КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
ФАКУЛЬТЕТ УКРАЇНСЬКОЇ ФІЛОЛОГІЇ КУЛЬТУРИ І МИСТЕЦТВА

Кафедра інформаційних комунікацій

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ О. А. Політова
«13» травня 2026 р.

КВАЛІФІКАЦІЙНА (БАКАЛАВРСЬКА) РОБОТА

на тему:

ФОРМУВАНИЯ КУЛЬТУРИ ІНФОРМАЦІЙНОЇ ГІГІЄНИ ГРОМАДЯН ЯК ЕЛЕМЕНТ БЕЗПЕКИ ДЕРЖАВИ

випускника першого (бакалаврського) рівня освіти

Виконала:
Студентка 4-го курсу, групи ІБАС6-1-22-40д
Перетятко Анастасія Михайлівна

Науковий керівник:
Завідувач кафедри інформаційних комунікацій, кандидат історичних наук
Політова Олена Аркадіївна

Цим підписом засвідчую, що поданий на захист рукопис та електронний документ є ідентичний
10.06.2026

2026

ЗМІСТ

ВСТУП

Актуальність теми дослідження. В умовах переходу суспільства до інформаційної ери та тривалої гібридної агресії проти України, кіберпростір та медіасередовище перетворилися на повноцінний театр бойових дій. Традиційні методи захисту державного суверенітету виявляються недостатніми перед обличчям масштабних інформаційно-психологічних операцій (ІПСО), розповсюдження дезінформації через нерегульовані месенджери та використання новітніх технологій генеративного штучного інтелекту (діпфейків). За таких умов виключно державні заборони втрачають свою ефективність. Інформаційна безпека держави сьогодні нерозривно пов’язана з когнітивною стійкістю її громадян.

Попри значні кроки у вдосконаленні вітчизняного законодавства, зокрема прийняття Закону України «Про медіа», в інформаційному полі залишаються суттєві прогалини. Масовий перехід аудиторії до споживання новин через анонімні соціальні мережі (насамперед Telegram) створює ідеальне середовище для маніпуляцій масовою свідомістю. Саме це актуалізує необхідність переходу від моделі пасивного споживання інформації до проактивного формування культури медіаграмотності на всіх рівнях суспільства.

Тому формування високого рівня культури інформаційної гігієни, розвиток критичного мислення та впровадження надійних алгоритмів цифрового захисту (систем електронного документообігу, кібергігієни персоналу) на рівні кожної окремої установи є надзвичайно нагальною проблемою. Дослідження практичних аспектів захисту інформаційного простору, ролі освітніх закладів та бібліотек у цьому процесі є запорукою забезпечення загальнонаціональної інформаційної стійкості та збереження суверенітету України, що й зумовлює актуальність даного дослідження.

Стан розробки проблеми. Проблематика інформаційної політики, безпеки та медіаграмотності є предметом вивчення багатьох вітчизняних та зарубіжних науковців. Фундаментальні засади державної інформаційної політики закладені у працях Г. Почепцова та С. Чукут [22]. Питання інформаційних війн, гібридних загроз та механізмів когнітивного захисту ґрунтовно досліджувалися Д. Кулебою [14], З. М. Бржевською, Н. М. Довженко та Р. В. Киричком [8]. Практичні аспекти ідентифікації маніпуляцій та фейків у сучасних медіа розкриті у дослідженнях О. В. Курбана [15]. Технологічні виклики кібербезпеки в епоху штучного інтелекту розглядаються в роботах О. Лунгола та А. Ільєнка [16]. Незважаючи на ґрунтовну теоретичну базу, стрімкий розвиток цифрових технологій та перехід аудиторії до анонімних месенджерів вимагають постійного оновлення методології захисту та розробки нових практичних рекомендацій, що зумовлює вибір теми даної бакалаврської роботи.

Мета дослідження полягає у комплексному дослідженні інформаційної гігієни як невід'ємної складової державної інформаційної політики та національної безпеки України, а також у розробці практичних рекомендацій щодо підвищення інформаційної стійкості громадян і персоналу сучасних установ в умовах гібридних загроз.

Завдання дослідження. Для досягнення поставленої мети було визначено та вирішено такі завдання:

- розкрити теоретико-методологічні засади поняття інформаційної гігієни та дослідити еволюцію новітніх загроз, зокрема вплив технологій штучного інтелекту на інформаційний простір.
- проаналізувати стан нормативно-правового забезпечення державної інформаційної політики України в умовах воєнного стану.

- дослідити вплив гібридної агресії на суспільну свідомість шляхом аналізу статистичних даних медіаспоживання та індексу медіаграмотності.
- охарактеризувати роль публічних бібліотек та громадсько-державних ініціатив у процесі формування цифрової грамотності населення.
- розробити комплекс універсальних практичних рекомендацій щодо вдосконалення електронного документообігу, кібергігієни персоналу та оптимізації комунікаційних процесів у сучасних установах.

Об'єкт дослідження - національна інформаційна безпека України в умовах глобальної цифровізації та гібридної війни.

Предмет дослідження - формування культури інформаційної гігієни серед громадян та механізми практичного захисту інформаційного середовища сучасних установ і організацій.

Методи дослідження. Для вирішення поставлених завдань у роботі використано комплекс загальнонаукових та спеціальних методів:

- метод аналізу та синтезу (для опрацювання наукової літератури та нормативно-правових актів);
- системний метод (для розгляду складових інформаційної гігієни як єдиної структури);
- метод порівняння (при дослідженні еволюції загроз від традиційних фейків до ШІ);
- статистичний метод (для обробки та узагальнення кількісних даних щодо медіаспоживання та рівня медіаграмотності населення);
- метод моделювання (при розробці практичних рекомендацій щодо впровадження СЕД та кібергігієни персоналу).

Інформаційна база дослідження включає Конституцію України, чинні законодавчі та нормативно-правові акти (Закони України «Про інформацію»,

«Про доступ до публічної інформації», «Про медіа», «Про національну безпеку»), Укази Президента України (Стратегія інформаційної безпеки), актуальні статистичні звіти та соціологічні опитування (USAID-Internews, ГО «Детектор медіа»), аналітичні матеріали Центру протидії дезінформації при РНБО, а також внутрішні регламентні документи установ.

Новизна отриманих результатів. У дослідженні набуло подальшого розвитку розуміння сутності інформаційної гігієни, яку адаптовано до реалій використання генеративного штучного інтелекту (діпфейків); обґрунтовано необхідність застосування принципу «нульової довіри» в освітньому процесі. Вперше комплексно систематизовано синергію між державним регулюванням, проєктами протидії дезінформації та діяльністю публічних бібліотек. Також узагальнено універсальну модель формування «цифрової броні» (на основі СЕД, КЕП та систем OCR), яка довела визначальний вплив особистої інформаційної культури керівника на безпеку установи.

Практичне значення отриманих результатів. Результати дослідження мають високий ступінь готовності до використання як на інституційному, так і на загальносуспільному рівнях.

З інституційного погляду, розроблені авторські рекомендації (зокрема щодо оновлення інструкцій з діловодства в частині заборони використання відкритих месенджерів та обмежень ШІ, впровадження симуляційних фішингових тренінгів для персоналу, створення адаптаційних курсів з кібергігієни) є універсальними інструментами. Вони можуть бути безпосередньо впроваджені в операційну діяльність закладів вищої освіти, державних структур та приватних компаній з метою посилення захисту електронного документообігу.

З суспільного погляду, висновки та матеріали дослідження становлять значну практичну цінність для пересічних громадян. Узагальнені підходи до ідентифікації маніпуляцій, ІПСО та згенерованих нейромережами діпфейків

можуть використовуватися як методична база для просвітницьких програм, бібліотечних курсів та ініціатив з підвищення медіаграмотності населення. Сформована концепція інформаційної гігієни має довгостроковий характер: вона є життєво необхідною для захисту свідомості громадян не лише в умовах поточної гібридної війни, але й залишатиметься критично актуальною у мирний час, гарантуючи безпечне та усвідомлене функціонування суспільства у глобальному цифровому світі.

Апробація результатів дослідження. Основні теоретичні та практичні положення бакалаврського дослідження обговорювалися під час проходження фахових практик і конференцій та були опубліковані у вигляді наукових статтей:

- Перетятко А. Інформаційна стійкість України: синергія державної політики та культури інформаційної гігієни громадян // Громадська думка. 2026. № 1-2. С. 13-17.
- Перетятко А. Аналіз сучасної інформаційної політики України: виклики, рішення та стратегічні перспективи // Студії з інформаційної науки, соціальних комунікацій та філології в сучасному світі: зб. наук. конф. МДУ, 2025. С. 384-389.

Структура бакалаврської роботи. Робота складається зі вступу, трьох розділів (які містять підрозділи), загальних висновків, списку використаних джерел та додатків. Загальний обсяг роботи становить 71 сторінки.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ ГІГІЄНИ ТА БЕЗПЕКИ

1.1. Поняття, сутність та складові інформаційної гігієни в умовах сучасних викликів

У XXI столітті стрімкий розвиток інформаційно-комунікаційних технологій та перехід людства від індустріальної до інформаційної ери докорінно змінили структуру суспільних відносин. Інформація перетворилася на ключовий стратегічний ресурс, що зумовило необхідність формування нових підходів до управління нею. У цьому контексті фундаментальним підґрунтям для розуміння процесів взаємодії людини з даними виступає поняття «інформаційна політика», яка є базою для формування інформаційної гігієни у суспільства.

Якщо проаналізувати зарубіжний науковий дискурс, стає очевидно, що еволюція підходів до трактування цього явища: від суто технічного управління даними до розуміння інформаційної політики як інструменту влади. У західній науковій думці базовим вважається підхід британського дослідника. У своїх дослідженнях з інформаційного менеджменту він пропонує розглядати інформаційну політику як багаторівневу систему формальних та неформальних правил, які обмежують, заохочують або іншим чином цілеспрямовано формують інформаційні потоки в межах певної інституції чи держави [28].

Проте найбільш вагомий внесок у сучасну концептуалізацію цього терміна зробила видатна американська дослідниця Сандра Браман (Sandra Braman). У своїй фундаментальній праці «Зміна стану: інформація, політика та влада» (Change of State: Information, Policy, and Power, 2006), виданій Массачусетським технологічним інститутом (MIT Press), вона доводить, що в сучасному світі інформаційна політика вже не є просто вузькою галуззю права. С. Браман значно розширює це поняття, визначаючи його як глобальну макросистему законів, доктринальних позицій та усталених політичних практик, що стосуються всього

життєвого циклу інформації: її створення, обробки, доступу та використання [27]. За її концепцією, саме інформаційна політика визначає архітектуру суспільства та межі влади у XXI столітті, що робить інформаційну гігієну невід'ємною частиною державотворення.

В українській науці акцент традиційно робиться на державотворчому та безпековому аспектах, що об'єктивно зумовлено складними геополітичними реаліями та тривалим перебуванням країни в епіцентрі безперервних інформаційних війн. Вітчизняні дослідники, зокрема Г. Почепцов та С. Чукут, трактують державну інформаційну політику як системну управлінську стратегію органів влади, головним завданням якої є впорядкування національного інфопростору та захист стратегічних інтересів держави [22]. Іншими словами, вчені наголошують, що держава має виступати не пасивним спостерігачем, а активним «архітектором» комунікацій: вона повинна встановлювати прозорі правила гри для медіа, формувати власні національні наративи та будувати інституційні бар'єри проти ворожої пропаганди. У їхніх працях прослідковується чітка проблематика: вразливість масової свідомості до зовнішніх маніпуляцій та систематичних інформаційно-психологічних операцій (ІПСО). Як один з основних варіантів вирішення проблеми вони пропонують розбудову потужної системи державних стратегічних комунікацій та перехід до проактивної захисної моделі, де інформація розглядається як стратегічна «зброя» та інструмент забезпечення національного суверенітету.

В свою чергу, В. Негодченко розглядає її як сукупність напрямів і способів реалізації правових та організаційних заходів, метою яких є вплив на інформаційний простір для досягнення суспільно корисного результату [20]. Основна проблема, яку виділяє даний науковець та його колеги-правознавці - це фрагментарність правового поля та відсутність єдиного інституційного механізму протидії зовнішній інформаційній експансії. Вирішення цієї проблеми українські

дослідники вбачають у жорсткій законодавчій регламентації інформаційних потоків, цензуруванні відверто ворожого контенту та посиленні ролі силових структур у моніторингу медіапростору.

Якщо порівняти підходи вітчизняних дослідників із західними концепціями (зокрема, І. Роулендса та С. Браман), можна простежити як концептуальні збіги, так і фундаментальні відмінності у розстановці акцентів. Спільною рисою є розуміння інформації як ключового ресурсу влади у XXI столітті: обидві наукові школи погоджуються, що управління потоками даних є фундаментом сучасної політики, а неконтрольований інформаційний простір становить загрозу. Проте проблематика та пропоновані рішення різняться радикально через різний історичний контекст.

Західна наукова думка досліджує інформаційну політику переважно через макроекономіку, захист приватності (Data Privacy), авторське право та глобальне управління, намагаючись знайти ідеальний баланс між державним контролем і демократичною свободою слова. Західні рішення тяжіють до розбудови відкритої інфраструктури та ліберального регулювання.

Натомість українська наукова парадигма, сформована в умовах екзистенційної загрози та гібридної агресії, є значно прагматичнішою і має яскраво виражений оборонний (мілітаризований) характер. Вітчизняні вчені розглядають інформаційний простір насамперед як поле бою. Відповідно, якщо іноземні науковці вирішують проблеми оптимізації економіки даних, то українські - проблеми фізичного та когнітивного виживання нації. Це зумовлює те, що в українському дискурсі на перший план виходить саме концепт інформаційної безпеки та гігієни: створення надійних захисних бар’єрів, протидія дезінформації та формування стійкості суспільства як елемента національної оборони.

Проте в умовах сучасних викликів - глобальної цифровізації та тривалої гібридної війни - ефективність інформаційної політики не може забезпечуватися виключно державним регулюванням. На перший план виходить здатність самого суспільства свідомо споживати та фільтрувати контент, що концептуалізується через поняття «інформаційна гігієна».

Інформаційну гігієну доцільно трактувати як систему знань, навичок та поведінкових установок особистості, спрямованих на безпечне споживання, обробку та поширення інформації, а також захист власної свідомості від деструктивних інформаційних впливів. Як зазначає Д. Кулеба у своїй праці «Війна за реальність», сучасне протистояння ведеться не лише за території, а й за свідомість громадян, де вміння розрізняти правду і фейки стає базовою умовою виживання [14].

