ПЛАТФОРМА ПРАВ ЛЮДИНИ

ZMINA

Фінансується Європейським Союзом

Стан дотримання цифрових прав в Україні: підсумковий аналітичний звіт за вересень 2025 - травень 2026 року

Стан дотримання цифрових прав в Україні: підсумковий аналітичний звіт за вересень 2025 - травень 2026 року / Л. Опришко, Ю. Мельник. — Київ:
ГО “Платформа прав людини”, 2026. — 74 с.

Це видання опубліковано в рамках проєкту “Посилення захисту цифрових прав в Україні”, який реалізується ГО “Платформа прав людини” у співпраці з Центром прав людини ZMINA за фінансової підтримки Європейського Союзу. Його зміст є виключною відповідальністю ГО “Платформа прав людини” і не обов’язково відображає позицію Європейського Союзу.

Звіт підсумовує результати моніторингу стану дотримання цифрових прав в Україні, проведеного протягом вересня 2025 - травня 2026 року. В ньому відображено відомості про виявлені загрози, пов’язані із реалізацією цифрових прав, існуючі проблеми, а також позитивні зміни, що відбуваються в зазначеній сфері.

Видано ГО “Платформа прав людини”
м. Київ, 2026
www.ppl.org.ua

ЗМІСТ

I. ВСТУП 2
II.ЦИФРОВІ ПРАВА ПІД ТИСКОМ 4
СУЧАСНИЙ СТАН ЦИФРОВОГО СЕРЕДОВИЩА ТА ЦИФРОВОЇ БЕЗПЕКИ... 4
ФІШИНГ 5
ПОШИРЕННЯ ДЕЗІНФОРМАЦІЇ ТА МАНІПУЛЯТИВНОЇ ІНФОРМАЦІЇ..... 6
СВОБОДА ВИРАЖЕННЯ ПОГЛЯДІВ 12
ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ 15
III. МОНІТОРИНГ СУДОВОЇ ПРАКТИКИ У СПРАВАХ ПРО ПОШИРЕННЯ ІНФОРМАЦІЇ В ЦИФРОВОМУ СЕРЕДОВИЩІ..... 16
АДМІНІСТРАТИВНІ СПРАВИ 16
СПРАВИ ПРО АДМІНІСТРАТИВНІ ПРАВОПОРУШЕННЯ 20
ГОСПОДАРСЬКІ СПРАВИ 21
ЦИВІЛЬНІ СПРАВИ 22
КРИМІНАЛЬНІ СПРАВИ 28
IV. БЛОКУВАННЯ ВЕБРЕСУРСІВ 30
V. ВИСНОВКИ І РЕКОМЕНДАЦІЇ..... 39
VI. ДОДАТКИ
Додаток 1. Звіт за результатами проведення зустрічі на тему: "Захист від інформаційних онлайн-атак"..... 45
Додаток 2. Звіт за результатами проведення публічного обговорення на тему: "Протидія поширенню дезінформації та маніпулятивної інформації"..... 53
Додаток 3. Звіт за результатами проведення публічного обговорення на тему: "Стан забезпечення права на доступ до публічної інформації в цифровому середовищі в Україні"..... 61
Додаток 4.Відповідь ЦПД при РНБО щодо методології та системи оцінки інформаційних загроз 69
Додаток 5. Відповідь НПУ щодо розблокування вебресурсу у вересні - листопаді 2025 року 72
Додаток 6.Перелік розблокованих вебресурсів у січні - травні 2026 року.... 73
Додаток 7. Інформація про заблоковані вебресурси 74

ВСТУП

Протягом дев'яти місяців з вересня 2025 по травень 2026 року команда ППЛ збирала інформацію з відкритих онлайнджерел, а також шляхом направлення запитів до органів державної влади чи інших уповноважених органів, щоб оцінити стан дотримання цифрових прав в Україні. Виявлені факти описані у відповідних аналітичних документах, оприлюднених раніше[1].

Цей звіт відображає результати якісного аналізу отриманих відомостей: виявлені проблеми, виклики та загрози для реалізації цифрових прав, види та джерела небезпек, а також позитивні тенденції у зазначеній сфері.

Окремим важливим напрямком спостереження був стан дотримання права на доступ до публічної інформації в цифровому середовищі. Результати цього дослідження містяться в "Звіті за результатами моніторингу стану дотримання права на доступ до публічної інформації в цифровому середовищі в Україні за вересень 2025 - травень 2026 року"[2]. Цей документ є завершеним продуктом, який відображає виклики, проблеми, загрози і досягнення у сфері доступу до публічної інформації. Тому зроблені у ньому висновки і рекомендації не включались до цього звіту. Проте, результати експертного обговорення основних трендів, виявлених під час моніторингу у згаданій області, можна знайти в додатку до цього звіту (Додаток 3).

Одним із основних фокусів цього дослідження є свобода вираження поглядів в інтернеті. Триваюча повномасштабна війна Росії проти України та введений внаслідок цього воєнний стан чинять значний тиск на здійснення зазначеного права. Спеціальні інформаційні операції, широкі кампанії дезінформації та інший деструктивний інформаційний вплив держави-агресора на українців потребують адекватного реагування. Але це в свою чергу створює значні ризики надмірного обмеження свободи вираження та свободи інформації. Чи вдалось Україні знайти необхідний баланс між цим правом та необхідністю захистити національні інтереси? Звіт допоможе знайти відповідь на це запитання.

Інші цифрові права також не залишились поза увагою. Звіт описує стан кібер- та інформаційної безпеки, дотримання цифрових прав дітей та виявлені у зазначеній царині проблеми, способи втручання у приватне життя та іншу важливу інформацію. Аналіз судової практики дає можливість зрозуміти ситуацію із захистом цифрових прав в Україні.

1. Аналітичний звіт ГО "Платформа прав людини" за вересень-листопад 2025 року, https://ppl.org.ua/wpcontent/uploads/2026/03/analitychnyj-zvit-czyfrovi-prava.pdf;
Аналітичний звіт ГО "Платформа прав людини" за грудень 2025-лютий 2026 року, https://ppl.org.ua/wp-content/uploads/2026/05/zvit-czyfrovi-prava-1.pdf;
Аналітичний звіт ГО "Платформа прав людини" за березень-травень 2026 року, https://ppl.org.ua/wp-content/uploads/2026/07/zvit-berezen-traven-2026.pdf;
Аналітичний звіт ГО "Платформа прав людини" "Судова практика у кримінальних справах, пов'язаних із поширенням інформації в мережі Інтернет" за вересень-грудень 2025 року, https://ppl.org.ua/wp-content/uploads/2026/03/zvit-po-porushenyah-czyfrovyh-prav-kryminal.pdf
2. Звіт за результатами моніторингу стану дотримання права на доступ до публічної інформації в цифровому середовищі в Україні за вересень 2025-травень 2026 року, https://ppl.org.ua/wp-content/uploads/2026/07/zvit-dostup-1.pdf

Зазначене дослідження проводилось за методологією, розробленою експертами ГО “Платформа прав людини”.

Підготовлений звіт має чотири основні розділи: “Цифрові права під тиском”, в якому на основі узагальнення зібраної під час моніторингу із відкритих онлайнджерел інформації описано виявлені тренди, проблеми, загрози та виклики, “Моніторинг судової практики у справах про поширення інформації в цифровому середовищі”, де узагальнено основні тренди судової практики, “Блокування вебресурсів”, де описано адміністративну практику блокування сайтів та “Висновки і рекомендації”.

Викладена у цьому звіті інформація може бути корисною дослідникам, аналітикам, медіа та іншим особам, які мають інтерес до теми цифрових прав. Вона також може стати у нагоді органам державної влади і органам місцевого самоврядування при підготовці та реалізації відповідних стратегій, політик і процедур, а також суддям, адвокатам та іншим юристам, які розглядають чи беруть участь у розгляді справ, пов’язаних із поширенням інформації в інтернеті. Це дослідження також робить свій внесок у поширення медіаграмотності.

СУЧАСНИЙ СТАН ЦИФРОВОГО СЕРЕДОВИЩА ТА ЦИФРОВОЇ БЕЗПЕКИ

Інтернет-технології прогресують надзвичайно стрімко і все потужніше впливають на життя людей. Пришвидшення розвитку та використання штучного інтелекту супроводжується значною автоматизацією інтернет трафіку, який вже перевищив діяльність людини в інтернеті. За оцінкою Imperva шкідливі боти складають 37% усього вебтрафіку. Відповідно зростають і пов'язані з цим загрози, оскільки знижується поріг входу для зловмисників і збільшується обсяг атак простих ботів.[3]

Це створює сприятливі умови для збільшення кібернападів та кіберзагроз, широкого поширення дез- та маніпулятивної інформації, вчинення онлайн шахрайства, здійснення скоординованих кампаній дискредитації.

Моніторинг показав, що основними цілями кібернападів є об'єкти життєзабезпечення держави, громади, людини, зокрема у сферах енергетики, логістики, охорони здоров'я, освіти, телекомунікацій та в інформаційній сфері.

Такі напади спрямовувались переважно на державні установи, органи місцевого самоврядування, державні та комунальні підприємства, Сили оборони України та військовослужбовців, банки, журналістів і медіа, неурядові організації, а також бізнес, який виступає підрядником або партнером сектору безпеки і оборони чи державних установ.

Внаслідок кібератак мали місце:

- зупинки або спроби зупинки електронних сервісів;
- зараження комп'ютерів шкідливим програмним забезпеченням;
- видалення інформації та поширення недостовірних відомостей;
- гальмування роботи веб-сайтів або тимчасова зупинка їх роботи;
- викрадення інформації, зокрема, персональних даних;
- списання грошових коштів з рахунків в банках;
- викрадення криптовалюти;
- "злам" домашніх Wi-Fi роутерів та наступне перенаправлення їх трафіку через заздалегідь розгорнуту мережу DNS-серверів з метою збору паролів, токенів автентифікації та іншої чутливої інформації, включно з електронними листами тощо.

Окремою ціллю зловмисників є діти. Цифрові технології полегшують їх залучення до вчинення злочинів. Зокрема, неповнолітніх систематично вербують для здійснення диверсій і терористичних актів, використовуючи для цього як телеграм-канали, так і онлайн-ігри.[4]

3. https://www.imperva.com/resources/resource-library/reports/2025-bad-bot-report/
4. https://www.facebook.com/kidspoliceNPU/posts/pfbid02Txf4dRj9AJkEg52GkY8iAP3hjIMrfscu5xZLLUTdKKFjFV8tJ1KQQhQdc7AyJmKCl?rdid=aiT9djLn8f8zP4zg

ФІШИНГ

Серед кіберзагроз чи не найпоширенішою є фішинг - тип кібератаки, під час якої зловмисники вдають із себе надійні джерела, щоб вкрасти конфіденційну інформацію. Він нерідко використовується з метою вчинення шахрайства.

Розвиток цифрових технологій і, зокрема, штучного інтелекту, полегшили вчинення фішингу. Створення підроблених вебсайтів і онлайн-повідомлень стало дешевшим, а виготовлена фальшивка стала якіснішою. Відрізняти цифрову імітацію від оригіналу стає все важче. Водночас шахрайські оголошення можуть швидко поширюватись і масштабуватись на числених цифрових інформаційних майданчиках. І як наслідок - активно впливати на поведінку все більшої кількості людей, граючи на їхніх емоціях: страху, економічній вразливості, поспіху тощо.

