній сфері, визначає спектр загроз цим інтересам і формує цілі та ключові напрями державної політики у відповідному секторі [42]. Її прийняття відбулося в умовах активної російської агресії, що зумовило значний акцент документа на протидії інформаційному впливу та веденню інформаційної війни з боку Російської Федерації. У Доктрині виокремлено основні загрози інформаційній безпеці України, серед яких – здійснення інформаційних операцій проти держави, поширення деструктивної пропаганди та маніпулятивних наративів, спрямованих на підрив суспільної єдності, дискредитацію органів влади та формування негативного іміджу

України у світовому інформаційному середовищі.

Стратегія інформаційної безпеки України, ухвалена у 2021 році, стала модернізованим концептуальним документом, який замінив попередню Доктрину та відобразив як появу нових типів загроз у інформаційному середовищі, так і поступ України на шляху інтеграції до Європейського Союзу [41]. У Стратегії інформаційна безпека трактується як такий стан функціонування держави, суспільства та окремої особи, за якого життєво важливі інтереси не зазнають шкоди внаслідок поширення неточної, несвоєчасної чи недостовірної інформації, негативних інформаційних впливів, зловживань інформаційними технологіями або порушення конфіденційності, цілісності та доступності інформаційних ресурсів. Документ також формує систему стратегічних орієнтирів, серед яких – утвердження інформаційного суверенітету України, підвищення стійкості суспільства до деструктивних інформаційних впливів, розбудова сучасного інформаційного суспільства та розвиток медіаграмотності населення.

Важливо відзначити, що Стратегія інформаційної безпеки 2021 року приділяє значну увагу питанням гармонізації національного законодавства з європейськими стандартами. Документ передбачає імплементацію положень Директиви ЄС про аудіовізуальні медіа-послуги, Директиви про захист персональних даних, Директиви про безпеку мережевих та інформаційних систем. Стратегія визначає необхідність розвитку співпраці з європейськими інституціями у сфері протидії дезінформації, участі у європейських проєктах у сфері стратегічних комунікацій, обміну досвідом з державами-членами ЄС щодо кращих практик забезпечення інформаційної безпеки.

Стратегія кібербезпеки України, ухвалена у 2021 році, окреслює довгострокове бачення розвитку державної політики у сфері кіберзахисту та визначає ключові орієнтири її реалізації до 2025 року [40]. У документі робиться наголос на необхідності суттєвого зміцнення стійкості об’єктів критичної інфраструктури до кібератак, формуванні власних висококваліфікованих фахових спроможностей у галузі кібербезпеки, а також на розбудові ефективної національної системи реагування на кіберінциденти. Окремо підкреслюється

важливість поширення знань про кіберзагрози серед громадян та суб'єктів господарювання з метою підвищення загального рівня кіберкультури. Стратегія також визначає інтеграцію України до європейського кібербезпекового простору як один із пріоритетів: передбачено адаптацію національного законодавства до норм і стандартів ЄС, імплементацію положень Директиви NIS2 та участь у відповідних європейських програмах і ініціативах.

Концепція розвитку цифрових компетентностей та Концепція розвитку штучного інтелекту в Україні відіграють суттєву роль у зміцненні інформаційної безпеки держави, оскільки задають стратегічні напрямки формування цифрової грамотності громадян, підготовки висококваліфікованих кадрів у сфері ІТ та впровадження інноваційних технологічних рішень у систему безпекового управління. Підвищення рівня цифрових навичок населення є ключовою умовою для формування суспільної інформаційної стійкості: воно забезпечує здатність громадян ідентифікувати дезінформаційні матеріали, протистояти маніпулятивним впливам, усвідомлено та безпечно взаємодіяти з цифровими сервісами й платформами. Таким чином, розвиток цифрових компетентностей стає фундаментом не лише для модернізації освіти та ринку праці, а й для підвищення загальної резилієнтності держави в умовах сучасних інформаційних загроз.

Комплексний розгляд чинної нормативно-правової бази України у сфері інформаційної безпеки показує, що поряд із певними успіхами система все ще містить низку структурних недоліків. До позитивних аспектів варто віднести формування окремого масиву законодавства у сфері кібербезпеки, ухвалення стратегічних документів, що визначають довгострокові пріоритети державної політики, а також створення інституційної архітектури, відповідальної за захист інформаційного простору. Проте залишаються й вагомі проблеми, які перешкоджають підвищенню ефективності державної політики. Насамперед ідеться про фрагментарний характер нормативного регулювання: положення, що стосуються інформаційної безпеки, розпорошені між численними актами різного рівня, ухваленими в різні періоди та не завжди узгодженими між собою. Другою проблемою є застарілість частини законодавчих норм, що були прийняті ще в

1990-х роках і вже не відповідають вимогам цифрової трансформації та сучасним загрозам. Третім суттєвим недоліком є неповна реалізація вже ухвалених законів, що зумовлено відсутністю належної системи підзаконних актів, недостатнім ресурсним забезпеченням і обмеженою інституційною спроможністю органів, відповідальних за їх імплементацію.

Одним із визначальних обов'язків України у межах виконання Угоди про асоціацію з Європейським Союзом є гармонізація національного законодавства у сфері інформаційної безпеки з правом ЄС [47]. Даний міжнародний документ охоплює широке коло сфер, безпосередньо пов'язаних із інформаційною безпекою, включно з електронними комунікаціями, захистом персональних даних, кібербезпекою, медійною політикою та протидією кіберзлочинності. Додаток XVII до Угоди встановлює перелік директив, регламентів і рішень Європейського Союзу у сфері електронних комунікацій, імплементацію яких Україна зобов'язалася поступово забезпечити шляхом приведення свого законодавства у відповідність до acquis ЄС.

Серед нормативних актів Європейського Союзу, адаптація яких є пріоритетною для України, особливе місце посідає Загальний регламент про захист даних (GDPR). Цей документ формує один із найжорсткіших у світі режимів охорони персональної інформації та суттєво підвищує вимоги до обробки даних громадян ЄС [71]. Україна ще у 2010 році ухвалила спеціальний закон щодо захисту персональних даних, частково узгоджений із попередньою європейською директивою. Проте для повноцінного наближення до стандартів GDPR необхідне глибоке оновлення законодавства та створення дієвих інституційних механізмів регулювання й контролю у цій сфері.

Важливим елементом є також імплементація Директиви NIS та її оновленої версії NIS2, яка встановлює вимоги до кіберзахисту операторів критичної інфраструктури й постачальників цифрових послуг. Реалізація положень цієї директиви передбачає законодавче визначення переліку критичних об'єктів, розроблення стандартів безпеки для їхніх операторів, створення обов'язкових процедур звітування про кіберінциденти та посилення національних спроможностей у сфері реагування на кіберзагрози.

Директива про аудіовізуальні медіа-послуги регулює діяльність телерадіомовників і провайдерів сервісів відео-на-вимогу, встановлюючи вимоги до змісту, рекламної політики, захисту дітей та просування європейського продукту. Україна вже адаптувала значну частину її положень шляхом модернізації законодавства у сфері телерадіомовлення.

Крім того, у 2022 році Європейський Союз прийняв Акт про цифрові послуги (DSA) та Акт про цифрові ринки (DMA), які формують нову архітектуру регулювання цифрових платформ. Ці документи спрямовані на вдосконалення механізмів модерації контенту, протидію дезінформації, забезпечення прозорості алгоритмів, захист користувачів, а також обмеження зловживань ринковою владою з боку великих онлайн-компаній. Хоча Україна поки що не має формального обов'язку імплементувати ці акти, їх врахування при розробці національної політики регулювання цифрового середовища є стратегічно доцільним у контексті майбутнього членства в ЄС.

Процес гармонізації українського законодавства з європейськими стандартами стикається з низкою викликів. По-перше, це складність та обсяг європейського законодавства, що потребує значних ресурсів для аналізу, перекладу, адаптації до національного контексту. По-друге, необхідність не лише формального перенесення норм європейських актів у національне законодавство, а й створення ефективних механізмів їхньої імплементації, що потребує організаційних змін, підготовки кадрів, ресурсного забезпечення. По-третє, потреба балансування між європейськими стандартами та специфікою безпекового середовища України, зокрема необхідністю протидії російській агресії та гібридним загрозам.

Водночас європейська інтеграція створює значні можливості для зміцнення інформаційної безпеки України. По-перше, це доступ до кращих європейських практик, технологій, експертизи у сфері кібербезпеки, протидії дезінформації, захисту даних. По-друге, можливість участі у європейських програмах та ініціативах, таких як програма Горизонт Європа, програма Цифрова Європа, ініціативи у сфері стратегічних комунікацій. По-третє, зміцнення інституційної спроможності українських органів через навчання,

обмін досвідом, технічну допомогу з боку європейських партнерів. По-четверте, підвищення довіри міжнародних партнерів та інвесторів до рівня захисту інформації в Україні завдяки відповідності європейським стандартам.

Важливим напрямом співпраці України з Європейським Союзом у сфері інформаційної безпеки є участь у проєктах протидії дезінформації. Україна активно співпрацює з East StratCom Task Force Європейської служби зовнішніх дій, обмінюється інформацією про виявлені дезінформаційні кампанії, бере участь у спільних дослідженнях та аналітичних проєктах. Центр стратегічних комунікацій та інформаційної безпеки при Міністерстві культури та інформаційної політики України здійснює моніторинг дезінформації, проводить фактчекінг, реалізує проєкти з підвищення медіаграмотності у співпраці з європейськими партнерами.

У сфері кібербезпеки Україна розвиває співпрацю з Агентством Європейського Союзу з кібербезпеки (ENISA), бере участь у навчальних заходах, тренінгах, обмінюється інформацією про кіберзагрози та інциденти. Державна служба спеціального зв'язку та захисту інформації України співпрацює з національними центрами реагування на комп'ютерні надзвичайні події держав-членів ЄС, що дозволяє оперативно обмінюватися інформацією про кіберзагрози та координувати відповіді на транснаціональні кіберінциденти. Повномасштабна російська агресія продемонструвала важливість міжнародної співпраці у сфері кібербезпеки, оскільки Україна отримала значну технічну допомогу від європейських та інших міжнародних партнерів для захисту критичної інфраструктури від кібератак.

Перспективи розвитку нормативно-правової бази інформаційної безпеки України визначаються як внутрішніми потребами зміцнення системи безпеки, так і євроінтеграційними процесами. До пріоритетних напрямів вдосконалення законодавства належать кодифікація нормативних актів у сфері інформаційної безпеки, оновлення застарілих законів з урахуванням розвитку цифрових технологій, прийняття нових законодавчих актів у сферах, що недостатньо врегульовані, зокрема щодо регулювання діяльності цифрових платформ, протидії дезінформації, захисту критичної інформаційної інфраструктури.

Важливим є забезпечення повної імплементації вже прийнятих законів шляхом розробки необхідних підзаконних актів, створення ефективних механізмів контролю та нагляду, забезпечення ресурсами відповідальних органів.

Узгоджений масив нормативно-правових та стратегічних документів, що регулюють сферу інформаційної безпеки України, формує фундамент, на якому вибудовується національна система захисту інформаційного простору. Чинне законодавство охоплює широкий спектр регуляторних напрямів – від кіберзахисту і технічної охорони інформації до управління медіасферою, діяльності цифрових платформ та розвитку стратегічних комунікацій. Стратегічні документи визначають довготривалі пріоритети державної політики, орієнтуючись на характер сучасних загроз і динаміку євроінтеграційних процесів.

Важливим вектором подальшого розвитку правової бази є її зближення з acquis Європейського Союзу. Цей процес охоплює впровадження загальноєвропейських стандартів у галузях захисту персональних даних, кібербезпеки, регулювання цифрових послуг і медійної політики. Водночас адаптація норм ЄС потребує урахування українських реалій, пов’язаних насамперед із необхідністю протидії гібридним загрозам і системній інформаційній агресії з боку Російської Федерації.

Таким чином, аналіз нормативно-правових засад забезпечення інформаційної безпеки створює необхідне підґрунтя для подальшого вивчення інституційної структури та механізмів функціонування системи інформаційної безпеки України. Саме ці питання стануть предметом розгляду у наступному розділі роботи.

Висновки до розділу 1

Теоретичні засади аналізу інформаційної безпеки держави в умовах європейської інтеграції охоплюють концептуалізацію сутності інформаційної безпеки, методологічний інструментарій її аналізу та нормативно-правові засади практичної реалізації політики у цій сфері. Проведений аналіз дозволяє

сформулювати низку принципових висновків.

Інформаційна безпека є складним багатовимірним феноменом, що охоплює захист інформації, інформаційних систем та інформаційного простору держави від різноманітних ризиків та викликів, що формуються як у внутрішньому середовищі держави, так і поза її межами при забезпеченні балансу інтересів особи, суспільства і держави. Еволюція концепції інформаційної безпеки відображає трансформацію від вузького розуміння як захисту державних секретів до широкого комплексного підходу, що включає технологічні, правові, організаційні, психологічні та культурні аспекти забезпечення цілісності національного інформаційного середовища. Структура інформаційної безпеки включає кілька взаємопов'язаних блоків: охорону інформаційних ресурсів, захист інфраструктур, що забезпечують обробку та передачу даних, безпеку всього інформаційного простору держави, а також підтримання високого рівня суспільної інформаційної стійкості. Її роль у системі національної безпеки є визначальною, оскільки інформаційна складова пронизує всі інші сфери безпеки та безпосередньо впливає на функціонування політичних, економічних, оборонних і соціальних механізмів держави.

Концепції цифрового та інформаційного суверенітету Європейського Союзу визначають стратегічні орієнтири розвитку інформаційної безпеки у європейському просторі. Цифровий суверенітет розуміється як здатність ЄС діяти незалежно у цифровому просторі, контролювати критичні технології та інфраструктури, захищати власні цінності та інтереси у цифровій сфері. Інформаційний суверенітет передбачає значно ширший спектр напрямів, серед яких культурні, політичні та ідентичнісні виміри інформаційного простору. Європейська стратегія реалізації цих концепцій включає розвиток власних технологічних компетенцій, встановлення жорстких регуляторних стандартів для цифрових платформ, захист європейських даних, забезпечення кібербезпеки критичних інфраструктур. Для України ці концепції відіграють ключову прикладну роль, адже окреслюють траєкторію адаптації національної системи інформаційної безпеки до європейських стандартів.

Нормативно-правова база інформаційної безпеки України сформована на

конституційному рівні та включає спеціалізоване законодавство у сфері кібербезпеки, захисту інформації, регулювання медіапростору. Ключовими законодавчими актами є Закон України «Про національну безпеку України», Закон України «Про основні засади забезпечення кібербезпеки України», а також низка інших законів, що регулюють різні аспекти інформаційних відносин. Стратегічні документи, зокрема Стратегія національної безпеки України, Стратегія інформаційної безпеки України, Стратегія кібербезпеки України, визначають довгострокові цілі, пріоритети та напрями державної політики з урахуванням актуальних загроз та євроінтеграційних процесів.

Гармонізація національного законодавства з правом Європейського Союзу є ключовим зобов'язанням України за Угодою про асоціацію та передбачає імплементацію європейських стандартів у площині регулювання обробки та безпеки персональної інформації, кібербезпеки, регулювання електронних комунікацій, медіаполітики. Процес гармонізації стикається з певними викликами, включаючи складність європейського законодавства, необхідність створення ефективних механізмів імплементації, потребу балансування між європейськими стандартами та специфікою національного безпекового середовища. Водночас європейська інтеграція створює значні можливості для зміцнення інформаційної безпеки через доступ до кращих практик, технологій, міжнародної технічної допомоги, участь у європейських програмах та ініціативах.

Аналіз нормативно-правових засад виявив як певні досягнення, так і проблеми, що потребують вирішення. До проблемних аспектів належать фрагментарність законодавства, застарілість окремих нормативних актів, недостатня імплементація прийнятих законів через брак підзаконних актів та ресурсного забезпечення. Пріоритетними напрямами вдосконалення законодавства є кодифікація нормативних актів, оновлення застарілих законів, прийняття нових актів у недостатньо врегульованих сферах, забезпечення повної імплементації існуючого законодавства.

РОЗДІЛ 2. СУЧАСНИЙ СТАН ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

2.1. Інституційна система забезпечення інформаційної безпеки України

Теоретичні основи та нормативно-правові засади інформаційної безпеки, розглянуті у першому розділі роботи, створюють необхідне підґрунтя для аналізу інституційної системи гарантування стійкості національного інформаційного простору. Перехід від аналізу концептуальних і правових засад до дослідження практичного функціонування інституційних механізмів є логічно необхідним кроком, оскільки саме інституції виступають операційним рівнем реалізації реалізації державної політики у галузі інформаційної безпеки та сприяючи практичному втіленню нормативно-правових приписів, стратегічних цілей та євроінтеграційних зобов’язань. Інституційна архітектура системи інформаційної безпеки України характеризується множинністю суб’єктів, розподілом повноважень між різними органами державної влади, необхідністю забезпечення ефективної координації та взаємодії як на національному рівні, так і з міжнародними партнерами, особливо з інституціями Європейського Союзу.

Проблематика інституційного питання інформаційної безпеки дедалі більше фокусує увагу значної кількості дослідників. В. Горбулін та О. Додонов проаналізували систему державних інституцій, наділених повноваженнями у сфері захисту національного інформаційного простору, та виявили проблеми координації їхньої діяльності [7, с. 156]. Їхні напрацювання стали основою для подальших досліджень інституційних дисфункцій у сфері національної безпеки. Д. Дубов досліджував інституційні механізми протидії гібридним загрозам та обґрунтував необхідність створення єдиного координаційного центру у сфері інформаційної безпеки [9, с. 89], що пізніше знайшло відображення у законодавчих ініціативах щодо формування Координаційного центру кібербезпеки. О. Золотар розглядала питання розподілу повноважень між різними органами влади у сфері кібербезпеки та захисту інформації [11, с. 201], акцентуючи на проблемах дублювання функцій та нечіткості розмежування відповідальності. Водночас динамічний характер інституційних трансформацій, створення нових органів та перерозподіл повноважень, особливо в умовах

воєнного стану, зумовлюють необхідність постійного оновлення аналізу національної інституційної архітектури, що відповідає за захист інформаційного простору України.

У системі органів, відповідальних за формування та реалізацію державної політики у сфері інформаційної безпеки, ключову координаційну роль виконує Рада національної безпеки і оборони України. Як консультативно-дорадчий орган при Президенті України, вона забезпечує узгодженість дій різних державних інституцій у питаннях національної безпеки, включно з безпекою інформаційного простору. Правові засади її діяльності, структура та компетенції закріплені в Конституції України та детально врегульовані Законом України «Про Раду національної безпеки і оборони України» [38]. Функціональне призначення РНБО полягає не у безпосередньому виконанні оперативних завдань, а у забезпеченні стратегічного планування, координації діяльності різних суб'єктів механізмів забезпечення національної безпеки та нагляду за виконанням прийнятих рішень. Це робить РНБО унікальною інституцією, здатною забезпечувати міжвідомчу координацію у такій складній та багатоаспектній сфері як інформаційна безпека.

Аналіз практики діяльності РНБО у напрямі захисту інформаційного простору демонструє про еволюцію підходів до розуміння ролі цього органу. Якщо до 2014 року РНБО епізодично розглядала питання інформаційної безпеки, переважно в контексті загальних питань національної безпеки, однак із початком збройної агресії Російської Федерації інформаційний вимір безпеки перетворився на один із пріоритетних напрямів діяльності Ради. Це виявилося у регулярному розгляді питань протидії інформаційним загрозам, прийнятті рішень щодо блокування діяльності інформаційних ресурсів, що загрожують національній безпеці, координації діяльності органів влади у протидії дезінформації. Однак критичний аналіз ефективності координаційної функції РНБО виявляє певні обмеження, зумовлені як об'єктивними факторами (складність координації діяльності численних суб'єктів з різними відомчими інтересами), так і суб'єктивними (недостатність ресурсного забезпечення апарату РНБО, обмежені можливості контролю за виконанням прийнятих

рішень).