Спираючись на дослідження З. М. Бржевської, Н. М. Довженко та Р. В. Киричка, присвячені проблемам інформаційних війн, можна стверджувати, що загрози в інформаційному просторі зазнали безпрецедентної еволюції [8]. Якщо на ранніх етапах розвитку цифрового суспільства небезпека зводилася переважно до технічного зламу апаратних чи програмних систем - таких як масовані DDoS-атаки на державні сервери, дефейсмент (візуальна підміна) офіційних веб-сайтів, розповсюдження комп’ютерних вірусів, програм-шифрувальників та пряме викрадення баз даних, то сьогодні вектор атаки докорінно змінився.

В нинішніх умовах гібридного протистояння основною мішенню є не комп’ютерні мережі, а безпосередньо людська психіка, емоції та когнітивна сфера громадян. Замість зламу систем захисту агресор застосовує масштабний «соціальний інжиніринг» та алгоритмічні маніпуляції: створення гіпереліптичних діпфейків (Deepfakes) за допомогою штучного інтелекту, клонування голосу публічних діячів, застосування армій ботів для штучного розпалювання суспільної паніки (астротурфінг), а також алгоритмічний

мікротаргетинг дезінформації через нерегульовані соціальні платформи та месенджери.

Відповідно до цих кардинальних змін, сутність інформаційної гігієни також вийшла за вузькі межі простої «комп'ютерної грамотності» (яка раніше обмежувалася базовим вмінням встановити антивірус чи використовувати складний пароль). Сьогодні вона трансформувалася у складний когнітивний захисний механізм. Сучасна інформаційна гігієна вимагає від особистості навичок критичного мислення, емоційної стійкості, розуміння механізмів роботи генеративних нейромереж та здатності верифікувати першоджерела в умовах агресивного інформаційного середовища.

Узагальнюючи погляди науковців (зокрема О. В. Курбана щодо ідентифікації фейків у сучасних медіа [15]), у структурі інформаційної гігієни в умовах сучасних викликів можна виокремити три базові складові:

- когнітивно-аналітична складова: передбачає наявність розвиненого критичного мислення, здатності до аналізу джерел інформації, виявлення логічних хиб, емоційних маніпуляцій та пропагандистських наративів.
- технологічна (цифрова) складова: включає розуміння принципів роботи алгоритмів соціальних мереж, методів поширення вірусного контенту, а також обізнаність щодо новітніх загроз, таких як технології генеративного штучного інтелекту (діпфейки, клонування голосу, автоматизовані ботоферми). Як зазначається у дослідженнях О. Лунгола та А. Ільєнка, інтеграція штучного інтелекту змінює ландшафт кібербезпеки, вимагаючи від користувачів нових технічних знань для верифікації контенту [11].
- поведінкова складова: відображається у практичному застосуванні принципу «нульової довіри» до емоційно забарвлених повідомлень,

навичці перевіряти сенсаційну інформацію через офіційні державні першоджерела та відповідальному ставленні до поширення (репостів) неперевірених даних.

Отож, у сучасному вимірі інформаційна гігієна перестала бути виключно питанням особистої обізнаності окремого індивіда. Вона набула ознак системного суспільного явища і виступає критично важливим елементом забезпечення інформаційної стійкості держави.

Підсумовуючи вищевикладене, варто зазначити, що теоретико-методологічна база дослідження інформаційної гігієни є доволі широкою, проте вона потребує постійної актуалізації. Зважаючи на стрімкий розвиток цифрових технологій, трансформацію методів когнітивного впливу та еволюцію інструментів штучного інтелекту, існує об’єктивна необхідність у проведенні подальших наукових досліджень. Зокрема, глибокого вивчення потребують механізми адаптації традиційних правил медіаграмотності до нових технологічних реалій, що дозволить розробити більш ефективні стратегії захисту національного інформаційного простору.

1.2. Інформаційна безпека як невід’ємна складова національної безпеки України

В умовах глобалізації, стрімкого розвитку цифрових комунікацій та тривалої гібридної агресії, традиційні уявлення про безпеку держави зазнали докорінної трансформації. Інформаційний простір перестав бути виключно допоміжним середовищем для передачі даних, перетворившись на повноцінний театр бойових дій. Відповідно, інформаційна безпека виокремилася у самостійну та критично важливу складову національної безпеки України.

Як зазначається у вітчизняному науковому дискурсі, інформаційна безпека держави є станом захищеності її життєво важливих інтересів в інформаційній

сфері, за якого забезпечується сталий розвиток суспільства, надійне функціонування інформаційної інфраструктури та протидія деструктивним інформаційним впливам [9].

Зокрема, у своєму фундаментальному дослідженні В. Л. Бурячок детально аналізує архітектуру захисту критичної інфраструктури. На конкретних прикладах автор доводить, що державна система кібернетичної безпеки має гарантувати так звану «тріаду безпеки»: цілісність, конфіденційність та доступність стратегічно важливих даних. Його дослідження фокусується на запобіганні технічним загрозам - унеможливленні хакерського втручання в роботу державних електронних реєстрів, систем управління енергетичним сектором, банківських мереж та урядового зв'язку. Тобто, на цьому рівні безпека розглядається переважно як захист «заліза» та програмного забезпечення від кібертероризму.

Однак еволюція гібридної війни показала, що технічного захисту інфраструктури вже недостатньо. Спираючись на апаратний фундамент, про який зазначають фахівці з кібербезпеки, варто розуміти, що вектор агресії суттєво змістився. У сучасному контексті національна інформаційна безпека формується не лише за рахунок криптографічного захисту державних таємниць чи побудови файрволів (мережевих екранів) навколо комп’ютерних мереж.

Сьогодні критично важливим стає когнітивний вимір безпеки - захист масової свідомості громадян. Найбільш руйнівні наслідки для держави нині несе не злам урядового сервера, а успішно реалізована інформаційно-психологічна операція (ІПСО), яка здатна спровокувати паніку, недовіру до інституцій або розкол у суспільстві. Відповідно, безпека держави сьогодні залежить від того, наскільки суспільство здатне протистояти глибинним фейкам, цілеспрямованій дезінформації та маніпуляціям, що поширюються через нерегульовані соціальні мережі.

Фундаментальне значення інформаційної безпеки для існування держави закріплено на найвищому законодавчому рівні. Згідно зі статтею 17 Конституції України, захист суверенітету і територіальної цілісності України, а також забезпечення її економічної та інформаційної безпеки визначаються як найважливіші функції держави і є справою всього Українського народу [1].

Це конституційне положення має не лише декларативний, а й глибокий практичний та юридичний характер, тому що законодавець свідомо ставить інформаційну безпеку в один концептуальний ряд із захистом фізичних кордонів (територіальною цілісністю). На практиці це означає, що посягання на національний інформаційний простір розцінюється правовою системою держави як загроза, тотожна збройній агресії. Це формує базовий фундамент для прийняття всіх подальших законів, стратегій національної безпеки та рішень РНБО щодо блокування ворожих медіаресурсів чи санкційної політики.

У законі зустрічається формулювання про те, що це є «справою всього Українського народу», яке встановлює чіткий імператив: забезпечення інформаційного суверенітету не є монопольною відповідальністю виключно силових структур (таких як Служба безпеки України, кіберполіція чи Держспецзв'язок). Ця норма Конституції легітимізує ключову тезу даного дослідження про те, що кожен громадянин, працівник установи, заклад вищої освіти чи публічна бібліотека є повноцінними суб’єктами національної безпеки.

У практичному вимірі застосування цієї статті означає, що в умовах гібридної війни дотримання базових правил інформаційної гігієни, розвиток критичного мислення, верифікація даних та свідоме споживання цифрового контенту перестають бути виключно особистим вибором людини. Вони перетворюються на громадянський обов'язок щодо захисту своєї країни. Отже, без реалізації цього положення на рівні суспільної свідомості успішний захист конституційного ладу стає неможливим, оскільки ворог здатен зруйнувати

державність зсередини, використовуючи інформаційно-психологічний вплив як альтернативу військовому вторгненню.

Базові принципи формування державної політики у цій сфері регулюються Законом України «Про інформацію». У ньому закладено напрями діяльності держави щодо забезпечення доступу до об'єктивної інформації, розбудови національних інформаційних систем, а також створення єдиної системи захисту інформації [3]. Проте нормативно-правова база, сформована переважно у мирний час, потребує постійної адаптації до викликів воєнного стану.

Дослідження еволюції стратегічного планування України в інформаційній сфері дозволяє виділити перехід від пасивної оборони до концепції проактивної стійкості. Указом Президента України у 2021 році було введено в дію «Стратегію інформаційної безпеки», розраховану до 2025 року. Документ окреслив ключові цілі: захист інформаційного простору, протидію незаконному контенту та підвищення медіаграмотності [24]. Водночас аналіз реалізації цієї стратегії в умовах повномасштабного вторгнення виявив низку вразливостей, зокрема відсутність чітких індикаторів ефективності (KPI) та розрив між масштабом реальних загроз і прописаними механізмами реагування.

Усвідомлення цих викликів зумовило розробку нового циклу планування - проєкту Стратегії інформаційної безпеки до 2030 року. Інноваційність цього документа полягає у зміні самої філософії: впроваджується концепт «інформаційної стійкості суспільства та держави» [13]. Стійкість трактується не просто як здатність відбивати атаки, а як спроможність системи (державних інституцій та громадянського суспільства) швидко адаптуватися до нових викликів та відновлюватися після кризових ситуацій.

Інституційне забезпечення інформаційної безпеки в Україні покладено на багаторівневу систему спеціалізованих державних органів, серед яких ключову координаційну та практичну роль відіграють Рада національної безпеки і оборони

України (РНБО), Центр протидії дезінформації (ЦПД) та Центр стратегічних комунікацій та інформаційної безпеки. Кожна з цих інституцій має чітко визначений функціонал, що дозволяє комплексно протидіяти загрозам.

РНБО виступає головним стратегічним центром, який формує загальний вектор інформаційної оборони. Її функціонал включає координацію всіх силових відомств, прийняття рішень щодо застосування санкцій проти ворожих пропагандистів та юридичне блокування деструктивних медіаресурсів і соціальних платформ на території України.

На оперативно-аналітичному рівні провідну роль відіграє Центр протидії дезінформації (робочий орган РНБО). Його основне завдання полягає у цілодобовому моніторингу національного та глобального інформаційного простору, ранньому виявленні російських інформаційно-психологічних операцій (ІПСО), аналізі ворожих наративів та оперативному спростуванні (дебункінгу) фейків. Практика доводить, що еволюція та розширення функцій ЦПД - від простого пасивного моніторингу до проактивної деанонімізації ворожих мереж (зокрема, розкриття адміністраторів проросійських Telegram-каналів та ботоферм) спільно з кіберполіцією та СБУ - є вкрай дієвим кроком у боротьбі з дезінформацією [7].

Зі свого боку, Центр стратегічних комунікацій та інформаційної безпеки зосереджений на проактивній діяльності, адже його головна функція - не лише відбивати атаки, а й формувати власні, стійкі українські наративи, забезпечувати комунікацію державних органів єдиним голосом («One voice policy») та тісно співпрацювати з громадянським суспільством задля розвитку медіаграмотності. Така розгалужена інституційна архітектура є потужним інструментом захисту інформаційного суверенітету на макрорівні.

Але, незважаючи на активну та масштабну діяльність цих державних структур, вітчизняні та зарубіжні дослідники наголошують: в умовах

демократичного устрою, свободи слова та відкритого доступу до глобальної мережі Інтернет інформаційна безпека не може будуватися виключно на заборонах, блокуваннях та зусиллях державних центрів.

Ворог робить ставку на «війну на виснаження», намагаючись розхитати внутрішню єдність суспільства [8]. За таких обставин державна політика виявляється неефективною, якщо вона не спирається на підтримку свідомого суспільства.

Впевнено можна констатувати, що інформаційна безпека є фундаментальною складовою національної безпеки України, захист якої вимагає комплексного підходу. Успішне протистояння в інформаційній війні можливе лише за умови синергії: поєднання жорсткої інституційної та нормативно-правової рамки держави з «м'якою силою» громадянського суспільства. Саме тому навички медіаграмотності та високий рівень культури інформаційної гігієни кожного окремого громадянина перетворюються з категорії особистого розвитку на категорію державного виживання.

1.3. Трансформація загроз: еволюція від традиційних фейків до технологій штучного інтелекту

Інформаційний простір характеризується надзвичайною динамічністю, що зумовлює постійну еволюцію методів деструктивного впливу на масову свідомість. Якщо на початку гібридної агресії проти України основними інструментами інформаційної війни були традиційні фейки, розповсюджувані через мережі ботоферм, то сьогодні спектр загроз вийшов на принципово новий технологічний рівень.

Досліджуючи еволюцію ворожого інформаційного впливу, вітчизняні науковці, зокрема О. В. Курбан, зазначають, що традиційні фейки в сучасних

медіа здебільшого спиралися на примітивні маніпуляції: вирвані з контексту цитати, постановочні фотографії або тексти з помітними граматичними помилками та русизмами, які виникали внаслідок неякісного машинного перекладу [15]. Протидія таким загрозам базувалася на розвитку базових навичок фактчекінгу - пошуку першоджерела зображення чи аналізі стилістики тексту.

Проте, як було досліджено та систематизовано в ході проходження фахової практики, за останні роки відбувся стрімкий перехід від ручного або напівавтоматичного створення дезінформації до масового застосування технологій генеративного штучного інтелекту (ШІ). Інформаційні атаки змістили свій фокус із технічного зламу комп'ютерних систем на прямий, високотехнологічний вплив на емоції та свідомість пересічних громадян.

Сьогодні алгоритми штучного інтелекту (ШІ) здатні генерувати текст, аудіо та відео практично без візуальних чи смислових недоліків. У своїх дослідженнях українські фахівці О. Лунгол та А. Ільєнко детально вивчають цю подвійну роль нейромереж у сучасному цифровому світі.

З одного боку, у їхніх працях ШІ розглядається як потужний інструмент для захисту. Дослідники описують, як сучасні алгоритми допомагають будувати надійні системи кібербезпеки: вони здатні блискавично аналізувати величезні обсяги мережевого трафіку, виявляти аномалії, блокувати спам та автоматично розпізнавати хакерські атаки швидше, ніж це зробила б людина.

З іншого боку, автори наголошують на критичній проблемі: ці ж самі технології, потрапивши до рук зловмисників, перетворюються на справжню зброю масового інформаційного ураження [11].