Інформація, зібрана під час моніторингу свідчить про те, що фішингові атаки нерідко здійснюються шляхом поширення повідомлень на підроблених вебсайтах чи вебсторінках. Наприклад, шахрайські листи розповсюджувались на підробленій сторінці для оплати товару, що продавався через інтернет, яка копіювала дизайн сервісу “ОЛХ-доставка” або банківський термінал. Крім того, у месенджері Telegram створювали фальшиві профілі, що маскувались під офіційні сторінки мобільних операторів або робили вебресурси, які імітували легітимні торгові криптоплатформи.

Фішинг також вчиняється шляхом розповсюдження оголошень, що мають айдентику органів державної влади чи місцевого самоврядування, а також через розсилку повідомлень, зокрема, від імені:

- органів державної влади (Державної податкової служби України, Міністерства енергетики України, НАБУ, БЕБ, CERT-UA та Держспецзв’язку тощо);
- державних сервісів (наприклад, офіційного вебресурсу Головного сервісного центру МВС України);
- державних підприємств (НЕК “Укренерго”);
- банків (зокрема, Національного банку України, Приватбанку, Ощадбанку);
- поштових операторів, переважно "Укрпошти" та "Нової пошти";
- бізнесу (наприклад, АЗС);
- популярних медіа, які мають довіру значної аудиторії, серед яких “Українська правда”, “1+1”, 5 канал та інші, а також платформи Мета.

Часто густо такі повідомлення таргетуються на конкретно визначені аудиторії шляхом зазначення теми, яка викликає довіру, зокрема:

- "протидія російським диверсійно-розвідувальним групам" - для військових;
- бухгалтерська тематика, повідомлення про проведення “фінансової перевірки за фактом легалізації коштів”, “розбіжностей у звітності”, про нібито наявний податковий борг з вимогою його термінового погашення - для бухгалтерів, керівників підприємств, установ, організацій, інших платників податків;
- “графік відключення електроенергії” - для жителів населених пунктів, де введено обмеження електропостачання внаслідок російських обстрілів;
- присвоєння “синьої галочки” - для користувачів Instagram та Facebook;

ФІШИНГ

- “Зимова допомога”, “Тепло весни”, виплати від міжнародних організацій, “гуманітарна допомога”, “еДопомога”, “соціальна допомога” - для соціально незахищених осіб;
- "оновити дані для доставки посилки" - для користувачів поштових сервісів;
- “підтвердити вік” - для пенсіонерів;
- “супровід” у торгівлі криптовалютою - для тих, хто купував чи продавав такі активи тощо.

Моніторинг показав, що **для вчинення фішингу використовувались також бренди популярних медіа**, зокрема таких як “Українська правда”, “1+1”, “5 канал” та інші, а також платформа Мета.

Крім того, були випадки, коли невідомі, представляючись журналістами російських медіа, писали у Telegram і пропонували організувати відеозв’язок із полоненими. У таких повідомленнях часто надсилались файли, які пропонували встановити на телефон, як “спеціальний додаток для відеоконференцій”. Але насправді ці файли містили віруси, після встановлення яких зловмисники отримували віддалений доступ до телефону, особистих даних і навіть до інтернет-банкінгу користувача.

ПОШИРЕННЯ ДЕЗІНФОРМАЦІЇ ТА МАНІПУЛЯТИВНОЇ ІНФОРМАЦІЇ

Інформаційне поле України насичене повідомленнями про фейки, дезінформацію та маніпулювання суспільною думкою, а також їх спростуваннями. Тут на регулярній основі працюють Центр протидії дезінформації при Раді національної безпеки і оборони та Центр стратегічних комунікацій, який став частиною комунікаційної спільноти МЗС України. Крім того, до публічного спростування недостовірної інформації долучаються органи державної влади, органи місцевого самоврядування та їхні представники.

Активну роль у боротьбі із шкідливими інформаційними впливами відіграють фактчекерські та інші неурядові організації, журналісти, медіа, блогери тощо.

Всі вони регулярно розвінчують дезінформацію та інформаційні маніпуляції, публікуючи як окремі повідомлення на цю тему, так і аналітичні звіти.

Це свідчить про те, що в Україні вже склалась певна децентралізована екосистема протидії шкідливим інформаційним впливам, що включає широке коло як державних, так і недержавних учасників, яка функціонує на демократичних засадах. Дослідники деструктивних інформаційних впливів часто густо в своїй роботі оперують термінами “дезінформація” та “маніпуляція інформацією”. Проте, кожен із них здійснює оцінку шкідливого контенту на власний розсуд, послуговуючись при цьому й власною методологією.

Ба більше, деякі з цих методологій віднесено до інформації з обмеженим доступом. Зокрема, це стосується методології та системи оцінки інформаційних загроз і оперативного реагування на них Центру протидії дезінформації при РНБО, яку наказом Центру від 25.12.2023 No 76 віднесено до службової інформації (див. Додаток 4).

Відповідно, у публічному та політичному дискурсі поняття “дезінформація” та “маніпулятивна інформація” вживаються переважно у дуже загальному і неточному значенні.

Такий стан речей не є критичним, поки мова йде про швидке публічне розвінчання неправдивих фактів, що можуть завдати суттєвої шкоди державі, зокрема її обороноздатності, підірвати довіру до інституцій чи спотворити демократичні процеси.

Але коли наведена термінологія використовується для ухвалення рішень про застосування правових санкцій за поширення шкідливої інформації, ситуація кардинально змінюється.

Наприклад, під час моніторингу виявлено судову справу про блокування онлайн медіа “Антикор” (ідентифікатор медіа: R40-05143) на підставі рішення Національного центру оперативно-технічного управління електронними комунікаційними мережами України (далі – НЦУ). З судових документів[5] слідує, що причиною блокування стали звинувачення у тривалому систематичному поширенні російської дезінформації та сприянні РФ у здійсненні деструктивних інформаційних впливів в Україні та світі. Тобто, за поширення “дезінформації” застосовано реальні санкції у виді блокування діяльності медіа.

Вказане рішення викликає серйозне занепокоєння. Адже для накладення юридичних санкцій необхідно мати чіткі і точні дефініції “дезінформації”, “маніпулятивної інформації”, “наративу”, “інформаційного впливу”, а також науково обгрунтовану методологію їх ідентифікації, доступну широкому загалу. І це окрім відповідних правових підстав, які б дозволяли застосовувати такого роду обмеження діяльності медіа, яких наразі в українському законодавстві також немає.

Таким чином, ні програмні документи публічної політики, ні законодавство України не містять визначення зазначених понять. Таке становище не дозволяє забезпечити аналітичну та юридичну точність і передбачуваність в означеній сфері.

Водночас, робота по напрацюванню згаданих визначень в Україні ведеться. Зокрема, Міністерство культури України розробило і оприлюднило на своєму веб-сайті проект Стратегії інформаційної безпеки[6]. Цей документ містить, зокрема, визначення “дезінформації”, під якою пропонується розуміти “цілеспрямоване поширення

5. https://reyestr.court.gov.ua/Review/130697730#
6. https://mincult.gov.ua/wp-content/uploads/2025/11/proyekt_strategiyi.pdf

неправдивої або маніпулятивної інформації з метою введення в оману, дестабілізації суспільних процесів, підриву довіри до державних інституцій та впливу на ухвалення рішень".

Включення зазначеного терміну до документу програмного характеру може допомогти вирішити описану проблему. Проте, ця дефініція потребує уточнення з кількох причин.

По-перше, вона не узгоджується з європейськими підходами до визначення дезінформації, в якому основний акцент зроблено на контенті, а не на діяльності - "поширенні інформації". Зокрема, відповідно до Рекомендації CM/Rec(2022)11 Комітету міністрів державам-членам щодо принципів управління медіа та комунікаціями, дезінформація - це інформація, неправдивість, неточність або оманливість якої підтверджено, що створюється і поширюється умисно з метою заподіяння шкоди або отримання економічної чи політичної вигоди шляхом обману громадськості.[7] Зважаючи на процес євроінтеграції України, видається доцільним привести зміст терміна "дезінформація" у відповідність до вищенаведеного.

По-друге, запропоноване визначення ставить знак рівності між дезінформацією та маніпулятивною інформацією, що також не узгоджується із європейським підходом. Останній розглядає маніпулювання інформацією як спосіб дії в інформаційній сфері і не виділяє таку інформацію в окремий підвид дезінформації. Натомість, залежно від умислу і шкоди, яку може завдати інформація, застосовує ширший спектр термінів: окрім "дезінформації", ще й "місінформація" ("misinformation") - помилкова інформація - неправдива або оманлива інформація, поширена без наміру заподіяти шкоду та "малінформація" ("malinformation") - зловмисна інформація - достовірна інформація, поширена з метою заподіяння шкоди, часто шляхом переміщення інформації, призначеної для приватного використання, у публічну сферу. Такий термінологічний апарат дозволяє точніше ідентифікувати шкідливий контент і визначити засоби протидії його впливу.

З огляду на це аналогічні визначення доцільно було б включити до програмних документів України. Це дозволило б краще розмежовувати різні види шкідливого контенту і відділяти допустимі в демократичному суспільстві висловлювання, від тих, що спрямовані на підрив демократії, демократичних цінностей і процесів.

Водночас, на нашу думку, закріплення понять "дезінформація", "маніпулятивна інформація" в законодавстві України нестиме значні ризики надмірного втручання у свободу вираження поглядів, оскільки їх зміст є надто широким і неточним. Адже застосування такої термінології неодмінно вимагатиме оцінки правдивості інформації, що дуже важко неупереджено зробити на практиці. Постануть також питання про те, хто саме повинен визначати ступінь правдивості інформації і що буде еталоном правди; чи можна буде вважати дезінформацією відомості, які є

7. Рекомендація CM/Rec(2022)11 Комітету міністрів державам-членам щодо принципів управління медіа та комунікаціями: https://search.coe.int/cm/eng?i=09125948802680f5

неправдивими лише частково та багато інших. Не менш проблемним буде питання доказування умислу на поширення дезінформації, оскільки в сучасному світі відомості підхоплюються і поширюються численними медіаучасниками, кожен з яких має свою мету і може просто не знати про недобрі наміри творців шкідливого контенту. Ще складніше буде довести причинно-наслідковий зв'язок між поширенням дезінформації та ймовірною шкодою, яку може вона спричинити.

З огляду на це, до введення терміну "дезінформація" в законодавство України потрібно ставитись надзвичайно обережно, щоб не завдати шкоди публічним обговоренням і демократії в цілому.

Цілі дезінформації. Неправдиві повідомлення, виявлені під час моніторингу, спрямовувались на:

- отримання політичних дивідендів або економічної вигоди;
- дискредитацію українських органів влади, зокрема, Президента України, НАБУ, НГУ, ТЦК, ЗСУ, СОУ;
- дискредитацію Європейського Союзу та його політиків;
- дискредитацію українських політиків, волонтерів, військових, капеланів;
- дискредитацію мобілізації в Україні;
- залякування, глорифікацію злочинів РФ і нав'язування мовних наративів Росії, перекручення історії;
- збільшення рівня напруги в українському суспільстві;
- розпалювання ворожнечі стосовно "мігрантів", що прибули до України тощо.