Запуск у 2021 році Координаційного центру кібербезпеки при РНБО став одним із ключових рішень, спрямованих на посилення державної інституційної спроможності в галузі кіберзахисту. Створена структура виконує функції спеціалізованого робочого підрозділу РНБО, відповідального за координацію дій державних інституцій у реагуванні на кіберзагрози, узгодження політики та оперативного обміну інформацією у сфері кібербезпеки з метою координації діяльності суб'єктів забезпечення кібербезпеки, проведення оцінки стану кібербезпеки держави, підготовки пропозицій щодо державної політики у цій сфері. Значення цієї інституції виявилося особливо виразно в умовах повномасштабної російської агресії, коли Україна зіткнулася з безпрецедентною кількістю кібератак на критичну інфраструктуру, державні інформаційні системи, об'єкти енергетики та телекомунікацій. Координаційний центр забезпечив оперативну взаємодію між різними суб'єктами кібербезпеки, координував реагування на масштабні кіберінциденти, сприяв залученню міжнародної технічної допомоги. Водночас практика функціонування Центру виявила потребу у подальшому зміцненні його інституційної спроможності, насамперед через розширення штату, підвищення рівня технічної оснащеності, розвиток аналітичних можливостей.

Розгортання повномасштабної російської агресії докорінно трансформувало напрями та інтенсивність роботи РНБО у сфері захисту інформаційного простору. Рада перетворилася на оперативний центр прийняття критично важливих рішень щодо протидії інформаційним операціям противника, забезпечення безперервності функціонування об'єктів інформаційно-комунікаційної інфраструктури підвищеної важливості, узгодження стратегічних комунікацій держави на міжнародній арені. Рішення РНБО щодо блокування діяльності інформаційних ресурсів, пов'язаних з агресором, хоча і викликали дискусії у контексті необхідності поєднання вимог безпеки й дотримання принципів свободи слова, були визнані виправданими в умовах війни та відповідали міжнародним стандартам щодо можливих обмежень основоположних прав і свобод особи в ситуаціях, коли постають ризики для

національної безпеки. Це додатково засвідчує, що національна інституційна архітектура інформаційної безпеки має бути достатньо гнучкою для адаптації до різних безпекових контекстів, зберігаючи при цому базові принципи демократичного управління.

Державна служба спеціального зв'язку та захисту інформації України відіграє особливе місце в інституційній системі як центральну позицію серед органів виконавчої влади, відповідальних за розроблення та практичне втілення державної політики у сферах кіберзахисту, охорони державних інформаційних ресурсів, а також криптографічного й технічного забезпечення безпеки інформації. На відміну від РНБО, яка виконує координаційні функції, Держспецзв'язку є безпосереднім виконавцем, оператором критично важливих систем захисту інформації. Функціональний спектр діяльності Держспецзв'язку надзвичайно широкий і охоплює організацію захисту інформації у центральних органах влади, а також відповідає за стабільне функціонування урядової системи зв'язку, проведення сертифікації технічних засобів захисту інформації та нагляд за дотриманням установлених нормативних вимог у сфері інформаційної безпеки.

Особливої ваги діяльність Держспецзв'язку набула після початку повномасштабної російської агресії. Служба забезпечила безперервність забезпечення стабільної роботи ключових елементів національної інформаційно-комунікаційної інфраструктури в умовах масованих кібератак противника, координувала міжнародну технічну допомогу у галузі кіберзахисту виконувала оперативне реагування на кіберінциденти. Державний центр кіберзахисту, що функціонує у структурі Держспецзв'язку, відіграв ключову роль у відбитті кібератак на критичну інфраструктуру, державні інформаційні системи, об'єкти енергетики. Аналіз досвіду протидії кіберагресії виявив як сильні сторони інституційної моделі Держспецзв'язку (високий рівень технічної компетентності, розвинені міжнародні зв'язки, оперативність реагування), так і певні вразливості (обмеженість ресурсів у порівнянні з масштабом загроз, недостатня координація з іншими суб'єктами кібербезпеки, потреба у модернізації технічної інфраструктури).

Функціонування у структурі Держспецзв'язку національної системи реагування на комп'ютерні надзвичайні події України (CERT-UA) є показовим прикладом ефективного інституційного рішення, спрямованого на посилення національних можливостей у сфері кіберзахисту. CERT-UA здійснює моніторинг кіберзагроз, аналізує кіберінциденти, надає рекомендації щодо усунення вразливостей, координує реагування на масштабні кібератаки. Важливою особливістю діяльності CERT-UA є активна міжнародна співпраця з аналогічними командами реагування країн-партнерів, що дозволяє оперативно обмінюватися інформацією про нові загрози, отримувати технічну підтримку, долучатися до міжнародних тренувань і симуляційних заходів у сфері кіберзахисту. Проте масштаб та інтенсивність кіберзагроз, з якими стикається Україна, вимагають подальшого зміцнення спроможностей CERT-UA, розширення його людських та технічних ресурсів, поглиблення аналітичних можливостей.

Міністерство культури та інформаційної політики України посідає важливе місце в системі захисту інформаційного простору, завдяки формуванню та реалізації державної політики у сферах медіа, стратегічних комунікацій, протидії дезінформації. Створення цього міністерства у 2019 році стало відповіддю на усвідомлення критичної важливості стратегічних комунікацій та інформаційної політики як складової національної безпеки. На відміну від суто технічних орієнтованої Держспецзв'язку, МКІП зосереджується на контентних, комунікаційних аспектах інформаційної безпеки, що включає розвиток незалежних медіа, підвищення медіаграмотності населення, протидію протидії маніпулятивним інформаційним впливам та просування сприятливого міжнародного образу України.

У межах організаційної структури МКІП діє Центр стратегічних комунікацій та інформаційної безпеки, який відіграє провідну роль у моніторингу та аналізі дезінформаційних кампаній, проведенні фактчекінгу, розробці контрнаративів. Діяльність Центру охоплює систематичний моніторинг інформаційного простору з метою виявлення дезінформаційних меседжів, аналіз джерел та каналів поширення дезінформації, підготовку аналітичних матеріалів

для органів державної влади та громадськості, координацію з громадськими організаціями та медіа у сфері протидії дезінформації. Особливо важливою є діяльність Центру з документування російських інформаційних операцій проти України, що створює доказову базу для міжнародних майданчиків та судових процесів.

Критичний аналіз ефективності інституційної моделі МКІП у сфері інформаційної безпеки виявляє як досягнення, так і проблемні аспекти. До позитивних сторін належить системність підходу до стратегічних комунікацій, активна міжнародна співпраця, залучення громадянського суспільства та медіа до протидії маніпулятивних інформаційних впливів. Разом із тим залишається низка проблем, зумовлених браком ресурсів (фінансових, людських, технічних) у порівнянні з масштабом дезінформаційних кампаній противника, недостатньою координацією з іншими органами влади, що також займаються питаннями стратегічних комунікацій, потребою у розвитку аналітичних спроможностей для виявлення складних, багатошарових дезінформаційних операцій. Повномасштабна війна виявила критичну важливість ефективних стратегічних комунікацій як для підтримки внутрішньої стійкості суспільства, так і для забезпечення міжнародної підтримки України, що актуалізує потребу у подальшому зміцненні інституційної спроможності МКІП.

Служба безпеки України займає особливе місце в системі національної інформаційної безпеки, оскільки її діяльність зосереджена на контррозвідувальному вимірі захисту держави. Основні функції СБУ охоплюють нейтралізацію діяльності іноземних спецслужб в інформаційній сфері, охорону державної таємниці, протидію проявам кібершпигунства та боротьбу зі злочинами, що посягають на інформаційну безпеку держави. Її статус як спеціального правоохоронного органу визначає специфіку компетенцій, які включають ідентифікацію, документування та припинення роботи агентурних мереж, спрямованих на здобуття або викривлення інформації, а також розслідування правопорушень, пов’язаних із незаконними діями в інформаційному та кіберпросторі. Ці функції є критично важливими для забезпечення інформаційного суверенітету держави та протидії найбільш

небезпечним формам інформаційних загроз.

Реформування Служби безпеки України, розпочате після 2014 року та прискорене в умовах повномасштабної війни, вплинуло змінивши акценти в оцінюванні та забезпеченні інформаційної безпеки. Проведена реформа орієнтувала СБУ на виконання притаманних демократичним спецслужбам функцій – контррозвідувальний захист, протидію терористичним загрозам і охорону державного суверенітету. Це передбачало поступове відмовлення від низки повноважень, які не відповідають сучасним підходам до діяльності розвідувально-безпекових структур у країнах Європи.

У площині інформаційної безпеки така трансформація означала перехід від широкого контролю над інформаційним середовищем до цільового реагування на конкретні загрози, що походять від іноземних держав, розвідувальних структур та терористичних угруповань. Подібне фокусування узгоджується з європейськими стандартами чіткого розмежування функцій спецслужб і класичних правоохоронних органів. Водночас реалізація такого підходу потребує чіткої регламентації компетенцій СБУ, визначення меж її діяльності в інформаційній сфері та створення ефективних механізмів демократичного і парламентського контролю за діяльністю служби.

Огляд практичної роботи СБУ в царині кіберзахисту демонструє певну дихотомію між необхідністю ефективної протидії кіберзагрозам та потребою дотримання прав людини в цифровому просторі. З одного боку, СБУ володіє унікальними спроможностями для виявлення та нейтралізації складних кібероперацій іноземних спецслужб, розслідування кіберзлочинів, захисту критичної інфраструктури від цілеспрямованих атак. З іншого боку, діяльність спецслужби у кіберпросторі потребує чіткого правового регулювання, прозорих процедур та ефективного парламентського і судового контролю для запобігання можливим зловживанням. Європейська практика свідчить про необхідність балансу між забезпеченням ефективності спецслужб у протидії кіберзагрозам та захистом конституційних прав громадян, що залишається актуальним викликом для України в контексті євроінтеграції.

Питання узгодженості дій між різними інституціями, відповідальними за

захист інформаційного простору, належить до числа найбільш складних і чутливих в українському контексті. Множинність органів, які мають повноваження у сфері інформаційної безпеки, за відсутності чітких механізмів координації призводить до перетину повноважень, нераціонального розподілу ресурсів та виникнення прогалин у покритті певних сегментів загроз. Створення Координаційного центру кібербезпеки при РНБО було спробою вирішити цю проблему, принаймні у сфері кібербезпеки, однак практика засвідчує, що координаційні механізми потребують подальшого вдосконалення. Європейський досвід демонструє різні моделі координації у сфері інформаційної безпеки, від створення єдиного координаційного органу до розвитку горизонтальних механізмів міжвідомчої взаємодії, що може мати значний практичний потенціал для української держави.

Міжнародна співпраця, особливо з європейськими структурами, стала критично важливою складовою діяльності українських інституцій у сфері інформаційної безпеки. Ця співпраця набула різноманітних форм і включає обмін інформацією про загрози та інциденти, спільні навчання та тренінги, технічну допомогу, участь у європейських програмах та ініціативах. МКІП активно співпрацює з East StratCom Task Force Європейської служби зовнішніх дій, обмінюючись інформацією про дезінформаційні кампанії та координуючи зусилля з протидії російській пропаганді. Держспецзв'язку розвиває партнерство з Агентством Європейського Союзу з кібербезпеки (ENISA), національними центрами реагування на кіберінциденти держав-членів ЄС, що дозволяє оперативно реагувати на транснаціональні кіберзагрози. СБУ співпрацює з європейськими спецслужбами у протидії кібершпигунству та кіберзлочинності.

Повномасштабна російська агресія значно інтенсифікувала міжнародну співпрацю України у сфері інформаційної безпеки. Європейські партнери надали Україні значну технічну допомогу для захисту критичної інфраструктури від кібератак, поділилися експертизою з протидії дезінформації, підтримали розвиток українських спроможностей у сфері стратегічних комунікацій. Створено механізми оперативного обміну інформацією про кіберзагрози, розгорнуто спільні проєкти з підвищення кіберстійкості критичної

інфраструктури, запроваджено програми навчання українських фахівців з інформаційної безпеки у європейських центрах досконалості. Ця співпраця не лише посилила оперативні спроможності України, але й сприяла адаптації українських інституцій до європейських стандартів, процедур та культури роботи у сфері інформаційної безпеки.

Водночас аналіз міжнародної співпраці виявляє й певні обмеження та виклики. По-перше, асиметрія у спроможностях між українськими інституціями та їхніми європейськими партнерами іноді ускладнює повноцінну взаємодію та вимагає додаткових зусиль з підвищення інституційної спроможності української сторони. По-друге, різниця у правових рамках, процедурах, культурі роботи потребує значних зусиль для узгодження підходів та забезпечення сумісності систем. По-третє, надання міжнародної технічної допомоги іноді супроводжується певною залежністю від зовнішніх партнерів, що актуалізує питання розвитку власних національних спроможностей. По-четверте, координація міжнародної співпраці між різними українськими інституціями не завжди є оптимальною, що може спричиняти паралельне виконання однакових завдань різними структурами або прогалин у покритті певних напрямів.

Перспективи розвитку інституційної системи формування та реалізація державної політики у сфері захисту інформаційного простору України ґрунтуються на як внутрішніми потребами підвищення ефективності протидії загрозам, так і вимогами європейської інтеграції. До пріоритетних напрямів інституційного розвитку належать подальше зміцнення координаційних механізмів, чітке розмежування повноважень між різними суб’єктами, підвищення інституційної спроможності через розвиток людських ресурсів та технічної інфраструктури, посилення механізмів демократичного контролю та підзвітності, поглиблення інтеграції до європейських структур підтримання належного рівня захищеності національного інформаційного простору. Досвід протидії російській агресії продемонстрував як сильні сторони української інституційної моделі (гнучкість, здатність до швидкої адаптації, високий рівень мотивації), так і вразливості (обмеженість ресурсів, проблеми координації, недостатня аналітична спроможність), що має бути враховано у процесі

подальшого інституційного розвитку.

Таким чином, інституційна система стан та розвиток системи захисту національного інформаційного простору України визначаються множинністю суб'єктів з розподіленими повноваженнями, що створює як переваги (різноманітність підходів, спеціалізація функцій), так і виклики (проблеми координації, дублювання функцій, прогалини у покритті загроз). Ключові інституції – РНБО, Держспецзв'язку, МКІП, СБУ, Центр стратегічних комунікацій – виконують специфічні функції та мають власні сильні і слабкі сторони. Координація між органами влади залишається проблемним аспектом, який вимагає подальшої модернізації у зв'язку з розвитком як формальних координаційних механізмів, так і неформальної культури міжвідомчої співпраці. Міжнародна співпраця, особливо з європейськими структурами, стала критично важливою складовою забезпечення інформаційної безпеки України та каталізатором інституційних трансформацій у напрямі європейських стандартів. Досвід протидії російській агресії виявив необхідність подальшого зміцнення інституційної спроможності, що має стати пріоритетом державної політики у контексті євроінтеграції. Аналіз інституційної системи створює необхідне підґрунтя для розгляду конкретних викликів та загроз інформаційній безпеці України, що становитиме предмет дослідження наступного параграфа.

2.2. Сучасні виклики та загрози інформаційній безпеці України

Огляд функціонування національної інституційної архітектури у сфері захисту інформаційного простору, представлений у попередньому параграфі, створює необхідну основу для дослідження конкретних викликів та загроз, з якими стикається Україна в інформаційній сфері. Перехід від розгляду інституційних механізмів до характеристики загроз є логічно необхідним, оскільки саме розуміння природи, джерел та специфіки загроз визначає адекватність інституційних відповідей, ефективність застосовуваних інструментів протидії, напрями вдосконалення системи інформаційної безпеки. Ландшафт загроз інформаційній безпеці України характеризується

надзвичайною складністю, багатовимірністю та динамічністю, що зумовлено як глобальними трендами розвитку інформаційних технологій та трансформації медіапростору, так і специфікою безпекового контексту, в якому перебуває Україна, насамперед тривалою російською агресією з використанням широкого спектру гібридних інструментів.

Наукове осмислення сучасних загроз інформаційній безпеці України привертає увагу широкого кола дослідників. В. Горбулін комплексно проаналізував феномен гібридної війни та роль інформаційного компонента у стратегії російської агресії проти України [7, с. 234], що стало основою для розуміння системного характеру інформаційних загроз. Д. Дубов та М. Ожеван дослідили механізми російських інформаційних операцій, виявивши їхню багатошаровість, комплексність та координованість [9, с. 156]. Г. Почепцов розробив типологію інформаційних війн та проаналізував специфіку інформаційного протиборства у цифрову епоху [30, с. 89], акцентуючи на трансформації методів інформаційного впливу під впливом розвитку цифрових технологій. Зарубіжні дослідники, зокрема аналітики НАТО StratCom Centre of Excellence, документували російські дезінформаційні кампанії та виявляли закономірності їхньої організації [67, с. 67]. Водночас динамічний характер загроз, поява нових форм інформаційних атак, еволюція тактик противника вимагають постійного оновлення аналізу загроз інформаційній безпеці України.

Гібридні інформаційні впливи Російської Федерації проти України становлять найбільш комплексну та системну загрозу інформаційній безпеці держави. Концепція гібридної війни передбачає координоване використання широкого спектру інструментів впливу – військових, політичних, економічних, інформаційних – для досягнення стратегічних цілей без формального оголошення війни або з мінімізацією масштабу відкритого військового протиборства. В. Горбулін справедливо зазначає, що інформаційний компонент є невід’ємною складовою російської гібридної стратегії, що виявляється у систематичному використанні дезінформації, пропаганди, психологічних операцій для дестабілізації ситуації в країні-жертві агресії [7, с. 245]. Аналіз російської агресії проти України з 2014 року підтверджує центральну роль

інформаційного компонента на всіх етапах конфлікту – від підготовки до вторгнення через формування сприятливого інформаційного середовища до супроводу військових операцій інформаційними кампаніями та спроб легітимізації агресії на міжнародній арені.

Системний характер російських інформаційних операцій проти України виявляється у координації діяльності різних суб'єктів – державних медіа, підконтрольних кремлю інтернет-ресурсів, мереж ботів та тролів у соціальних мережах, окремих блогерів та лідерів думок, політичних акторів в Україні та за кордоном. Дослідження, проведені NATO StratCom COE, документують високий рівень координації між різними каналами поширення російської пропаганди, синхронізацію месседжів, використання єдиних наративів через різноманітні платформи [67, с. 78]. Це свідчить про існування централізованої системи управління інформаційними операціями, значних ресурсів, що виділяються на цю діяльність, та стратегічного планування інформаційних кампаній як інтегрованої частини загальної агресивної політики Російської Федерації.

Еволюція російських інформаційних операцій проти України демонструє адаптацію до змін в інформаційному середовищі та відповідей українських інституцій. Якщо на початковому етапі агресії у 2014 році російська пропаганда значною мірою спиралася на традиційні медіа та пряме мовлення російських телеканалів в Україні, то після обмеження їхньої діяльності акцент перейшов у площину функціонування цифрових сервісів, соціальних мереж та комунікаційних застосунків. Російські інформаційні операції стали більш складними, багатошаровими, такими, що використовують методи таргетованого впливу на різні цільові аудиторії з урахуванням їхніх психологічних особливостей, ціннісних орієнтацій, інформаційних уподобань. Використовуються технології мікротаргетингу, коли різні месседжі доставляються різним сегментам аудиторії через персоналізовані канали, що ускладнює виявлення та протидію таким операціям.