На практиці це означає повну автоматизацію процесів створення дезінформації, бо якщо раніше написання фішингових (шахрайських) листів чи продукування фейкових новин для ботоферм вимагало значного часу та залучення «живих» людей (тролів), які часто робили граматичні чи стилістичні

помилки, то зараз генеративні ШІ-моделі (на зразок ChatGPT) здатні за секунди створювати тисячі унікальних, бездоганно написаних текстів будь-якою мовою. Крім того, використання зловмисниками технології діпфейків (Deepfakes) дозволяє синтезувати голос або підробляти відеозвернення публічних осіб настільки реалістично, що без спеціального програмного забезпечення відрізнити їх від оригіналу стає майже неможливо.

Найбільшу небезпеку сьогодні становлять такі новітні інструменти впливу:

- гіперреалістичні відеопідробки (deepfakes): створення фальшивих, але візуально бездоганних відеозвернень політичних лідерів, військового керівництва чи публічних осіб із закликами, що сіють паніку або деморалізують населення.
- клонування голосу (voice cloning): використання коротких аудіозаписів (наприклад, із соціальних мереж) для створення синтезованого голосу, який неможливо відрізнити від оригіналу, що активно застосовується у шахрайських схемах та цілеспрямованих ІПСО.
- автоматизована генерація маніпулятивних текстів: використання великих мовних моделей для створення тисяч унікальних, психологічно продуманих коментарів та публікацій без жодних мовних чи граматичних помилок.

Аналіз цих технологічних трансформацій, проведений під час практичної підготовки, дозволяє зробити критично важливий висновок: традиційні правила інформаційної гігієни остаточно втратили свою ефективність. Навички пошуку граматичних помилок чи візуальних дефектів на фотографіях більше не можуть слугувати надійним захистом.

У зв’язку з цим, виникає об’єктивна необхідність концептуального оновлення підходів до цифрової грамотності населення. Сучасна інформаційна гігієна має базуватися на принципі «нульової довіри» до будь-яких емоційно

забарвлених повідомлень. Головна небезпека сучасного ШІ полягає в тому, що він цілеспрямовано впливає на людські емоції (страх, злість, паніку). Відповідно, базовим правилом захисту стає розвиток емоційної стійкості та формування непохитної звички верифікувати будь-яку сенсаційну чи тривожну інформацію виключно через офіційні державні першоджерела. Вміння пересічного громадянина розпізнавати згенерований нейромережами контент та відрізняти правду від штучної брехні перетворилося з питання особистої обізнаності на критично важливу умову збереження загальної безпеки держави.

Висновки до розділу І:

Таким чином, у розділі 1 до кваліфікаційної роботи був проведений комплексний аналіз теоретико-методологічних засад дозволяє стверджувати, що в умовах глобальної цифровізації та тривалої гібридної агресії питання інформаційної гігієни вийшло за межі особистої відповідальності та перетворилося на фундаментальний елемент національної безпеки України. Дослідження наукових джерел, нормативно-правової бази та специфіки сучасного інформаційного простору дало змогу сформулювати низку ключових висновків.

Для початку, було з’ясовано, що концепт інформаційної гігієни зазнав докорінної сутнісної трансформації. Якщо на ранніх етапах розвитку інформаційного суспільства гігієна ототожнювалася переважно з базовою цифровою грамотністю, то сьогодні вона розглядається як складний, багаторівневий механізм когнітивного захисту. Установлено, що структура сучасної інформаційної гігієни базується на трьох нерозривних складових: когнітивно-аналітичній (критичне мислення та виявлення маніпуляцій), технологічній (розуміння алгоритмів та роботи нейромереж) і поведінковій (відповідальне споживання та поширення контенту). Відповідно, формування цієї

культури є передумовою профілактики деструктивних впливів на масову свідомість.

Також, проаналізовано місце інформаційної безпеки в системі державних пріоритетів. Доведено, що захист національного інформаційного простору, гарантований Конституцією України, сьогодні потребує переходу від моделі пасивної заборони (цензури чи блокування) до концепції проактивної «інформаційної стійкості». Дослідження еволюції стратегічного планування та діяльності державних інституцій (зокрема РНБО та Центру протидії дезінформації) засвідчило, що в умовах демократичного відкритого суспільства держава не здатна самостійно виграти інформаційну війну виключно адміністративними методами. Ключовою умовою успіху є синергія – об'єднання зусиль державних органів та громадянського суспільства, де високий рівень медіаграмотності кожного громадянина формує загальнонаціональний імунітет проти ІПСО та пропаганди.

Наприкінці особливу увагу приділено безпрецедентній трансформації інформаційних загроз. Досліджено, що стрімкий розвиток технологій генеративного штучного інтелекту кардинально змінив правила ведення інформаційної війни. Масове застосування гіперреалістичних відеопідробок (deepfakes), інструментів клонування голосу та великих мовних моделей для автоматизованої генерації текстів знівелювало ефективність традиційних методів фактчекінгу. Доведено, що пошук технічних чи граматичних помилок більше не є надійним критерієм верифікації інформації, оскільки ШІ мінімізує подібні артефакти.

У зв'язку з цим обґрунтовано нагальну потребу в оновленні освітніх підходів до формування цифрової компетентності населення. Встановлено, що в умовах високотехнологічних загроз базисом інформаційної гігієни має стати

принцип «нульової довіри» до будь-якого емоційно забарвленого контенту та розвиток емоційної стійкості.

Отже, формування високого рівня культури інформаційної гігієни серед громадян є не просто бажаним освітнім орієнтиром, а критично важливим, стратегічним бар'єром, що забезпечує інформаційну стійкість та суверенітет держави в епоху постправди та новітніх технологічних викликів. Це підтверджує актуальність подальшого дослідження практичних механізмів реалізації державної політики у цій сфері, що буде здійснено у наступних розділах роботи.

РОЗДІЛ 2. ДЕРЖАВНА ПОЛІТИКА ТА АНАЛІЗ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

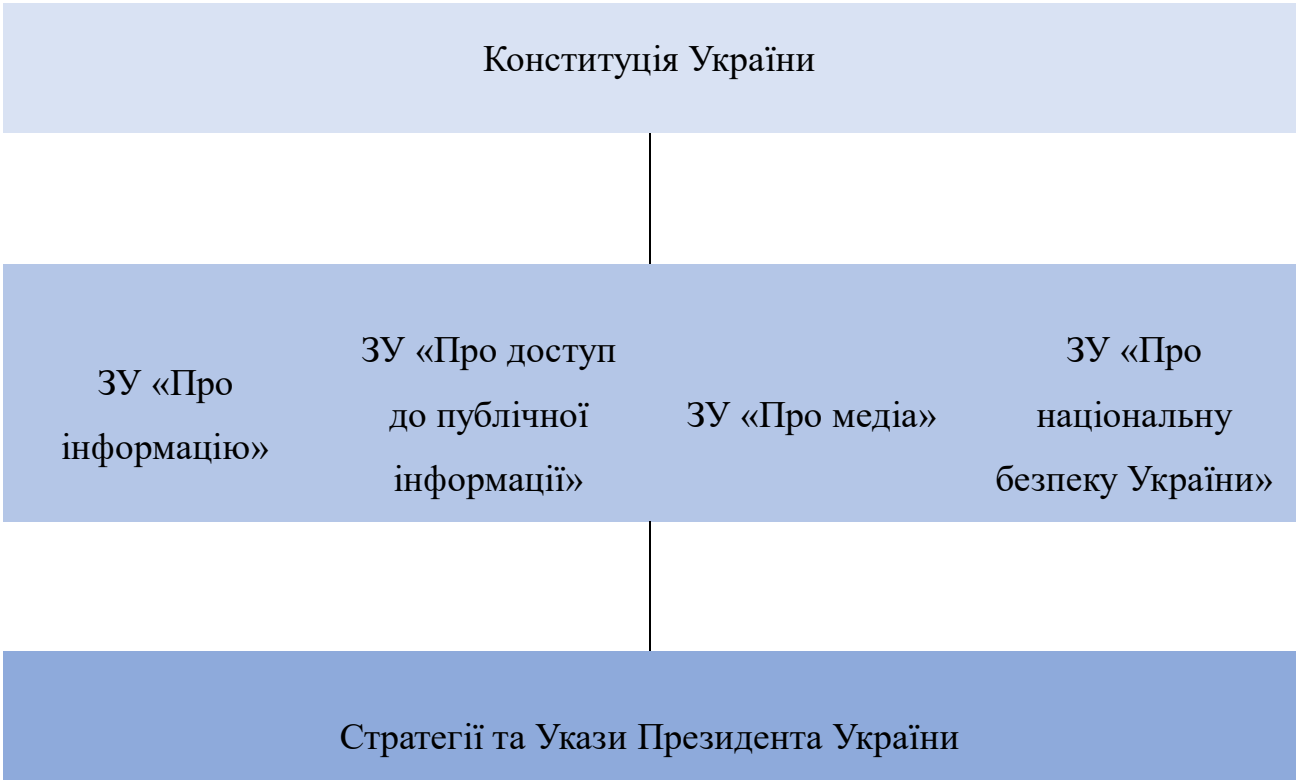
2.1. Нормативно-правове забезпечення державної інформаційної політики та захисту інформаційного простору

Ефективність функціонування системи інформаційної безпеки держави та формування культури інформаційної гігієни громадян безпосередньо залежить від якості, повноти та актуальності нормативно-правової бази. Для глибокого розуміння інституційних механізмів державного регулювання в рамках даної бакалаврської роботи було проведено комплексний аналіз чинного законодавства України у сфері інформаційної політики.

Метою цього етапу дослідження стало з’ясування того, наскільки наявна правова база здатна захистити національний інформаційний простір від сучасних гібридних загроз і чи створює вона належні умови для розвитку медіаграмотності населення. Основним методом виступив системно-правовий аналіз, а емпіричною базою для дослідження слугували тексти Конституції України, ключових профільних законів та підзаконних актів (стратегій, доктрин, указів Президента).

Проведене дослідження дозволяє стверджувати, що вітчизняна правова база проходить етап активної трансформації, зумовленої як процесами європейської інтеграції, так і гострою потребою протидії повномасштабній агресії. За результатами опрацювання нормативних джерел було виокремлено та візуалізовано на рис. 1.1, ключові рівні правового регулювання інформаційної сфери, які формують єдину ієрархічну систему захисту.

Рис. 1.1. Ієрархічна структура нормативно-правового забезпечення інформаційної безпеки України



Дана схема є примітивною, але вона чітко демонструє архітектуру нормативно-правового забезпечення, яке базується на трьох взаємопов'язаних рівнях, де кожен з них виконує специфічну функцію:

- верхній рівень (фундаментальний базис): представлений виключно Конституцією України, яка має найвищу юридичну силу, як зазначалося у попередньому розділі, саме Основний Закон встановлює концептуальний імператив: забезпечення інформаційної безпеки є найважливішою функцією держави і справою всього народу. Цей рівень задає незмінний вектор для всіх інших нормативних актів, унеможливлюючи прийняття законів, які б загрожували інформаційному суверенітету.

- середній рівень (законодавчий каркас): він формується системою спеціалізованих законів України, які деталізують конституційні норми. У ході аналізу було виділено чотири ключові нормативні акти цього рівня:
  1. Закон України «Про інформацію» - закладає правові основи циркуляції даних, визначає види інформації та право на її вільне одержання.
  2. Закон України «Про доступ до публічної інформації» - є базовим антикорупційним інструментом, що забезпечує прозорість діяльності державних органів влади.
  3. Закон України «Про медіа» - найновіший комплексний документ, який імплементує європейські директиви, регулює діяльність традиційних і онлайн-медіа та встановлює запобіжники проти мови ворожнечі і пропаганди.
  4. Закон України «Про національну безпеку України» - визначає кібербезпеку та захист інформаційного простору як ключові складові оборони держави.
- нижній рівень (стратегічно-оперативний): включає Стратегії, Доктрини та Укази Президента України (наприклад, Стратегію інформаційної безпеки). Висновки аналізу свідчать, що саме цей рівень є найбільш гнучким і життєво необхідним. Закони приймаються довго, тоді як Укази Президента та рішення РНБО дозволяють державі блискавично реагувати на нові гібридні загрози (наприклад, оперативно накладати санкції на ворожі інформаційні ресурси чи затверджувати плани протидії ІПСО).

Загалом, результати аналізу цієї ієрархії підтверджують, що в Україні сформовано міцний та структурно логічний правовий каркас інформаційної

безпеки. Водночас системний аналіз виявляє і певні недоліки: навіть найдосконаліша ієрархія законів виявляється безсилою перед загрозами, які розповсюджуються через транснаціональні анонімні платформи (такі як Telegram або TikTok), що об’єктивно не підпадають під дію національного права.

Усім відомо, що фундаментальним актом найвищої юридичної сили є Конституція України, відповідно до якої у статті 17, захист суверенітету і територіальної цілісності, а також інформаційної безпеки України є найважливішими функціями держави, справою всього Українського народу [1].

Ця норма є визначальною, оскільки вона юридично прирівнює захист інформаційного простору до захисту фізичних кордонів держави. Окрім того, стаття 34 цього ж закону гарантує кожному право на свободу думки і слова, вільне вираження своїх поглядів, але водночас встановлює, що здійснення цих прав може бути обмежене законом в інтересах національної безпеки та територіальної цілісності.

Натомість базовим документом прямої дії, що заклав фундамент усіх правовідносин у цій сфері, є Закон України «Про інформацію» (прийнятий ще у 1992 році, але з урахуванням концептуальних подальших змін). Його фундаментальність полягає в тому, що він уперше в історії незалежної України нормативно визначив інформацію як об’єкт правовідносин та здійснив перехід від тоталітарної моделі державної цензури до європейської демократичної парадигми. Проаналізувавши цей закон ми бачимо, що він закріпив не просто декларативні, а юридично обов’язкові критерії якості інформаційного простору: гарантованість права на інформацію, її відкритість, об’єктивність, достовірність, а також законність її одержання та поширення [3]. В умовах гібридної агресії ці принципи набувають нового змісту: оскільки закон вимагає достовірності та об’єктивності, будь-яке поширення дезінформації чи згенерованих діпфейків є

прямим порушенням правового поля України, що надає державним органам легітимні підстави для блокування таких джерел.