Найпоширеніші дез- та маніпулятивні повідомлення стосувались таких тем:

- мобілізації і військової служби в Україні, зокрема, нібито зниження мобілізаційного віку, нібито масових спроб уникнути служби та мобілізації жінок, а також "примусової мобілізації осіб з особливостями розвитку";
- нібито підготовки Україною провокацій, зокрема, атак на НПЗ в Європі, "хімічної провокації, щоб звинуватити в цьому Росію" тощо;
- нібито наявності катастрофічних втрат на війні, скарг на те, що влада "не хоче завершення війни";
- про "злочини під час української евакуації", "зникнення дітей" і навіть "чорну трансплантологію";
- перемоги у війні та переговорів про мир, в тому числі про "мир будь-якою ціною", про те, щоб "віддати стільки землі, скільки потрібно для миру, а на залишках будувати нове";
- "недоговороспроможності" Президента України В. Зеленського, його нечесності (підроблене відеозвернення Президента на фоні викраденої картини);
- нібито наявності у Президента України Володимира Зеленського паспортів "однієї або декількох" іноземних держав, начебто наявності в нього наміру втекти з України через "неминуче" викриття причетності до розкрадання іноземної допомоги та невдоволення адміністрації США діями політичного керівництва України;

- нібито наміру першої леді України Олени Зеленської взяти участь в організації евакуації українських дітей-сиріт до Туреччини, щоб передати їх у рабство;
- нібито "привласнення" Україною перемоги в Ірані;
- відмови ОАЕ від українських систем боротьби з безпілотниками через їхню "повну неефективність";
- економічних та гуманітарних проблем, пов'язаних із війною, зокрема, нібито запровадження графіків обмеження газопостачання; відключення світла тощо, які не вводились;
- нібито підготовки заворушення в Будапешті за сценарієм Майдану;
- мігрантів в Україні;
- нібито роздачі "благодійних великодніх наборів" від міжнародних організацій чи "грошової допомоги" від Пенсійного фонду України.

Важливо звернути увагу й на **методи дезінформування та маніпуляції громадською думкою.** Зокрема, під час моніторингу зафіксовано, що для таких цілей:

- поширювали відео, згенероване штучним інтелектом, зміст якого спрямовувався на підрив суспільної стійкості (наприклад, із закликами здатись або відео про "масові протести в містах України", яких насправді не було);
- створювали та поширювали підроблені аудіофайли та відео. Деякі з них виготовлялись на основі реальних відеозаписів із накладенням нового звуку, інші - переважно провокативного характеру (наприклад, ролик про нібито підготовку Україною атак дронами на НПЗ у Європі) - розповсюджувались під фальшивим авторством, приписаним, наприклад, організації С14. Подекуди точками входу такого роду інформації в інформаційне поле України ставали деякі українські веб-ресурси;
- розповсюджували постановочні відео (наприклад, про підготовку заворушення в Будапешті за сценарієм Майдану);
- поширювали підроблені матеріали (статті, відео тощо), замасковані під публікації західних медіа;
- створювали на різних інформаційних онлайн-платформах (зокрема, у Telegram) підроблені сторінки, канали тощо, в тому числі, імітовані під офіційні вебресурси органів влади, військового командування, державних підприємств, установ і організацій, а також міських голів, державних службовців, на яких поширювали неправдиву інформацію;
- створювали та поширювали неправдиві матеріали через російські медіа, зокрема: пропагандистський телепроєкт "Вести недели" з Андрієм Григор'євим, видання: "Комсомольская правда", "Аргументы и факты" і Rambler;
- підробляли за допомогою ШІ зображення нібито полонених військових для обману родичів українських Захисників і Захисниць з шахрайською метою;
- створювали неправдиві оголошення і поширювали їх в мережі інтернет;

[6]

- створювали за допомогою ШІ матеріали із використанням цифрового образу популярних українських ведучих для просування проросійських меседжів, сюжетів чи наративів, а також образу однієї з перекладачок жестової мови - для поширення неправдивої інформації;
- зламували акаунти журналістів та/або їхні блоги для поширення на цих вебресурсах неправдивого контенту.

Крім того, для розповсюдження російської дезінформації використовувались колишні працівники українських спецслужб, які зрадили Україну. Їх залучали до написання і презентації пропагандистської літератури, а потім додатково поширювали цю інформацію в медіа.

Дезінформація проти України та українців поширювалась не лише в Україні, але й за кордоном. Нерідко інформаційні потоки мали ознаки спланованих та скоординованих дезінформаційних кампаній. Вони були особливо помітними під час проведення Олімпійських ігор в Італії, напередодні міжнародних зустрічей, виборів в Угорщині тощо. Це означає, що системну роботу з протидії дезінформації необхідно вести не лише в Україні, а й за її межами.

Найбільшим першоджерелом дезінформації є Російська Федерація, пов'язані з нею державні і недержавні актори та їхні мережі (спецслужби РФ, проросійські мережі ботів і блогерів, а також колишні співробітники українських спецслужб, залучені до створення пропаганди).

Технологічним інструментом, що збільшує ризики широкого поширення дезінформації, все частіше стає генеративний ШІ, який здешевив і масштабував виробництво підробок. Монетизація платформами акаунтів осіб, що перебувають під санкціями ЄС (дослідження What to Fix), та економічний інтерес шахраїв вказують на економічні чинники, які сприяють поширенню дезінформації. До того ж, недостатня спроможність офіційної державної комунікації перехопити увагу користувачів платформ на фоні алгоритмічних рекомендацій, які пропонують емоційний і клікбейтний контент, роблять неправдиві повідомлення більш видимими.

Разом з тим, під час моніторингу зафіксовано два випадки, коли джерелом поширення неправдивої або оманливої інформації виступали посадові особи місцевого самоврядування[8][9].

Підсумовуючи викладене, необхідно зазначити, що в Україні сформувалась дієва екосистема виявлення та розвінчання неправдивої та оманливої інформації. Взаємодоповнююча діяльність органів влади, недержавних організацій, медіа та журналістів із викриття дезінформації зменшує її шкідливий вплив і сприяє медіаграмотності українців. Водночас, продукування дезінформації у великих

8. https://www.facebook.com/mbakhmatov/posts/pfbid0MFdKK7AF3Xrvw13WmRz6Am9uETTT14C3gsT4oyShTyy4Ub3mbEzcRbMzzJwhUMHel; https://kyivcity.gov.ua/news/kmda_zvernulasya_do_natspolitsi_schodo_poshirennya_golovoyu_desnyansko_rda_nedostovirno_informatsi/
9. https://www.facebook.com/mbakhmatov/posts/pfbid0MFdKK7AF3Xrvw13WmRz6Am9uETTT14C3gsT4oyShTyy4Ub3mbEzcRbMzzJwhUMHel; https://kyivcity.gov.ua/news/kmda_zvernulasya_do_natspolitsi_schodo_poshirennya_golovoyu_desnyansko_rda_nedostovirno_informatsi/

масштабах, зокрема, завдяки використанню штучного інтелекту, широке її поширення внаслідок застосування цифрових технологій, експлуатація чутливих тем посилюють її вплив на суспільство і потребують подальшої системної роботи щодо протидії цим деструктивним впливам.

СВОБОДА ВИРАЖЕННЯ ПОГЛЯДІВ

Цифрові технології сприяють створенню значної кількості онлайн майданчиків для публічних обговорень усіх суспільно-важливих питань. Вони забезпечили доступ широкої громадськості до різнобічної інформації і дозволили кожному робити свій власний внесок у суспільну дискусію. Створено також нові можливості у сфері освіти, розваг тощо. І цей вплив, безумовно, є позитивним.

Водночас, цифрові технології значно полегшили здійснення системного контролю за діяльністю журналістів. Відтепер стеження за ними не обмежується лише окремими державними операціями. Сучасна система спостереження перетворилася на глобальну індустрію, що включає комерційних постачальників шпигунського програмного забезпечення, телекомунікаційну інфраструктуру та слабкий або відсутній нагляд.[10] І це, безумовно, чинить значний тиск на свободу вираження поглядів.

Поряд з цим, додаткові загрози виникають у зв'язку з повномасштабною війною, яку вже більше чотирьох років Росія веде проти України. Вербування російськими спецслужбами виконавців диверсій і терактів з використанням цифрових застосунків, зокрема Telegram, викликає дедалі палкіші дискусії щодо обмеження його роботи з міркувань безпеки, або, принаймні, унормування користування ним в Україні.[11]

Окремою проблемою є зловживання свободою слова. Наприклад, моніторинг показав, що розповсюджуються заклики до повалення конституційного ладу (зокрема, заклики до створення так званої "Української самоврядної народної республіки" (УСНР). І, що найгірше, поширювачі такої інформації мали журналістські посвідчення.[12]

На глобальному рівні - виявлено, що Facebook, YouTube, TikTok та X укладали угоди про монетизацію з особами, що мають проросійські облікові записи, які перебувають під санкціями ЄС за їхню залученість до інформаційних маніпуляцій і втручань (FIMI). Більшість із них залишалися активними станом на квітень 2026 року.[13] Відповідне дослідження оприлюднила некомерційна організація What to Fix.

Моніторинг також зафіксував, що у період з вересня 2025 по травень 2026 року серйозну загрозу реалізації права на свободу вираження поглядів онлайн в Україні становили: погрози і тиск на журналістів і медіа; перешкоджання законній професійній діяльності журналістів; кампанії дискредитації; обмеження свободи

10. https://www.ifj.org/media-centre/news/detail/category/brave/article/global-ifj-study-exposes-worldwide-systemic-surveillance-of-journalists
11. https://www.radiosvoboda.org/a/news-mvs-sbu-vrehulyuvannya-robota-telehram/33686273.html
12. https://vin.gp.gov.ua/ua/news.html?_m=publications&_t=rec&id=412933 https://drive.google.com/file/d/1L1tmswlS_yv7hTLFwNKjAP9aVRRaEQ2A/view;
13. https://ms.detector.media/sotsmerezhi/post/39271/2026-05-25-prorosiyski-akaunty-povyazani-z-lyudmy-pid-sanktsiyamy-ies-mayut-dostup-do-monetyzatsii-u-feysbuku-yutubi-tiktoku-y-x-doslidzhennya/

слова з боку Росії на тимчасово окупованих територіях України та щодо громадян України. Спостерігалось також гендерно-зумовлене онлайн насильство щодо жінок-журналісток та керівниць видань.[14]

Погрози і тиск застосовувались до журналістів і журналісток, які публікували матеріали на гострі теми: розслідування ймовірного завищення ціни на дрони; загибелі мобілізованого ТЦК від черепно-мозкової травми; стану об'єктів критичної інфраструктури (зокрема, водогону); критики керівництва Збройних сил України; непрозорого використання благодійних коштів; нападів на співробітників Територіальних центрів соціальної підтримки та комплектування; діяльності релігійних організацій в Україні тощо. До тиску також вдавались для перешкоджання оприлюдненню статті про сумнівні бронювання від мобілізації працівників та власників одного з підприємств.

Моніторинг дозволив виявити такі способи незаконного впливу:

- погрози зверненням до СБУ;
- приниження ділової репутації медіа, честі, гідності журналісток та журналістів шляхом поширення у дописах в соціальних мережах, коментарях, а також у приватних повідомленнях неправдивої та або маніпулятивної інформації та образ, в тому числі мізогінних коментарів, як то: "іді варі борщі", "на кухню" тощо на адресу журналісток;
- погрози поширення дискредитуючої інформації;
- публічні заклики до збору персональних даних і їх оприлюднення;
- поширення фотографій із персональними даними та адресою редакції;
- направлення безпідставних скарг до Google нібито у зв'язку з порушенням авторських прав та ймовірно з метою вилучення журналістських матеріалів з індексації пошуковими системами або для зменшення їх охоплення;
- анонімні дзвінки та повідомлення із залякуванням, зокрема — із погрозами фізичної розправи тощо.