Тематичний спектр російської дезінформації проти України надзвичайно широкий і охоплює практично всі аспекти суспільного життя. Аналіз моніторингових даних Центру стратегічних комунікацій та інформаційної

безпеки виявляє кілька ключових наративів, що систематично просуваються російською пропагандою. По-перше, це наративи, спрямовані на делегітимацію української держави через заперечення її суверенітету, твердження про штучність української нації, дискредитацію органів державної влади. По-друге, наративи про внутрішню слабкість та дисфункціональність України, економічну кризу, соціальні проблеми, корупцію, спрямованих на розмивання суспільної довіри до національних інституцій та державної влади. По-третє, вердження про нібито контроль Заходу над українською державою, спроби представити українську владу як залежну чи підпорядковану зовнішнім центрам впливу, втрату суверенітету внаслідок євроінтеграції. По-четверте, наративи, спрямовані на розкол українського суспільства через розпалювання міжрегіональних, міжконфесійних, мовних протиріч.

Особливу увагу заслуговує аналіз трансформації російської пропаганди після початку повномасштабної війни у лютому 2022 року. Масована військова агресія супроводжувалася інтенсифікацією інформаційних операцій, спрямованих на деморалізацію українського суспільства, послаблення солідарності світової спільноти з Україною, легітимізацію агресії на внутрішній російській та міжнародній аренах. Російська пропаганда намагалася створити враження неминучості поразки України, перебільшувала російські військові успіхи, применшувала втрати російської армії, поширювала фейки про злочини українських військових, дезінформацію про внутрішню ситуацію в Україні. Водночас повномасштабна війна виявила певні межі ефективності російської інформаційної машини, оскільки реальність війни, особливо успішний опір українських військових та єдність українського суспільства, суперечили пропагандистським наративам про слабкість України та підривали довіру до російських джерел інформації.

Кіберзагрози становлять окрему категорію викликів інформаційній безпеці України, що характеризуються технічною складністю, потенційно катастрофічними наслідками та тісним зв’язком з традиційними формами агресії. Досвід України з протидії кібератакам є унікальним у світовому контексті за масштабом, інтенсивністю та різноманітністю загроз. За даними

Державної служби спеціального зв'язку та захисту інформації України, з початку повномасштабної війни Україна щоденно відбиває сотні кібератак різного рівня складності, спрямованих на критичну інфраструктуру, державні інформаційні системи, об'єкти енергетики, телекомунікацій, фінансового сектору. Це робить Україну своєрідним полігоном кібервійни, де відпрацьовуються нові методи кібератак та засоби протидії їм.

Типологія кіберзагроз, з якими стикається Україна, включає широкий спектр атак різного рівня складності та з різними цілями. DDoS-атаки (distributed denial of service) є найбільш масовими, хоча і відносно простими за технічним виконанням, їхня мета – перевантаження цільових систем запитами для припинення їхнього функціонування. Масовані DDoS-атаки часто використовуються як інструмент психологічного тиску, супроводу військових операцій, дестабілізації роботи критично важливих сервісів. Більш небезпечним явищем є кібератаки, що здійснюються за допомогою спеціально створеного шкідливого програмного забезпечення – від програм-вимагачів (ransomware) і троянів до різноманітних інструментів цифрового шпигунства. Окрему категорію становлять високотехнологічні цільові операції типу advanced persistent threats (APT), спрямовані на ураження об'єктів критичної інфраструктури. Такі атаки відрізняються ретельною та довготривалою підготовкою, використанням складних методів проникнення у комп'ютерні мережі, а також здатністю зловмисників залишатися непоміченими в інфікованих системах протягом тривалого часу.

Аналіз найбільш резонансних кіберінцидентів виявляє еволюцію тактик кіберагресії проти України. Кібератака NotPetya у червні 2017 року, яка завдала багатомільярдних збитків українській економіці та поширилася на комп'ютерні системи у багатьох країнах світу, продемонструвала вразливість ланцюгів постачання програмного забезпечення та потенційно глобальні наслідки кібератак. Неодноразові успішні кібератаки на енергетичну інфраструктуру України у 2015-2016 роках показали вразливість критичних систем та можливість використання кіберзброї для досягнення фізичних ефектів, таких як відключення електропостачання. Масовані кібератаки напередодні та на початку

повномасштабної війни у лютому 2022 року, спрямовані на державні інформаційні системи, телекомунікаційні мережі, фінансовий сектор, мали на меті дезорганізацію управління державою та паралізування її функціонування.

Атрибуція кібератак, тобто встановлення їхнього джерела та відповідальних за них акторів, є складним технічним та політичним завданням. Проте систематичний аналіз технічних характеристик атак, цільового спрямування, контексту їхнього здійснення дозволяє з високим ступенем ймовірності ідентифікувати російські державні структури та підконтрольні їм хакерські групи як основне джерело кіберзагроз для України. Міжнародні дослідження, зокрема компаній з кібербезпеки Microsoft, CrowdStrike, Mandiant, документують діяльність російських державних хакерських груп, таких як APT28 (Fancy Bear), APT29 (Cozy Bear), Sandworm, проти українських цілей. Координація кібератак з військовими операціями, політичними подіями, інформаційними кампаніями свідчить про інтеграцію кібероперацій у загальну стратегію російської агресії проти України.

Соціальні мережі як інструменти інформаційного впливу набули критично важливого значення у сучасному ландшафті загроз інформаційній безпеці. Трансформація медіаспоживання, коли значна частина населення, особливо молодше покоління, отримує інформацію переважно через соціальні мережі, а не традиційні медіа, робить ці платформи ключовим каналом інформаційного впливу. Водночас архітектура соціальних мереж, що базується на алгоритмічній курації контенту, персоналізації стрічки новин, вірусному поширенні контенту, створює нові вразливості для маніпулятивних впливів. Алгоритми соціальних мереж, налаштовані на максимізацію залученості користувачів, часто сприяють поширенню емоційно забарвленого, поляризуючого, сенсаційного контенту, включаючи дезінформацію, що отримує більше переглядів, коментарів, поширень порівняно з виваженою, фактичною інформацією.

Аналіз використання соціальних мереж для інформаційних операцій проти України виявляє кілька ключових тактик. По-перше, це створення та використання мереж фейкових акаунтів (ботів, тролів) для штучного посилення певних месседжів, створення враження масової підтримки певних ідей, атак на

опонентів через координовані кампанії негативних коментарів. Дослідження виявляють існування російських «фабрик тролів» – організованих структур, що систематично створюють та поширюють дезінформацію у соціальних мережах. По-друге, це використання автентичних акаунтів через їхнє зламування, купівлю або маніпулювання власниками для поширення потрібного контенту. По-третє, це експлуатація алгоритмічних особливостей соціальних мереж для максимізації охоплення дезінформаційного контенту через використання емоційно забарвлених заголовків, провокативних зображень, маніпуляцію механізмами рекомендацій.

Месенджери як окрема категорія комунікаційних платформ також стали важливим інструментом інформаційного впливу. Telegram, що набув надзвичайно широкого поширення в Україні, насамперед у контексті розгортання широкомасштабних бойових дій, характеризується специфічними особливостями, що створюють як можливості, так і ризики для інформаційної безпеки. З одного боку, Telegram забезпечує оперативне поширення інформації, можливість прямої комунікації влади з громадянами, координацію волонтерських ініціатив, що виявилося критично важливим в умовах війни. З іншого боку, відносна анонімність, обмежені можливості модерації контенту, легкість можливість безперешкодно запускати й масштабувати канали перетворює Telegram зручною платформою для дезінформації, російської пропаганди, психологічних операцій. Аналітики фіксують існування численних Telegram-каналів, що систематично поширюють російські наративи, дезінформацію про ситуацію на фронті, фейки про внутрішню ситуацію в Україні, при цьому часто маскуючись під проукраїнські або нейтральні джерела інформації.

Залучення інструментів штучного інтелекту для генерування та масового розповсюдження маніпулятивного контенту стає відносно новою, але швидко зростаючою загрозою. Технології синтезу зображень, відео, аудіо на основі штучного інтелекту (так звані дипфейки) дозволяють створювати надзвичайно реалістичний контент, що демонструє події, які насправді не відбувалися, або приписує публічним особам висловлювання, яких вони не робили. Хоча поки що

використання дипфейків у дезінформаційних кампаніях проти України залишається обмеженим, технологічний прогрес у цьому напрямі формує серйозні ризики для майбутнього. Великі мовні моделі та інші технології генеративного штучного інтелекту можуть використовуватися для масового виробництва дезінформаційного контенту, персоналізації месседжів для різних цільових аудиторій, автоматизації дезінформаційних кампаній, що кратно збільшує масштаб та ефективність інформаційних операцій.

Психологічні операції як складова інформаційної агресії проти України спрямовані на цілеспрямований вплив на емоційний стан, свідомість, поведінку цільових аудиторій. На відміну від класичної дезінформації, що фокусується на поширенні неправдивих фактів, психологічні операції можуть використовувати і реальну інформацію, подаючи її у спотвореному контексті, акцентуючи на певних аспектах, замовчуючи інші, для досягнення необхідного психологічного ефекту. Аналіз російських психологічних операцій проти України виявляє кілька типових тактик. Використання шокуючого, травматичного контенту для створення атмосфери страху, паніки, безнадійності. Поширення чуток, неперевірених повідомлень про загрози для посилення тривожності та невизначеності. Цілеспрямоване створення відчуття втоми від війни, безперспективності опору для підриву мотивації до боротьби. Розпалювання внутрішніх конфліктів, протиставлення різних соціальних груп для дестабілізації суспільства.

Вразливість різних сегментів українського суспільства до інформаційних впливів є нерівномірною та визначається комплексом факторів, включаючи вік, освіту, географічне розташування, мовні уподобання, джерела отримання інформації. Дослідження медіаграмотності в Україні виявляють, що найбільш вразливими до дезінформації є люди старшого віку, які отримують інформацію переважно з телебачення, жителі прикордонних регіонів з історично інтенсивнішими зв’язками з Росією, особи з нижчим рівнем освіти та критичного мислення. Водночас повномасштабна війна суттєво змінила інформаційний ландшафт та сприйнятливість до російської пропаганди, оскільки безпосередній досвід війни, втрати близьких, руйнування міст російськими військами створили

потужний імунітет до російських наративів у більшості населення України. Це не означає повного зникнення загрози, оскільки російська пропаганда адаптується, шукаючи нові вразливості, використовуючи більш складні тактики впливу.

Економічні наслідки інформаційних загроз для України є значними, хоча і складно піддаються точній кількісній оцінці. Прямі економічні втрати від кібератак, зокрема від інцидентів на кшталт NotPetya, оцінюються у мільярди доларів. Непрямі втрати через підрив довіри до української економіки, відлякування інвесторів, додаткові витрати на забезпечення інформаційної безпеки є ще більшими. Дезінформаційні кампанії, спрямовані на дискредитацію України на міжнародній арені, ускладнюють залучення міжнародної підтримки, інвестицій, здатні позначатися на процесі ухвалення рішень іноземних партнерів щодо співпраці з Україною. Водночас інвестиції у зміцнення інформаційної безпеки, хоча і потребують значних ресурсів, є необхідними витратами, що забезпечують довгострокову стійкість держави та економіки.

Міжнародний вимір прояву сучасних викликів для національної інформаційної безпеки України полягає у тому, що російські інформаційні операції не обмежуються територією України, а поширюються на країни-партнери, міжнародні організації, глобальний інформаційний простір. Дезінформаційні кампанії, спрямовані на дискредитацію України, поширення неправдивих наративів про причини та перебіг війни, створення альтернативної реальності активно ведуться у західних країнах, що може коригувати підходи іноземних урядів до ухвалення рішень та міжнародних організацій щодо підтримки України. Російська пропаганда експлуатує існуючі розколи у західних суспільствах, посилює поляризацію, підживлює антиукраїнські настрої, що створює додаткові виклики для України у забезпеченні міжнародної підтримки. Це актуалізує необхідність не лише внутрішньої протидії дезінформації, але й активних стратегічних комунікацій на міжнародній арені, співпраці з партнерами у виявленні та спростуванні російської пропаганди.

Таким чином, актуальний спектр ризиків і небезпек, що постають перед інформаційною безпекою України характеризуються системністю,

комплексністю, багатовимірністю та динамічністю. Гібридні інформаційні впливи Російської Федерації є найбільш масштабною та організованою загрозою, що включає координоване використання дезінформації, пропаганди, психологічних операцій через різноманітні канали та платформи. Кіберзагрози становлять окрему категорію викликів, що характеризуються технічною складністю, потенційно катастрофічними наслідками та тісним зв'язком з традиційними формами агресії. Соціальні мережі та месенджери перетворилися на ключові інструменти інформаційного впливу, що зумовлює необхідність формування оновлених стратегій і механізмів протидії дезінформації з урахуванням специфіки цих платформ. Використання технологій штучного інтелекту, хоча і залишається поки обмеженим, створює серйозні ризики для майбутнього. Повномасштабна війна інтенсифікувала всі категорії загроз, водночас виявивши як вразливості, так і сильні сторони системи захисту національного інформаційного простору України. Практика протидії цим загрозам є унікальним у світовому контексті та може бути корисним для європейських партнерів, що створює підґрунтя для аналізу європейського досвіду протидії дезінформації та можливостей взаємного навчання, що становитиме предмет розгляду наступного параграфа.

2.3. Європейський досвід протидії дезінформації та забезпечення інформаційної стійкості

Аналіз викликів та загроз інформаційній безпеці України, здійснений у попередньому параграфі, логічно підводить до необхідності вивчення міжнародного, зокрема європейського, досвіду протидії подібним загрозам. Перехід від характеристики загроз до розгляду механізмів протидії є важливим з точки зору виявлення ефективних практик, інструментів та підходів, що можуть бути адаптовані до українського контексту в процесі європейської інтеграції. Європейський Союз, стикаючись з власними викликами у сфері інформаційної безпеки, насамперед з російськими дезінформаційними кампаніями, спрямованими на підрив єдності ЄС, втручання у виборчі процеси,

дестабілізацію демократичних інституцій, розробив комплексну систему протидії дезінформації та забезпечення інформаційної стійкості. Ця система базується на поєднанні регуляторних, технологічних, освітніх та комунікаційних інструментів, відображає специфічні європейські цінності та підходи до балансу між безпекою та свободою інформації.

Проблематика європейського досвіду протидії дезінформації привертає увагу як європейських, так і українських дослідників. Аналітики East StratCom Task Force систематично документують російські дезінформаційні кампанії проти країн ЄС та країн Східного партнерства, виявляють закономірності та тактики цих операцій [61, с. 45]. Європейська комісія у своїх звітах аналізує ефективність різних інструментів протидії дезінформації, оцінює виконання платформами своїх зобов'язань у цій сфері [57, с. 89]. Українські дослідники, зокрема М. Ожеван та Д. Дубов, розглядають можливості імплементації європейського досвіду в українську практику, враховуючи специфіку національного контексту [24, с. 123]. Науковці акцентують на важливості адаптації, а не механічного копіювання європейських практик, оскільки інтенсивність та характер загроз, з якими стикається Україна, у багатьох аспектах відрізняються від європейського досвіду. Водночас динамічний розвиток європейської політики у сфері протидії дезінформації, прийняття нових регуляторних актів, еволюція підходів вимагають постійного моніторингу та аналізу європейського досвіду.

Метою цього параграфа є систематичний аналіз європейського досвіду протидії дезінформації та забезпечення інформаційної стійкості, характеристика ключових механізмів та інструментів Європейського Союзу у цій сфері, оцінка їхньої ефективності та обмежень, а також виявлення можливостей імплементації цих механізмів в українську практику з урахуванням національної специфіки та євроінтеграційних зобов'язань. Особлива увага приділяється аналізу діяльності East StratCom Task Force, проєкту EU vs Disinfo, Digital Services Act, Code of Practice on Disinformation та інших європейських ініціатив у сфері інформаційної безпеки.

East StratCom Task Force є одним із найбільш помітних та ефективних

інструментів Європейського Союзу у протидії дезінформації, особливо російській пропаганді. Створена у 2015 році у структурі Європейської служби зовнішніх дій як відповідь на активізацію російських інформаційних кампаній після анексії Криму та початку війни на Донбасі, Task Force спочатку мала обмежений мандат та ресурси, проте поступово розширила свою діяльність та перетворилася на важливий елемент європейської системи протидії дезінформації. Функціональне призначення East StratCom полягає не у цензуруванні або блокуванні контенту, а у моніторингу дезінформаційних кампаній, їхньому аналізі, публічному викритті та спростуванні, що відповідає демократичним цінностям ЄС та принципу свободи слова.

Аналіз методології роботи East StratCom Task Force виявляє кілька ключових елементів їхнього підходу. По-перше, це систематичний моніторинг широкого спектру джерел інформації у країнах ЄС та Східного партнерства для раннього виявлення дезінформаційних наративів. По-друге, це верифікація інформації через перевірку фактів, консультації з експертами, аналіз первинних джерел для встановлення відповідності або невідповідності реальності. По-третє, це публічне викриття виявленої дезінформації через веб-платформу EU vs Disinfo, соціальні мережі, співпрацю з медіа. По-четверте, це аналіз закономірностей дезінформаційних кампаній, виявлення повторюваних наративів, тактик, джерел для формування системного розуміння проблеми. Така методологія дозволяє не лише реагувати на конкретні випадки дезінформації, але й виявляти стратегічні патерни інформаційних операцій.

EU vs Disinfo як публічна база даних викритої дезінформації є унікальним ресурсом, що документує тисячі випадків російської пропаганди та дезінформації. Станом на 2024 рік база містить понад 15000 задокументованих кейсів дезінформації, що дозволяє аналізувати динаміку, тематику, географічну спрямованість російських інформаційних операцій. Критичний аналіз ефективності EU vs Disinfo виявляє як сильні сторони, так і певні обмеження цього інструменту. До переваг належить створення достовірної доказової бази дезінформаційних кампаній, підвищення обізнаності журналістів та громадськості про тактики дезінформації, надання матеріалів для

журналістських розслідувань та наукових досліджень. Водночас існують обмеження, пов’язані з тим, що спростування дезінформації часто охоплює значно меншу аудиторію, ніж сама дезінформація, затримка між появою фейку та його спростуванням дозволяє дезінформації поширитися, фокус на російській дезінформації може залишати поза увагою інші джерела маніпулятивного контенту.

Досвід співпраці України з East StratCom Task Force є позитивним прикладом глобальної співпраці, спрямованої на боротьбу з маніпулятивними інформаційними впливами. Україна як країна, що стикається з найбільш інтенсивними російськими інформаційними операціями, є важливим партнером Task Force, надаючи інформацію про виявлені дезінформаційні кампанії, ділячись досвідом протидії, отримуючи аналітичну підтримку та методологічну допомогу. Центр стратегічних комунікацій та інформаційної безпеки України систематично взаємодіє з East StratCom, що дозволяє координувати зусилля, уникати дублювання, забезпечувати комплексність протидії дезінформації. Водночас потенціал цієї співпраці може бути поглиблений через більш інтенсивний обмін даними, спільні аналітичні проєкти, координацію стратегічних комунікацій на міжнародній арені.

Code of Practice on Disinformation є прикладом європейського підходу до саморегулювання цифрових платформ у сфері протидії дезінформації. Вперше прийнятий у 2018 році та оновлений у 2022 році (Code of Practice on Disinformation 2022), цей документ встановлює добровільні зобов’язання великих онлайн-платформ щодо боротьби з дезінформацією на своїх сервісах. Підписантами Кодексу є провідні технологічні компанії, включаючи Meta (Facebook, Instagram), Google (YouTube), Twitter (X), TikTok, Microsoft та інші, що означає охоплення більшості популярних онлайн-платформ. Філософія Кодексу базується на ідеї, що платформи мають брати на себе відповідальність за контент, що поширюється через їхні сервіси, при цьому зберігаючи свободу слова та уникаючи цензури.