Особливе значення в контексті дослідження інформаційної безпеки має стаття 3 цього закону, яка визначає основні напрями державної інформаційної політики. Важливість цієї статті полягає в тому, що вона перетворює захист інформаційного простору з абстрактної ідеї на прямий обов'язок держави. Зокрема, вона зобов’язує державні інституції діяти у трьох ключових напрямах:

- забезпечення доступу кожного до об’єктивної інформації- це правовий механізм боротьби з інформаційним вакуумом, у якому найшвидше поширюються паніка та ворожі ІПСО.
- захист інформації та інформаційних прав громадян - ця норма є юридичною основою для розбудови систем кібербезпеки, захисту персональних даних та боротьби з кіберзлочинністю.
- розбудова національних інформаційних систем - цей пункт є надзвичайно актуальним сьогодні, адже він доводить необхідність створення суверенної цифрової інфраструктури (національних медіа, платформ і захищених державних реєстрів), яка б зменшила залежність українського суспільства від неконтрольованих транснаціональних соцмереж та анонімних месенджерів.

З огляду на вищезазначені пункти, стаття 3 Закону України «Про інформацію» фактично є законодавчим мандатом для розбудови інформаційної стійкості держави та впровадження практик інформаційної гігієни у суспільстві.

Особливе місце в системі забезпечення прозорості держави та боротьби з маніпуляціями посідає Закон України «Про доступ до публічної інформації» (від 13.01.2011 № 2939-VI). Його аналіз виявляє кардинальну зміну правової презумпції: відтепер уся інформація, що знаходиться у володінні суб’єктів владних повноважень, вважається відкритою за замовчуванням [2].

У контексті інформаційної гігієни цей закон не є простою бюрократичною процедурою - він виступає потужним інструментом фактчекінгу адже його унікальність та ефективність базується на декількох ключових статтях. Одним з фундаментальних кроків стала стаття 6 цього закону, яка запровадила революційний для вітчизняного права механізм - так званий «трискладовий тест». Ця норма унеможливлює свавільне засекречення даних: посадовці можуть обмежити доступ до інформації виключно у випадку, якщо її оприлюднення завдасть істотної шкоди національній безпеці, і ця шкода переважає суспільний інтерес знати цю інформацію. Саме це ліквідувало радянську практику приховування суспільно важливих фактів, яка раніше створювала інформаційний вакуум - ідеальне середовище для зародження чуток та теорій змови.

Не менш критичне значення має стаття 20, яка встановлює безпрецедентно короткий термін надання відповіді на інформаційний запит - всього 5 робочих днів (або 48 годин у надзвичайних ситуаціях). В умовах гібридної війни та блискавичного поширення ворожих ІПСО саме швидкість отримання офіційних даних дозволяє журналістам, OSINT-дослідникам та пересічним громадянам оперативно спростовувати фейки, спираючись на легітимні першоджерела.

Наостанок важливо зазначити статтю 15 в цьому законі, яка зобов’язує державні органи проактивно оприлюднювати інформацію у форматі відкритих даних (зокрема, через функціонування єдиного порталу data.gov.ua). З точки зору інформаційної безпеки, така абсолютна відкритість державних реєстрів, бюджетів та рішень діє як «когнітивне щеплення» для суспільства. Вона суттєво звужує поле для ворожих маніпуляцій, оскільки генерувати фальшиві наративи чи дискредитувати діяльність державних органів значно важче, коли кожен громадянин має прямий доступ до первинної, неспотвореної статистичної інформації.

Ще одним критично важливим етапом у формуванні сучасної державної політики стало прийняття Закону України «Про національну безпеку України» 2018 року. Його ухвалення ознаменувало остаточний перехід держави від мирної до оборонної парадигми в управлінні національним інформаційним простором. Згідно з пунктом 6 частини 1 статті 3 цього закону, кібербезпека та інформаційна безпека офіційно визначені як фундаментальні національні інтереси [5].

Таке законодавче формулювання має принципове концептуальне та практичне значення, що ставить інформаційну безпеку в один юридичний ряд із державним суверенітетом та територіальною цілісністю, держава кардинально змінила статус інформаційної сфери, перевівши її до категорії питань національного виживання та оборони. Якщо в попередні десятиліття медіапростір і комунікації розглядалися переважно в культурно-просвітницькому чи гуманітарному контексті, то цей закон офіційно закріпив визнання інформації як повноцінної зброї масового ураження.

Інтеграція захисту інформаційного простору до сектору безпеки і оборони України створює потужне юридичне підґрунтя для залучення не лише цивільних регуляторів, але й розвідувальних органів, кіберполіції та Збройних Сил до прямої протидії ворожим ІПСО. У контексті теми даного дослідження цей закон остаточно доводить, що розбудова надійного електронного документообігу в установах та формування високого рівня інформаційної гігієни громадян перестають бути просто адміністративними або освітніми завданнями. Вони перетворюються на стратегічну вимогу національного виживання та ключовий елемент загальнонаціональної стійкості, без якого неможлива перемога у сучасній гібридній війні.

Якщо закони формують статичний правовий каркас (про який йшлося вище), то практичний механізм реагування на поточні виклики реалізується через документи стратегічного планування. Таким ключовим документом, що

репрезентує нижній (оперативний) рівень правового забезпечення, є «Стратегія інформаційної безпеки», введена в дію Указом Президента України № 685/2021.

Винятковість та важливість цього документа полягає в тому, що він не просто декларує загальні принципи, а проводить чітку діагностику інформаційного простору. Стратегія офіційно називає речі своїми іменами: вона деталізує конкретні інструменти, якими користується агресор, та встановлює пряму відповідність між конкретною загрозою та державним механізмом її подолання. Для наочної візуалізації цієї логіки протидії мною було систематизовано ключові положення документа та сформовано аналітичну матрицю на табл. 1.1.

Таблиця 1.1. Матриця загроз та стратегічних цілей відповідно до Стратегії інформаційної безпеки України

Глобальні загрози	**Стратегічні цілі**
Інформаційно-психологічні операції (ІПСО)	Розвиток стратегічних комунікацій та державної інформаційної політики
Дезінформація та поширення фейкових новин	Підвищення рівня медіаграмотності населення
Інформаційний вплив Російської Федерації	Протидія пропаганді та зміцнення інформаційного суверенітету
Маніпуляції громадською думкою через медіа та соцмережі	Розвиток критичного мислення та підтримка незалежних медіа
Поширення незаконного або шкідливого контенту	Протидія незаконному контенту та вдосконалення регуляторної політики

Аналізуючи дані, які наведені у таблиці 1, можна зробити важливий висновок щодо еволюції державного підходу. Як бачимо з правої колонки,

держава усвідомлює, що симетрична відповідь (лише заборони чи блокування) є неефективною. Тому головним «щитом» проти ІПСО та маніпуляцій (ліва колонка) визначено когнітивний захист: розвиток критичного мислення, підтримку незалежної журналістики та стратегічні комунікації. Документ Стратегії вперше в історії України на найвищому державному рівні закріпив формування культури медіаграмотності та інформаційної гігієни не як факультативну навичку, а як стратегічну ціль національної безпеки [6]. Він остаточно легітимізує потребу у впровадженні масових освітніх програм з цифрової грамотності на рівні кожної установи та громадської організації.

Новітнім і найбільш масштабним регуляторним кроком стало набуття чинності Законом України «Про медіа» (від 13.12.2022 № 2849-IX). Його імплементація стала потужним інструментом внутрішньої безпеки. Дослідження норм цього Закону дозволяє виділити такі інноваційні аспекти:

- розширення об’єкта регулювання: закон вперше ввів у правове поле поняття «онлайн-медіа» та провайдерів платформ спільного доступу до відео, що дозволило частково реагувати на загрози у цифрових платформах.
- прозорість власності: встановлено жорсткі вимоги щодо розкриття кінцевих бенефіціарів медіа, що мінімізує ризики прихованого фінансування пропагандистських ресурсів.
- обмеження щодо держави-агресора: у розділі IX Закону закріплено безпрецедентні обмеження, що прямо забороняють діяльність суб’єктів у сфері медіа, якщо в їхній структурі власності є громадяни або резиденти держави-агресора[4].

Однак, попри суттєве оновлення нормативної бази, результати дослідження вказують на наявність певних прогалин. Зокрема, поза межами жорсткого правового регулювання залишаються месенджери (наприклад, Telegram), які

наразі виступають основними каналами споживання новин і водночас - головним джерелом поширення дезінформації.

Підсумовуючи, можна стверджувати, що нормативно-правова база України у сфері інформаційної безпеки є достатньо розвиненою. Проте динаміка гібридних загроз вимагає переходу від реагування на наслідки до превентивних заходів, серед яких пріоритетним має стати законодавче стимулювання громадських програм із підвищення інформаційної гігієни.

2.2. Вплив інформаційної агресії на суспільну свідомість в умовах гібридної війни

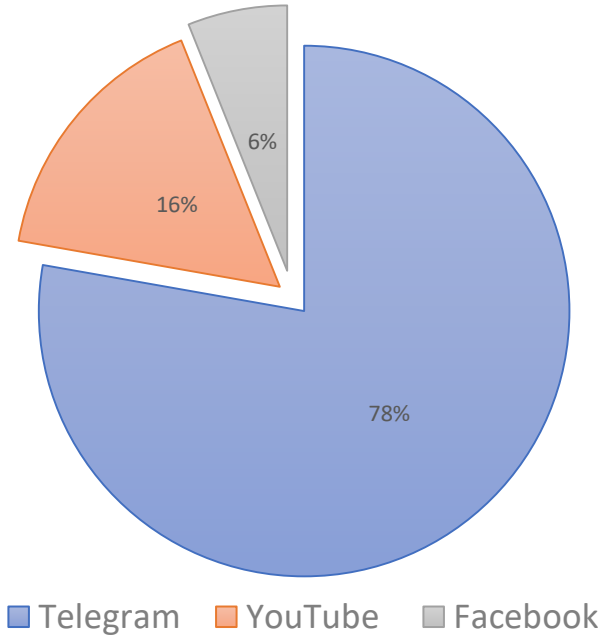
В умовах повномасштабного вторгнення інформаційний простір України зазнав безпрецедентного, багатовекторного тиску з боку держави-агресора. Метою цього впливу є не просто ситуативне поширення окремих неправдивих новин (фейків), а проведення довготривалих, багаторівневих інформаційно-психологічних операцій (ІПСО). Такі операції ретельно плануються російськими спецслужбами з урахуванням соціологічних та психологічних вразливостей українського суспільства. Більшість з них спрямовані на досягнення кількох стратегічних цілей: виснаження психологічних ресурсів (стимулювання так званої «втоми від війни»), глибоку поляризацію думок навколо чутливих соціальних маркерів (мова, мобілізація, переселенці), дискредитацію військово-політичного керівництва та міжнародних партнерів України, а також штучне розпалювання масових панічних настроїв під час кризових ситуацій.

Однак для успішної реалізації будь-якої ІПСО агресору необхідний ефективний канал доставки деструктивного контенту безпосередньо до свідомості громадянина, тому аналіз поточного стану інформаційної безпеки неможливий без глибокого розуміння того, які саме платформи українці

використовують для споживання новин і чому ці платформи формують зону критичної вразливості.

Для об’єктивної оцінки цієї ситуації нами було проаналізовано статистичні дані щодо сучасних тенденцій медіаспоживання населенням. За результатами масштабного щорічного опитування USAID-Internews «Ставлення населення до медіа та споживання інформації в Україні» (2023 р.) демонструють кардинальну зміну звичок українських громадян. Традиційні медіа (телебачення, радіо, друкована преса), які піддаються правовому регулюванню та змушені дотримуватися базових журналістських стандартів, остаточно поступилися лідерством соціальним мережам та месенджерам. Згідно зі звітом, абсолютна більшість - 72% українців - використовують месенджер Telegram як основне джерело для отримання новин, залишаючи далеко позаду YouTube (16%) та Facebook (6%), що наведено на рис 1.2. [25].

Рис. 1.2. Українські ЗМІ: споживання новин та довіра у 2025 році



Включення та аналіз даної діаграми має принципове значення для нашого дослідження, оскільки вона візуалізує головну проблему сучасної української інформаційної безпеки - масовий перехід аудиторії до «сірої зони» медіапростору. Домінування показника Telegram (72%) над іншими платформами пояснює, чому ворожі ІПСО досягають такого розголосу:

- для початку звертаємо увагу, що архітектура цього месенджера базується на абсолютній анонімності. Більшість популярних новинних каналів не мають офіційних редакцій, власників чи контактних даних, що створює ідеальне середовище для російських спецслужб, які маскуються під «українські патріотичні» чи «інсайдерські» канали для вкидання дезінформації.
- також формат платформи передбачає швидкість та емоційність за рахунок відсутності фактчекінгу. На відміну від традиційних ЗМІ, де

новина проходить перевірку редактором, у месенджері інформація публікується миттєво. Короткі емоційні тексти у поєднанні з шокуючими фото чи відео вимикають критичне мислення користувача, змушуючи його миттєво поширювати панічний контент серед знайомих.

- говорячи про низькі показники Facebook (6%) та YouTube (16%) як джерел новин пояснюються жорсткою політикою модерації цих компаній, які часто блокують або обмежують охоплення контенту про війну (так званий тіньовий бан). Telegram, натомість, практично не модерує контент, що робить його зручним як для українців (для швидкого отримання сповіщень про тривоги), так і для ворога (для безперешкодного проведення психологічних операцій).

Отже, дані діаграми доводять критичну тезу: оскільки держава законодавчо та технічно не може контролювати чи цензурувати анонімні месенджери, з яких 72% громадян черпають інформацію, традиційні методи державної безпеки тут не працюють. Єдиним дієвим механізмом захисту суспільної свідомості за таких умов стає внутрішня когнітивна стійкість кожного окремого користувача - тобто його особиста інформаційна гігієна та медіаграмотність.