Моніторинг підтвердив наявність давньої проблеми надмірної й непрозорої модерації інформації з боку платформ (Facebook, Instagram, YouTube, BlueSky), які блокували чи видаляли український контент про колишнього українського високопосадовця, задіяного в одному з корупційних скандалів, про руйнування, завдані російськими військами цивільним об'єктам в Україні (будівлі Суспільного мовника, житловому будинку тощо); зображення українського військовослужбовця в уніформі, інші дописи, пов'язані із війною Росії проти України, а також дописи, які не подобались прихильникам певних політичних сил (зокрема, В. Орбана).

Цілеспрямовані та скоординовані кампанії дискредитації також фіксувалися під час моніторингу. Вони набули поширеності і стали вагомим інструментом тиску на учасників публічних обговорень та на демократичні процеси. Зокрема, зафіксовано

14. https://wim.org.ua/materials/study-ai-unesco/

дискредитаційні кампанії проти журналістів, медіа, неурядових організацій та їх очільників, народних депутатів, а також кандидатів на посаду ректора закладу вищої освіти напередодні проведення відповідних виборів.

Моніторинг показав, що зазначені кампанії як правило велись із використанням анонімних вебресурсів. Вони супроводжувались широким розповсюдженням протягом нетривалого часу компроменуючих повідомлень, заснованих на одних й тих самих неправдивих фактах, або містили маніпулятивний контент. Як правило така інформація стосувалась особи жертви, а не його чи її публічних виступів або висловлювань. Зокрема, вона містила звинувачення у здійсненні “пропаганди”, фігуруванні у “секс-скандалах”, “підозрі в корупції”, ухиленні від мобілізації та служби в армії”, “роботі за російські гроші” чи на виконання завдань від “проросійських осіб” тощо. Зафіксовано також непоодинокі випадки виготовлення дискредитуючих матеріалів за допомогою штучного інтелекту і їх наступне поширення.

Моніторинг зафіксував й факти перешкоджання законній професійній діяльності журналістів. Такі справи розслідуються доволі довго і нерідко - під тиском народних депутатів чи публікацій в медіа, що ставить під сумнів ефективність зазначених розслідувань.

Фіксується значне обмеження свободи вираження поглядів з боку Російської Федерації на окупованих територіях України. Зокрема, мають місце:

- ухвалення вироків через поширення інформації на підтримку України з призначенням покарань у виді позбавлення волі на значні терміни (подекуди до 26 років);
- створення “кабінетів кіберволонтерів”, які відстежують “недостовірну” інформацію, деструктивні теми, а також “роботу центру інформаційно-психологічних операцій” в інтернеті;
- примус встановлювати російський застосунок "Max", який обмежує можливість отримувати і передавати інформацію поза контрольованим Росією цифровим середовищем;
- уповільнення або відключення мобільного інтернету;
- покладення на власників телеграм-каналів зобов’язання після офіційної реєстрації використовувати спеціальний бот, який має право адміністратора і може редагувати та видаляти публікації, а також блокувати коментарі;
- покладення на соцмережі, месенджери, сайти знайомств та інші сервіси з реєстру організаторів поширення інформації (ОРІ) обов’язок зберігати дані користувачів для ФСБ протягом трьох років;
- внесення українського журналіста й блогера до реєстру “іноагентів”;
- блокування мессенджеру Telegram і VPN-сервісів тощо.

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

В сучасних умовах захист персональних даних набуває особливого значення. Адже стрімкий розвиток цифрових технологій і штучного інтелекту залишає все менше простору для приватності. Персональні дані часто густо продаються, купуються і обмінюються як товар. Це створює чимало ризиків і загроз для приватного життя людини, для її душевного спокою і добробуту.

Моніторинг показав, що одним із основних каналів незаконного збору персональних даних залишається фішинг, до якого додаються злами і витоки відповідних баз даних. Крім того, незаконний збір персональних даних користувачів розважальних онлайн-платформ здійснювався за допомогою шкідливого програмного скрипту.

Окремою тенденцією стало опрацювання персональних даних штучним інтелектом без належної згоди (автоматичне сканування пошти Gmail для навчання Gemini; відмова Meta від наскрізного шифрування в Instagram; ризики розумних окулярів Ray-Ban), а також виявлена неефективність cookie-банерів.
Мали місце й випадки **незаконного збору і поширення персональних даних посадовими особами державних органів**, зокрема: безпідставне внесення персональних даних жінки до реєстру військовозобов'язаних; незаконний збір інформації про місце перебування особи за допомогою системи міського відеонагляду "Безпечне місто" і її незаконна передача третім особам.

Спостерігається й інший тривожний тренд, який лише набирає обертів: зростає поширення так званої "**mal-information**". Виявлено цілу низку випадків розповсюдження в інтернеті інтимних фото і відео з метою компроментування жертв. Для тиску на останніх використовуються й погрози оприлюднення такого роду відомостей.

Нерідко поширювачами інтимного контенту виступали колишні партнери потерпілих. Але, в одному з інцидентів звинувачення в незаконному оприлюдненні інтимного фото лунали на адресу Державного бюро розслідувань та Офісу Генерального прокурора України.
Зафіксовано також, що спецслужби активно використовують сервіси онлайн-знайомств для вербування. Вони створюють фейкові жіночі акаунти, через які спілкуються з українськими чоловіками і виманюють їхні персональні дані та контакти, а потім схиляють до співпраці.

Таким чином, **чимало порушень у сфері захисту персональних даних має інтимний вимір.**

Крім того, під час моніторингу зафіксовано факт "крадіжки" ідентифікаційних даних особи.[15] Зокрема, зловмисники у соціальній мережі TikTok створили низку фейкових акаунтів, використавши для цього справжнє ім'я відомого українського військовослужбовця, Героя України. Через них вони кілька років збирали кошти

15. https://cyberpolice.gov.ua/news/zbyraly-donaty-vid-imeni-vidomogo-geroya-ukrayiny-stolychni-policzejski-vykryly-shaxrayiv-4408/

нібито на потреби Збройних сил України та привласнювали їх.

Моніторинг виявив також повідомлення про незаконне використання фотографії загиблої військовослужбовиці і журналістки для збору коштів на потреби армії, про отримання доступу до персональних даних іншої особи після купівлі цифрової SIM-картки одного з операторів мобільного зв'язку.[16]

Виявлено й факти незаконного оприлюднення посадовими особами МОН України персональних даних неповнолітніх, а також співзасновником одного з банків - фотографії користувачки банку, зробленої під час відеоверифікації. В цьому контексті важливо відмітити швидке реагування на зазначені події з боку Уповноваженого Верховної Ради України з прав людини, втручання якого допомогло швидко ідентифікувати проблему і вжити заходи, спрямовані на виправлення ситуації, мінімізацію завданої шкоди.[17]

III. МОНІТОРИНГ СУДОВОЇ ПРАКТИКИ У СПРАВАХ ПРО ПОШИРЕННЯ ІНФОРМАЦІЇ В ЦИФРОВОМУ СЕРЕДОВИЩІ

АДМІНІСТРАТИВНІ СПРАВИ

Досліджені під час моніторингу адміністративні справи стосувались порушень мовного законодавства, правил поширення реклами в інтернеті, дискримінаційної реклами, а також блокування онлайн медіа.

Останні, наш погляд, потребують найбільшої уваги. Під час моніторингу, як вже зазначалось, виявлено справу № 320/36779/25, що стосувалась оспорювання рішення Національного центру оперативно-технічного управління електронними комунікаційними мережами України (НЦУ) про блокування онлайн медіа "Антикор" (ідентифікатор медіа: R40-05143). Як слідує з ухвали суду, ймовірною причиною блокування стало тривале систематичне поширення російської дезінформації та сприяння РФ у здійсненні деструктивних інформаційних впливів в Україні та світі.
Позитивним є те, що суд своєю ухвалою про забезпечення позову зупинив дію відповідного розпорядження НЦУ, що дозволило швидко відновити роботу онлайн медіа.

Проте, це не вирішує саму проблему. Непрозорі блокування за рішенням НЦУ і надалі створюватимуть загрозу свободі вираження поглядів. Адже відсутність чітких визначень понять "дезінформація", "наратив", "деструктивні інформаційні впливи" в законодавстві України, їх розмите трактування в публічному дискурсі і аналітичних матеріалах створюють правову невизначеність. До наведеного слід додати, що рішення НЦУ про блокування вебресурсів не містять навіть мінімальної фактичної основи для обмежень, а також належного правового обгрунтування і мотивів

16. Докладніше див., зокрема, Аналітичний звіт ГО "Платформа прав людини" за грудень 2025-лютий 2026 року, стор. 23, https://ppl.org.ua/wp-content/uploads/2026/05/zvit-czyfrovi-prava-1.pdf
17. Докладніше див., зокрема, Аналітичний звіт ГО "Платформа прав людини" за вересень - листопад 2025 року, стор. 15-16, https://ppl.org.ua/wp-content/uploads/2026/03/analitychnyj-zvit-czyfrovi-prava.pdf

ухвалення рішення, що значно ускладнює їх оскарження.

З огляду на це для дотримання вимог частини 2 статті 10 Європейської Конвенції про захист прав людини і основоположних свобод НЦУ та ініціаторам блокувань під час прийняття рішень щодо обмеження доступу до вебресурсів, що мають ознаки медіа, варто бути обачнішими.
Все це підштовхує до висновку: існує нагальна потреба переглянути практику блокування вебресурсів за рішеннями НЦУ.

СПРАВИ ПРО АДМІНІСТРАТИВНІ ПРАВОПОРУШЕННЯ

Під час моніторингу проаналізовано практику розгляду судами справ про булінг (кібербулінг) та невиконання батьками або особами, що їх замінюють, обов'язків щодо виховання дітей (статті 173-4, 184 КУпАП), дрібне хуліганство, пов'язане з поширенням ненормативної лексики в мережі інтернет (стаття 173 КУпАП), поширення неправдивих чуток (стаття 173-1 КУпАП), захист персональних даних і незаконне поширення службової та оборонної інформації (статті 212-5, 212-6 КУпАП), незаконне використання ознак належності до правоохоронних органів (стаття 184-3 КУпАП), порушення мовного законодавства (стаття 188-52 КУпАП), а також про сексуальне домагання з використанням електронних комунікацій (стаття 173-7 КУпАП).

Порушення цифрових прав дітей та інших учасників освітнього процесу виявлено в результаті аналізу рішень у справах про кібербулінг (онлайн цькування) та про невиконання батьками або особами, що їх замінюють, обов'язків щодо виховання дітей. Останні є найчисленнішими, що, на наш погляд, може вказувати на існування серйозних проблем у зазначеній сфері.