Аналіз змісту Кодексу практик щодо дезінформації виявляє широкий спектр зобов’язань платформ. По-перше, це забезпечення прозорості політичної

реклами через маркування політичних оголошень, розкриття інформації про їхніх замовників, обмеження таргетування політичної реклами. По-друге, це боротьба з фейковими акаунтами та ботами через виявлення та видалення автоматизованих акаунтів, що поширюють дезінформацію, верифікацію автентичності акаунтів. По-третє, це зменшення економічних стимулів для поширення дезінформації через обмеження можливостей монетизації контенту, що містить дезінформацію, перекриття фінансування сайтів, що систематично поширюють фейки. По-четверте, це підвищення медіаграмотності користувачів через надання інструментів для оцінки достовірності інформації, інформування про факт-чекінгові ресурси. По-п’яте, це співпраця з фактчекерами та дослідниками через надання доступу до даних для аналізу, підтримку незалежних організацій з перевірки фактів.

Критична оцінка ефективності Кодексу практик виявляє як позитивні результати, так і значні обмеження. До досягнень можна віднести створення рамки для відповідальності платформ, стимулювання розвитку внутрішніх систем модерації контенту, посилення відкритості та підзвітності у сфері політичної агітації, а також скорочення фінансових мотивацій, що живлять індустрію дезінформаційних кампаній. Водночас існують серйозні проблеми, пов’язані з добровільним характером зобов’язань, що дозволяє платформам самостійно визначати рівень та способи їхнього виконання, недостатньою прозорістю та незалежністю механізмів оцінки виконання зобов’язань, різним рівнем імплементації Кодексу різними платформами, обмеженими санкціями за невиконання зобов’язань. Європейська комісія у своїх оціночних звітах неодноразово вказувала на недостатність зусиль деяких платформ та необхідність посилення механізмів контролю та відповідальності [57, с. 112].

Digital Services Act, прийнятий Європейським Союзом у 2022 році та набравший чинності поетапно протягом 2023-2024 років, є радикально новим регуляторним підходом до управління цифровим простором, що включає й питання протидії дезінформації. На відміну від добровільного Кодексу практик, DSA встановлює обов’язкові правові норми для цифрових платформ, недотримання яких тягне за собою значні фінансові санкції. Філософія DSA

полягає у формуванні цифрового середовища, яке є безпечним, відкритим і підконтрольним суспільству, та у якому гарантується дотримання прав і свобод користувачів, обмежується поширення незаконного та шкідливого контенту, забезпечується прозорість алгоритмів та бізнес-практик платформ. Це відображає еволюцію європейського підходу від м'якого регулювання через саморегулювання до жорсткішої правової рамки з чіткими вимогами та санкціями.

Аналіз положень DSA, релевантних для протидії дезінформації, виявляє кілька ключових елементів. По-перше, серед ключових вимог — обов'язок дуже великих онлайн-платформ (Very Large Online Platforms, VLOP) щороку здійснювати комплексний аудит системних ризиків, зокрема тих, що пов'язані з поширенням дезінформаційного контенту та вживати адекватних заходів для їхнього мітигації. По-друге, це вимоги прозорості алгоритмічних систем рекомендацій, що має дозволити зрозуміти, як платформи визначають, який контент показувати користувачам, та виявити потенційні механізми посилення дезінформації. По-третє, це надання користувачам права оскаржувати рішення платформ про видалення контенту або блокування акаунтів, що забезпечує баланс між протидією шкідливому контенту та захистом свободи слова. По-четверте, це механізми нагляду та контролю з боку національних регуляторів та Європейської комісії, включаючи можливість проведення аудитів платформ, запитів інформації, накладення санкцій за порушення.

Імплементація DSA на практиці стикається з численними викликами. Визначення того, що саме становить системний ризик дезінформації, як його вимірювати, які заходи є адекватними для мітигації, залишається складним питанням, що потребує розробки методологій та стандартів. Забезпечення прозорості алгоритмів без розкриття комерційних таємниць платформ вимагає балансу між різними інтересами. Створення ефективних механізмів нагляду та контролю потребує значних ресурсів та технічної експертизи з боку регуляторів. Застосування санкцій до глобальних технологічних гігантів може стикатися з політичним та економічним тиском. Водночас сам факт існування DSA як обов'язкової правової рамки створює значно сильніші стимули для платформ

серйозно ставитися до своїх зобов'язань у сфері протидії дезінформації, ніж попередні добровільні підходи.

Механізми підвищення медіаграмотності становить один із ключових елементів підходу Європейського Союзу до зміцнення власної інформаційної стійкості. Європейський Союз визнає, що технологічні та регуляторні рішення самі по собі недостатні для протидії дезінформації, якщо громадяни не мають навичок критичного аналізу інформації, розпізнавання маніпулятивних технік, перевірки джерел. Медіаграмотність розглядається як ключова компетентність сучасного громадянина, що дозволяє орієнтуватися у складному інформаційному середовищі, захищатися від маніпуляцій, робити поінформовані рішення. Європейські програми з підвищення медіаграмотності охоплюють різні цільові аудиторії – від школярів до дорослих, від журналістів до педагогів, та використовують різноманітні формати – від шкільних навчальних програм до онлайн-курсів, від медіакампаній до тренінгів для професіоналів.

Аналіз європейського досвіду підвищення медіаграмотності виявляє кілька ефективних практик. Інтеграція медіаграмотності у шкільні навчальні програми як обов'язкової складової освіти сприяє цілісному й послідовному розвитку здатності до критичного аналізу інформації та усвідомленого сприйняття медіаконтенту у молодого покоління. Підтримка незалежних організацій громадянського суспільства, що працюють у сфері медіаграмотності, через гранти та програми фінансування дозволяє масштабувати діяльність та охоплювати різноманітні цільові групи. Розробка та поширення навчальних матеріалів, методологій, інструментів для освітян та тренерів забезпечує якість та стандартизацію програм медіаграмотності. Проведення медіакампаній, спрямованих на підвищення обізнаності про дезінформацію та способи її розпізнавання, охоплює широку аудиторію та створює суспільний дискурс навколо цієї проблеми.

Факт-чекінг як інструмент протидії дезінформації набув значного розвитку в Європейському Союзі та отримує підтримку як з боку інституцій ЄС, так і цифрових платформ. Факт-чекінгові організації здійснюють систематичну перевірку публічних висловлювань політиків, медійних повідомлень, вірусного

контенту у соціальних мережах, спростовують неправдиві твердження, надають контекст та роз'яснення. Європейська модель факт-чекінгу базується на принципах незалежності від політичних та комерційних інтересів, прозорості методології, дотримання професійних стандартів, що гарантується через членство у міжнародних мережах факт-чекерів, таких як International Fact-Checking Network. Платформи, згідно з Code of Practice on Disinformation та Digital Services Act, зобов'язані співпрацювати з факт-чекерами, надаючи їм доступ до даних, підтримуючи їхню діяльність, враховуючи їхні висновки при модерації контенту.

Водночас критичний аналіз ефективності факт-чекінгу виявляє певні обмеження цього інструменту. По-перше, факт-чекінг є реактивним інструментом, що спростовує дезінформацію вже після її появи, тоді як дезінформація часто поширюється швидше, ніж її спростування. По-друге, спростування часто не досягає тієї самої аудиторії, що була експонована до дезінформації, особливо якщо люди споживають інформацію у закритих спільнотах або ехо-камерах. По-третє, існує феномен бумеранг-ефекту, коли спростування дезінформації парадоксально може посилювати віру в неї у людей з уже сформованими переконаннями. По-четверте, факт-чекінг вимагає значних ресурсів та не може охопити весь обсяг потенційно дезінформаційного контенту. Ці обмеження не означають безперспективності факт-чекінгу, але вказують на необхідність його поєднання з іншими інструментами протидії дезінформації.

Можливості імплементації європейського досвіду в українську практику потребують ретельного аналізу з урахуванням як спільних рис, так і відмінностей між європейським та українським контекстами. Спільним є визнання серйозності загрози дезінформації, необхідності комплексного підходу до протидії, важливості балансу між безпекою та свободою слова, цінності міжнародної співпраці. Водночас існують значні відмінності. Україна стикається з набагато більш інтенсивними та агресивними дезінформаційними кампаніями, ніж більшість країн ЄС, оскільки є безпосередньою жертвою російської військової агресії, складовою якої є інформаційна війна. Україна перебуває у стані війни, що створює специфічний контекст для балансу між безпекою та свободою

інформації, дозволяючи певні обмеження, що були б неприйнятними у мирний час. Україна має менші ресурси для інвестування у протидію дезінформації порівняно з Європейським Союзом, що вимагає пріоритизації та фокусування на найбільш ефективних інструментах.

Аналіз конкретних напрямів можливої імплементації європейського досвіду виявляє кілька пріоритетних сфер. По-перше, це розвиток інституційної співпраці між Україною та європейськими структурами, насамперед поглиблення партнерства з East StratCom Task Force, участь у європейських мережах з протидії дезінформації, обмін найкращими практиками та експертизою. По-друге, це адаптація регуляторних підходів ЄС до українського законодавства, зокрема імплементація принципів DSA щодо відповідальності цифрових платформ, прозорості алгоритмів, захисту прав користувачів. Це не означає механічного копіювання європейського законодавства, а вимагає його адаптації до українського правового контексту та безпекових потреб. По-третє, це розвиток системи медіаграмотності через інтеграцію у шкільні програми, підтримку громадських організацій, створення навчальних ресурсів, що може спиратися на європейські методології та матеріали. По-четверте, це зміцнення екосистеми факт-чекінгу через підтримку незалежних організацій, розвиток професійних стандартів, інтеграцію з міжнародними мережами факт-чекерів.

Виклики імплементації європейського досвіду в Україні пов’язані з кількома факторами. Обмеженість ресурсів вимагає пріоритизації та фокусування на найбільш критичних напрямах, що може означати відмову від деяких менш пріоритетних європейських практик. Воєнна реальність обумовлює необхідність творчого переосмислення та пристосування європейських моделей до українських умов, розроблених для мирного часу, до реалій збройного конфлікту, що може означати більш жорсткі обмеження у певних сферах. Різниця у рівні розвитку цифрової інфраструктури та медіаграмотності між Україною та країнами ЄС вимагає врахування цього розриву при плануванні імплементації. Необхідність балансування між адаптацією до європейських стандартів та збереженням ефективних власних напрацювань у протидії дезінформації, оскільки український досвід у деяких аспектах є більш передовим

через інтенсивність загроз.

Синергія між українським та європейським досвідом у протидії дезінформації може бути взаємовигідною. Україна може навчитися у Європи регуляторним підходам, розробці системних стратегій медіаграмотності, механізмам саморегулювання платформ, методологіям оцінки ефективності заходів. Водночас Європа може вивчати український досвід оперативного реагування на масштабні дезінформаційні кампанії, координації різних інструментів протидії в умовах кризи, мобілізації громадянського суспільства для боротьби з дезінформацією, інноваційних підходів до стратегічних комунікацій. Повномасштабна війна перетворила Україну на своєрідну лабораторію протидії дезінформації, де в екстремальних умовах тестуються різні підходи, що може бути цінним для підготовки європейських країн до можливих майбутніх викликів.

Перспективи розвитку співпраці України та ЄС у сфері протидії дезінформації визначаються як євроінтеграційними процесами, так і спільним усвідомленням загроз. Надання Україні статусу кандидата на вступ до ЄС створює додаткові стимули та механізми для поглиблення співпраці, імплементації європейських стандартів, інтеграції до європейських систем протидії дезінформації. Спільний досвід протистояння російській дезінформаційній агресії створює основу для солідарності та взаємопідтримки. Разом із тим ефективне використання цього потенціалу можливе лише за умови послідовної та координованої діяльності відповідних українських і європейських структур, виділення достатніх ресурсів, політичної волі до поглиблення співпраці, готовності вчитися один у одного та адаптувати найкращі практики до власних контекстів.

Таким чином, європейський досвід протидії дезінформації та забезпечення інформаційної стійкості представляє собою комплексну систему регуляторних, технологічних, освітніх та комунікаційних інструментів, що базується на демократичних цінностях та принципі балансу між безпекою та свободою інформації. Ключові механізми ЄС, такі як East StratCom Task Force, EU vs Disinfo, Code of Practice on Disinformation, Digital Services Act, програми

медіаграмотності та підтримки факт-чекінгу, демонструють як досягнення, так і певні обмеження у протидії складним та динамічним загрозам дезінформації. Можливості імплементації європейського досвіду в українську практику є значними, особливо в контексті європейської інтеграції, проте вимагають адаптації до специфіки національного контексту, врахування інтенсивності загроз та обмеженості ресурсів. Синергія між українським та європейським досвідом може бути взаємовигідною та посилювати спроможності обох сторін у протидії спільним викликам інформаційній безпеці. Аналіз європейського досвіду завершує інституційно-аналітичне дослідження реального стану справ у сфері інформаційної безпеки України та створює основу для формулювання висновків щодо другого розділу роботи.

Висновки до розділу 2

Другий розділ роботи було присвячено інституційно-аналітичному дослідженню нинішньої конфігурації національної системи інформаційної безпеки, що логічно продовжує теоретико-методологічний аналіз, здійснений у першому розділі, та переводить дослідження на рівень фактичного функціонування інституційної моделі забезпечення інформаційної безпеки. Аналіз охопив три взаємопов’язаних аспекти: сукупність інституцій та їх взаємозв’язків, що формують механізми забезпечення інформаційної безпеки, характеристику сучасних викликів та загроз, а також вивчення європейського досвіду протидії дезінформації з точки зору можливостей його імплементації в українську практику.

Дослідження інституційної системи виявило її багатосуб’єктний характер з розподіленими повноваженнями між різними органами державної влади, що створює як переваги у вигляді спеціалізації функцій, так і виклики, пов’язані з координацією діяльності. Ключові інституції – Рада національної безпеки і оборони України, Державна служба спеціального зв’язку та захисту інформації, Міністерство культури та інформаційної політики, Служба безпеки України – виконують специфічні функції та демонструють різний рівень інституційної

спроможності. Створення Координаційного центру кібербезпеки при РНБО стало важливим кроком у посиленні координації, проте практика його функціонування засвідчує необхідність подальшого зміцнення. Повномасштабна війна виявила як сильні сторони української інституційної моделі, зокрема здатність до швидкої адаптації та оперативного реагування, так і вразливості, насамперед проблеми міжвідомчої координації та обмеженість ресурсів. Міжнародна співпраця, особливо з європейськими структурами, перетворилася на критично важливу складову функціонування системи інформаційної безпеки та каталізатор інституційних трансформацій.

Аналіз сучасних викликів та загроз підтвердив їхній системний, комплексний та динамічний характер. Гібридні інформаційні впливи Російської Федерації становлять найбільш масштабну та організовану загрозу, яке вирізняється скоординованою взаємодією різних платформ і механізмів розповсюдження маніпулятивного контенту, адаптацією тактик до змін в інформаційному середовищі, багатовимірністю наративів. Кіберзагрози виявилися тісно інтегрованими з традиційними формами агресії, при цьому Україна стикається з безпрецедентною інтенсивністю кібератак, що робить її унікальним полігоном кібервійни. Соціальні мережі та месенджери перетворилися на ключові канали інформаційного впливу, що вимагає розробки нових підходів до протидії з урахуванням специфіки цих платформ. Досвід повномасштабної війни продемонстрував як еволюцію загроз, так і формування певного імунітету українського суспільства до російської пропаганди.

Узагальнення європейського досвіду протидії дезінформації виявило комплексну систему регуляторних, технологічних, освітніх та комунікаційних інструментів, що базується на демократичних цінностях та принципі балансу між безпекою та свободою інформації. Ключові європейські механізми, зокрема East StratCom Task Force, Code of Practice on Disinformation, Digital Services Act, демонструють як ефективність у певних аспектах, так і обмеження, зумовлені складністю та динамічністю загроз дезінформації. Можливості імплементації європейського досвіду в українську практику є значними, передусім у зв’язку з активізацією євроінтеграційного поступу України, проте вимагають адаптації до

специфіки національного контексту, зокрема до інтенсивності загроз в умовах війни та обмеженості ресурсів. Виявлено потенціал для взаємовигідного обміну досвідом, оскільки Україна може навчитися у Європи регуляторним підходам та системним стратегіям, тоді як європейські партнери можуть вивчати український досвід оперативного реагування на масштабні інформаційні кампанії.

Узагальнення результатів другого розділу засвідчує комплексний і багатоаспектний характер викликів, пов’язаних із організацією захисту інформаційного простору України в умовах європейської інтеграції та збройної агресії. Ефективна протидія сучасним загрозам потребує не лише зміцнення інституційної спроможності та вдосконалення координаційних механізмів на національному рівні, але й поглиблення міжнародної співпраці, адаптації європейських стандартів та інструментів, розвитку власних інноваційних підходів з урахуванням унікального досвіду протистояння гібридній агресії.

РОЗДІЛ 3. НАПРЯМИ ТРАНСФОРМАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В КОНТЕКСТІ ЄВРОПЕЙСЬКОЇ ІНТЕГРАЦІЇ

3.1. Європейська інтеграція як чинник трансформації системи інформаційної безпеки України

Аналіз сучасного стану інформаційної безпеки України, здійснений у другому розділі роботи, виявив як досягнення у протидії інформаційним загрозам, так і численні виклики, що потребують системного реформування національної системи. Перехід від аналітичного дослідження існуючого стану до визначення напрямів трансформації є логічно необхідним кроком, оскільки розуміння проблем має трансформуватися у стратегію їхнього вирішення. Європейська інтеграція України, що набула нового імпульсу після офіційного визнання України країною-кандидатом на вступ до Європейського Союзу влітку 2022 року, виступає не просто зовнішнім контекстом реформ, а потужним каталізатором та орієнтиром трансформації системи інформаційної безпеки. Євроінтеграційний вектор створює одночасно зобов'язання щодо адаптації до європейських стандартів, можливості для залучення технічної допомоги та експертизи, стимули для інституційного розвитку та критерії оцінювання прогресу реформ.

Концептуальне розуміння європейської інтеграції як чинника трансформації вимагає виходу за межі вузького трактування цього процесу як простої імплементації законодавства Європейського Союзу. Європейська інтеграція є комплексним процесом адаптації політичних, економічних, соціальних, правових систем держави до стандартів, цінностей, процедур Європейського Союзу. У сфері інформаційної безпеки це означає не лише гармонізацію законодавства, але й трансформацію інституційної культури, зміну підходів до балансу між безпекою та свободою інформації, розвиток нових компетентностей, інтеграцію до європейських мереж співпраці, адаптацію технічних систем до європейських стандартів. Така багатовимірність трансформації створює як можливості для якісного стрибка у розвитку системи інформаційної безпеки, так і ризики поверхневої, формальної адаптації без глибинних змін.

Гармонізація національної політики інформаційної безпеки з правовими рамками Європейського Союзу становить один із ключових напрямів трансформації. Правова рамка ЄС у сфері інформаційної безпеки є комплексною та динамічною системою регламентів, директив, рекомендацій, що охоплює різні аспекти – від захисту персональних даних до кібербезпеки критичної інфраструктури, від регулювання цифрових платформ до протидії дезінформації. Для України як держави-кандидата на членство в ЄС гармонізація з цією правовою рамкою є не просто технічним завданням транспонування норм європейського права у національне законодавство, а стратегічним процесом побудови правової системи, що відповідає європейським стандартам захисту прав людини, верховенства права, демократичного управління.