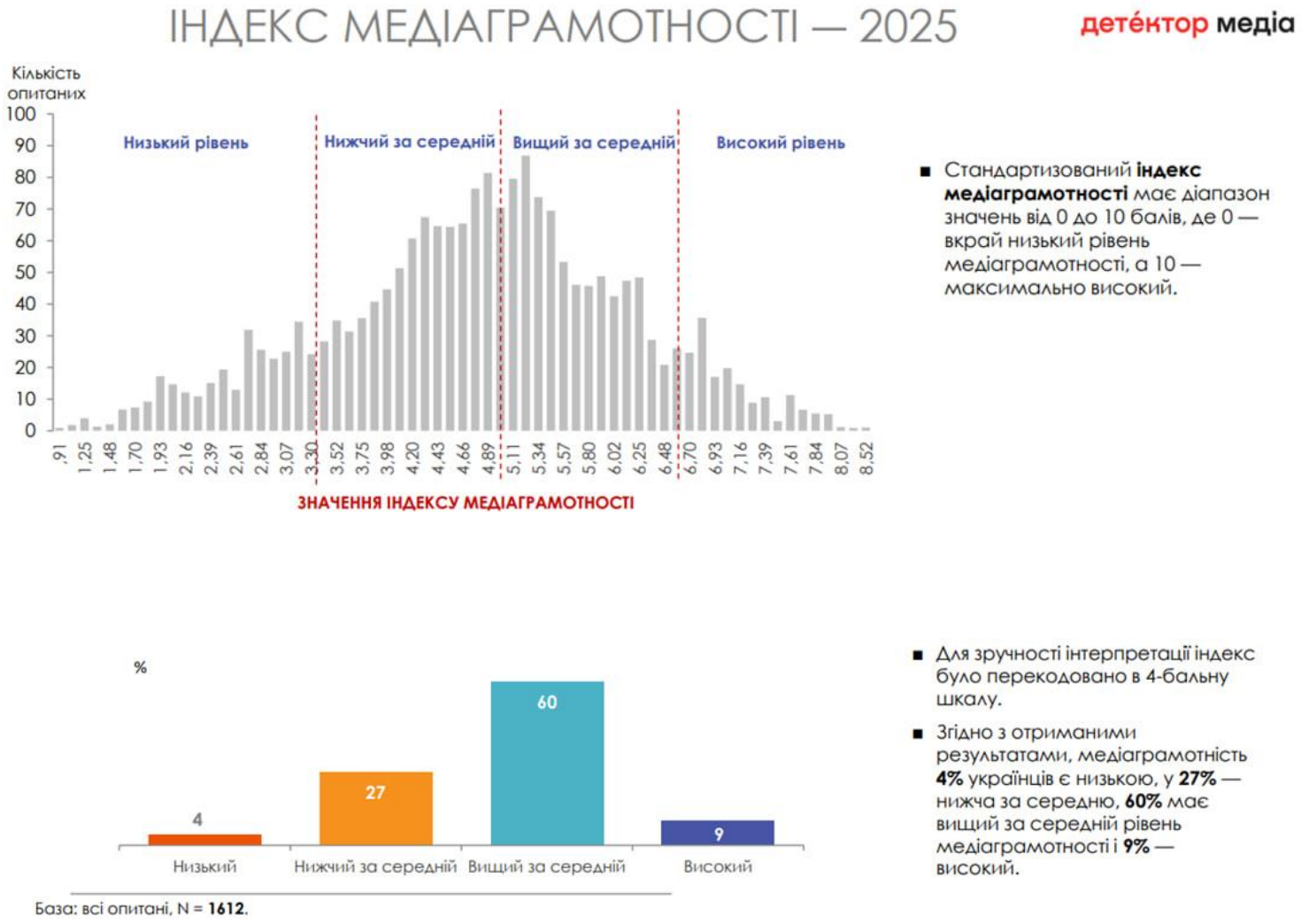
Така безпрецедентна тенденція формує одну з найбільших вразливостей національної інформаційної безпеки. Як зазначається у профільних дослідженнях, ситуація, коли головні інформаційні артерії воюючої країни проходять через іноземні, юридично нерегульовані платформи (Telegram та TikTok), є критичною загрозою національному суверенітету. Анонімність власників та адміністраторів Telegram-каналів дозволяє агресору безперешкодно створювати масштабні мережі впливу. Ці мережі віртуозно маскуються під українські патріотичні, новинні чи місцеві регіональні пабліки (наприклад, сумнозвісна мережа каналів «Легендарний», «Пліткарка», канали, що мімікрують під підрозділи ЗСУ тощо). Вони часто використовують тактику «бутерброда»:

змішують 80% правдивих новин із 20% деструктивного контенту, формуючи довіру аудиторії для подальших маніпуляцій.

Звіти Центру протидії дезінформації (ЦПД) при РНБО систематично фіксують використання цих платформ для «вкидів» не лише текстових ІПСО, а й гіперреалістичних діпфейків (Deepfakes). Як приклад можна навести неодноразові спроби поширення фейкових відеозвернень військово-політичного керівництва України, або згенеровані штучним інтелектом (ШІ) аудіозаписи нібито перехоплених розмов українських військових. Такі високотехнологічні підробки, що розповсюджуються зі швидкістю світла через нерегульовані канали, значно ускладнюють процес фактчекінгу. Вони вимагають від громадян навичок цифрової стійкості, що виходять далеко за межі традиційної медіаграмотності минулих років [26].

Для об’єктивної оцінки здатності українського суспільства опиратися такій масованій та витонченій агресії доцільно проаналізувати результати найсвіжішої, шостої хвилі загальнонаціонального дослідження «Індекс медіаграмотності українців» [12], презентованого ГО «Детектор медіа» у березні 2026 року. Цей індекс є ключовим індикатором національної стійкості, який вимірює рівень розуміння громадянами медіапростору, їхні практичні навички верифікації контенту та, що найголовніше в сучасних реаліях, рівень цифрової компетентності у взаємодії зі штучним інтелектом, на рис. 1.3.

Рис. 1.3. ГО «Детектор медіа» - Індекс медіаграмотності українців 2025-2026р.



Аналіз актуальних статистичних даних за 2025 рік свідчить про наявність складної та неоднорідної динаміки суспільної стійкості. Більшість українців продовжує демонструвати задовільні показники: 69% аудиторії мають високий (9%) або вищий за середній (60%) рівні медіаграмотності. Водночас майже третина населення країни (31%) перебуває у зоні критичного ризику, маючи низький (4%) або нижчий за середній (27%) рівень компетенцій.

Особливої наукової уваги заслуговує той факт, що частка громадян із «високим» рівнем медіаграмотності зазнала зниження порівняно з першим роком повномасштабного вторгнення. Соціологи пояснюють такий спад двома ключовими факторами: сильно дається взнаки накопичена емоційна втома від безперервного споживання важкої інформації, пов'язаної з воєнними діями. І другий фактор, що методологія оцінки ускладнилася: тепер вона включає індикатори розпізнавання контенту, згенерованого штучним інтелектом. Відповідно, стрімкий розвиток генеративних нейромереж (діпфейків) кинув суспільству новий виклик, до якого значна частина громадян виявилася технологічно не готовою.

Детальний аналіз звіту підтверджує ці побоювання: хоча 70% аудиторії цілком слушно вимагають від медіа обов'язково позначати матеріали, створені за допомогою ШІ, навички самостійної перевірки інформації залишаються недостатніми. Так, 30% українців зізнаються, що взагалі ніколи не перевіряють медіаконтент на достовірність, покладаючись виключно на довіру до джерела. Це формує значний «когнітивний пролом» в обороні держави, який ворог продовжує активно використовувати для проведення інформаційно-психологічних операцій [12].

Водночас дослідження доводить, що в умовах гібридної війни найвищу ефективність показують заходи, які базуються на принципі синергії, тісній взаємодії державних інституцій та громадських ініціатив (краудсорсингу). Яскравими прикладами такої взаємодії, що не лише теоретично просвіщають, а й формують практичні навички активної інформаційної гігієни громадян, є:

- національний проєкт з медіаграмотності «Фільтр» (ініціатива Міністерства культури та інформаційної політики України). Проєкт реалізує масштабні, доступні для різних вікових груп просвітницькі кампанії та щорічно проводить Національний тест з медіаграмотності. У

2023 році цей тест об’єднав понад 100 тисяч учасників, ставши своєрідним зрізом рівня інформаційної обізнаності та продемонструвавши високий суспільний запит на набуття навичок самозахисту в інтернеті [19].

- всеукраїнський проєкт «BRAMA» (масштабна ініціатива Департаменту кіберполіції Національної поліції України у партнерстві з волонтерами). Це унікальний приклад успішної гейміфікації національного інформаційного спротиву. Станом на 2024 рік проєкт залучив сотні тисяч активних користувачів, об’єднаних спільною метою - блокуванням ресурсів агресора. Завдяки скоординованим, спільним діям громадян (через надсилання масових скарг) було заблоковано десятки тисяч ворожих Telegram-каналів, ботоферм та фішингових сайтів. Діяльність у рамках проєкту «BRAMA» є еталонним проявом високого рівня цифрової свідомості та переходу від пасивного споживання інформації до активного захисту кіберпростору [23].

Підсумовуючи отримані та проаналізовані дані, можна сказати, що вплив інформаційної агресії на суспільну свідомість українців залишається критично високим і постійно еволюціонує. Агресор швидко адаптує свої стратегії, роблячи ставку на генеративний штучний інтелект та максимальне використання популярних неврегульованих месенджерів (насамперед Telegram, яким користується 72% населення). Проте об’єктивна статистика зростання індексу медіаграмотності та масовий успіх волонтерсько-державних проєктів взаємодії (таких як «BRAMA» і «Фільтр») доводять ключову тезу цього дослідження, що в епоху глобальних комунікацій найкращим, найстійкішим інструментом проти дезінформації є не виключно державна заборона чи цензура, а формування

усвідомленого громадянина та системний розвиток навичок критичного мислення на загальнонаціональному рівні.

2.3. Роль публічних бібліотек та закладів освіти у формуванні цифрової та інформаційної грамотності населення

В умовах масованої інформаційної агресії та стрімкої цифровізації всіх сфер життя, навички медіаграмотності та інформаційної гігієни стають життєво необхідними для всіх без винятку демографічних груп населення. Як показав аналіз статистичних даних у попередньому підрозділі, найбільш вразливими до маніпуляцій, діпфейків та фішингу залишаються люди старшого віку, мешканці невеликих громад та особи з низьким рівнем комп'ютерної грамотності. Відповідно, держава постає перед складним завданням: як забезпечити масове, безкоштовне та доступне навчання цих категорій громадян. У цьому контексті ключовим інструментом реалізації державної політики стають публічні бібліотеки та заклади освіти.

Сучасна публічна бібліотека зазнала глибокої функціональної трансформації. З традиційних установ для зберігання та видачі друкованих видань вони перетворилися на сучасні інформаційні центри, хаби цифрової освіти та простори неформального навчання. Головна перевага бібліотек як осередків формування інформаційної гігієни полягає у їхній інклюзивності, розгалуженій мережі та безкоштовності послуг. Крім того, бібліотечні працівники, будучи фахівцями з управління інформацією, володіють необхідними компетенціями для навчання громадян алгоритмам пошуку, фактчекінгу та верифікації даних.

Яскравим прикладом системної трансформації на загальнонаціональному рівні є масштабне залучення публічних бібліотек у проєкт Міністерства цифрової

трансформації України. Сьогодні на базі понад 6000 публічних, обласних та територіальних бібліотек успішно функціонують офлайн-хаби національної мережі «Дія. Освіта» (раніше - «Дія. Цифрова освіта»). Стратегічне значення цих просторів полягає у подоланні цифрової нерівності, яка є однією з головних причин вразливості старшого покоління та жителів невеликих громад до інформаційних маніпуляцій. Згідно з офіційними даними Міністерства, завдяки цій мережі доступ до цифрової освіти отримали майже 2 мільйони українців, значну частину з яких становлять люди поважного віку та внутрішньо переміщені особи (ВПО) [17].

Ключовою інновацією цієї ініціативи стала зміна функціональної ролі персоналу: бібліотекар виступає в ролі фасилітатора (цифрового амбасадора), який безпосередньо супроводжує процес навчання. Відвідувачі хабів не просто отримують доступ до Інтернету, а проходять спеціалізовані освітні серіали, такі як «Обережно! Кібершахраї», «Основи кібербезпеки» та «Кіберняні». Дослідження показує, що такий формат парної роботи (громадянин + бібліотекар) дозволяє людям подолати психологічний бар'єр перед новими технологіями та на практиці сформувати навички розпізнавання фішингових посилань і захисту персональних даних.

Для більш глибокого розуміння практичного виміру цієї проблеми було досліджено діяльність Публічної бібліотеки імені Лесі Українки міста Києва, яка є флагманом із впровадження програм медіаграмотності на муніципальному рівні. Детальний аналіз її активностей дозволяє стверджувати, що заклад веде комплексну роботу, яку можна розділити на два ключові напрями.

Перший напрям - це системна просвітницька діяльність. Бібліотека є активним учасником Глобального тижня медійної та інформаційної грамотності (Global Media and Information Literacy Week), ініційованого ЮНЕСКО. В рамках цього тижня фахівцями організовуються масштабні тематичні лекції,

інтерактивні тренінги та інформаційні кампанії, спрямовані на розвиток критичного мислення відвідувачів, що виконує функцію масового «когнітивного щеплення» для місцевої громади [18].

Другий, найбільш дієвий напрям - це впровадження постійних практичних курсів для найвразливіших категорій громадян. На базі бібліотеки організовано систематичне навчання комп'ютерній та медіаграмотності, орієнтоване насамперед на пенсіонерів та людей старшого віку. Дослідження навчальної програми цих курсів засвідчило її виняткову практичну орієнтованість. Під керівництвом бібліотечних фахівців громадяни на конкретних прикладах вчаться:

- розпізнавати клікбейтні заголовки та маніпулятивні емоційні наративи;
- користуватися системами зворотного пошуку зображень (Google Images) для верифікації фотографій та виявлення постановочних кадрів;
- безпечно налаштовувати приватність у популярних месенджерах (зокрема у Viber та Telegram), блокувати спам-розсилки та ідентифікувати шахрайські повідомлення про «державні виплати» або фейкові збори коштів;
- аналізувати джерела інформації та перевіряти їхню надійність через спеціалізовані фактчекінгові ресурси [18].

Не менш масштабну діяльність розгорнула і ВГО «Українська бібліотечна асоціація» (УБА). Використовуючи каскадний метод навчання (Training of Trainers), УБА організовує спеціалізовані школи та вебінари, де самих бібліотекарів навчають новітнім методикам фактчекінгу та алгоритмам виявлення ІПСО. Отримавши ці знання, бібліотечні працівники стають локальними тренерами у своїх громадах, створюючи потужний мультиплікаційний ефект.

Крім того, на базі бібліотеки впроваджено постійні курси з навчання медіаграмотності під час яких будь хто на практиці може навчитися розпізнавати клікбейтні заголовки, перевіряти джерела звідки надходить інформація, безпечно

користуватися соціальними мережами та захищати свої персональні дані від шахраїв [18]. Такий підхід доводить, що бібліотека є ідеальним майданчиком для подолання цифрової нерівності та поширення «інформаційного антивірусу» в суспільстві.

Говорячи про діяльність мережі «Дія. Освіта» та Публічної бібліотеки імені Лесі Українки, можна констатувати, що саме публічні бібліотеки сьогодні є найбільш інклюзивним, безкоштовним та ефективним інфраструктурним майданчиком для подолання цифрової нерівності. Вони виконують критично важливу державну функцію - перетворюють найвразливіші верстви населення з пасивних споживачів контенту (і потенційних жертв ІПСО) на когнітивно стійких громадян.