Аналіз постанов у справах про невиконання батьками або особами, що їх замінюють, обов'язків щодо виховання дітей показав, що батьків, **найчастіше — матерів** — притягували до адміністративної відповідальності за вчинення їхніми дітьми таких дій:

- здійснення зйомки на телефон однокласників без їх згоди, що викликало обурення останніх і призвело до порушення правил поведінки;
- перегляд у класному кабінеті одного з ліцеїв відео із соціальної мережі "TikTok" та повторення небезпечних дій — так званої гри "собачий кайф" — яка полягала в навмисному створенні стану гіпоксії шляхом затримки дихання та натискання на грудну клітину. Ці дії фіксувались на мобільний телефон, а відео в подальшому розповсюджувалось в соціальній мережі "Instagram";
- оприлюднення відео однокласників із субтитрами, що містять непристойну лексику, та з озвучкою російською музикою, що підриває національно-патріотичний дух громадян та учасників освітнього середовища;
- створення образливого відео та зображення учнів і їх подальше оприлюднення в соціальній мережі;

СПРАВИ ПРО АДМІНІСТРАТИВНІ ПРАВОПОРУШЕННЯ

- поширення фотографій оголених однокласників, деякі з яких були згенеровані за допомогою штучного інтелекту;
- поширення відео інтимного чи порнографічного характеру або фото із зображенням статевих органів;
- здійсненням відеозйомки у вбиральні шкільного туалету та наступному розповсюдженні зробленого запису;
- створення в телеграм-каналі знайомств публікації із використанням фото неповнолітньої особи, яке супроводжувалось образливим підписом, а також подальше її розповсюдження в загальному чаті класу;
- поширення образливих відомостей щодо іншої дитини з використанням “нецензурної лайки”; “нецензурна” лайка під час прямого ефіру у відкритій соціальній мережі; приниження честі та гідності однокласниці під час листування у соціальній мережі Telegram внаслідок використання російської ненормативної лексики;
- поширення стікерів з фотографіями педагогів, що містять ненормативну лексику, та/або поширення коментарів, іншої інформації образливого змісту стосовно педагога;
- створенні відео образливого характеру з фотографій педагогічних працівників без їхньої згоди, інколи - з накладанням аудіодоріжки, що містить нецензурну лексику, та оприлюднення такого відео у групі в соціальній мережі;
- вчинення у школі дрібного хуліганства чи побиття дитини, зйомка таких дій на відео та поширення їх у соціальній мережі;
- знущання над тілом мертвої собаки, зйомка таких дій на відео і поширення останнього в інтернеті;
- обробка фотографії працівника поліції за допомогою додатку “ТікТок”, внаслідок якої останньому накладено маску, що спотворює обличчя, а також оприлюднення в мережі інтернет у соціальній мережі “Facebook” фото, в якому незаконно використано найменування та ознаки належності до Національної поліції України;
- таємному викраденні в приміщенні ліцею мобільного телефону однокласника (за відсутності складу кримінального правопорушення).
- Як покарання у цій категорії справ суд обирав в більшості випадків штраф або попередження, хоча у деяких справах застосовувалось також усне зауваження. Низка проваджень була закрита судами у зв’язку із закінченням строків давності притягнення до адміністративної відповідальності, через відсутність події чи складу адміністративного правопорушення.

Аналіз справ про кібербулінг дозволив виявити таке:

- кібербулінг часто густо пов’язаний із систематичним поширенням в інтернеті словесних образ і принижень, в тому числі з використанням обсценної лексики, а інколи - містить погрози фізичною розправою;
- він нерідко супроводжувався поширенням фотографій або відео жертви без її згоди, деякі з яких містили зображення статевих органів;

- поширення зазначеної інформації здійснювалось у соціальних мережах, в тому числі шляхом створення окремої папки з принизливою назвою, безпосередньо спрямованою проти потерпілої дитини, а також у шкільних чатах.

Найпоширенішим покаранням у справах про булінг був штраф у розмірі від 850 до 1700 гривень. Деякі з таких проваджень було закрито у зв'язку із відсутностістю складу адміністративного правопорушення або через закінчення строків давності притягнення до адміністративної відповідальності. До відповідальності за таке правопорушення як правило притягували **матерів** неповнолітніх правопорушників. Мав місце також випадок притягнення до відповідальності директора ліцею у зв'язку з неповідомленням уповноваженого органу Національної поліції про факт булінгу.

Таким чином, в результаті моніторингу виявлено низку проблем, пов'язаних із захистом прав дітей, а також інших учасників освітнього процесу в цифровому середовищі. Серед них:

- низький рівень знань учнів про основоположні права людини та їх здійснення в цифровому середовищі, зокрема, в частині поваги до гідності і честі людини, її приватності, необхідності забезпечення належного балансу між цими правами і правом на свободу вираження та негативних наслідків порушення зазначених прав;
- прогалини у сексуальному вихованні дітей і пов'язані з цим проблеми визначення меж дозволеного;
- упущення в національно-патріотичному вихованні неповнолітніх;
- деформація ціннісного розвитку дітей і підлітків, внаслідок чого вони часто густо використовують у спілкуванні ненормативну лексику;
- недостатність критичного мислення, через що діти легко погоджуються брати участь у небезпечних інтернет-челенджах тощо.

Усуненню цих недоліків варто вже зараз придяляти значну увагу. І, вочевидь, до вирішення цих питань потрібно залучати не лише батьків, але й учбові заклади, а також широке коло фахівців, оскільки зазначені проблеми мають комплексний характер.

У справах, пов'язаних із поширенням ненормативної лексики в інтернеті (дрібне хуліганство) спостерігається такий основний тренд: суди дедалі частіше визнають соціальні мережі, чати і форуми «громадським місцем», відходячи від вузького, «аналогового» тлумачення цього поняття (показовими є постанови у справах № 583/844/26 та № 708/354/26). Такий підхід існує поруч з більш усталеним, відповідно до якого поширення "нецензурних висловлювань" в інтернеті кваліфікується як вчинення дій, що порушують громадський порядок та спокій. Обидві наведені правові позиції є взаємодоповнюючими і не суперечать одна одній.

Втім, важливо відмітити, що на обґрунтування першої суди навели вагомі, адекватні викликам сьогоднішнього дня аргументи. Вони врахували роль цифрових технологій в сучасному світі, рівень їх використання і вплив на сучасні суспільства. І хоча інерція все ще може гальмувати вкорінення зазначеного підходу до розуміння інтернету, як “громадського місця”, на нашу думку, за ним майбутнє.

До того ж, наведена інтерпретація вже пройшла певну перевірку Європейським судом з прав людини. У справі “Міладзе проти Грузії (Miladze v. Georgia)” заявник наполягав, що втручання у свободу вираження не було передбачене законом, оскільки його притягнули до адміністративної відповідальності за поширення “нецензурних висловлювань” в інтернеті, який не є “громадським місцем”. Він стверджував, що цей термін поширюється лише на фізичне середовище і не може застосовуватись до кіберпростору. Однак, ЄСПЛ цей аргумент відхилив. Він врахував усталену національну судову практику з цього питання і зауважив, що існує загальноприйняте правове розуміння поняття «публічне місце», яке охоплює кіберпростір, зокрема соціальні мережі та інтернет-блоги.[18]

Необхідно також наголосити на тому, що деякі суди намагаються розмежовувати дрібне хуліганство, пов’язане із поширенням в інтернеті ненормативної лексики на адресу інших осіб, від інших, схожих порушень прав людини, зокрема тих, що посягають на честь, гідність і ділову репутацію і мають розглядатись в порядку цивільного судочинства. Такий диференційований підхід дозволяє прицільніше визначати об’єкт правопорушення і застосовувати адекватніші способи правового захисту.

В практиці розгляду справ про поширення неправдивих чуток, що можуть викликати паніку серед населення або порушення громадського порядку спостерігається два протилежні тренди.

З одного боку статтю 173-1 КУпАП намагаються використовувати для боротьби із поширенням ймовірно недостовірних відомостей про особу, які можуть завдати шкоди її честі, гідності та діловій репутації або для протидії поширенню критичних висловлювань чи дезінформації. Втім, такий спосіб правового захисту є неналежним і у разі його вкорінення може негативно впливати на стан свободи вираження в Україні.

З іншого боку, нерідко суди закривають провадження у справах, які мають наведені вище ознаки через відсутність події чи складу адміністративного правопорушення, що є доволі позитивним явищем і обмежує зазначені ризики для свободи вираження поглядів.

Проблематичним для цієї категорії справ залишається мотивування висновків про можливість настання негативних наслідків у виді паніки чи порушення громадського

18. “Miladze v. Georgia”, рішення від 19 травня 2026 у справі за заявою № 41585/23, п. 62, https://hudoc.echr.coe.int/?i=001-250113

порядку. Нерідко судам достатньо гіпотетичної, уявної можливості викликати паніку. Але, такий підхід суттєво знижує поріг доказування і фактично уможливлює покарання за поширення будь-якої недостовірної інформації, створюючи тиск на публічні обговорення.

Крім того, у цій категорії справ суди як правило послуговуються надто широким визначенням поняття "неправдиві чутки", до яких відносять "будь-яке повідомлення переважно усного характеру про **будь-кого та будь-що**, що суперечить (не відповідає) дійсності (формальний склад)".[19] Такий правовий погляд не дозволяє відділити чутки від плітоk і фактично безпідставно охоплює останні.
Зважаючи на це, на нашу думку, доцільно оновити правові підходи до тлумачення зазначеного визначення, врахувавши відповідні сучасні наукові розробки в галузі суспільних наук.

Важливо відмітити ще й те, що починає з'являтись судова практика у справах про **сексуальне домагання (стаття 173-7 КУпАП).** За час моніторингу виявлено одну таку справу.[20]

ГОСПОДАРСЬКІ СПРАВИ

Моніторинг дозволив виявити і проаналізувати низку рішень господарських судів у справах, пов'язаних із поширенням інформації. Ця судова практика не така численна, як у цивільних провадженнях, проте формує важливі орієнтири для вирішення спорів.
Зокрема, під час дослідження знайдено судові рішення, які закріплюють пріоритет спростування недостовірної інформації над її видаленням, тобто фактичним знищенням. В них послідовно проводиться підхід, відповідно до якого видалення недостовірної інформації допускається лише тоді, коли в інший спосіб усунути порушення прав неможливо.[21] Така правова позиція відображає прагнення встановити баланс між правом на свободу слова та правом на повагу до ділової репутації, що є особливо важливим в умовах, коли позови про видалення матеріалів можуть використовуватися для тиску на медіа та обмеження доступу суспільства до важливої інформації.

Суттєвим також є те, що у проаналізованих рішеннях увага акцентувалась на неприпустимості підміни правового аналізу спірної інформації чи сюжету, який повинен робити лише суд, висновком експерта-лінгвіста. Адже це може призвести до помилкового віднесення спірних відомостей до фактичних тверджень чи оціночних суджень.

Крім того, суди дедалі більше зважають на контекст, в якому поширюються спірні висловлювання, і відмічають його значення для розмежування фактів і оціночних суджень.

19. Див. до прикладу: https://reyestr.court.gov.ua/Review/131180905; https://reyestr.court.gov.ua/Review/132271854#
20. https://reyestr.court.gov.ua/Review/135314772
21. https://reyestr.court.gov.ua/Review/130595111#

ГОСПОДАРСЬКІ СПРАВИ

Не менш важливі правові позиції формуються щодо гіперпосилань. Варто наголосити, що Верховний Суд у складі колегії суддів Касаційного господарського суду у цьому питанні орієнтується на підходи, закріплені в рішенні ЄСПЛ у справі "Magyar Jeti Zrt v. Hungary". Зокрема, він наголосив на необхідності здійснення в кожному випадку індивідуальної оцінки ролі гіперпосилання у спірній публікації та надання відповіді на питання про те, чи схвалив відповідач спірний контент, чи лише розмістив гіперпосилання на нього; чи знав або міг знати про його дифамаційний характер; чи діяв добросовісно і чи дотримувався журналістських стандартів. Такий підхід дозволяє уникнути автоматичного покладення відповідальності за саме лише розміщення посилання. Це поступово наближає господарську практику до європейських стандартів свободи вираження.