Загальний регламент захисту даних, відомий як GDPR, запроваджує розширені нормативні вимоги щодо безпеки та належної обробки персональної інформації, що базуються на принципах мінімізації збору даних, прозорості обробки, захисту за замовчуванням, підзвітності контролерів даних. Імплементація вимог GDPR в українське законодавство вимагає не просто зміни Закону України про захист персональних даних, але й створення ефективної системи регулювання та нагляду, розвитку культури захисту даних у бізнесі та державному секторі, підготовки спеціалістів з data protection. Україна вже здійснила певні кроки у цьому напрямі було зроблено істотні кроки, зокрема шляхом ухвалення у 2010 році основоположного закону, що регламентує обробку персональної інформації, а також запровадження інституту Уповноваженого Верховної Ради з прав людини як наглядового органу, відповідального за контроль у цій сфері. Водночас повна відповідність вимогам GDPR потребує подальших законодавчих змін, зміцнення інституційної спроможності регулятора, розвитку судової практики у справах про захист даних, запровадження сертифікаційних механізмів для підтвердження відповідності обробки даних європейським стандартам.

Практичне значення імплементації GDPR для України виходить за межі формального виконання євроінтеграційних зобов'язань. Високі стандарти захисту персональних даних є важливим чинником довіри до цифрової

економіки, що критично важливо з метою активізації притоку капіталу з-за кордону, розвитку IT-сектору, інтеграції українських компаній до глобальних ланцюгів створення вартості. Для громадян відповідність стандартам GDPR означає посилення захисту приватності, більший контроль над власними даними, можливості оскарження незаконної обробки персональної інформації. Для держави впровадження принципів GDPR у діяльність органів влади сприяє підвищенню прозорості, підзвітності, довіри громадян до державних інституцій. Водночас слід визнати, що повна імплементація GDPR є ресурсомістким процесом, що вимагає значних інвестицій у технічну інфраструктуру, навчання персоналу, розвиток аналітичних систем.

Директива NIS2 про заходи для високого спільного рівня кібербезпеки в Союзі, прийнята у 2022 році як оновлення попередньої Директиви NIS, встановлює комплексні вимоги до забезпечення кібербезпеки операторів критичної інфраструктури та провайдерів цифрових послуг. Ця директива значно розширює коло суб'єктів, що підпадають під вимоги кібербезпеки, посилює зобов'язання держав-членів щодо створення національних стратегій кібербезпеки, національних центрів реагування на кіберінциденти, систем звітування про кіберінциденти. Імплементація NIS2 в Україні вимагає перегляду існуючого законодавства у галузі кіберзахисту, передусім Закону України «Про основні засади забезпечення кібербезпеки», що потребує оновлення та доопрацювання з метою повної відповідності розширеним положенням оновленої європейської директиви.

Ключовими елементами імплементації NIS2 в українську практику мають стати чітке визначення критичної інфраструктури та суттєвих суб'єктів у різних секторах економіки, встановлення обов'язкових вимог до кібербезпеки для суб’єктів, відповідальних за функціонування об’єктів критичної інфраструктури, створення ефективної системи звітування про кіберінциденти з балансом між необхідністю інформування та захистом репутації організацій, посилення інституційних та технічних можливостей Держспецзв’язку як головного державного органу, що формує та реалізує політику у сфері кіберзахисту, посилення координації між різними суб'єктами забезпечення кібербезпеки.

Досвід протидії російським кібератакам під час повномасштабної війни виявив як сильні сторони українських спроможностей у кібербезпеці, так і вразливості, що потребують системного усунення через імплементацію європейських стандартів.

Digital Europe Programme як флагманська програма Європейського Союзу з цифрової трансформації створює значні можливості для України у розвитку цифрових спроможностей, включаючи сферу інформаційної безпеки. Програма передбачає спрямування фінансових ресурсів на розвиток п’яти пріоритетних сфер – високопродуктивних обчислень, штучного інтелекту, кіберзахисту, формування передових цифрових компетенцій та масштабного впровадження цифрових рішень у різні сегменти економіки й суспільного життя. . Для України участь у Digital Europe Programme може означати доступ до передових європейських технологій кібербезпеки, можливості співфінансування проєктів з цифрової трансформації сектору безпеки, участь у європейських дослідницьких консорціумах, навчання українських фахівців у провідних європейських центрах компетенцій.

Водночас слід розуміти, що повноцінна участь України у Digital Europe Programme потребує виконання певних передумов, зокрема приведення національного законодавства у відповідність із європейськими вимогами, створення інституційної структури для управління участю в програмі, забезпечення національного співфінансування проєктів. Стратегічні пріоритети участі України у програмі мають визначатися виходячи з національних потреб та спроможностей, зокрема фокусуючись на кібербезпеці критичної інфраструктури, розвитку штучного інтелекту для цілей національної безпеки, створенні захищених систем електронного урядування, підготовці кадрів у сфері цифровізації та кібербезпеки.

Формування спільного цифрового простору Україна-ЄС є амбітним, але необхідним стратегічним завданням, що виходить за межі простої технічної інтеграції систем. Спільний цифровий простір передбачає взаємне визнання електронних ідентифікаторів та електронних довірчих послуг, можливість транскордонного надання цифрових послуг, взаємодію електронних систем

державного управління, координацію політик у сфері цифровізації. Для громадян це означатиме можливість використання українських електронних документів у країнах ЄС, доступ до європейських цифрових послуг, спрощення процедур транскордонної взаємодії. Для бізнесу спільний цифровий простір створює можливості для розширення ринків, зменшення транзакційних витрат, участі у європейських цифрових екосистемах. Для держави це означає підвищення ефективності публічного управління, покращення якості публічних послуг, інтеграцію до європейських систем обміну інформацією.

Критично важливим елементом формування спільного цифрового простору є забезпечення високого рівня кібербезпеки та захисту даних. Інтеграція інформаційних систем створює нові вразливості, оскільки кіберінцидент в одній системі може поширитися на інтегровані системи інших країн. Це вимагає не лише технічної інтероперабельності систем захисту, але й узгодження підходів до управління ризиками, координації реагування на інциденти, обміну інформацією про загрози. Україна має демонструвати високий рівень кібербезпеки власних систем як передумову інтеграції до європейського цифрового простору, що створює додаткові стимули для впровадження європейських стандартів та інвестування у кібербезпеку.

Трансформаційний вплив європейської інтеграції на систему інформаційної безпеки України виявляється не лише у прямих вимогах щодо гармонізації законодавства чи адаптації технічних систем, але й у менш видимих, проте не менш важливих процесах зміни інституційної культури, підходів до управління, балансу між різними цінностями. Європейська модель інформаційної безпеки базується на принципах верховенства права, захисту прав людини, прозорості та підзвітності державних інституцій, залучення громадянського суспільства до формування політики. Ці принципи іноді вступають у напруження з традиційними підходами до національної безпеки, що акцентують на секретності, централізації прийняття рішень, мінімізації зовнішнього контролю. Процес європейської інтеграції вимагає знаходження нового балансу, що поєднує ефективність забезпечення безпеки з дотриманням демократичних цінностей та принципів.

Трансформація національної системи інформаційної безпеки в контексті європейської інтеграції супроводжується низкою складних і багатовимірних викликів. Насамперед, у ситуації воєнного стану гострий дефіцит фінансових ресурсів ставить державу перед необхідністю шукати баланс між негайними потребами оборони та довгостроковими інвестиціями в модернізацію інформаційно-безпекової інфраструктури. Брак кваліфікованих кадрів у сфері кібербезпеки, захисту даних, цифрової трансформації ускладнює впровадження складних європейських стандартів. Інституційна інерція та опір змінам з боку окремих органів влади можуть сповільнювати процеси адаптації. Необхідність балансування між адаптацією до європейських стандартів та збереженням ефективних власних напрацювань у протидії гібридним загрозам вимагає виваженого підходу. Водночас досвід успішної цифрової трансформації державних послуг через систему Дія демонструє спроможність України до швидких та ефективних реформ за наявності політичної волі та адекватних ресурсів.

Стратегія трансформації системи інформаційної безпеки під впливом європейської інтеграції має бути комплексною та реалістичною, що враховує як амбітні цілі повної інтеграції до європейського безпекового простору, так і обмеження та виклики, з якими стикається Україна. Пріоритизація напрямів трансформації виходячи з критичності для національної безпеки, готовності інституцій до змін, доступності ресурсів дозволить забезпечити поетапний, але послідовний прогрес. Залучення міжнародної технічної та фінансової допомоги від європейських партнерів для підтримки реформ має стати важливим елементом стратегії. Розвиток партнерств з європейськими інституціями, участь у європейських мережах та ініціативах створюватиме можливості для навчання, обміну досвідом, доступу до технологій. Комунікація з громадськістю щодо цілей та вигод європейської інтеграції у сфері інформаційної безпеки допоможе забезпечити суспільну підтримку реформ.

У підсумку, процес європейської інтеграції стає ключовим рушієм оновлення та перебудови української системи інформаційної безпеки, формуючи для держави не лише нові вимоги й нормативні рамки, але й відкриваючи

додаткові можливості, інструменти та стратегічні напрями для комплексної модернізації цієї сфери. Гармонізація національної політики з правовими рамками ЄС, зокрема імплементація GDPR, NIS2 Directive, інтеграція до Digital Europe Programme, передбачає необхідність ґрунтовного оновлення нормативної бази та узгодження ключових законодавчих актів із сучасними стандартами, інституційній архітектурі, технічних системах, компетентностях. Формування спільного цифрового простору Україна-ЄС є амбітним завданням, що потребує не лише технічної інтеграції, але й забезпечення високого рівня кібербезпеки та захисту даних. Трансформаційний вплив європейської інтеграції виходить за межі формальних змін та охоплює зміну інституційної культури, підходів до балансу між безпекою та свободою, залучення громадянського суспільства. Виклики трансформації є численними, проте досвід України у цифровізації та протидії гібридним загрозам створює підґрунтя для успішних реформ. Аналіз європейської інтеграції як чинника трансформації створює основу для розгляду конкретних інституційних та технологічних напрямів реформування національної системи інформаційної безпеки, що становитиме предмет наступного параграфа.

3.2. Інституційні та технологічні напрями реформування національної системи інформаційної безпеки

Констатація того, що процес європейської інтеграції виступає рушійною силою оновлення та модернізації системи інформаційної безпеки України, зроблена в попередньому параграфі, створює необхідну основу для конкретизації напрямів реформування національної системи. Перехід від аналізу загальних трансформаційних процесів до визначення конкретних інституційних та технологічних напрямів реформування є логічно необхідним кроком, оскільки успіх трансформації залежить від чіткості розуміння того, що саме потребує змін, яких результатів слід досягти, якими засобами та у які терміни. Інституційні та технологічні виміри реформування є взаємопов'язаними та взаємозалежними – інституційні зміни створюють організаційні передумови для технологічної

модернізації, тоді як впровадження нових технологій часто вимагає інституційних інновацій та зміни усталених процедур. Комплексність підходу до реформування, що поєднує інституційний та технологічний виміри, є критично важливою для досягнення системних змін та уникнення фрагментарності реформ.

Модернізація інституційного механізму гарантування інформаційної безпеки потребує розпочинатися з удосконалення координаційних механізмів між різними суб'єктами цієї системи. Аналіз, проведений у другому розділі, виявив проблему дублювання функцій, недостатньої узгодженості дій, прогалин у покритті певних сегментів загроз. Координаційний центр кібербезпеки при Раді національної безпеки і оборони України, створений відповідно до Закону про кібербезпеку, має потенціал стати ефективним механізмом координації, проте для цього потребує зміцнення інституційної спроможності. Розширення штату Центру за рахунок залучення висококваліфікованих фахівців з кібербезпеки, стратегічного планування, міжнародної співпраці дозволить підвищити якість аналітичної роботи та стратегічного планування. Надання Центру більших повноважень щодо координації діяльності суб'єктів кібербезпеки, включаючи можливість вимагати інформацію, давати рекомендації, моніторити виконання рішень, посилить його роль у системі.

Водночас координація у сфері інформаційної безпеки не може обмежуватися лише кібербезпекою та потребує створення більш широких механізмів узгодження дій різних органів влади, що мають повноваження у сфері протидії дезінформації, стратегічних комунікацій, медіаполітики. Формування міжвідомчої координаційної платформи з інформаційної безпеки при РНБО, до складу якої увійшли б представники всіх провідних інституцій, здатне було б створити умови для регулярний обмін інформацією, узгодження позицій, вироблення спільних підходів до протидії загрозам. Розвиток неформальних механізмів координації через створення професійних спільнот практиків, проведення регулярних міжвідомчих нарад, спільних навчань та тренінгів доповнить формальні структури та сприятиме формуванню культури співпраці.

Підвищення інституційної ефективності Державної служби спеціального

зв’язку та захисту інформації України як профільного центрального органу виконавчої влади у сфері кібербезпеки становить один із ключових напрямів модернізації національної системи. Саме Держспецзв’язку виконує базові функції із захисту критично важливої цифрової інфраструктури, забезпечення безпеки державних інформаційних ресурсів та організації оперативного реагування на кіберінциденти, що робить її спроможність визначальною для стійкості держави у цифровому середовищі. Водночас масштаб та складність завдань, що стоять перед Службою, вимагають значного зміцнення її спроможностей. Розширення штату за рахунок залучення талановитих молодих фахівців з кібербезпеки через конкурентоспроможну оплату праці, можливості професійного розвитку, цікаві завдання дозволить забезпечити Службу необхідними людськими ресурсами. Модернізація технічної інфраструктури Державного центру кіберзахисту через придбання сучасних систем моніторингу кіберзагроз, інструментів аналізу кіберінцидентів, захищених комунікаційних систем підвищить оперативні спроможності.

Розвиток аналітичних можливостей Держспецзв'язку у сфері кіберзагроз має стати окремим пріоритетом. Ефективна протидія складним кібератакам вимагає не лише технічних спроможностей для виявлення та блокування атак, але й глибокого розуміння тактик, технік, процедур противника, здатності атрибутувати атаки, прогнозувати майбутні загрози. Створення у структурі Держспецзв'язку спеціалізованого аналітичного підрозділу з кіберзагроз, укомплектованого фахівцями з технічної розвідки, аналізу шкідливого програмного забезпечення, атрибуції кібератак, дозволить підвищити якість стратегічного аналізу. Розвиток співпраці з науковими установами, IT-компаніями, міжнародними партнерами у сфері дослідження кіберзагроз створить можливості для доступу до передових методологій та інструментів аналізу.

Реформування Міністерства культури та інформаційної політики України з огляду на завдання зі зміцнення інформаційної безпеки має фокусуватися на посиленні його спроможностей у сфері стратегічних комунікацій, протидії дезінформації, розвитку медіаграмотності. Центр стратегічних комунікацій та

інформаційної безпеки відіграє важливу роль у моніторингу та аналізі дезінформаційних кампаній, проте потребує зміцнення для ефективного виконання своїх функцій. Розширення можливостей Центру для автоматизованого моніторингу великих обсягів інформації у соціальних мережах, месенджерах, онлайн-медіа завдяки інтеграції рішень, побудованих на технологіях штучного інтелекту, стане можливим підвищити оперативність виявлення дезінформації. Розвиток методологій аналізу складних, багатошарових дезінформаційних кампаній, що використовують комбінацію різних каналів та тактик, підвищить якість аналітичної роботи.

Посилення координації між Центром стратегічних комунікацій та іншими суб'єктами забезпечення інформаційної безпеки, зокрема Держспецзв'язку у сфері виявлення технічних аспектів інформаційних операцій, Службою безпеки України у сфері контррозвідувальних аспектів, міжнародними партнерами у сфері обміну інформацією про дезінформаційні кампанії, дозволить забезпечити комплексність протидії. Розвиток спроможностей МКІП у сфері проактивних стратегічних комунікацій, коли держава не лише реагує на дезінформацію, але й активно формує порядок денний, просуває власні наративи, будує довгострокову комунікаційну стратегію, підвищить ефективність інформаційної політики. Створення професійної системи підготовки та підвищення кваліфікації фахівців з стратегічних комунікацій забезпечить сталість спроможностей у цій критично важливій сфері.

Переосмислення та оновлення функціональної ролі Служби безпеки України в архітектурі інформаційної безпеки повинно здійснюватися в руслі загальної реформи спецслужби, спрямованої на її фокусування на контррозвідувальних функціях та захисті державного суверенітету. У сфері інформаційної безпеки це означає концентрацію зусиль СБУ на протидії найбільш небезпечним формам загроз, що виходять від іноземних спецслужб, терористичних організацій, організованих злочинних груп. Розвиток спроможностей СБУ у сфері контррозвідувальної діяльності в кіберпросторі, виявлення та припинення діяльності агентурних мереж іноземних спецслужб в інформаційній сфері, протидії кібершпигунству має стати пріоритетом.

Водночас критично важливим є забезпечення балансу між ефективністю діяльності спецслужби та дотриманням прав людини, що вимагає чітких правових рамок діяльності, ефективного парламентського та судового контролю, прозорості процедур.

Розвиток механізмів демократичного цивільного контролю за діяльністю суб'єктів забезпечення інформаційної безпеки є необхідним елементом інституційного реформування, що відповідає європейським стандартам. Посилення ролі парламентських комітетів, що здійснюють нагляд за діяльністю органів національної безпеки, через надання їм більших повноважень щодо доступу до інформації, проведення слухань, запрошення керівників відповідальних органів для звітування підвищить підзвітність системи. Розвиток інституту парламентського контролю за спецслужбами, включаючи можливість створення спеціалізованого комітету з нагляду за спецслужбами з участю депутатів, що мають відповідний допуск до секретної інформації, відповідатиме кращим європейським практикам. Залучення громадянського суспільства до моніторингу та оцінювання політики інформаційної безпеки через створення громадських рад при відповідних органах влади, проведення публічних консультацій щодо стратегічних документів, підтримку незалежних досліджень посилить зовнішній контроль.

Цифрова трансформація сектору безпеки та оборони є масштабним завданням, що вимагає системного підходу та значних інвестицій. Сектор безпеки та оборони традиційно характеризується певною консервативністю у впровадженні нових технологій, що пояснюється специфікою завдань, вимогами до надійності та захищеності систем, необхідністю збереження секретності. Водночас сучасні виклики, зокрема досвід протидії російській агресії, демонструють критичну важливість цифрових технологій для ефективності сектору безпеки та оборони. Цифрова трансформація має охоплювати різні аспекти діяльності сектору – від систем управління та зв'язку до аналітичних платформ, від кіберзахисту критичної інфраструктури до використання штучного інтелекту для обробки розвідувальної інформації.

Створення інтегрованої цифрової екосистеми безпеково-оборонного

комплексу, який гарантує захищений інформаційний обіг і належну комунікацію між усіма залученими інституціями, координацію дій, спільне ситуаційне усвідомлення, є амбітним, але необхідним завданням. Така екосистема має базуватися на принципах інтероперабельності систем різних органів, масштабованості для можливості розширення функціоналу, кіберстійкості для захисту від атак противника, зручності використання для кінцевих користувачів. Розробка національних стандартів обміну інформацією у секторі безпеки та оборони, гармонізованих з стандартами НАТО та ЄС, забезпечить технічну основу для інтеграції систем. Впровадження сучасних технологій шифрування, багатофакторної автентифікації, розподілених систем зберігання даних підвищить захищеність цифрової екосистеми.