Публічні бібліотеки, як було зазначено вище, відіграють надзвичайно важливу роль у неформальній освіті, вони допомагають охопити найрізноманітніші групи дорослого населення, зокрема й ті, що є найменш захищеними від інформаційних маніпуляцій. Натомість заклади формальної освіти, наприклад: школи та університети, виконують іншу, не менш критичну функцію: вони забезпечують фундаментальну, професійну підготовку молоді саме в освітньому середовищі, де закладаються базові навички критичного мислення та цифрової грамотності, на яких згодом формується загальнонаціональна здатність протистояти інформаційним загрозам.

У цьому процесі заклади вищої освіти відіграють подвійну роль. З одного боку, вони є центрами, де студенти отримують теоретичні знання, а з іншого боку, сучасний університет - це масштабна та складна організація, яка щоденно обробляє величезні обсяги інформації. Для будь-якого університету питання інформаційної безпеки - це не лише теорія з підручників, а й сувора щоденна практика управління. Це стосується всіх робочих процесів: від створення

безпечної системи електронного обміну документами між відділами до надійного захисту персональних даних тисяч студентів та викладачів.

Отже, саме в межах освітньої установи культура інформаційної гігієни проходить реальну перевірку на міцність. Вона проявляється в конкретних діях персоналу: наскільки відповідально співробітники працюють із конфіденційними документами, чи використовують вони надійні електронні підписи для підтвердження своїх дій, і наскільки чітко в установі визначено, хто саме має право доступу до певної інформації. Такий практичний вимір інформаційної безпеки неможливо дослідити лише теоретично, адже він потребує детального розгляду та аналізу на прикладі роботи конкретної організації, що й обумовлює необхідність вивчення досвіду реальної бази практики у наступному розділі.

Висновки до розділу ІІ:

Проведений у другому розділі кваліфікаційної роботи комплексний аналіз державної політики та поточного стану інформаційної безпеки України дозволяє зробити низку важливих висновків щодо практичного виміру протидії сучасним загрозам.

По-перше, дослідження нормативно-правового забезпечення продемонструвало, що українське законодавство у сфері інформаційної політики пройшло значну еволюцію і загалом відповідає викликам воєнного часу та європейським стандартам. Наприклад, базові Закони «Про інформацію» та «Про доступ до публічної інформації» заклали фундамент відкритості державних даних, а новітній Закон «Про медіа» (2022 р.) вперше запровадив європейські механізми регулювання онлайн-медіа та вимоги щодо прозорості їхньої власності. Водночас виявлено суттєву юридичну прогалину: відсутність дієвих механізмів державного регулювання популярних іноземних платформ і

месенджерів (таких як Telegram та TikTok), що ускладнює інституційний захист інформаційного простору від анонімних мереж впливу агресора.

По-друге, на основі аналізу статистичних даних (зокрема звітів USAID-Internews, ГО «Детектор медіа» та ЦПД при РНБО) доведено, що рівень інформаційної агресії проти України залишається критичним і постійно трансформується. Встановлено, що 72% населення використовують нерегульований месенджер Telegram як основне джерело новин, що створює ідеальне середовище для поширення ворожих ІПСО та згенерованих штучним інтелектом діпфейків. Хоча загальний індекс медіаграмотності українців поступово зростає (76% аудиторії мають рівень вище середнього), близько чверті населення (24%) все ще перебуває у зоні високого ризику. Це доводить, що в епоху цифрових комунікацій виключно державні заборони та блокування є неефективними без системного підвищення рівня когнітивної свідомості самих громадян.

По-третє, обґрунтовано критично важливу роль публічних бібліотек та закладів освіти у формуванні культури інформаційної гігієни суспільства. Досліджено успішний досвід розбудови цифрових хабів мережі «Дія. Цифрова освіта» на базі регіональних бібліотек, а також проаналізовано практичну діяльність Публічної бібліотеки імені Лесі Українки з проведення курсів медіаграмотності для дорослого населення. З’ясовано, що саме бібліотеки, завдяки своїй інклюзивності, розгалуженій мережі та фаховості персоналу, є найбільш ефективними та безкоштовними майданчиками для навчання вразливих груп населення базовій цифровій безпеці. Окрім того, відзначено високу результативність проєктів, побудованих на синергії держави та суспільства, таких як ініціатива кіберполіції «BRAMA» та національний проєкт «Фільтр».

Одержані результати підтверджують наукову новизну підходу, за якого інформаційна безпека держави розглядається не лише як військова чи

законодавча категорія, а як синергія нормативного регулювання та практичної просвітницької роботи з населенням. Водночас встановлено, що загальнонаціональна інформаційна стійкість завжди починається з безпеки окремих інституцій та підприємств. Це зумовлює необхідність переходу від загальнодержавного аналізу до вивчення практичного досвіду організації захисту інформації, кібергігієни персоналу та системи електронного документообігу на рівні конкретної установи (бази практики), що буде розглянуто в наступному розділі.

РОЗДІЛ 3. ПРАКТИЧНИЙ ВИМІР ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ДОКУМЕНТООБІГУ

3.1. Організація захищеного документообігу як фактор інформаційної стійкості установи

Забезпечення інформаційної безпеки держави є комплексним процесом, що починається з надійної організації роботи з даними у кожній окремій установі. Заклади вищої освіти, які оперують значними масивами персональних даних, науковими розробками та стратегічною документацією, є критично важливими елементами національної інформаційної інфраструктури.

У цьому контексті Маріупольський державний університет (МДУ) - як провідний освітній центр, що функціонує в надскладних умовах евакуації та підвищених кіберзагроз - виступає репрезентативною базою для дослідження того, як культура інформаційної гігієни персоналу впливає на безпеку інституції. Введення досвіду цієї установи до нашого дослідження обумовлено необхідністю практичної верифікації концептів, викладених у попередніх розділах. Як було доведено у першому розділі, сучасні гібридні загрози еволюціонували від прямого технічного зламу до методів соціальної інженерії, де головною мішенню є людська свідомість та психологія. Своєю чергою, аналіз статистичних даних у другому розділі підтвердив, що масове використання нерегульованих месенджерів та недостатній рівень медіаграмотності роблять пересічного користувача найслабшою ланкою в системі інформаційної безпеки. З огляду на це, саме на мікрорівні - у щоденному електронному та паперовому документообігу конкретної організації - перевіряється реальна здатність протистояти гібридним атакам, цілеспрямованому фішингу та витокам конфіденційної інформації громадян. Практичний досвід доводить, що жодні макрорівневі державні стратегії кіберзахисту не будуть ефективними, якщо на

рівні окремої установи працівник не дотримується базових правил інформаційної гігієни під час обробки чутливих службових даних.

У ході проходження фахової організаційної практики було досліджено практичну модель забезпечення внутрішньої безпеки. Встановлено, що ключовим структурним підрозділом, який відповідає за цілісність, достовірність та правомірність інформаційних потоків в МДУ, є загальний відділ.

Організаційна структура Загального відділу побудована за принципом централізованого контролю, що має на меті мінімізувати ризики несанкціонованого доступу до службової інформації. Практика показала, що основним внутрішнім нормативно-правовим актом, який регламентує ці процеси, є «Посадова інструкція фахівця загального відділу» (додаток А), затверджена ректором у 2023 році.

Проаналізувавши документ, у контексті теми нашої роботи доводить, що посадова інструкція є не просто бюрократичним формалізмом, а базовим інструментом забезпечення інституційної інформаційної гігієни. Відповідно до пунктів 15-20 Інструкції, фахівець зобов’язаний дотримуватися норм ділової поведінки, організовувати документообіг та виконувати вимоги щодо безпечного поводження з устаткуванням. На практиці це означає, що працівники загального відділу здійснюють обов’язкову верифікацію всієї вхідної кореспонденції, перевіряють повноваження підписантів та контролюють використання електронної інформаційної бази. Це є першим рівнем когнітивного захисту: критичне ставлення фахівця до будь-якого вхідного документа унеможливлює легітимізацію ворожих вкидів, фішингових розсилок чи фейкових розпоряджень (ІПСО) у межах університету.

Критично важливим елементом інформаційної стійкості та управління доступом в МДУ є також впровадження «зведеної номенклатури справ». Під час проходження практики було досліджено, що номенклатура слугує

систематизованим алгоритмом класифікації інформації за ступенем важливості, конфіденційності та термінами зберігання.

Зокрема, практичний аналіз формування наказів за номенклатурою справ виявив такі механізми захисту інформації громадян:

- простежуваність та незмінність: кожен створений або отриманий документ отримує унікальний реєстраційний індекс. Ця система унеможливлює безслідне вилучення чи підробку документа в інформаційному просторі університету;
- розмежування доступу (Data Privacy): формування справ за номенклатурними індексами дозволяє логічно розділити інформаційні потоки. Наприклад, робота з наказами щодо особового складу, які містять чутливі персональні дані громадян, ведеться суворо обмеженим колом уповноважених осіб. Це прямо відповідає вимогам законодавства про захист персональних даних та запобігає їх потраплянню до рук зловмисників;
- контроль життєвого циклу: чітке дотримання термінів передачі справ до архіву запобігає накопиченню неактуального «інформаційного шуму» та гарантує надійне збереження юридично важливої документації бази практики.

Отже, результати дослідження діяльності бази практики дозволяють зробити висновок, що класична організація документообігу в МДУ є дієвою моделлю захисту внутрішнього інформаційного середовища.

Проте, як показав подальший аналіз, в умовах глобальної цифровізації забезпечення повноцінної інформаційної стійкості неможливе виключно на паперовому рівні. Воно вимагає неминучої інтеграції традиційних правил діловодства із сучасними технологічними рішеннями та системами електронного

документообігу, що є наступним рівнем еволюції інформаційної безпеки установи.

3.2. Впровадження цифрових технологій та забезпечення кібергігієни в управлінні електронною документацією

Трансформація інформаційних загроз, яку було досліджено у попередніх розділах, вимагає від будь-якої сучасної установи кардинальних змін у підходах до роботи. Сьогодні вже недостатньо просто зберігати папери у сейфах чи архівних шафах. В умовах гібридної війни, постійних кібератак та загрози надзвичайних ситуацій, суто паперова бюрократія стає небезпечною та неефективною, адже якщо установа працює виключно з паперовими документами, вона ризикує в один момент назавжди втратити критично важливу інформацію (наприклад, особові справи працівників, бази даних студентів чи громадян) через фізичне знищення приміщення. Тому стратегічним завданням для керівництва стає створення надійного, безперебійного та захищеного електронного середовища. Організація повинна мати змогу відновити свою роботу за будь-яких умов. Практичний досвід доводить, що єдиним надійним рішенням цієї проблеми є повний перехід до сучасних систем електронного документообігу (СЕД), а також формування стійкої звички кібергігієни у кожного окремого працівника.

Процес переходу організації у цифровий формат (цифровізація) складається з кількох послідовних кроків, які разом утворюють для установи надійний «цифровий щит». Найпершим і базовим кроком є переведення паперових архівів в електронний вигляд. Однак просто відсканувати документ чи зробити його цифрову фотографію - це лише половина справи. Для комп’ютера звичайний скан - це так зване «сліпе» зображення. Машина бачить лише набір

пікселів (картинку), але не розпізнає літер чи цифр на ній. Відповідно, у такому файлі неможливо виділити та скопіювати текст або швидко знайти потрібне слово через комп'ютерний пошук.

Щоб вирішити цю проблему, сучасні установи впроваджують технології оптичного розпізнавання символів (відомі як OCR - Optical Character Recognition). Це спеціальні «розумні» програми, які вміють аналізувати відскановані картинки і перетворювати їх на повноцінний, «живий» текст. Завдяки таким технологіям електронний архів стає чітко структурованим і зручним для використання.

На практиці це приносить величезну користь, бо замість того, щоб працівник годинами вручну перебирав папки чи переглядав сотні файлів-картинок на моніторі, йому достатньо ввести в електронний рядок пошуку прізвище, дату або ключове слово. Програма за кілька секунд знайде потрібний наказ чи довідку серед тисяч інших. Такий підхід не лише значно пришвидшує і полегшує роботу персоналу, але й гарантує, що жоден важливий документ не загубиться у хаосі великих і неорганізованих електронних архівів.

Однак центральним елементом інформаційної безпеки будь-якої сучасної організації виступає повноцінна система електронного документообігу (СЕД). Аналіз функціонування таких систем показує, що вони виконують не лише логістичну (передача файлів), але й глибоку безпекову функцію. В основу стійкої СЕД покладено такі обов'язкові механізми захисту:

- **авторизація та КЕП:** фундаментальною вимогою кібергігієни є обов'язкове використання кваліфікованого електронного підпису (КЕП). КЕП працює як надійна цифрова печатка, що замінює традиційний власноручний підпис. Її використання вирішує одразу дві проблеми інформаційної безпеки. По-перше, система завжди стовідсотково знає, яка саме людина створила чи затвердила документ. Це повністю виключає ситуації, коли зловмисники можуть непомітно підкинути в

систему фальшивий наказ від імені керівництва. По-друге, КЕП захищає документ від непомітних маніпуляцій. Якщо після накладання електронного підпису хтось спробує змінити в тексті хоча б одну літеру, суму чи дату, система негайно зафіксує втручання: підпис автоматично стане недійсним, і підробка буде виявлена.

- **суворе розмежування прав доступу (Role-Based Access Control):** в умовах гібридної війни найслабшою ланкою в захисті будь-якої установи часто стає звичайний працівник. Зловмисникам набагато простіше виманити пароль у людини (наприклад, змусивши її перейти за шахрайським посиланням у листі), ніж намагатися зламати захищені сервери. Якщо працівник випадково віддає свій пароль хакерам, його обліковий запис стає зламаним (небезпечним). Щоб запобігти катастрофі у таких випадках, надійна СЕД налаштовується за принципом «мінімально необхідних прав». Це означає, що кожен співробітник бачить у системі лише ті документи, які безпосередньо потрібні йому для щоденної роботи. Наприклад, звичайний викладач чи менеджер фізично не матиме доступу до наказів з кадрових питань або фінансових звітів установи. Завдяки такому бар’єру, навіть якщо хакери отримають доступ до комп'ютера одного працівника, вони не зможуть вкрасти або знищити всю базу даних організації.
- **безперервне фіксування дій (Логування / Audit Trail):** безпечна комп’ютерна система працює за принципом прихованої цифрової відеокамери. Вона автоматично записує в спеціальний електронний журнал (лог-файл) кожен крок будь-якого користувача. Система фіксує абсолютно все: хто саме увійшов до програми, о котрій годині, з якого пристрою та з якої інтернет-адреси. Більше того, записується кожна дія з документом - чи його просто переглянули, чи завантажили собі на

комп’ютер, чи внесли правки. Цей «аудиторський слід» є надзвичайно важливим інструментом. Якщо в установі стається витік конфіденційної інформації, службі безпеки не потрібно гадати, хто це зробив: завдяки збереженим електронним записам можна миттєво знайти винуватця та заблокувати йому доступ.