Європейського стандарту захисту критики публічної влади з суспільно важливих питань (як-от забезпечення громад укриттями) також дотримуються господарські суди. Зокрема, у справі про якість укриттів у Кривому Розі суд надав пріоритет свободі вираження поглядів, підкресливши, що критика органу публічної влади не виходить за межі допустимої.[22]

Таким чином, під час розгляду справ, пов'язаних із поширенням інформації, господарські суди переважно орієнтуються на стандарти Європейського суду з прав людини у справах по статті 10 ЄКПЛ. Водночас, практика судів першої та апеляційної інстанцій подекуди залишається суперечливою навіть у межах одного суду (Північний апеляційний суд у двох справах про видалення інформації займав протилежні позиції).[23] Відповідно, зберігається потреба в подальшій уніфікації правових підходів.

ЦИВІЛЬНІ СПРАВИ

Судова практика у цивільних справах, пов'язаних із поширенням інформації в інтернеті, стосувалася захисту честі, гідності й ділової репутації, права на використання імені в контексті кримінальних проваджень, права на відповідь, права на приватність та вимог про відшкодування моральної шкоди (у тому числі за булінг, вчинений дітьми).

У справах про захист честі, гідності та ділової репутації простежуються такі основні тренди:

- суди активно використовують практику ЄСПЛ і правові позиції Верховного Суду, що забезпечує формування єдиного стандарту доказування у цій категорії справ;
- Верховним Судом активно створюються нові правові орієнтири до вирішення спірних питань, зокрема, щодо відповідальності особи за недбале зберігання даних її облікового запису в соціальних мережах;
- щодалі частіше наголошується на необхідності врахування контексту публікації, її змісту в цілому, а не лише окремих спірних висловлювань, що відображає європейські підходи до розв'язання таких спорів;

практика розмежування фактів і оціночних суджень все ще залишається

22. https://reyestr.court.gov.ua/Review/135768839#
23. До порівняння: https://reyestr.court.gov.ua/Review/128813244 та https://reyestr.court.gov.ua/Review/130595111#

суперечливою; спостерігаються дві протилежні тенденції: з одного боку існують практичні труднощі у здійсненні зазначеного розмежування, але з іншого - судовий аналіз фактичних обставин справ покращується, якість мотивування рішень - зростає;

- дедалі чіткіше окреслюється роль лінгвістичних експертиз, визначається їх доказова сила; послідовно втілюється в життя припис, що предметом висновку експерта не можуть бути питання права, а відтак - розмежування фактичного твердження та оціночного судження має здійснюватись судами на підставі їхньої правової оцінки обставин справи;
- доказова сила висновків семантико-текстуальних експертних досліджень по-різному оцінюється судами залежно від виду установи чи експерта, які їх здійснили (державні чи недержавні), від обгрунтованості експертних висновків та розкриття в них лексичного значення слів і словосполучень, а також від дій експерта - в межах його компетенції чи виходу за них і вирішення питань права;
- зростає кількість справ, пов'язаних із формою спірного висловлювання (принизливою чи образливою). Відповідна судова практика допоки є суперечливою: одне й те саме висловлювання різними судами може оцінюватись неоднаково, що призводить до ухвалення протилежних рішень;
- суди досі застосовують такий спосіб правового захисту, як "спростування спірної інформації шляхом її видалення", хоча він не передбачений ЦК України та іншими законами України;
- проблемними залишаються справи, пов'язані із презумпцією невинуватості та захистом права на використання імені особи в контексті кримінального провадження.
- Порушення презумпції невинуватості є однією з найпоширеніших підстав судових позовів.
- У цій категорії справ спостерігаються дві суперечливі тенденції, які впливають на свободу вираження в цифровому середовищі, зокрема:
- з одного боку, має місце надто широке розуміння презумпції невинуватості, за якого будь-яке пов'язування особи з кримінальним провадженням розглядається як порушення її прав, навіть якщо мова повідомлення є нейтральною; застосовується формальний підхід, за якого відсутність обвинувального вироку автоматично кваліфікується як порушення презумпції невинуватості позивача. Такі судові рішення чинять надмірний тиск на свободу вираження і можуть створити значні перешкоди у висвітленні фактів корупції чи інших тяжких злочинів;
- з іншого боку, застосовується й зважений комплексний підхід, за якого одного лише факту згадування особи у зв'язку з кримінальним провадженням недостатньо для порушення презумпції невинуватості, а натомість враховується ціла низка факторів, серед яких: зміст, форма спірного висловлювання, наявність достатньої фактичної основи, джерела інформації, дотримання журналістських стандартів тощо; використовується мовно-контекстний аналіз спірних фраз, коли вживання кримінально забарвленої лексики (наприклад, "шахрай", "аферист", "зливав", "відмазуючись") тлумачиться й з урахуванням їхнього

загальновживаного, переносного чи оціночного значення, а також контексту їх поширення.

Нерідко правильне розв'язання питання про порушення презумпції невинуватості залежить від належного розмежування фактів і оціночних суджень. Значення має й наявність достатньої фактичної основи. Якщо інформація має характер твердження про факт вчинення кримінального правопорушення, а не є оцінкою, припущенням чи повідомленням про перебіг розслідування, якщо вона не має належної фактичної основи - такі твердження з урахуванням обставин справи дійсно можуть кваліфікуватись як порушення презумпції невинуватості. І приклади таких судових рішень також виявлені під час моніторингу.

Порушенням презумпції невинуватості нерідко обґрунтовуються позовні вимоги про визнання недостовірними фактичних обставин, що підлягають встановленню у ході досудового розслідування. Судова практика в таких випадках стає дедалі уніфікованішою - у задоволенні позовних вимог відмовляють[24] або провадження закривають.[25]

Сучасні судові рішення віддзеркалюють особливості застосування цифрових технологій. Зокрема, судам доводилось формувати правовий підхід щодо наслідків недбалого зберігання даних облікового запису в соціальних мережах, робити оцінку доказової сили певних цифрових елементів, наприклад, хештегів. Все це розвиває правозастосовчу практику, дає кращі орієнтири користувачам інтернету.

Порушення презумпції невинуватості дедалі тісніше пов'язується із правом на використання імені. Кількість таких спорів зростає. І цьому сприяє правова позиція, викладена Верховним Судом у постанові від 10 вересня 2025 року у справі № 757/19417/23, відповідно до якої заборону на оприлюднення імені особи в контексті підозр чи обвинувачення у вчиненні кримінального правопорушення до набрання обвинувальним вироком суду законної сили визнано абсолютною.

Втім, такий правовий підхід порушує фундаментальний європейський стандарт, відповідно до якого право на захист приватності та право на свободу слова є рівноправними, не перебувають у ієрархічній залежності, а тому повинні збалансовуватись.

Викладене, на наш погляд, відображає наявність правової проблеми балансування трьох конкуруючих рівноправних прав та інтересів: прав особи на використання імені, на повагу до її репутації і пов'язану з ними презумпцію невинуватості та права суспільства отримувати інформацію про кримінальні провадження.
Встановлення абсолютної заборони на використання імені шляхом його оприлюднення до набрання вироком законної сили створює значний перекіс на користь захисту приватності за рахунок обмеження свободи інформації.

24. Див., до прикладу: https://reyestr.court.gov.ua/Review/135856271#
25. Див. до прикладу: https://reyestr.court.gov.ua/Review/138668659

Він віддзеркалює хибну, на наш погляд, ідею, що суспільного інтересу до осіб, які лише підозрюються чи обвинувачуються у вчиненні кримінальних правопорушень не існує, навіть якщо ці особи є фігурантами резонансних злочинів або впливовими публічними особами чи підозрюються у корупційних правопорушеннях, які завдали значних збитків державі.

Ця проблема має і суто практичний вимір: суди ухиляються від застосування шестискладового тесту Європейського суду з прав людини, викладеного, зокрема, в рішеннях у справах "Axel Springer AG v. Germany (no. 2)", (див. пункт 57 рішення), "Редакція газети "Гривна» проти України"(пункт 97 рішення). Ймовірно, його застосування викликає труднощі. Методичні рекомендації з цього питання та практичні навчання могли б допомогти розв'язати описану проблему. Значний вклад у її розв'язання міг би внести Верховний Суд, показавши приклад практичного застосування цього тесту.

Спостереження під час моніторингу показало, що судова практика у справах про захист права на використання імені впевнено рухається в фарватері правової позиції Верховного Суду, викладеної у постанові від 10 вересня 2025 року у справі № 757/19417/23. Суди вищих інстанцій як правило скасовують рішення нижчих судів, що містять інші правові підходи. Особливо суворо вони оцінюють повідомлення державних органів, як це було, зокрема, у справах № 761/45437/23[26] та № 629/5109/25.[27] Все це, на наш погляд, вказує на появу серйозних перешкод для свободи інформації в Україні.

Водночас, моніторинг дозволив виявити й відступи від наведених висновків Верховного Суду. Зрідка суди нижчих інстанцій ухвалюють рішення, в яких обгрунтовують не лише наявність суспільного інтересу до кримінального провадження, але й до його фігурантів та наводять аргументи на користь оприлюднення імені особи, підозрюваної у вчиненні кримінального правопорушення. Таке правозастосування може допомогти відновити дисбаланс конкуруючих прав, зробити внесок у розробку методологічних підходів до їх урівноваження і частково нівелювати згадані вище ризики і загрози для свободи слова.

Таким чином, судова практика з окресленого питання залишається **суперечливою**: поряд із формальним підходом, який право на використання імені ставить вище за свободу поширення суспільно важливої інформації, формується практика урівноваження згаданих конкуруючих прав. При цьому перший створює ризик «охолоджувального ефекту» для журналістів і медіа, оскільки внаслідок значного поширення може стримувати оприлюднення відомостей про підозрюваних та обвинувачених у кримінальних провадженнях через побоювання цивільно-правової відповідальності.

26. https://reyestr.court.gov.ua/Review/134511090
27. https://reyestr.court.gov.ua/Review/135847011#

На завершення варто зауважити, що 22 червня 2026 року Верховний Суд у складі Об'єднаної палати Касаційного цивільного суду у справі № 761/1004/20 ухвалив постанову,[28] в якій конкретизував правову позицію щодо захисту права на використання імені. Хоч це рішення прийнято після завершення моніторингу, йому варто приділити увагу в контексті описаної проблеми.Згадана справа передана на розгляд Об'єднаної палати ВС з міркувань необхідності відступлення від висновку щодо застосування норм права у подібних правовідносинах, викладеного у згаданій постанові Верховного Суду від 10 вересня 2025 року в справі № 757/19417/23. Потреба у конкретизації висновку обгрунтовувалась необхідністю розподілу суб'єктів, які можуть або не можуть здійснювати використання (обнародування) імені фізичної особи, яка підозрюється чи обвинувачується у вчиненні кримінального правопорушення, на певні групи, зокрема журналістів та державні органи. Законність дій суб'єкта стосовно використання (обнародування) імені фізичної особи, яка підозрюється чи обвинувачується у вчиненні кримінального правопорушення, пропонувалось оцінювати залежно від приналежності до однієї з цих груп.