Застосування технологій штучного інтелекту та алгоритмів машинного навчання у сфері безпеки й оборони формує принципово нові інструменти для підсилення аналітичного потенціалу, оптимізації процесів ухвалення управлінських рішень та автоматизації операційної діяльності, що раніше вимагала значних людських ресурсів. Системи на базі штучного інтелекту можуть аналізувати величезні обсяги даних з різних джерел для виявлення паттернів, прогнозування загроз, підтримки прийняття рішень. У сфері кібербезпеки штучний інтелект може використовуватися для автоматичного виявлення аномалій у мережевому трафіку, ідентифікації нових видів шкідливого програмного забезпечення, прогнозування можливих векторів атак. У сфері протидії дезінформації технології обробки природної мови можуть допомагати у автоматичному виявленні маніпулятивного контенту, аналізі емоційного забарвлення текстів, виявленні координованих дезінформаційних кампаній.

Водночас впровадження штучного інтелекту у секторі безпеки та оборони вимагає відповідального підходу з урахуванням етичних, правових, безпекових аспектів. Розробка національної стратегії використання штучного інтелекту у секторі безпеки та оборони має визначити принципи, рамки, обмеження такого використання. Забезпечення прозорості та пояснюваності рішень, прийнятих системами на базі штучного інтелекту, особливо коли такі рішення можуть

впливати на права людини, є критично важливим. Захист систем штучного інтелекту від маніпуляцій, отруєння даних, адверсаріальних атак потребує спеціальних технічних та організаційних заходів. Підготовка фахівців, що розуміють як можливості, так і обмеження штучного інтелекту, забезпечить відповідальне його використання.

Впровадження європейських стандартів кіберзахисту у національну практику є комплексним процесом, що виходить за межі простого прийняття технічних специфікацій. Європейські стандарти кіберзахисту, розроблені такими організаціями як Європейське агентство з кібербезпеки, Європейський інститут телекомунікаційних стандартів, Міжнародна організація стандартизації, охоплюють різні аспекти – від управління інформаційною безпекою до технічних вимог до криптографічних засобів, від стандартів реагування на інциденти до вимог до безпеки Інтернету речей. Адаптація цих стандартів в українську практику вимагає не лише їхнього формального затвердження як національних стандартів, але й створення екосистеми для їхнього впровадження.

Розвиток національної системи сертифікації відповідності стандартам кібербезпеки, що включає акредитацію сертифікаційних органів, підготовку аудиторів, розробку методологій оцінювання, створить механізми для підтвердження відповідності організацій та систем європейським стандартам. Запровадження вимоги обов’язкової сертифікації для суб’єктів, що управляють критичною інфраструктурою, надають цифрові послуги чи здійснюють державне управління, стане ефективним механізмом стимулювання системного підвищення стандартів кіберзахисту. Створення системи підтримки малих та середніх підприємств у впровадженні стандартів кібербезпеки через надання методологічної допомоги, навчання, можливо фінансової підтримки, забезпечить інклюзивність процесу. Міжнародне визнання української системи сертифікації через гармонізацію з європейськими підходами полегшить інтеграцію українських компаній до європейського цифрового ринку.

Розвиток системи моніторингу інформаційних загроз на національному рівні вимагає створення інтегрованої платформи, що агрегує дані з різних джерел, аналізує їх за допомогою сучасних технологій, надає своєчасну

інформацію для прийняття рішень. Така платформа має інтегрувати дані від різних суб'єктів забезпечення інформаційної безпеки, комерційних провайдерів threat intelligence, міжнародних партнерів, відкритих джерел. Використання технологій великих даних та машинного навчання для обробки та аналізу величезних обсягів інформації дозволить виявляти складні, багатошарові загрози, що не очевидні при аналізі окремих джерел. Створення системи класифікації та приоритизації загроз забезпечить фокусування уваги на найбільш критичних ризиках.

Розвиток спроможностей для атрибуції джерел інформаційних загроз, зокрема складних кібератак та дезінформаційних кампаній, є критично важливим для ефективної протидії. Атрибуція дозволяє не лише розуміти, хто стоїть за атаками, але й адаптувати стратегію протидії до специфіки противника, притягувати винних до відповідальності, демонструвати міжнародній спільноті докази агресії. Водночас атрибуція є складним завданням, що вимагає поєднання технічного аналізу, розвідувальної інформації, аналізу контексту. Розвиток національних спроможностей для атрибуції через підготовку спеціалістів, придбання спеціалізованих інструментів, розвиток міжнародної співпраці для обміну інформацією підвищить ефективність протидії загрозам.

Побудова ефективної системи кризових комунікацій у сфері інформаційної безпеки є критично важливою для оперативного та злагодженого реагування на інциденти великого масштабу, наслідки яких можуть суттєво позначитися на стані національної безпеки, стабільності економіки та суспільному житті. Під кризовими комунікаціями розуміють узгоджену взаємодію між усіма задіяними інституціями під час виникнення інцидентів, інформування населення про характер загрози та необхідні заходи безпеки, а також налагоджену координацію з міжнародними партнерами. Вироблення та постійне оновлення чітких протоколів кризових комунікацій – із визначенням відповідальних суб’єктів, алгоритмів обміну інформацією та процедур ухвалення рішень – створює умови для скоординованих і результативних дій у надзвичайних ситуаціях.

Проведення регулярних навчань та тренінгів з відпрацювання кризових комунікацій з участю всіх ключових суб'єктів дозволить виявити та усунути

проблеми у процедурах, розвинути навички персоналу, побудувати довіру між різними організаціями. Створення захищених каналів комунікації для обміну чутливою інформацією під час кризи забезпечить можливість оперативної координації без ризику перехоплення інформації противником. Розвиток спроможностей для стратегічних комунікацій під час кризи, включаючи підготовку повідомлень для різних аудиторій, координацію з медіа, моніторинг суспільних настроїв, дозволить мінімізувати паніку та дезінформацію, що часто супроводжують кризові ситуації.

Впровадження принципів безпеки за дизайном та приватності за замовчуванням у розробку та експлуатацію інформаційних систем державного сектору має стати обов'язковою практикою. Традиційний підхід, коли безпека додається до вже розробленої системи, виявився неефективним у протидії сучасним складним загрозам. Безпека за дизайном передбачає врахування вимог безпеки на всіх етапах життєвого циклу системи – від планування та проєктування до розробки, впровадження, експлуатації, виведення з експлуатації. Приватність за замовчуванням означає, що системи мають бути налаштовані таким чином, щоб за замовчуванням забезпечувати найвищий рівень захисту персональних даних без необхідності додаткових налаштувань користувачем.

Впровадження цих принципів вимагає зміни підходів до закупівлі, розробки, експлуатації інформаційних систем у державному секторі. Включення вимог безпеки за дизайном та приватності за замовчуванням у тендерну документацію на закупівлю або розробку інформаційних систем забезпечить їхнє врахування з самого початку. Підготовка фахівців державного сектору з принципів безпеки за дизайном через спеціалізовані навчальні програми підвищить компетентність замовників систем. Розробка методологій оцінювання відповідності систем принципам безпеки за дизайном та приватності за замовчуванням створить інструменти для контролю. Поширення кращих практик через публікацію кейсів успішного впровадження, проведення конференцій, створення професійних спільнот сприятиме масштабуванню підходу.

Таким чином, інституційні та технологічні напрями реформування національної системи інформаційної безпеки є взаємопов'язаними та взаємодоповнюючими елементами комплексної трансформації. Інституційне реформування охоплює вдосконалення координаційних механізмів, посилення інституційної спроможності ключових суб'єктів, розвиток механізмів демократичного контролю, що створює організаційні передумови для ефективного функціонування системи. Технологічні напрями включають цифрову трансформацію сектору безпеки та оборони, впровадження європейських стандартів кіберзахисту, розвиток систем моніторингу загроз та кризових комунікацій, впровадження принципів безпеки за дизайном, що забезпечують технічну основу для протидії сучасним складним загрозам. Комплексність підходу, що поєднує інституційні та технологічні зміни, є необхідною умовою успішності реформ. Визначення конкретних напрямів реформування створює основу для формулювання практичних рекомендацій щодо вдосконалення інформаційної безпеки України в умовах євроінтеграції, що становитиме предмет наступного параграфа.

3.3. Рекомендації щодо вдосконалення інформаційної безпеки України в умовах євроінтеграції

Аналіз інституційних та технологічних напрямів реформування національної системи інформаційної безпеки, здійснений у попередньому параграфі, створює необхідну основу для формулювання конкретних практичних рекомендацій щодо вдосконалення системи в умовах європейської інтеграції. Перехід від визначення напрямів реформування до формулювання конкретних рекомендацій є завершальним етапом дослідження, що має трансформувати аналітичні висновки у практичні пропозиції для суб'єктів формування та реалізації політики інформаційної безпеки. Рекомендації мають враховувати наявні ресурси, інституційні спроможності, політичний контекст, при цьому визначаючи амбітні цілі трансформації. Вони мають бути конкретними, визначаючи не лише що доцільно зробити, але й як, ким, у які

терміни, з якими ресурсами. Водночас рекомендації мають бути достатньо гнучкими, щоб дозволяти адаптацію до динамічних змін у ландшафті загроз, технологічному середовищі, геополітичній ситуації.

Удосконалення міжвідомчої координації у сфері інформаційної безпеки доцільно розпочати з розширення повноважень та ресурсів Координаційного центру кібербезпеки при Раді національної безпеки і оборони України. Перетворення його на повноцінний координаційний механізм не лише у сфері кібербезпеки, але й у ширшому контексті інформаційної безпеки посилить ефективність системи. Збільшення штату Центру до п'ятдесяти фахівців, включаючи експертів з кібербезпеки, стратегічних комунікацій, аналізу дезінформації, міжнародної співпраці, правового забезпечення, забезпечить необхідну експертизу. Надання Центру повноважень щодо затвердження щорічного плану координованих дій у сфері інформаційної безпеки з визначенням конкретних завдань для кожного суб'єкта системи, термінів виконання, відповідальних осіб, очікуваних результатів створить чіткість у розподілі відповідальності.

Доцільно створити при Координаційному центрі постійно діючі робочі групи за ключовими напрямами інформаційної безпеки – кібербезпека критичної інфраструктури, протидія дезінформації, захист персональних даних, стратегічні комунікації, міжнародна співпраця. Включення до складу робочих груп представників усіх релевантних органів державної влади, а також представників бізнесу, громадянського суспільства, наукових установ забезпечить багатосторонній підхід. Регулярні засідання робочих груп для обміну інформацією про загрози, узгодження підходів до протидії, вироблення спільних рекомендацій посилять оперативність реагування. Запровадження практики щоквартальних звітів суб'єктів забезпечення інформаційної безпеки перед Координаційним центром про виконання покладених завдань, виявлені загрози, вжиті заходи протидії підвищить підзвітність системи.

Розробка та затвердження Національної стратегії координації у сфері інформаційної безпеки визначить принципи, механізми, процедури координації між різними суб'єктами системи. Стратегія може чітко розмежувати

повноваження та відповідальність різних органів влади для уникнення дублювання функцій та прогалин у покритті загроз. Визначення процедур обміну інформацією між суб'єктами системи з урахуванням різних рівнів секретності інформації та необхідності оперативного реагування сприятиме ефективності. Встановлення механізмів вирішення конфліктів та суперечностей між різними органами влади щодо їхніх повноважень чи підходів до вирішення певних питань запобігатиме інституційним тертям. Запровадження системи моніторингу та оцінювання ефективності координації через визначення конкретних індикаторів та проведення щорічних незалежних оцінювань забезпечить постійне вдосконалення системи.

Посилення спроможностей у сфері стратегічних комунікацій вимагає системного підходу, що охоплює інституційне зміцнення, розвиток методологій, підготовку кадрів, технологічне оснащення. Створення при Міністерстві культури та інформаційної політики України Національного центру стратегічних комунікацій як спеціалізованої інституції з розширеними повноваженнями та ресурсами порівняно з існуючим Центром стратегічних комунікацій та інформаційної безпеки може посилити ефективність комунікаційних зусиль держави. Національний центр міг би координувати стратегічні комунікації всіх органів державної влади для забезпечення єдності меседжів, узгодженості дій, максимізації ефекту комунікаційних зусиль. Розширення штату Центру до ста фахівців, включаючи стратегічних комунікаторів, аналітиків медіа, фахівців з цифрового маркетингу, дизайнерів, продюсерів мультимедійного контенту забезпечить комплексність підходу.

Розробка Національної стратегії стратегічних комунікацій України на період до 2030 року визначить довгострокові цілі, пріоритетні аудиторії, ключові наративи, інструменти та канали комунікації. Стратегія може базуватися на ретельному аналізі цільових аудиторій, їхніх інформаційних потреб, уподобань, вразливостей до маніпулятивних впливів. Визначення окремих комунікаційних стратегій для різних сегментів аудиторії – внутрішньої та зовнішньої, різних вікових, соціальних, регіональних груп дозволить підвищити ефективність комунікацій. Розробка системи оцінювання ефективності стратегічних

комунікацій через моніторинг охоплення, залученості, зміни ставлень та поведінки цільових аудиторій забезпечить зворотний зв'язок для вдосконалення. Запровадження практики регулярного оновлення стратегії на основі результатів моніторингу та змін у зовнішньому середовищі забезпечить її актуальність.

Створення системи навчання та підвищення кваліфікації фахівців з стратегічних комунікацій через запровадження спеціалізованих освітніх програм у провідних українських університетах, організацію стажувань у провідних європейських інституціях, проведення регулярних тренінгів та семінарів з участю міжнародних експертів забезпечить сталість спроможностей. Розробка професійних стандартів для фахівців з стратегічних комунікацій у державному секторі, що визначатимуть необхідні компетенції, кваліфікаційні вимоги, етичні принципи, підвищить професіоналізм сектору. Створення професійної асоціації стратегічних комунікаторів для обміну досвідом, розвитку кращих практик, підвищення статусу професії сприятиме розвитку галузі. Запровадження конкурентоспроможної оплати праці для фахівців з стратегічних комунікацій у державному секторі сприятиме залученню та утриманню талантів.

Модернізація технологічної інфраструктури для стратегічних комунікацій через впровадження сучасних систем моніторингу медіа та соціальних мереж, аналітичних платформ на базі штучного інтелекту для виявлення трендів та настроїв аудиторій, інструментів для створення та поширення мультимедійного контенту підвищить технологічну спроможність. Створення єдиної цифрової платформи стратегічних комунікацій держави, що інтегруватиме різні канали комунікації, забезпечуватиме координацію між різними органами влади, дозволятиме оперативно реагувати на виклики інформаційного простору, посилить ефективність. Розвиток спроможностей для таргетованих комунікацій через використання технологій цифрового маркетингу, що дозволяють доставляти персоналізовані меседжі різним сегментам аудиторії через найбільш ефективні для них канали, підвищить точність комунікацій.

Підвищення медіаграмотності населення як ключового елемента інформаційної стійкості суспільства вимагає комплексного підходу, що охоплює формальну освіту, неформальне навчання, інформаційні кампанії. Інтеграція

медіаграмотності як обов'язкової складової навчальних програм на всіх рівнях освіти – від початкової школи до університету – забезпечить системність підходу. У початковій школі доцільно зосередитися на розвитку базових навичок критичного мислення, розпізнавання різних типів інформації, усвідомлення власної поведінки в інформаційному просторі. У середній школі можливе поглиблене вивчення механізмів функціонування медіа, тактик маніпуляції інформацією, способів перевірки фактів, етичних аспектів створення та поширення контенту. У вищій освіті медіаграмотність може стати частиною базових компетентностей випускника незалежно від спеціальності.

Розробка національної програми підвищення медіаграмотності дорослого населення з особливим фокусом на найбільш вразливі групи – людей старшого віку, жителів сільської місцевості, осіб з низьким рівнем освіти – охопить широкі верстви населення. Програма може передбачати проведення безкоштовних тренінгів та семінарів у бібліотеках, будинках культури, громадських центрах у всіх регіонах України. Створення мережі тренерів з медіаграмотності через підготовку бібліотекарів, вчителів, соціальних працівників, активістів громадських організацій забезпечить масштабованість програми. Розробка та поширення доступних навчальних матеріалів з медіаграмотності у різних форматах – брошури, відеоролики, онлайн-курси, мобільні застосунки – з урахуванням потреб різних цільових аудиторій підвищить доступність знань.

Підтримка розвитку незалежних організацій громадянського суспільства, що працюють у сфері медіаграмотності, через надання грантів на реалізацію проєктів, створення сприятливих умов для діяльності, залучення до формування державної політики посилить спроможності громадянського сектору. Створення Національної коаліції з медіаграмотності, що об'єднуватиме органи влади, громадські організації, медіа, освітні установи, міжнародних партнерів для координації зусиль, обміну досвідом, адвокації політики медіаграмотності забезпечить системність підходу. Запровадження щорічного Тижня медіаграмотності в Україні з проведенням численних заходів по всій країні може привернути увагу до важливості медіаграмотності. Створення національної премії за внесок у розвиток медіаграмотності визнає зусилля організацій та

окремих осіб.

Поглиблення партнерства з інституціями Європейського Союзу у сфері інформаційної безпеки може стати стратегічним пріоритетом зовнішньої політики України у цій сфері. Активізація співпраці з East StratCom Task Force Європейської служби зовнішніх дій через призначення постійного українського представника при Task Force забезпечить систематичний обмін інформацією та координацію дій. Розширення обміну інформацією про виявлені дезінформаційні кампанії, тактики та джерела дезінформації, ефективні практики протидії посилить спільні спроможності. Ініціювання спільних дослідницьких проєктів з аналізу російської дезінформації, виявлення нових тактик, оцінювання ефективності різних інструментів протидії поглибить розуміння загроз. Організація регулярних обмінів делегаціями між українськими та європейськими інституціями для вивчення досвіду, побудови довіри, розвитку особистих зв'язків між фахівцями зміцнить партнерство.

Розвиток співпраці з Агентством Європейського Союзу з кібербезпеки через участь українських фахівців у робочих групах ENISA, спільних навчаннях з кіберзахисту, програмах обміну персоналом підвищить компетентності. Надання Україні статусу асоційованого члена ENISA дозволить повноцінно брати участь у діяльності Агентства, отримувати доступ до аналітичних матеріалів, технічної експертизи, навчальних ресурсів. Впровадження механізмів регулярного обміну інформацією про кіберзагрози між українськими та європейськими центрами реагування на кіберінциденти посилить колективну кіберстійкість. Участь українських експертів у розробці європейських стандартів кібербезпеки забезпечить врахування українського досвіду та полегшить подальшу імплементацію цих стандартів.

Участь України у спільних проєктах Європейського Союзу у сфері кібер- та інформаційної безпеки створює можливості для доступу до фінансування, технологій, експертизи. Активна участь у програмі Digital Europe через подання якісних проєктних пропозицій у сфері кібербезпеки, штучного інтелекту, цифрової трансформації може принести значні ресурси для модернізації системи. Приєднання до європейських проєктів з кіберзахисту критичної

інфраструктури дозволить скористатися передовими технологіями та методологіями. Участь у європейських дослідницьких консорціумах з інформаційної безпеки забезпечить доступ до новітніх розробок. Використання можливостей програми Горизонт Європа для фінансування досліджень у сфері протидії дезінформації, кібербезпеки, захисту даних підтримає розвиток науки.

Для максимізації вигод від участі у європейських програмах доцільно створити при Координаційному центрі кібербезпеки спеціалізований підрозділ з координації міжнародної співпраці, що відслідковуватиме можливості для участі у європейських проєктах, допомагатиме українським інституціям у підготовці заявок, координуватиме участь у проєктах. Розвиток спроможностей для проєктного менеджменту відповідно до європейських стандартів підвищить успішність заявок. Створення бази даних українських експертів з інформаційної безпеки, готових брати участь у європейських проєктах, полегшить формування консорціумів. Організація інформаційних сесій та тренінгів для потенційних учасників європейських програм підвищить обізнаність про можливості.