Особливу увагу при управлінні інформаційними потоками необхідно приділяти питанню гарантованого збереження даних. У сучасному цифровому світі, незалежно від того, чи йдеться про масштабну державну інституцію, приватну бізнес-структуру, чи про персональні дані пересічного громадянина, безповоротна втрата електронної інформації має катастрофічні наслідки. Для організації це означає повну зупинку управлінської діяльності, втрату баз даних клієнтів або фінансової звітності. Для окремої людини - це втрата особистих архівів, документів, фотографій або доступу до власних фінансових кабінетів.

Найбільшу загрозу в цьому контексті сьогодні становлять спеціальні вірусні програми - так звані віруси-шифрувальники (відомі як Ransomware). Потрапивши на комп’ютер чи сервер, така програма миттєво кодує (замикає) всі файли, роблячи їх нечитабельними, і вимагає фінансовий викуп за їх розблокування. В умовах гібридної війни хакерські атаки такого типу часто здійснюються не заради грошей, а з метою цілеспрямованого знищення критичної інфраструктури або паралізації роботи установ.

Саме тому невід’ємною та обов’язковою складовою як інституційної, так і особистої кібергігієни є наявність автоматизованої системи резервного копіювання (відомої як BackUp). Резервне копіювання - це процес створення та збереження додаткових копій усіх важливих файлів на зовнішніх пристроях, які не підключені до основної робочої мережі.

Для того щоб резервне копіювання було справді ефективним і захищало від сучасних загроз, воно повинно базуватися на кількох чітких правилах:

копіювання має здійснюватися регулярно та автоматично, без покладання на пам’ять чи ініціативу самого працівника. Друге правило: резервні копії ключових баз даних та архівів повинні зберігатися на фізично відокремлених носіях (наприклад, на окремих серверах, відключених від загальної мережі Інтернет) або у надійно зашифрованих хмарних сховищах. Це робиться для того, щоб у разі зараження комп’ютера вірус не зміг дістатися до резервної копії і зашифрувати ще й її. Дотримання цих правил гарантує формування справжньої «інформаційної стійкості». Це означає, що навіть у випадку масштабної кібератаки, фізичного пошкодження комп'ютерного обладнання або недбалості персоналу, установа чи окрема особа здатна в найкоротші терміни відновити всю свою інформацію з резервної копії і продовжити повноцінну діяльність.

Підсумовуючи цей підрозділ, можна стверджувати, що безпечне управління електронною документацією сьогодні вимагає комплексного, багаторівневого підходу. Як доводить аналіз практичних аспектів, відмова від вразливої паперової бюрократії та переведення архівів у структурований цифровий формат (за допомогою OCR-технологій) є лише першим, базовим кроком.

Справжній та надійний «цифровий щит» організації формується завдяки впровадженню сучасних систем електронного документообігу (СЕД), де кожен механізм відіграє свою критично важливу роль: кваліфікований електронний підпис (КЕП) працює як цифрова печатка, що гарантує авторство та незмінність документа; суворе розмежування прав доступу локалізує можливі витоки інформації; а безперервне логування дій забезпечує повний прозорий контроль за процесами. Окрім того, обов’язкове використання систем автоматизованого резервного копіювання (BackUp) виступає останньою лінією оборони, яка гарантує збереження критичних даних як установ, так і окремих громадян від катастрофічних наслідків хакерських атак.

Однак варто чітко усвідомлювати, що жодні, навіть найдорожчі та найсучасніші комп’ютерні програми, криптографічні засоби чи апаратні сервери не здатні гарантувати абсолютної безпеки. Головною вразливістю будь-якої, навіть найбільш захищеної електронної системи, завжди залишається людський фактор - працівник чи користувач, який не володіє достатнім рівнем інформаційної культури і може випадково скомпрометувати свої дані.

Відповідно, технологічна стійкість інституції має бути обов’язково синхронізована зі стійкістю кадровою, тому системне навчання персоналу основам кібергігієни та формування свідомого ставлення до інформації є тим невід'ємним компонентом, без якого побудувати справді безпечне інформаційне середовище просто неможливо.

3.3. Шляхи вдосконалення інформаційної культури персоналу та здобувачів освіти

Розглядаючи питання формування культури інформаційної гігієни громадян на макрорівні (загальнодержавному рівні), необхідно усвідомлювати, що практична реалізація та вимірювання ефективності цього процесу неможливі без фокусування на конкретних соціальних інституціях. Персонал публічних установ та здобувачі вищої освіти не є відокремленими чи ізольованими категоріями - вони виступають проактивним ядром громадянського суспільства. Заклад вищої освіти в даному контексті слугує ідеальною репрезентативною мікромоделлю держави.

Навчаючи студента чи співробітника алгоритмам захисту даних, виявленню фішингу та критичному мисленню в межах його навчального або корпоративного середовища, формується насамперед стійкий і свідомий громадянин. Набуті під час професійної діяльності чи навчання навички кібергігієни невідворотно

екстраполюються на повсякденне життя: ці громадяни згодом транслюють культуру безпечного медіаспоживання у свої родини, територіальні громади та майбутні робочі колективи. Отже, вдосконалення інформаційної культури персоналу та студентства є не відхиленням від генеральної теми дослідження, а навпаки - найбільш дієвим практичним інструментом і базовим рівнем реалізації державної політики з підвищення загальнонаціональної інформаційної безпеки громадян.

Саме тому важливо розуміти, що впровадження найсучасніших систем електронного документообігу (СЕД), криптографічного захисту та алгоритмів безперервного моніторингу не здатне гарантувати абсолютну інформаційну безпеку установи, якщо її персонал не володіє достатнім рівнем інформаційної культури. Як стверджують вітчизняні фахівці у сфері кібербезпеки, саме «людський фактор» та методи соціальної інженерії залишаються найвразливішою ланкою в системі захисту будь-якої організації [10]. Банальне відкриття фішингового листа пересічним співробітником, використання слабких паролів, необережний перехід за сумнівними посиланнями або передача службових документів через нерегульовані відкриті месенджери здатні повністю нівелювати роботу найдорожчих апаратних та програмних засобів захисту.

Аналіз організаційних процесів, проведений під час практик в ході навчання, а також узагальнення зібраної теоретичної бази дозволяють зробити висновок про критичний вплив людського фактора на загальний стан інформаційної стійкості. Особливу увагу в цьому варто приділити безпосередній ролі керівної ланки. Було з’ясовано, що в будь-якій сучасній структурі (від закладу освіти до державної установи) існує пряма, нерозривна кореляція між рівнем інформаційної культури керівника підрозділу та станом безпеки і ефективності керованого ним колективу.

Інформаційна культура керівника виступає своєрідним психологічним та професійним еталоном для підлеглих. Якщо керівництво неухильно дотримується правил кібергігієни - використовує виключно корпоративні канали зв'язку, не передає носії з кваліфікованим електронним підписом (КЕП) третім особам, суворо дотримується регламентів роботи в СЕД - це формує відповідний стійкий патерн поведінки у всього персоналу. Натомість толерування керівником порушень базових інструкцій заради удаваної «швидкості» чи «зручності» робочого процесу (наприклад, погодження робочих питань або пересилання скан-копій документів у Telegram чи Viber) автоматично знижує рівень стійкості всієї організації. Така поведінка створює системні вразливості для зовнішнього втручання та ризики витоку конфіденційних або персональних даних.

З метою комплексного вирішення проблеми людського фактора та підвищення рівня інформаційної стійкості сучасних установ і закладів освіти, пропонується впровадити низку універсальних рекомендацій:

- **модернізація та деталізація внутрішньої нормативної бази:** чинні інструкції з діловодства у більшості установ потребують оновлення та доповнення окремими розділами з «Цифрової та інформаційної гігієни». Зокрема, необхідно суворо, на рівні наказів, регламентувати заборону на пересилання службової документації через відкриті іноземні месенджери. Окрім того, надзвичайно актуальним є введення корпоративних протоколів щодо використання інструментів генеративного штучного інтелекту в адміністративній роботі, щоб запобігти випадковому завантаженню внутрішньої інформації організації у відкриті бази даних нейромереж.
- **перехід від формальних інструктажів до практичного навчання персоналу:** традиційна практика формального підписання інструкцій з техніки безпеки є неефективною в умовах цифрових загроз.

Рекомендується запровадити регулярні практичні тренінги (не рідше одного разу на півріччя) для всіх категорій співробітників. Високу ефективність демонструє метод симуляційних навчань - наприклад, проведення внутрішніх тестових фішингових розсилок, які дозволяють на практиці перевірити пильність персоналу та сформувати автоматичну звичку верифікувати відправника.

- **інтеграція модулів кібергігієни в процеси адаптації та освітні програми:** для нових співробітників будь-якої організації, а також для здобувачів освіти на першому курсі навчання, доцільно розробити та зробити обов'язковим вступний адаптаційний курс «Основи інформаційної гігієни в умовах гібридних загроз». Це дозволить ще на етапі входження в колектив сформувати стійку навичку «нульової довіри» до маніпулятивного контенту та забезпечить безпечну роботу індивіда в корпоративному чи освітньому цифровому середовищі.

Впровадження зазначених універсальних заходів дозволить організаціям та закладам освіти не лише мінімізувати ризики внутрішніх витоків інформації, але й перетворити кожного співробітника та здобувача освіти з потенційної «вразливості» на свідомий, активний елемент загальної системи національного інформаційного захисту.

Висновки до розділу ІІІ:

Проведене у третьому розділі дослідження дозволило екстраполювати загальнодержавні теоретичні та нормативні концепти інформаційної безпеки на практичний рівень функціонування установ та організацій. На прикладі аналізу процесів управління документацією було доведено, що інформаційна стійкість держави є похідною від безпеки та ефективності її базових інституцій.

Визначено, що класична організація діловодства відіграє роль первинного фільтра захисту даних та встановлено, що суворе дотримання внутрішніх інструкцій та номенклатури справ дозволяє чітко розмежувати права доступу до чутливої інформації та мінімізувати ризики витоків персональних даних.

Також, проаналізовано процес впровадження цифрових технологій в управління документацією. Доведено, що застосування систем оптичного розпізнавання (OCR), систем електронного документообігу (СЕД), кваліфікованих електронних підписів (КЕП) та алгоритмів регулярного резервного копіювання формує надійну «цифрову броню» сучасної установи, забезпечуючи безперервність управління.

Було обґрунтовано, що будь-який високотехнологічний захист втрачає свою ефективність без належного рівня інформаційної культури користувачів. Доведено визначальний вплив особистої інформаційної культури керівного складу на загальний рівень кібергігієни всього колективу. Для вирішення проблеми «людського фактора» запропоновано комплекс універсальних рекомендацій: від оновлення внутрішніх регламентів (включаючи обмеження на використання відкритих месенджерів та ШІ) до запровадження систематичних симуляційних тренінгів для персоналу та обов’язкових курсів з кібергігієни для здобувачів освіти.

Одержані результати показують, що реалізація запропонованих організаційних та освітніх кроків дозволить оптимізувати комунікаційні процеси, підвищити загальний рівень компетенцій фахівців та забезпечити надійний захист інформаційних активів, що повною мірою відповідає стратегічним цілям інформаційної безпеки держави.

ВИСНОВКИ

В умовах глобальної цифровізації та безперервної гібридної агресії проти нашої держави, захист національного інформаційного простору набув екзистенційного значення. Сучасний етап інформаційного протистояння доводить, що національна безпека більше не може спиратися виключно на силові чи регуляторні механізми держави, її міцність напряму залежить від когнітивної стійкості суспільства. Саме тому у кваліфікаційній (бакалаврській) роботі було успішно вирішено надзвичайно актуальне та гостре науково-практичне завдання.

Повною мірою досягнуто поставлену мету дослідження, яка полягала у комплексному дослідженні інформаційної гігієни як невід'ємної складової державної інформаційної політики та національної безпеки України, а також у розробці практичних рекомендацій щодо підвищення інформаційної стійкості громадян і персоналу сучасних установ в умовах гібридних загроз.

Досягнення вказаної мети стало можливим завдяки глибокому та всебічному опрацюванню масивів інформації. Під час підготовки роботи було не лише проаналізовано фундаментальну теоретико-методологічну та оновлену нормативно-правову базу України, а й залучено найсвіжіші емпіричні матеріали, зокрема, дослідження та аналіз, який спирається на актуальні соціологічні звіти, статистику тенденцій медіаспоживання, аналітику новітніх технологічних загроз (штучного інтелекту), а також на вивчення практичного досвіду функціонування сучасних інформаційних інституцій (публічних бібліотек та закладів вищої освіти).

Такий комплексний, багатоаспектний підхід дозволив об'єктивно оцінити стан проблеми та успішно, в повному обсязі виконати всі визначені у вступі завдання. За результатами проведеного кваліфікаційного дослідження логічно сформульовано такі основні висновки та науково-практичні пропозиції:

1. Досліджено теоретико-методологічні засади поняття інформаційної гігієни та еволюцію новітніх загроз. Встановлено, що в умовах глобальної цифровізації сутність інформаційної гігієни вийшла за межі базової комп'ютерної грамотності і трансформувалася у складний механізм когнітивного захисту. Виявлено, що її структура базується на трьох нерозривних складових: когнітивно-аналітичній, технологічній та поведінковій. Проаналізовано безпрецедентну еволюцію ворожого інформаційного впливу та доведено, що поява технологій генеративного штучного інтелекту (діпфейків, клонування голосу, автоматизованих ботоферм) знівелювала ефективність традиційних правил фактчекінгу. Показано, що сучасні високотехнологічні загрози вимагають переходу до принципу «нульової довіри» до будь-якого емоційно забарвленого контенту, що робить інформаційну гігієну не особистою справою громадянина, а питанням виживання держави.