Втім, Верховний Суд у складі Об'єднаної палати Касаційного цивільного суду **підстав для відступлення** від згаданого висновку Верховного Суду у в справі № 757/19417/23 **не знайшов**. За результатами судового розгляду він сформулював свою правову позицію наступним чином:
"*Частина четверта статті 296 ЦК України встановлює загальне правило, відповідно до якого використання (обнародування) імені фізичної особи, яка є затриманою, підозрюваною чи обвинуваченою у вчиненні кримінального правопорушення, допускається лише після набрання законної сили обвинувальним вироком суду або у випадках, прямо передбачених законом. За своєю правовою природою ця норма має гарантійний характер і спрямована на забезпечення конституційних цінностей - презумпції невинуватості, поваги до честі, гідності та репутації особи, а також права на приватність. У системному зв`язку з положеннями Конституції України та міжнародними стандартами захисту прав людини вона виконує функцію запобігання передчасній «кримінальній стигматизації» особи через публічну комунікацію".*

Не заперечуючи зазначеного легітимного інтересу для обмеження поширення інформації, необхідно наголосити, що його недостатньо для побудови балансу. Наведена правова позиція відображає цінність лише одного з конкуруючих прав - права на повагу до репутації. Вона не пояснює межі дозволеного і забороненого. Балансуючі критерії "необхідності в демократичному суспільстві", як то, суспільний інтерес, публічність особи, нагальність введення обмежень вона не враховує.
Тому описану проблему ця постанова ВС не розв'язала. Хоча дещо її пом'якшила.

Позитивним є те, що Суд констатував наявність встановленої законом можливості обнародувати ім'я особи в контексті її кримінального переслідування «в інших випадках, передбачених законом». ВС визнав, що це словосполучення з точки зору

28.https://reyestr.court.gov.ua/Review/138668659

нормотворення носить відсилочний (бланкетний) характер та фактично вказує на те, що наведений у ЦК України перелік підстав для оприлюднення (обнародування) імені особи, яка затримана, підозрюється чи обвинувачується у вчиненні кримінального правопорушення, або особи, яка вчинила адміністративне правопорушення, **не є вичерпним** і **законодавець допускає можливість розкриття імені такої особи у випадках, які прямо передбачені іншими законами України**.

Далі Суд наголосив, що законодавча техніка не наділяє цю норму властивостями вільної дискреції суб'єкта правозастосування і не може тлумачитись як така, що надає безумовний загальний дозвіл на розкриття імені фізичної особи з міркувань інформування суспільства або для звітності органів влади. Інакше бланкетна формула фактично перетворюється на спосіб обходу обмеження, встановленого статтею 296 ЦК України, що несумісно з вимогами правової визначеності та забороною свавільного втручання держави як складовими принципу верховенства права.

Він також підкреслив, що при вирішенні питання правомірності використання імені фізичної особи, яка затримана, підозрюється чи обвинувачується у вчиненні кримінального правопорушення, має бути збережений баланс між двома легітимними інтересами. З одного боку, це охорона особистого і сімейного життя, честі, гідності та дотримання презумпції невинуватості, а з іншого - потреба держави інформувати суспільство, забезпечувати громадську безпеку та ефективність кримінальної юстиції.

Таким чином, Верховний Суд фактично констатував необхідність проведення балансуючого тесту під час розгляду справ цієї категорії. Але прикладу застосування додаткових балансуючих критеріїв в тексті постанови не навів.
Ці правові підходи суттєво відрізняються від тих, що застосовано у постанові Верховного Суду від 10 вересня 2025 року. Тому, незважаючи на відмову від відступлення від правової позиції у згаданій справі 757/19417/23, все ж спостерігається певний зсув судової практики в напрямку відмови від абсолютизації заборони на оприлюднення імені. На жаль, цього недостатньо для забезпечення належного балансу згаданих конкуруючих прав. Не вистачає прикладів урівноваження легітимних інтересів в судових рішеннях, опису методичних підходів до розв’язання цього складного питання. Помічним у вирішенні зазначеної проблеми, як вже зазначалось, міг би бути шестискладовий тест Європейського Суду з прав людини. Без його застосування це питання ще довго залишатиметься суперечливим.
Таким чином, практика розгляду судами цивільних справ, пов’язаних із поширенням інформації в цифровому середовищі, залишається однією з найбільш непослідовних. Тут концентруються ризики надмірного обмеження свободи інформації в інтернеті.
З огляду на це існує потреба у продовженні спостереження за розвитком судової практики у зазначеній категорії справ, її періодичному аналізі і вжитті заходів, спрямованих на усунення виявлених недоліків.

КРИМІНАЛЬНІ СПРАВИ

В ході реалізації проекту здійснено моніторинг судових рішень у кримінальних справах, пов'язаних із поширенням інформації в інтернеті. Він тривав чотири місяці - з вересня по грудень 2025 року. За цей час проаналізовано 162 вироки, ухвали та постанови, ухвалені судами першої, апеляційної та касаційної інстанцій у справах за обвинуваченнями у вчиненні кримінальних правопорушень, передбачених статтями 109, 110, 111-1, 114-1, 114-4, 161, 182, 436-1, 436-2 Кримінального кодексу України.
Проведене дослідження не виявило суттєвих змін у судовій практиці порівняно з правовими підходами, відображеними в аналітичному звіті "Кримінальна відповідальність за поширення інформації в інтернеті до та після 24 лютого 2022 року".[29]

Водночас вивчення зібраного матеріалу дозволило актуалізувати інформацію про платформи спільного доступу до інформації та відео або месенджери, через які найчастіше поширюється незаконний контент. Лідером тут виступає Telegram, який використовували у майже 48% проаналізованих справ, за ним йдуть "Одноклассники" – майже 20% усіх проаналізованих вироків, далі з великим відривом - Viber - 10 %, Facebook - 6%, "Вконтакте" - 5%, TikTok - 5 %, YouTube - 2 % та всі інші - 4 %.

Значна частина кримінальних проваджень завершилась затвердженням угод про визнання винуватості. Покарання призначалось переважно у виді позбавлення волі строком на 5 (п'ять) років із звільненням від відбування покарання з випробуванням строком від одного до трьох років. Було кілька випадків призначення покарання нижче визначеної санкцією статті нижчої межі, коли на засуджених накладали штраф у розмірі від 3000 до 3200 неоподаткованих мінімумів доходів громадян, що становить 51000 - 54400 гривень без конфіскації майна.

Реальне позбавлення волі застосовувалось, як правило, у вироках, ухвалених у спеціальних судових провадженнях за відсутності обвинуваченого (in absentia) або у справах, де мала місце сукупність тяжких злочинів (зокрема, державна зрада, колабораційна діяльність). Їх кількість становить майже 20% від загальної кількості проаналізованих рішень.

Серед вироків виявлено й такі, якими засуджено кількох представників медіа, що здійснювали активну інформаційну підтримку Росії та її агресії проти України.

Моніторинг також показав, що суди не покладають на засуджених обов'язок видалити незаконний контент, доля останнього залишається невизначеною.
В період моніторингу Верховний Суд оприлюднив кілька важливих правових позицій. Одна з них викликає особливе занепокоєння, оскільки ВС визнав загальнодоступні особисті сторінки у соціальних мережах, зокрема, "Facebook", "Вконтакте" та "YouTube", засобами масової інформації".[30]

29. Аналітичний звіт "Кримінальна відповідальність за поширення інформації в інтернеті до та після 24 лютого 2022 року" / Вдовенко О., Воробйов Є., Гринишак М., – Київ: ГО "Платформа прав людини", 2022. – 88 с., https://ppl.org.ua/wp-content/uploads/2023/01/%D0%90%D0%9D%D0%90%D0%9B%D0%86%D0%A2%D0%98%D0%A7%D0%9D%D0%98%D0%99-%D0%97%D0%92%D0%86%D0%A2-A4-30-12-22.pdf
30. Постанова Верховного Суду від 28 жовтня 2025 року у справі № 639/1077/23 https://reyestr.court.gov.ua/Review/131853014

Фактично Суд запропонував автономне тлумачення зазначеного терміну для кримінальних справ, яке не узгоджується із законодавством у сфері діяльності медіа (засобів масової інформації). Присутні також ознаки застосування аналогії закону, що прямо заборонено КК України.
Зокрема, висновок, що соціальна мережа відноситься до засобів масової інформації (медіа), оскільки вона є засобом, за допомогою якого така інформація поширюється серед необмеженого (невизначеного) кола осіб суперечить Закону України "Про медіа" та відповідним міжнародних документам. В результаті зазначеної інтерпретації відбулась зміна правового статусу платформ спільного доступу до інформації та платформ спільного доступу до відео: вони втратили свою природну роль інтернет-посередника, набувши натомість невластиву їм роль медіа (засобу масової інформації). Це не відповідає пунктам 30, 38, 39 частини 1 статті 1 Закону України "Про медіа".

Зазначений підхід не узгоджується й з міжнародними стандартами у цій сфері. Зокрема, Рекомендація CM/Rec(2011)7 Комітету Міністрів державам-членам щодо нового визначення медіа[31] оперує шістьма критеріями, які допомагають відрізнити медіа від усіх інших медійно активних осіб, а EMFA робить чіткий наголос на наданні медіапослуг на професійній основі, а не спорадично, як це практикують звичайні дописувачі соцмереж. Викладене дозволяє зробити висновок: існує нагальна потреба у зміні підходів до тлумачення поняття "засоби масової інформації" для цілей кримінального судочинства. На наш погляд, воно не повинно бути автономним, відірваним від регуляторних актів у сфері медіа, а навпаки, має враховувати приписи медійного законодавства.

Висновок про зміну підходів не є суто теоретичним, оскільки помилкове тлумачення терміну "засіб масової інформації" призводить до серйозних правових наслідків - засудження осіб за тяжчі кримінальні правопорушення, ніж вони вчинили.

З іншого боку, описана ситуація піднімає на поверхню й питання про необхідність оновлення юридичної термінології, що використовується в Кримінальному кодексі України, зокрема, визначення "засіб масової інформації". Приведення його у відповідність з медійним законодавством дозволило б усунути виявлені розбіжності, покращити правову визначеність відповідних правових норм та усунути описані проблеми правозастосовчої практики.

Крім того, згадана правова позиція викрила й певний брак знань щодо механізмів поширення інформації в інтернеті, функціонування медіа та інших медіаучасників в онлайн середовищі, ролі кожного з них у передачі інформації тощо.
У зв'язку з цим, на наш погляд, доцільно приділити більше уваги навчанню суддів з питань правового регулювання поширення інформації в мережі Інтернет. Навчальні матеріали, посібники та інші роз'яснення із зазначених питань також могли б покращити ситуацію.

31. https://search.coe.int/cm?i=09000016805cc2c0

IV. БЛОКУВАННЯ ВЕБРЕСУРСІВ

ПРОЦЕДУРА ОБМЕЖЕННЯ ТА ВІДНОВЛЕННЯ ДОСТУПУ

Частина третя статті 18 Закону України “Про електронні комунікації” встановлює декілька самостійних підстав обмеження доступу до інтернет-ресурсу.
Зокрема, доступ повинен обмежуватись :

- до ресурсів, через які розповсюджується дитяча порнографія - на підставі рішення суду (пункт 13);
- на виконання розпоряджень Національного центру оперативно-технічного управління електронними комунікаційними мережами України (НЦУ) в умовах надзвичайного або воєнного стану (пункт 14);
- на виконання рішень Національної ради України з питань телебачення і радіомовлення (Нацради) або судових рішень щодо заборони поширення онлайн-медіа (пункт 15);
- до визначених Нацрадою аудіовізуальних сервісів держави-агресора (пункт 16);
- до вебсайтів, визначених рішенням органу у сфері азартних ігор та лотерей, через які азартні ігри організовуються без відповідної ліцензії (пункт 18).