Зміцнення спроможностей Державної служби спеціального зв'язку та захисту інформації України у сфері міжнародної співпраці дозволить повніше використовувати можливості партнерства з європейськими та іншими міжнародними партнерами. Створення у структурі Держспецзв'язку департаменту міжнародної співпраці з кібербезпеки з достатнім штатом фахівців, що володіють іноземними мовами та мають досвід міжнародної співпраці, забезпечить інституційну основу. Розвиток двосторонніх партнерств з національними агентствами кібербезпеки провідних європейських країн для обміну досвідом, спільних навчань, взаємної технічної допомоги поглибить співпрацю. Участь у міжнародних навчаннях з кіберзахисту, таких як Locked Shields, Cyber Europe, підвищить готовність до реагування на масштабні кіберінциденти.

Розвиток спроможностей України для надання міжнародної технічної допомоги іншим країнам у сфері протидії дезінформації та кібербезпеки на основі унікального досвіду протистояння російській агресії може стати новим напрямом міжнародного партнерства. Україна накопичила значний досвід у

протидії масштабним дезінформаційним кампаніям, кібератакам на критичну інфраструктуру, координації діяльності різних суб'єктів в умовах кризи, що може бути цінним для інших країн. Створення програми міжнародної технічної допомоги України у сфері інформаційної безпеки для країн Східного партнерства, Західних Балканів, інших регіонів посилить міжнародні позиції України. Організація навчальних програм для іноземних фахівців на базі українських інституцій з питань протидії гібридним загрозам може стати джерелом доходу та інструментом м'якої сили.

Вдосконалення законодавчої бази інформаційної безпеки має відбуватися у напрямі повної гармонізації з європейським правом при збереженні ефективності у протидії специфічним для України загрозам. Прийняття нового Закону України про захист персональних даних у повній відповідності з вимогами GDPR створить правову основу для інтеграції до європейського цифрового простору. Оновлення Закону України про основні засади забезпечення кібербезпеки з урахуванням вимог Директиви NIS2 посилить кіберстійкість. Прийняття Закону України про цифрові послуги за зразком Digital Services Act встановить правила для цифрових платформ. Розробка законодавства про протидію іноземному інформаційному втручанню забезпечить правові інструменти для захисту від маніпулятивних впливів.

Водночас законодавчі ініціативи мають супроводжуватися широкими публічними консультаціями з залученням громадянського суспільства, бізнесу, наукової спільноти, міжнародних експертів для забезпечення балансу різних інтересів та відповідності демократичним стандартам. Проведення оцінки впливу законодавчих змін на права людини, економіку, інституційні спроможності допоможе уникнути непередбачених негативних наслідків. Поетапне впровадження нових законодавчих вимог з наданням достатнього часу для адаптації зацікавленим сторонам забезпечить реалістичність імплементації. Супровід законодавчих змін роз'яснювальними кампаніями для інформування громадськості та бізнесу про нові права та обов'язки підвищить ефективність.

Таким чином, вдосконалення інформаційної безпеки України в умовах євроінтеграції потребує комплексного підходу, що охоплює інституційні,

технологічні, законодавчі, освітні, міжнародні аспекти. Пропозиції щодо удосконалення міжвідомчої координації, посилення спроможностей у стратегічних комунікаціях, підвищення медіаграмотності населення, поглиблення партнерства з європейськими інституціями, участі у спільних проєктах ЄС створюють дорожню карту трансформації системи. Реалізація цих пропозицій вимагатиме політичної волі, адекватного ресурсного забезпечення, координації зусиль різних суб'єктів, систематичності у впровадженні змін. Водночас досвід України у цифровій трансформації та протидії гібридним загрозам створює підґрунтя для оптимізму щодо можливості успішної реалізації цих амбітних завдань. Формулювання конкретних рекомендацій завершує аналітичну частину дослідження та створює основу для узагальнюючих висновків щодо третього розділу роботи.

Висновки до розділу 3

Третій розділ роботи було присвячено визначенню напрямів трансформації інформаційної безпеки України в контексті європейської інтеграції, що логічно завершує дослідження переходом від аналітичного розгляду існуючого стану системи до формулювання конкретних шляхів її вдосконалення. Дослідження охопило три взаємопов'язаних аспекти: аналіз європейської інтеграції як каталізатора трансформації, визначення інституційних та технологічних напрямів реформування, розроблення прикладних пропозицій, спрямованих на підвищення ефективності функціонування національної системи інформаційної безпеки.

Аналіз європейської інтеграції як чинника трансформації системи інформаційної безпеки України виявив її багатовимірний характер, що виходить за межі формальної імплементації законодавства Європейського Союзу. Європейська інтеграція створює одночасно зобов'язання у напрямі її приведення у відповідність до норм та підходів, що застосовуються в державах – членах Європейського Союзу, можливості для залучення технічної допомоги та експертизи, стимули для інституційного розвитку та критерії оцінювання

прогресу реформ. Гармонізація національної політики інформаційної безпеки з правовими рамками ЄС, зокрема імплементація GDPR, NIS2 Directive, інтеграція до Digital Europe Programme, вимагає системних змін у законодавстві, інституційній архітектурі, технічних системах, компетентностях. Формування спільного цифрового простору Україна-ЄС є амбітним завданням, що потребує не лише технічної інтеграції, але й забезпечення високого рівня кібербезпеки та захисту даних як передумови довіри до інтегрованих систем.

Трансформаційний вплив європейської інтеграції виходить за межі формальних змін та охоплює зміну інституційної культури, підходів до балансу між безпекою та свободою інформації, залучення громадянського суспільства до формування та моніторингу політики. Європейська модель інформаційної безпеки, що базується на принципах верховенства права, захисту прав людини, прозорості та підзвітності державних інституцій, вимагає адаптації традиційних підходів до національної безпеки. Виклики трансформації пов'язані з обмеженістю ресурсів в умовах війни, браком кваліфікованих кадрів, інституційною інерцією, необхідністю балансування між адаптацією до європейських стандартів та збереженням ефективних власних напрацювань у протидії гібридним загрозам. Водночас досвід успішної цифрової трансформації державних послуг через систему Дія демонструє спроможність України до швидких та ефективних реформ.

Визначення інституційних та технологічних напрямів реформування національної системи інформаційної безпеки конкретизує загальні трансформаційні процеси у практичні завдання. Інституційне реформування охоплює вдосконалення координаційних механізмів між різними суб'єктами системи, посилення інституційної спроможності ключових органів влади, розвиток механізмів демократичного цивільного контролю, що створює організаційні передумови для ефективного функціонування системи. Особлива увага приділена зміцненню Координаційного центру кібербезпеки при РНБО, Державної служби спеціального зв'язку та захисту інформації, Міністерства культури та інформаційної політики як ключових інституцій у забезпеченні інформаційної безпеки.

Технологічні напрями реформування включають цифрову глибинне оновлення та модернізацію всієї системи безпекових і оборонних інституцій через створення інтегрованої цифрової екосистеми, використання штучного інтелекту та машинного навчання для підвищення ефективності аналітичної роботи, автоматизації процесів, прогнозування загроз. Впровадження європейських стандартів кіберзахисту вимагає не лише формального затвердження стандартів, але й створення екосистеми для їхнього впровадження, включаючи розвиток системи сертифікації, підготовку фахівців, підтримку організацій у впровадженні. Розвиток систем моніторингу інформаційних загроз, вдосконалення кризових комунікацій, впровадження принципів безпеки за дизайном та приватності за замовчуванням у розробку інформаційних систем забезпечують технологічну основу для протидії сучасним складним загрозам.

Розроблення прикладних пропозицій, спрямованих на підвищення ефективності національної системи інформаційної безпеки України в умовах євроінтеграції трансформує аналітичні висновки у конкретні пропозиції для практичної реалізації. Пропозиції охоплюють удосконалення міжвідомчої координації через розширення повноважень Координаційного центру кібербезпеки, створення постійно діючих робочих груп за ключовими напрямами, розробку Національної стратегії координації. Посилення спроможностей у сфері стратегічних комунікацій передбачає створення Національного центру стратегічних комунікацій, розробку Національної стратегії стратегічних комунікацій, створення системи навчання фахівців, модернізацію технологічної інфраструктури.

Підвищення медіаграмотності населення як критично важливого елемента інформаційної стійкості суспільства вимагає інтеграції медіаграмотності у навчальні програми на всіх рівнях освіти, розробки національної програми для дорослого населення з особливим фокусом на вразливі групи, підтримки організацій громадянського суспільства у цій сфері. Поглиблення партнерства з інституціями Європейського Союзу передбачає активізацію співпраці з East StratCom Task Force, розвиток партнерства з ENISA, активну участь у спільних проєктах ЄС у сфері кібер- та інформаційної безпеки. Пропозиції щодо

вдосконалення законодавчої бази спрямовані на повну гармонізацію з європейським правом при збереженні ефективності у протидії специфічним для України загрозам.

Комплексність підходу, що поєднує інституційні, технологічні, законодавчі, освітні, міжнародні аспекти трансформації, є необхідною умовою успішності реформ у сфері інформаційної безпеки. Розрізнені, фрагментарні зміни не здатні забезпечити системного ефекту та можуть навіть створювати нові вразливості через несумісність різних елементів системи. Реалізація запропонованих напрямів трансформації та конкретних рекомендацій вимагатиме значної політичної волі, адекватного ресурсного забезпечення, координації зусиль різних суб'єктів, терпіння та систематичності у впровадженні змін, що часто дають відчутні результати лише через тривалий час.

Водночас існують вагомі підстави для оптимізму щодо можливості успішної реалізації амбітних завдань трансформації інформаційної безпеки України. Досвід цифрової трансформації державних послуг через систему Дія демонструє спроможність України до інноваційних реформ за наявності чіткого бачення, професійної команди, політичної підтримки. Унікальний досвід протидії російській гібридній агресії, включаючи інформаційні операції та кібератаки, виробив у українських інституціях та суспільстві стійкість, адаптивність, інноваційність у пошуку рішень. Надання Україні статусу кандидата на членство в Європейському Союзі створює потужні зовнішні стимули для реформ та відкриває доступ до ресурсів, експертизи, підтримки європейських партнерів.

Узагальнення результатів третього розділу підтверджує, що трансформація інформаційної безпеки України в контексті європейської інтеграції є не лише технічним завданням адаптації до європейських стандартів, але й стратегічною можливістю для якісного стрибка у розвитку системи, що поєднає кращі європейські практики з унікальним українським досвідом протистояння гібридним загрозам. Ця трансформація сприятиме не лише зміцненню національної безпеки України, але й посиленню колективної безпеки європейського простору, оскільки Україна може стати важливим донором

безпеки для Європи, ділячись досвідом та спроможностями у протидії спільним загрозам.

ВИСНОВКИ

У межах виконання магістерського дослідження було проведено всебічний аналіз еволюції національної системи інформаційної безпеки України в умовах її поступової інтеграції до європейського політичного та безпекового простору. Такий підхід дав змогу простежити ключові тенденції, визначити чинники й механізми адаптації української моделі інформаційної безпеки до стандартів Європейського Союзу, а також окреслити пріоритетні напрями її подальшого розвитку в ситуації зростання зовнішніх і внутрішніх викликів. Послідовне виконання дослідницьких завдань забезпечило формування комплексного бачення проблематики, що синтезує теоретичні підходи, аналіз актуального стану та оцінку перспектив трансформації системи інформаційної безпеки України в контексті євроінтеграційних процесів.

1. Осмислення сутності інформаційної безпеки виявило її еволюцію від вузького трактування як захисту державних секретів до широкого комплексного розуміння як багатовимірного феномену, що охоплює захист інформації, інформаційних систем та інформаційного простору держави при дотриманні гармонійного співвідношення між правами громадянина, потребами суспільства та стратегічними інтересами держави. Встановлено, що інформаційна безпека є багаторівневою системою взаємопов’язаних елементів, що включає безпеку інформації, безпеку інформаційної інфраструктури, безпеку інформаційного простору та інформаційну стійкість суспільства. Роль інформаційної безпеки в архітектурі національної безпеки зумовлена її інтегрованим, пронизуючим характером і тісною взаємодією з усіма ключовими сферами безпекової політики держави. Ця взаємозалежність проявилася особливо чітко в умовах російської збройної агресії, коли інформаційний вимір став одним із визначальних факторів стійкості та обороноздатності України.

2. Теоретичний аналіз підтвердив доцільність інтеграції системного, інституційного, комунікативного та конструктивістського підходів для комплексного дослідження інформаційної безпеки в контексті європейської інтеграції. Системний підхід дозволяє аналізувати процеси інтеграції національної системи до ширшої європейської системи безпеки, інституційний

розкриває механізми інституційних змін та трансферу європейських інституцій, комунікативний фокусується на стратегічних комунікаціях як інструменті забезпечення інформаційної стійкості, конструктивістський виявляє роль дискурсів та цінностей у формуванні політики. Концепції цифрового та інформаційного суверенітету Європейського Союзу визначають стратегічні орієнтири розвитку інформаційної безпеки у європейському просторі та впливають на траєкторію адаптації української системи, створюючи як можливості для посилення спроможностей, так і виклики щодо збереження національної специфіки.

3. Аналіз нормативно-правової бази інформаційної безпеки України виявив наявність спеціалізованого законодавства та стратегічних документів, що визначають пріоритети державної політики, водночас встановлено проблеми фрагментарності, застарілості окремих актів, недостатньої імплементації через брак підзаконних актів та ресурсного забезпечення. Гармонізація національного законодавства з правом Європейського Союзу є ключовим напрямом трансформації, що вимагає поетапного впровадження норм і підходів Європейського Союзу у сферах захисту персональної інформації, кіберзахисту, регулювання діяльності цифрових платформ та удосконалення медіа-політики. Процес гармонізації потребує врахування специфіки національного контексту, зокрема необхідності протидії гібридним загрозам та російській інформаційній агресії, що створює унікальні виклики для балансування між європейськими стандартами та безпековими потребами.

4. Інституційний аналіз засвідчив багатосуб’єктний характер системи забезпечення інформаційної безпеки України з розподіленими повноваженнями між різними органами державної влади, що створює як переваги у вигляді спеціалізації функцій, так і виклики координації діяльності. Ключові інституції – Рада національної безпеки і оборони України, Державна служба спеціального зв’язку та захисту інформації, Міністерство культури та інформаційної політики, Служба безпеки України – виконують специфічні функції та демонструють різний рівень інституційної спроможності. Створення Координаційного центру кібербезпеки при РНБО стало важливим кроком у посиленні координації, проте

практика його функціонування засвідчує необхідність подальшого зміцнення повноважень, ресурсів, аналітичних можливостей. Повномасштабна російська агресія виявила як сильні сторони української інституційної моделі, зокрема здатність до швидкої адаптації та оперативного реагування, так і вразливості, насамперед проблеми міжвідомчої координації та обмеженість ресурсів.

5. Систематизація сучасних викликів та загроз інформаційній безпеці України підтвердила їхній системний, комплексний та динамічний характер. Гібридні інформаційні впливи Російської Федерації становлять найбільш масштабну та організовану загрозу, що характеризується високим рівнем координації між різними каналами поширення дезінформації, адаптацією тактик до змін в інформаційному середовищі, багатовимірністю наративів. Кіберзагрози виявилися тісно інтегрованими з традиційними формами агресії, при цьому Україна стикається з безпрецедентною інтенсивністю кібератак, що фактично перетворює її на винятковий майданчик відпрацювання методів кібервійни та засобів протидії. Соціальні мережі та месенджери перетворилися на ключові канали інформаційного впливу, експлуатація алгоритмічних особливостей платформ, використання мереж ботів та тролів, поширення дипфейків створюють якісно нові виміри загроз. Досвід повномасштабної війни продемонстрував як еволюцію загроз, так і формування певного імунітету українського суспільства до російської пропаганди через безпосереднє зіткнення з реальністю агресії.

6. Обґрунтування європейської інтеграції як каталізатора трансформації системи інформаційної безпеки України виявило її багатовимірний вплив, що виходить за межі формальної імплементації законодавства. Європейська інтеграція створює одночасно зобов’язання щодо адаптації, можливості для залучення ресурсів та експертизи, стимули для інституційного розвитку, критерії оцінювання прогресу реформ. Гармонізація з правовими рамками ЄС, зокрема імплементація GDPR, NIS2 Directive, інтеграція до Digital Europe Programme, вимагає системних змін у законодавстві, інституційній архітектурі, технічних системах, компетентностях. Формування спільного цифрового простору Україна-ЄС є амбітним завданням, що вимагає надійного кіберзахисту й

бездоганного поводження з даними як ключової умови формування довіри. Трансформаційний вплив охоплює зміну інституційної культури, підходів до балансу між безпекою та свободою інформації, що вимагає адаптації традиційних підходів до національної безпеки при збереженні ефективності протидії специфічним загрозам.

Таким чином, у роботі запропоновано конкретні напрями вдосконалення інформаційної безпеки України в умовах євроінтеграції, що охоплюють удосконалення міжвідомчої координації через розширення повноважень Координаційного центру кібербезпеки, створення постійно діючих робочих груп, розробку Національної стратегії координації. Посилення спроможностей у сфері стратегічних комунікацій передбачає створення Національного центру стратегічних комунікацій, розробку Національної стратегії стратегічних комунікацій, створення системи навчання фахівців, модернізацію технологічної інфраструктури. Підвищення медіаграмотності населення вимагає інтеграції медіаграмотності у освітні плани всіх рівнів підготовки, створення загальнонаціональної ініціативи для дорослого населення, підтримки організацій громадянського суспільства. Поглиблення партнерства з інституціями ЄС передбачає активізацію співпраці з East StratCom Task Force, розвиток партнерства з ENISA, активну участь у спільних проєктах ЄС у сфері кібер- та інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Арістова І. В. Державна інформаційна політика: організаційно-правові аспекти : монографія. Харків : Вид-во Ун-ту внутр. справ, 2000. 368 с.

2. Баезнер М., Робін П. Кібербезпека в сучасному світі: загрози та виклики. Київ : К.І.С., 2018. 156 с.

3. Баранов О. А. Правове забезпечення інформаційної безпеки України : стан та перспективи розвитку : монографія. Київ : Логос, 2022. 252 с.

4. Бьола К., Паммент Дж. Протидія онлайн-пропаганді та екстремізму. Лондон : Рутледж, 2019. 238 с.

5. Гелмус Т., Бодін-Барон Е. Вплив російських соціальних медіа. Санта-Моніка : RAND Corporation, 2018. 338 с.

6. Горбулін В. П. Світова гібридна війна: український фронт : монографія / В. П. Горбулін та ін. ; за заг. ред. В. П. Горбуліна. Київ : НІСД, 2017. 496 с.

7. Горбулін В. П., Додонов О. Г., Ланде Д. В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія. Київ : Інтертехнологія, 2020. 164 с.

8. Довгань О. Д. Національна безпека України: еволюція проблем внутрішньої політики : монографія. Київ : НІСД, 2018. 528 с.

9. Дубов Д. В. Інформаційна безпека в умовах гібридної війни : стратегічні пріоритети та система протидії : монографія. Київ : НІСД, 2019. 223 с.

10. Дубов Д. В., Ожеван М. А., Гнатюк С. Л. Інформаційна безпека: визначення термінів. Київ : Видавництво НАУ, 2020. 432 с.

11. Золотар О. О. Інституційна система кібербезпеки України: проблеми та перспективи. Інформація і право. 2020. № 2 (33). С. 199–208.

12. Золотар О. О. Інформаційна безпека людини: теорія і практика : підручник. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с.