2. Проаналізовано стан нормативно-правового забезпечення державної інформаційної політики України. Досліджено, що вітчизняне законодавство пройшло значну еволюцію та загалом відповідає європейським стандартам і викликам гібридної війни. Встановлено, що прийняття Закону України «Про доступ до публічної інформації» створило презумпцію відкритості даних, а імплементація Закону України «Про медіа» (2022 р.) дозволила запровадити європейські механізми регулювання онлайн-медіа. Водночас виявлено суттєву прогалину: відсутність дієвих правових механізмів державного регулювання іноземних платформ і месенджерів (зокрема Telegram та TikTok). Доведено, що цей законодавчий вакуум значно ускладнює інституційний захист національного інформаційного простору і вимагає превентивних заходів не лише правового, а й освітнього характеру.

3. Досліджено вплив гібридної агресії на суспільну свідомість шляхом аналізу статистичних даних. На основі опрацювання офіційних звітів (USAID-

Internews, ГО «Детектор медіа», ЦПД при РНБО) доведено, що рівень інформаційної агресії проти України залишається критичним. Встановлено, що 72% населення використовують юридично нерегульований месенджер Telegram як основне джерело новин, що створює ідеальне середовище для масштабних ІПСО. Виявлено, що попри загальне зростання Індексу медіаграмотності українців (76% мають рівень вище середнього), близько 24% населення все ще перебуває у зоні високого когнітивного ризику. Отримані показники дали змогу обґрунтувати тезу про те, що в епоху цифрових комунікацій виключно державні заборони та блокування ресурсів є неефективними без системного підвищення рівня свідомості самих споживачів інформації.

4. Охарактеризовано практичний вимір діяльності публічних бібліотек та громадсько-державних ініціатив у формуванні когнітивної стійкості населення. Обґрунтовано, що публічні бібліотеки сьогодні є найбільш інклюзивним, безкоштовним та ефективним інфраструктурним майданчиком для подолання цифрової нерівності в Україні. Окрім того, підтверджено високу ефективність концепції синергії держави та суспільства: встановлено, що національні освітні ініціативи (проєкт «Фільтр») та гейміфіковані платформи інформаційного спротиву (проєкт кіберполіції «BRAMA») виступають найдієвішими інструментами трансформації населення з пасивних споживачів контенту на стійких захисників національного інформаційного суверенітету.

5. Розроблено комплекс універсальних практичних рекомендацій щодо захисту інформаційного середовища в сучасних установах. Доведено, що загальнонаціональна інформаційна стійкість починається з кібербезпеки та ефективного управління даними у базових інституціях (закладах освіти, державних структурах). На основі аналізу процесів управління документацією розроблено та обґрунтовано модель інституційної «цифрової броні». Встановлено, що обов'язковими елементами цієї моделі є:

- впровадження систем оптичного розпізнавання (OCR) та електронного документообігу (СЕД);
- суворе застосування кваліфікованого електронного підпису (КЕП);
- використання принципу розмежування прав доступу (Role-Based Access Control) та регулярне резервне копіювання.

Водночас виявлено визначальний вплив людського фактора та інформаційної культури керівника на безпеку установи. Для мінімізації цих ризиків запропоновано і рекомендовано до впровадження авторський комплекс заходів:

- оновлення внутрішніх регламентів та інструкцій з діловодства (зокрема, введення категоричної заборони на пересилання службової документації через відкриті месенджери та регламентація використання генеративного ШІ).
- запровадження систематичних симуляційних фішингових тренінгів замість формальних інструктажів.
- інтеграція адаптаційних курсів з кібергігієни для нових співробітників та здобувачів освіти на початкових етапах.

Загалом результати бакалаврського дослідження мають високий ступінь достовірності, оскільки базуються на репрезентативній статистичній базі, чинному законодавстві та апробованих практичних даних. Отримані наукові та практичні результати готові до масштабування та безпосереднього використання в операційній діяльності закладів вищої освіти, державних і приватних установ. Впровадження запропонованих рекомендацій сприятиме не лише оптимізації процесів електронного документообігу, але й формуванню стійкого імунітету суспільства до зовнішніх маніпуляцій, що є критично важливою умовою забезпечення національної безпеки та перемоги України в глобальному інформаційному протистоянні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 12.03.2026).
2. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 12.03.2026).
3. Про інформацію : Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 14.03.2026).
4. Про медіа : Закон України від 13.12.2022 № 2849-IX. URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text (дата звернення: 12.03.2026).
5. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 12.03.2026).
6. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 17.03.2026).
7. Бровко О. О. Інформаційно-комунікаційна безпека: сучасні тренди : монографія, за ред. О. В. Курбана, А. Л. Лісневської. Київ, 2022.
8. Бржевська З. М., Довженко Н. М., Киричок Р. В. Інформаційні війни: проблеми, загрози та протидія. Київ : КПІ ім. Ігоря Сікорського, 2021.
9. Бурячок В. Л. Основи формування державної системи кібернетичної безпеки : монографія. Київ, 2020.

10. Бурячок В. Л., Гулак Г. М., Толубко В. Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : підручник. Київ, 2021.
11. Ільєнко А., Ільєнко С., Яковенко О. Перспективи інтеграції штучного інтелекту в системи кібербезпеки. *Кібербезпека: освіта, наука, практика*. 2023. № 1. С. 112–119.
12. Індекс медіаграмотності українців: 2025 (Коротка презентація). ГО «Детектор медіа». 2026. URL: https://detector.media/infospace/article/248338/2026-03-15-indeks-mediagramotnosti-ukraintsiv-2025-korotka-prezentatsiya/ (дата звернення: 11.04.2026).
13. Інформаційна безпека України: виклики та нові стратегії. Національний інститут стратегічних досліджень. URL: https://niss.gov.ua (дата звернення: 11.04.2026).
14. Кулеба Д. Війна за реальність. Як перемагати у світі фейків, правд і спільнот. Київ : Книголав, 2019. 384 с.
15. Курбан О. В. Фейки у сучасних медіа: ідентифікація та нейтралізація. Київ, 2020.
16. Лунгол О. Огляд методів та стратегій кібербезпеки засобами штучного інтелекту. *Кібербезпека: освіта, наука, практика*. 2023. № 2. С. 18-25.
17. Мережа хабів цифрової освіти. Міністерство цифрової трансформації України. URL: https://osvita.diia.gov.ua/hubs (дата звернення: 04.05.2026).
18. Навчання медіаграмотності. Публічна бібліотека імені Лесі Українки. URL: https://lukl.kyiv.ua/navchannya-mediahramotnosti/ (дата звернення: 10.03.2026).
19. Національний проєкт з медіаграмотності «Фільтр» Міністерство культури та інформаційної політики України. URL: https://filter.mkip.gov.ua/ (дата звернення: 07.05.2026).
20. Негодченко В. Основні напрями державної інформаційної політики в Україні. *Підприємництво, господарство і право*. 2016. № 4. С. 77–81.

21. Пазиніна І. С., Корчомний Р. О. Розробка рекомендацій щодо зниження кіберзагроз на час віддаленої роботи з точки зору кібербезпеки. *Кібербезпека*. 2022. С. 45-51.
22. Почепцов Г. Г., Чукут С. А. Інформаційна політика : підручник. Київ : Знання, 2006. 663 с.
23. Проєкт BRAMA. Департамент кіберполіції. URL: https://cyberpolice.gov.ua/brama/ (дата звернення: 04.05.2026).
24. Пугачов О. І. Проблеми забезпечення інформаційної безпеки України в сучасних умовах. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. 2024. № 12. С. 45–52.
25. Українські медіа, ставлення та довіра у 2023 році. USAID-Internews. URL: https://internews.in.ua/uk/news/ukrainian-media-consumption-and-trust-in-2023/ (дата звернення: 04.05.2026).
26. Центр протидії дезінформації. Офіційний сайт. Аналітика та звіти. URL: https://cpd.gov.ua/ (дата звернення: 08.05.2026).
27. Braman S. Change of State: Information, Policy, and Power. Cambridge : MIT Press, 2006. 576 p.
28. Rowlands I. Understanding information policy: concepts, frameworks and research tools. *Journal of Information Science*. 1996. Vol. 22, No. 1. P. 13–25.

ДОДАТКИ

Додаток А

Маріупольський державний університет

ЗАТВЕРДЖУЮ
Ректор МДУ
Микола ТРОФИМЕНКО
18.09. 2023 р.

ПОСАДОВА ІНСТРУКЦІЯ
ФАХІВЦЯ ЗАГАЛЬНОГО ВІДДІЛУ

І. Загальні положення

1. Дана посадова інструкція визначає функціональні обов'язки, права і відповідальність фахівця загального відділу Маріупольського державного університету (далі - Університет).

2. Фахівець загального відділу (далі - Фахівець) належить до професійної групи «Фахівці» (КП – 3435.1).

3. Призначення на посаду Фахівця, звільнення з неї здійснюється наказом ректора Університету за погодженням начальника загального відділу з дотриманням вимог чинного законодавства про працю.

4. Фахівець безпосередньо підпорядковується начальнику загального відділу.

5. За відсутності Фахівця з поважних причин його обов'язки виконує особа, призначена у встановленому порядку, яка набуває відповідних прав та несе відповідальність за неналежне виконання покладених на неї обов'язків.

ІІ. Завдання та обов'язки

Фахівець зобов'язаний:

1. Приймати, реєструвати кореспонденцію і направляти її в структурні підрозділи Університету.

2. Відповідно до резолюцій ректора та/або проректорів Університету передавати документи на виконання працівникам структурним підрозділам, іншим працівникам.

3. Вести облік проходження документів, здійснювати контроль за їх виконанням.

4. Відправляти вихідну документацію адресатам.

5. Вести облік отриманої і відправленої кореспонденції, систематизувати і зберігати документи поточного архіву.

6. Здійснювати оформлення справ загального відділу, готувати і здавати до архівного відділу Університету документи постійного та тривалого строку зберігання.

7. Забезпечувати зберігання службової документації.

8. Засвідчувати копії або витяги установчих, службових документів Університету.

9. Приймати та передавати телефонограми, доводити до відома зацікавлених осіб їх зміст.

10. Здійснювати роботи щодо підготовки засідань і нарад, які проводить ректор (збирання необхідних матеріалів, повідомлення учасників про час, місце і порядок засідань або нарад, ведення реєстрації), оформляти протоколи.

11. Передавати та приймати інформацію за допомогою приймально-передавальних пристроїв.

12. Друкувати накази, розпорядження та службові листи.

13. Здійснювати облік, зберігання та видачу бланків документів, своєчасно подавати замовлення на їх виготовлення.

14.Забезпечувати досягнення цільових показників ефективності та щорічне звітування про їх виконання.

15. Організовувати діловодство в загальному відділі.

16. Раціонально й ефективно організовувати працю на робочому місці.

17. Додержуватися норм, методів і прийомів безпечного ведення робіт.

18. Знати та дотримуватися норм ділової поведінки та етики професійних відносин.

19. Забезпечувати розвиток єдиної електронної інформаційної бази документації університету, розширення системи електронного документообігу тощо.

20. Знати та виконувати вимоги нормативних актів про охорону праці і навколишнього середовища, правила безпечного поводження з устаткуванням, машинами, механізмами, користуватися засобами колективного та індивідуального захисту.

21. Знати, дотримуватися та виконувати положення Правил внутрішнього розпорядку Університету, Колективного договору, положень або інструкцій Університету стосовно діяльності Фахівця.

III. Права

Фахівець має право:

1. Ознайомлюватися з проєктами рішень Адміністрації Університету, що стосуються його діяльності.

2. Вносити на розгляд Адміністрації Університету пропозиції по вдосконаленню роботи, пов'язаної з обов'язками, що передбачені цією посадовою інструкцією.

3. В межах своєї компетенції повідомляти Адміністрацію Університету про всі виявлені недоліки в діяльності Університету (структурних підрозділів, окремих працівників) та вносити пропозиції щодо їх усунення.

4. Вимагати та отримувати особисто або за дорученням ректора, начальника загального відділу у керівників структурних підрозділів та інших працівників інформацію та документи, необхідні для виконання його обов'язків.

5. Вимагати від Адміністрації Університету сприяння у виконанні обов'язків, передбачених цією посадовою інструкцією.

IV. Відповідальність

1. За неналежне виконання або невиконання своїх посадових обов'язків, що передбачені цією посадовою інструкцією, - в межах, визначених чинним законодавством України про працю.

2. За правопорушення, скоєні в процесі здійснення своєї діяльності, - в межах, визначених чинним адміністративним, кримінальним та цивільним законодавством України.

3. За завдання матеріальної шкоди - в межах, визначених чинним цивільним законодавством та законодавством про працю України.

4. За скоєння корупційних порушень у порядку визначеному чинним антикорупційним законодавством України.

V. Повинен знати

1. Чинне законодавство України в сфері вищої освіти, інструктивні та методичні документи з організації діловодства.

2. Інструкцію з діловодства МДУ.

3. Структуру та режим роботи Університету.

4. Правила експлуатації комп'ютерної та організаційної техніки.

5. Правила протипожежної безпеки, техніки безпеки, охорони праці та навколишнього середовища.

6. Основи антикорупційного законодавства України.

7. Правила внутрішнього розпорядку Університету, Статут Університету, Колективний договір, Стратегічний план розвитку Університету та інші нормативно-правові документи, що регламентують діяльність МДУ.

VI. Кваліфікаційні вимоги

Фахівець загального відділу І категорії: повна або базова вища освіта відповідного напряму підготовки (магістр, спеціаліст або бакалавр); для магістра - без вимог до стажу роботи; для спеціаліста - стаж роботи на посаді фахівця загального відділу ІІ категорії - не менше 2 років; для бакалавра - не менше 3 років.

Фахівець загального відділу ІІ категорії: повна або базова вища освіта відповідного напряму підготовки (спеціаліст, магістр або бакалавр); для спеціаліста, магістра - без вимог до стажу роботи; для бакалавра - стаж роботи на посаді фахівця загального відділу - не менше 2 років.

Фахівець загального відділу: повна вища освіта відповідного напряму підготовки (спеціаліст або бакалавр) без вимог до стажу роботи.

VII. Взаємовідносини (зв'язки) за посадою

1. Для виконання обов'язків та реалізації прав Фахівець взаємодіє з:
- адміністрацією Університету;
- начальником загального відділу;
- керівниками структурних підрозділів Університету тощо.

Начальник загального відділу

_____ Оксана СТРЕТОВИЧ
«____» _____ 2023 р.

Начальник відділу кадрів

_____ Ольга БЛАГІНІНА
«____» _____ 2023 р.

Начальник юридичного відділу

_____ Вікторія ЛУКОВКА
«____ «_____ 2023 р.

Начальник відділу з питань запобігання
та виявлення корупції

_____ Алла НОВІКОВА
«____» _____2023 р.