13. Калиновський Ю. Ю. Інституційне забезпечення державної інформаційної політики України : монографія. Київ : НАДУ, 2022. 252 с.

14. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР.

Відомості Верховної Ради України. 1996. № 30. Ст. 141.

15. Литвиненко О. В. Інформаційна політика : монографія. Київ : ВІПОЛ, 2020. 261 с.

16. Лідберг Я. Стратегічні комунікації НАТО. Рига : Центр досконалості НАТО StratCom, 2016. 152 с.

17. Ліпкан В. А. Національна та міжнародна безпека у визначеннях та поняттях. Вид. 2-ге, доп. і перероб. Київ : Текст, 2008. 400 с.

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

19. Макаренко Є. А. Інформаційна безпека : навч. посібник. Київ : Центр учбової літератури, 2021. 280 с.

20. Манойло А. В. Государственная информационная политика в особых условиях : монография. Москва : МИФИ, 2022. 388 с.

21. Марущак А. І. Інформаційна безпека України в контексті євроінтеграційних процесів : монографія. Київ : Вид-во Європ. ун-ту, 2010. 220 с.

22. Марущак А. І. Інформаційний суверенітет у глобальному світі: виклики для України. Політичний менеджмент. 2018. № 4. С. 175–184.

23. Най Дж. М'яка сила у світовій політиці. Нью-Йорк : PublicAffairs, 2004. 191 с.

24. Ожеван М. А. Стратегічні комунікації в системі забезпечення національної безпеки : світовий досвід для України. Стратегічні пріоритети. 2021. № 3 (40). С. 119–130.

25. Ожеван М. А. Стратегічні комунікації у системі забезпечення національної безпеки. Стратегічні пріоритети. 2015. № 4 (37). С. 131–138.

26. Організація Об'єднаних Націй. Доповідь Генерального секретаря щодо розвитку у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки. A/75/172. Нью-Йорк, 21 липня 2020. 18 с.

27. Остроухов В. В. Інформаційна безпека : навч. посібник. Київ : КНТ, 2020. 392 с.

28. Панченко О. А. Інституційне забезпечення інформаційної безпеки України. Стратегічні пріоритети. 2021. № 1 (42). С. 89–96.

29. Петров В. В. Інформаційна безпека: організаційно-правові основи : навч. посібник. Київ : ДП «НВЦ «Євроатлантикінформ», 2009. 316 с.

30. Почепцов Г. Г. Сучасні інформаційні війни. Київ : Видавничий дім «Києво-Могилянська академія», 2021. 497 с.

31. Про Державну службу спеціального зв'язку та захисту інформації України : Постанова Кабінету Міністрів України від 03.09.2014 № 411. Офіційний вісник України. 2014. № 71. Ст. 2003.

32. Про друковані засоби масової інформації (пресу) в Україні : Закон України від 16.11.1992 № 2782-XII. Відомості Верховної Ради України. 1993. № 1. Ст. 1.

33. Про затвердження Положення про Координаційний центр кібербезпеки : Указ Президента України від 07.06.2021 № 225/2021. Офіційний вісник України. 2021. № 48. Ст. 3003.

34. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. Відомості Верховної Ради України. 1994. № 31. Ст. 286.

35. Про інформацію : Закон України від 02.10.1992 № 2657-XII. Відомості Верховної Ради України. 1992. № 48. Ст. 650.

36. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. Відомості Верховної Ради України. 2018. № 31. Ст. 241.

37. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 403.

38. Про Раду національної безпеки і оборони України : Закон України від 05.03.1998 № 183/98-ВР. Відомості Верховної Ради України. 1998. № 35. Ст. 237.

39. 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 № 392/2020. Офіційний вісник України. 2020.

№ 75. Ст. 2417.

40. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. Офіційний вісник України. 2021. № 71. Ст. 4478.

41. Про рішення Ради національної безпеки і оборони України від 24 березня 2021 року «Про Стратегію інформаційної безпеки України» : Указ Президента України від 24.03.2021 № 121/2021. Офіційний вісник України. 2021. № 27. Ст. 1449.

42. 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 № 47/2017. Офіційний вісник України. 2017. № 20. Ст. 540.

43. Про телебачення і радіомовлення : Закон України від 21.12.1993 № 3759-XII. Відомості Верховної Ради України. 1994. № 10. Ст. 43.

44. Резнікова О. О. Координація у сфері національної безпеки та оборони : проблеми та шляхи вирішення. Стратегічні пріоритети. 2021. № 1 (49). С. 78–89.

45. Рущенко І. П. Російсько-українська гібридна війна: погляд соціолога : монографія. Харків : ФОП Павленко О. Г., 2021. 268 с.

46. Соловйов С. Г., Остапенко Г. Л. Інформаційна безпека України : монографія. Київ : Арістей, 2007. 222 с.

47. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. Ратифіковано Законом України від 16.09.2014 № 1678-VII. Офіційний вісник України. 2014. № 75. Ст. 2125.

48. Флоріді Л. Боротьба за цифровий суверенітет: що це таке і чому це важливо для ЄС. Philosophy & Technology. 2020. Vol. 33. P. 369–378.

49. Шеломенцев В. П. Інформаційна безпека та інформаційний суверенітет в умовах глобалізації. Стратегічні пріоритети. 2013. № 4 (29). С. 199–204.

50. Rid T. Active Measures: The Secret History of Disinformation and Political Warfare. New York : Farrar, Straus and Giroux, 2020. 528 p.

51. Bjola C., Pamment J. Countering Online Propaganda and Extremism: The Dark Side of Digital Diplomacy. Abingdon : Routledge, 2020. 238 p.

52. Bodine-Baron E., Helmus T. C., Radin A., Treyger E. Countering Russian Social Media Influence. Santa Monica : RAND Corporation, 2021. 84 p.

53. Bradshaw S., Howard P. N. The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation. Oxford : Oxford Internet Institute, 2020. 26 p.

54. Brattberg E., Maurer T. Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks. Washington : Carnegie Endowment for International Peace, 2020. 42 p.

55. Conley H. A., Stefanov R., Vladimirov M., Mina L. The Kremlin Playbook 2: The Enablers. Washington : Center for Strategic and International Studies, 2021. 78 p.

56. European Commission. Action Plan against Disinformation. JOIN(2018) 36 final. Brussels, 5.12.2021. 10 p.

57. European Commission. Assessment of the Code of Practice on Disinformation: Achievements and areas for further improvement. SWD(2020) 180 final. Brussels, 10.9.2020. 34 p.

58. European Commission. Communication on Tackling online disinformation: a European Approach. COM(2018) 236 final. Brussels, 26.4.2021. 13 p.

59. European Commission. Guidance on Strengthening the Code of Practice on Disinformation. COM(2021) 262 final. Brussels, 26.5.2021. 24 p.

60. European Commission. Tackling online disinformation: a European Approach. COM(2018) 236 final. Brussels, 26.4.2018. 13 p.

61. European External Action Service. Questions and Answers about the East StratCom Task Force. Brussels : EEAS, 2021. 15 p.

62. European Union. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act). Official Journal of the European Union. L 277. 27.10.2022. P. 1–102.

63. Helmus T. C., Bodine-Baron E., Radin A. et al. Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe. Santa Monica : RAND Corporation, 2021. 338 p.

64. Jankowicz N., Hindelang M., Bialy O. et al. Malign Creativity: How Gender, Sex, and Lies are Weaponized Against Women Online. Washington : The Wilson Center, 2021. 89 p.

65. Lanoszka A. Disinformation in International Politics. European Journal of International Security. 2021. Vol. 4. Issue 2. P. 227–248.

66. Lucas E., Pomeranzev P. Winning the Information War: Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe. Washington : CEPA, 2022. 54 p.

67. NATO Strategic Communications Centre of Excellence. Analysis of Russia's Information Campaign Against Ukraine. Riga : NATO StratCom COE, 2022. 77 p.

68. Nimmo B. TrollTracker: How Russia Hacks Narratives. Digital Forensic Research Lab, 2021. 23 p.

69. Pamment J., Nothhaft H., Agardh-Twetman H., Fjällhed A. Countering Information Influence Activities: The State of the Art. Lund : Lund University, 2020. 112 p.

70. Polyakova A., Boyer S. The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition. Washington : Brookings Institution, 2020. 45 p.

71. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union. L 119. 4.5.2016. P. 1–88.

72. Schneier B. Click Here to Kill Everybody: Security and Survival in a Hyper-connected World. New York : W. W. Norton & Company, 2020. 288 p.

73. Thornton R., Karagiannopoulos M. The Russian Information Warfare Construct. London : The RUSI Journal, 2020. Vol. 161. Issue 1. P. 62–68.

74. Wardle C., Derakhshan H. Information Disorder: Toward an interdisciplinary framework for research and policymaking. Strasbourg : Council of Europe, 2021. 107 p.

АНОТАЦІЯ

Михайловський І. О. Трансформація системи інформаційної безпеки України в умовах європейської інтеграції (магістерська робота). Харків: Харківський національний університет імені В. Н. Каразіна, 2025. 108 с. (рукопис).

Мета дослідження полягає у визначенні нормативно-правових та стратегічних засад функціонування системи інформаційної безпеки України, розкритті інституційної системи забезпечення інформаційної безпеки, виявленні сучасних викликів і загроз, а також визначенні пріоритетних інституційних та технологічних напрямів трансформації системи інформаційної безпеки України в умовах європейської інтеграції.

Об’єктом дослідження є система забезпечення інформаційної безпеки України в контексті європейської інтеграції. Предметом дослідження є трансформація системи інформаційної безпеки України під впливом європейських інтеграційних процесів.

У першому розділі розглянуто теоретико-методологічні засади дослідження інформаційної безпеки України. Проаналізовано понятійний апарат та еволюцію концепту інформаційної безпеки, визначено основні підходи до її забезпечення у сучасних міжнародних відносинах та окреслено нормативно-правові рамки у сфері інформаційної безпеки.

У другому розділі здійснено інституційно-аналітичний аналіз системи забезпечення інформаційної безпеки України. Розкрито структуру органів управління у сфері інформаційної безпеки, механізми координації державних інституцій, роль міжнародних організацій та виявлено ключові проблеми функціонування національної системи інформаційної безпеки в умовах зовнішніх і внутрішніх викликів.

У третьому розділі визначено перспективні напрями трансформації системи інформаційної безпеки України з урахуванням європейського досвіду. Сформульовано стратегічні підходи до підвищення ефективності державної політики у сфері інформаційної безпеки, впровадження технологічних рішень, посилення міжвідомчої взаємодії та гармонізації української нормативної бази зі стандартами Європейського Союзу.

Ключові слова: безпека, дезінформація, інформаційна безпека, інформаційний простір, координація, комунікація, нормативне регулювання, ризики, стратегія, трансформація.

ANNOTATION

Mykhailovskyi I. O. Transformation of Ukraine's Information Security System in the Context of European Integration (Master's thesis). Kharkiv: V. N. Karazin Kharkiv National University, 2025. 108 p. (manuscript).

The aim of the research is to determine the regulatory and strategic foundations for the functioning of Ukraine's information security system, to reveal the institutional structure of information security, to identify current challenges and threats, and to define priority institutional and technological directions for transforming the information security system of Ukraine in the context of European integration.

The object of the study is the system of ensuring information security of Ukraine in the context of European integration.

The subject of the study is the transformation of Ukraine's information security system under the influence of European integration processes.

The first section presents the theoretical and methodological foundations for studying information security in Ukraine. It analyses the conceptual framework and evolution of the notion of information security, defines the main approaches to information security in modern international relations, and outlines the legal and regulatory framework in this field.

The second section provides an institutional and analytical examination of Ukraine's information security system. It reveals the structure of governance bodies in the field of information security, mechanisms of interagency coordination, the role of international organisations, and identifies current problems in the functioning of the national information security system under internal and external challenges.

The third section identifies promising directions for transforming Ukraine's information security system, taking into account European experience. It formulates strategic approaches to increasing the effectiveness of state policy, introducing technological solutions, enhancing interagency interaction, and harmonising Ukraine's legal framework with European Union standards.

Keywords: communication, coordination, information security, information space, normative regulation, risks, security, strategic transformation, threats.

ВІДГУК

на кваліфікаційну роботу магістра
студента 2-го курсу групи УМІБ-61 денної форми навчання
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
освітньо-професійної програми «Міжнародна інформаційна безпека»
Навчально-наукового інституту «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Харківського національного університету імені В. Н. Каразіна
Михайловського Дмитра Олександровича
на тему: «Трансформація інформаційної безпеки України в контексті європейської інтеграції»

Магістерська кваліфікаційна робота Михайловського Дмитра Олександровича присвячена вивченню процесів трансформації системи інформаційної безпеки України відповідно до європейських стандартів і практик. Актуальність дослідження визначається новими викликами у сфері захисту інформаційного простору, необхідністю протидії зовнішньому інформаційному впливу та потребою адаптації національного законодавства до вимог європейського правового поля. Автор робить акцент на значенні інформаційної безпеки як складової державної політики в умовах європейської інтеграції.

Робота містить логічно побудовану структуру. У першому розділі подано теоретичне обґрунтування поняття інформаційної безпеки, розглянуто етапи її розвитку в Україні та проаналізовано основні підходи до формування політики у цій сфері. У другому розділі проаналізовано європейські механізми та нормативні акти у сфері інформаційної безпеки, висвітлено практику Європейського Союзу щодо регулювання цифрових послуг, протидії дезінформації та забезпечення захисту персональних даних. Третій розділ присвячено оцінці можливостей запровадження європейських підходів в Україні, окреслено перспективи розвитку національної системи інформаційної безпеки, визначено пріоритетні напрями її модернізації.

Оцінка отриманих результатів свідчить, що мета дослідження досягнута, а

поставлені завдання реалізовано. Автор узагальнив широкий спектр документів та практик Європейського Союзу, продемонстрував вміння порівнювати національні та європейські підходи, сформулював висновки, які відповідають предмету і завданням роботи. Запропоновані рекомендації мають прикладний характер та можуть бути використані у процесі вдосконалення державної політики України у сфері інформаційної безпеки.

Разом з тим, доцільно було б ширше застосувати практичні кейси співпраці України з окремими європейськими інституціями та надати кількісні показники для оцінки ефективності впроваджених заходів. Це могло б посилити аналітичний компонент дослідження, однак зауваження має рекомендаційний характер і не впливає на загальну позитивну оцінку роботи.

Магістерська кваліфікаційна робота Михайловського Дмитра Олександровича відповідає вимогам до кваліфікаційних робіт другого (магістерського) рівня вищої освіти, відзначається структурною завершеністю, послідовністю викладу та актуальністю досліджуваної проблематики. Роботу можна рекомендувати до захисту перед екзаменаційною комісією.

Науковий керівник:

д. держ. упр., професор,

професор кафедри міжнародних відносин Солових В. П.

РЕЦЕНЗІЯ

на кваліфікаційну роботу магістра
студента 2-го курсу групи УМІБ-61 денної форми навчання
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
освітньо-професійної програми «Міжнародна інформаційна безпека»
Навчально-наукового інституту «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Харківського національного університету імені В.Н. Каразіна
Михайловського Костянтина Сергійовича
на тему: «Трансформація інформаційної безпеки України в контексті європейської інтеграції»

1. Актуальність теми

Тема, обрана автором, відповідає сучасним викликам національної безпеки України та динаміці європейських інтеграційних процесів. У роботі коректно зазначено, що цифровізація суспільного життя, поширення гібридних впливів та ускладнення структури інформаційного простору суттєво посилюють потребу в перегляді і оновленні національної системи інформаційної безпеки. Європейський Союз, який формує багаторівневу нормативно-інституційну архітектуру у сфері інформаційної політики, виступає ключовим орієнтиром для України у процесі адаптації до стандартів і практик, що регулюють захист інформаційного середовища. У цьому контексті дослідження трансформацій інформаційної безпеки України під впливом європейської інтеграції є цілком обґрунтованим і відповідає запитам державної політики.

2. Характеристика якості виконання розділів роботи

Структура дослідження є логічною та відповідає вимогам до магістерських робіт: вступ, три розділи, висновки, список джерел. Змістовне наповнення засвідчує системну роботу з нормативними, аналітичними та науковими матеріалами, зокрема законами України, документами ЄС і практиками інституцій, відповідальних за інформаційну та кібербезпеку.

Перший розділ присвячено теоретичним основам інформаційної безпеки держави та етапам її становлення в Україні. Автор здійснює послідовний огляд базових понять, розглядає інформаційну безпеку у взаємозв'язку з національною та міжнародною безпекою, а також аналізує підходи, представлені в українській та зарубіжній літературі.

Другий розділ містить аналіз системи інформаційної безпеки України та її інституційного забезпечення. У роботі розглянуто діяльність ключових органів – РНБО, Держспецзв'язку, Міністерства оборони, Центру стратегічних комунікацій, а також проаналізовано нормативні акти та загрози, що постали перед Україною в умовах гібридної агресії.

Третій розділ присвячений впливу європейської інтеграції на трансформацію української інформаційної безпеки. Автор розглядає європейські нормативні рамки – Digital Services Act, GDPR, регламенти щодо кіберстійкості, стратегії ЄС з боротьби з дезінформацією — та аналізує можливості їх імплементації в українську правову базу.

3. Ступінь обґрунтованості висновків

Висновки відповідають логіці дослідження та відображають основні результати проведеної роботи. Автор виокремлює ключові чинники трансформації системи інформаційної безпеки України, зокрема нормативне наближення до європейських стандартів, інституційну модернізацію та необхідність адаптації до гібридних загроз. Узагальнення зроблено коректно, на основі фактичного матеріалу і структурного аналізу.

4. Позитивні сторони роботи

Кваліфікаційна робота Михайловського Костянтина Сергійовича вирізняється логічною структурою, цілісністю викладу та системністю підходу до аналізу проблематики інформаційної безпеки. Автор упевнено використовує широку джерельну базу, що включає нормативні документи Європейського Союзу, акти українського законодавства та сучасні наукові дослідження у сфері міжнародної та інформаційної безпеки. Позитивним є також поєднання теоретичних положень із практичними аспектами державної політики, що дозволяє повніше оцінити трансформацію української системи інформаційної безпеки під впливом європейської інтеграції. Робота демонструє здатність автора узагальнювати значний масив інформації, виділяти ключові тенденції та формулювати обґрунтовані висновки та рекомендації.

5. Недоліки роботи

Водночас у роботі простежуються певні обмеження, що пов'язані з недостатнім рівнем порівняльного аналізу між українськими та європейськими моделями забезпечення інформаційної безпеки. Частина практичних пропозицій подана у дещо загальному вигляді і могла б бути розширена шляхом конкретизації механізмів реалізації. Крім того, у дослідженні бракує детальнішого аналізу ризиків і потенційних бар'єрів імплементації європейських інструментів інформаційної та кібербезпеки в українське законодавче і інституційне середовище. Проте ці недоліки не мають суттєвого впливу на загальну якість роботи і не зменшують її наукової та практичної цінності.

6. Загальна оцінка кваліфікаційної роботи

Кваліфікаційна робота Михайловського Костянтина Сергійовича відповідає встановленим вимогам до магістерських досліджень спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії». Дослідження виконано на належному теоретичному та аналітичному рівнях, містить практичні висновки та демонструє вміння автора працювати з комплексними нормативно-правовими матеріалами. Робота заслуговує на позитивну оцінку, а її автор – на присвоєння кваліфікації магістра.

Рецензент:
доктор історичних наук, професор,
професор кафедри світової політики,
дипломатії та туристичного бізнесу
ННІ «Каразинський інститут міжнародних відноси
та туристичного бізнесу» Харківського національн
університету імені В.Н. Каразіна С.І. Лиман