Пункт 14 має іншу юридичну конструкцію, ніж пункти 13, 15, 16 і 18. Він не визначає конкретний вид незаконного контенту чи діяльності, завдяки яким здійснюється блокування, а покладає на постачальника обов'язок виконувати розпорядження НЦУ.
НЦУ здійснює **оперативно-технічне** управління електронними комунікаційними мережами загального користування з метою **забезпечення оборони та безпеки держави**, а також їх сталого функціонування, для чого відповідно до частини восьмої статті 32 Закону України “Про електронні комунікації” та Порядку, затвердженого постановою Кабінету Міністрів України від 24.01.2025 № 75, видає обов’язкові для постачальників електронних комунікаційних мереж та/або послуг розпорядження про обмеження доступу до ресурсів Інтернету або припинення такого обмеження.

Безпосередніми ініціаторами можливого блокування/розблокування є Президент України, Кабінет Міністрів України, Рада національної безпеки і оборони України, Національний банк, Служба безпеки, Державне бюро розслідувань, Національна поліція, Бюро економічної безпеки, Національне антикорупційне бюро, спеціальні користувачі на тимчасове обмеження надання електронних комунікаційних послуг для цілей оборони та безпеки держави. З 17 червня 2026 року до цього переліку додано ДПС.
НЦУ в цьому випадку виконує роль операційного центру, що перетворює рішення або звернення ініціатора на обов’язкову до виконання команду для постачальників.
Саме тому для кожного блокування за цим механізмом важливими є два окремі питання:

- чи існувало рішення або звернення суб'єкта, на підставі якого НЦУ мав право діяти;
- яким чином конкретний захід пов'язаний із цілями оборони та безпеки держави, для яких Порядок № 75 передбачає цей механізм.

АНАЛІЗ ПРАКТИКИ БЛОКУВАННЯ ЗА КАТЕГОРІЯМИ ВЕБРЕСУРСІВ

На запит ГО “Платформа прав людини” НЦУ надав інформацію щодо вебресурсів, доступ до яких обмежувався і відновлювався протягом моніторингового періоду (Додатки № № 5 та 6). Ці відомості проаналізовано експертами ППЛ. Загалом досліджено дані щодо 1 227 унікальних ідентифікаторів ресурсів. Домени та URL становлять 1 071 позицію, IPv4-адреси - 185 позицій.

Найбільшим ініціатором є Служба безпеки України - 818 позицій. Друге місце посідає Бюро економічної безпеки - 293 позиції. Далі йдуть Департамент кіберполіції Національної поліції - 75 позицій, РНБО - 42, Національний банк України - 11, Печерський районний суд міста Києва та Служба зовнішньої розвідки - по 7, Національна поліція - 2, Новоодеський районний суд Миколаївської області - 1 позиція.

Проте практика блокування **не обмежується забезпеченням оборони та безпеки держави у вузькому розумінні**. Через змістовний аналіз доменів та URL, до яких обмежено доступ, можна припустити, що найбільші групи становлять азартні ігри та ставки - 375 позицій; алкоголь та цигарки - 305; російські пропагандистські та інші ресурси інформаційного впливу - 235; IP-адреси без розкритого змістового контексту - 138; книжкові та видавничі ресурси - 69; шахрайські, фішингові або імітаційні сервіси - 58; лікарські засоби та онлайн-аптеки - 45.

У своїй діяльності **НЦУ демонструє значно більшу прозорість щодо факту блокування, ніж щодо його обґрунтування**. У наданих на запити переліках зазначається заблокований вебресурс, ініціатор блокування, номер і дата розпорядження НЦУ. Але рішення про обмеження доступу до вебресурсів **не містить опису порушення та конкретних правових підстав для блокування, інформації про повідомлення власника ресурсу, механізму оскарження**.

Під час моніторингового періоду доступ до вебресурсів не лише обмежувався, але й розблоковувався. Зокрема, у наданих матеріалах виявлено 11 вебресурсів, щодо яких постачальникам належало припинити обмеження доступу, а саме: specznak.ua, avtovin.com.ua, znaj.ua, ucavtoshkola.com.ua, rozvytok-avto.com, smartpeople.com.ua, add.ua, apteka-ds.com.ua, etabletka.ua, totispharma.com, warontherocks.com.
Однак жодного обгрунтування, жодних фактичних і юридичних підстав для їх розблокування (хоча б мінімальних) також не наведено.

Це вказує на відсутність єдиного прозорого стандарту щодо ініціювання обмеження доступу до вебресурсів, мотивування ухвалених рішень, строків їх перегляду та розблокування. Це створює ризик появи неоднорідної адміністративної практики блокувань, дає простір для зловживань та ускладнює зовнішній незалежний контроль у цій сфері.

АЗАРТНІ ІГРИ І СТАВКИ

У цій категорії 359 позицій пов'язані із СБУ, ще 16 - із БЕБ, які виступили ініціаторами блокувань вебресурсів.

Водночас щодо такого контенту законодавство України встановлює спеціальний галузевий механізм блокування. Пункт 18 частини третьої статті 18 Закону України “Про електронні комунікації” покладає на постачальників електронних комунікаційних мереж та/або послуг обов’язок обмежувати доступ до веб-сайтів, з використанням яких організовуються, проводяться азартні ігри чи надається доступ до них без відповідної ліцензії, на підставі відповідного рішення Державного агентства України ПлейСіті.

Стаття 115-3 Закону України “Про електронні комунікації” передбачає порядок доведення такого рішення до постачальників електронних комунікаційних мереж та/або послуг через Національну комісію, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку у сфері електронних комунікацій (НКЕК). У 2026 році НКЕК публікувала рішення, якими повідомляла постачальників про обов’язок блокування на підставі рішень Державного агентства України ПлейСіті.

Втім, паралельно НЦУ на підставі Порядку № 75 під час дії воєнного стану видає розпорядження щодо обмеження доступу до нелегальних гральних вебсайтів шляхом блокування доменних імен за зверненнями СБУ чи БЕБ. Наприклад, розпорядження НЦУ №762/3563 від 14.10.2025 щодо блокування 16 гральних ресурсів видане саме за зверненням БЕБ.

Тобто фактично створено два паралельні механізми блокування однакових вебресурсів, один з яких передбачений законом, а інший - підзаконним актом. Але працюють вони одночасно. В результаті достеменно неможливо встановити, чому один нелегальний гральний сайт блокується ПлейСіті через НКЕК, а інший - за зверненням СБУ або БЕБ через НЦУ.
Однією з причин такого становища може бути відсутність чітких підстав їх застосування, які б давали можливість визначити сферу дії кожного з них.

АЛКОГОЛЬ ТА ЦИГАРКИ

У цій категорії 277 позицій, ініційованих БЕБ, 28 - СБУ.
Водночас тут так само законодавством встановлено спеціальний галузевий механізм блокування. Частина десята статті 71 Закону України “Про державне регулювання виробництва і обігу спирту етилового, спиртових дистилятів, біоетанолу, алкогольних напоїв, тютюнових виробів, тютюнової сировини, рідин, що використовуються в електронних сигаретах, та пального” передбачає спеціальну послідовність дій: ДПС здійснює моніторинг Інтернету; за наявності порушення направляє вимогу суб’єкту господарювання, постачальнику послуг хостингу та/або платформі цифрової дистрибуції, а також направляє вимогу до НЦУ для видання обов’язкового для

постачальників розпорядження про блокування доменних імен. Цей механізм діяв у період, охоплений дослідженням.

Втім, зміни до підпункту 5 пункту 16 Порядку № 75 щодо видання НЦУ розпорядження про блокування "на вимогу ДПС" внесено лише постановою Кабінету Міністрів України № 791 від 17.06.2026. Це означає, що у період, охоплений моніторингом, НЦУ таких повноважень не мав. Згаданий вище Закон покладав лише на ДПС обов'язок надсилати вимогу про обмеження доступу до веб-сайту, URL-адреси, доменного імені, IP-адреси, мобільного додатка та/або будь-якої іншої мережевої адреси до НЦУ для видання розпорядження про їх блокування, але останньому такі повноваження не надавав.[32] Тому нинішню редакцію Порядку № 75 не можна ретроспективно використовувати для пояснення всіх блокувань вересня 2025 - травня 2026 року.

Незрозумілим залишається й те, чому створено такий складний механізм блокування алкоголю і цигарок, яка потреба в залученні до нього НЦУ, як саме конкретні випадки незаконного продажу алкоголю чи цигарок впливають на оборону та безпеку держави.

РОСІЙСЬКІ ПРОПАГАНДИСТСЬКІ ТА ІНШІ РЕСУРСИ ІНФОРМАЦІЙНОГО ВПЛИВУ

Із відповіді НЦУ видно, що 207 вебресурсів заблоковано за зверненням СБУ, 14 - Департаменту кіберполіції, 7 - Служби зовнішньої розвідки, 5 - РНБО, 2 - Національної поліції без уточнення підрозділу.

Водночас пункти 15 і 16 частини третьої статті 18 Закону "Про електронні комунікації" створюють спеціальні механізми для онлайн-медіа та окремих аудіовізуальних сервісів: постачальники мають блокувати або відновлювати доступ до вебсайтів, визначених рішеннями Національної ради України з питань телебачення і радіомовлення, а щодо заборони поширення онлайн-медіа — також відповідним судовим рішенням.

Можна припустити, що частина заблокованих ресурсів може бути російськими пропагандистськими сайтами, блогами, інформаційними платформами, сайтами окупаційних адміністрацій, проте відсутність інформації про юридичний статус кожного ресурсу не дозволяє перевірити, чи мав застосовуватися спеціальний механізм Нацради, чи загальний безпековий механізм НЦУ.
Для ресурсів, які фактично є онлайн-медіа або аудіовізуальними сервісами, особливо важливо пояснювати, чому рішення прийняте через СБУ/НЦУ, а не профільним регулятором.

32. В умовах надзвичайного та воєнного стану, надзвичайної ситуації національний центр оперативно-технічного управління електронними комунікаційними мережами України виконує оперативно-технічне управління електронними комунікаційними мережами в межах повноважень, наданих йому Кабінетом Міністрів України (частина 4 статті 32 Закону України "Про електронні комунікації", https://zakon.rada.gov.ua/laws/show/1089-20#n735)

IP-АДРЕСИ БЕЗ РОЗКРИТОГО ЗМІСТОВНОГО КОНТЕКСТУ

138 вебсайтів заблоковано на підставі звернень СБУ.
Порядок № 75 прямо дозволяє обмежувати доступ не лише до доменних імен, а й до IP-адрес та автономних систем. Тому IP-адреса сама по собі може бути технічним об'єктом розпорядження НЦУ.

В той же час, у наданих переліках щодо цих 138 IP-адрес немає зв'язку з конкретним доменом, сервісом чи видом контенту. Це не дозволяє визначити:

- який ресурс фактично блокувався;
- чи була IP-адреса виділеною;
- чи могла вона використовуватися спільним хостингом, CDN або хмарним сервісом;
- чи існував ризик одночасного блокування сторонніх ресурсів.

Саме для IP-блокування відсутність індивідуального обґрунтування створює особливо високий ризик надмірного втручання.

КНИГИ, ВИДАВНИЦТВА, КНИЖКОВІ МАГАЗИНИ ТА ЕЛЕКТРОННІ БІБЛІОТЕКИ

39 блокувань здійснено за заявою СБУ, 30 - РНБО.

Окремої загальної процедури блокування саме “книжкових сайтів” Закон України “Про електронні комунікацій” не передбачає. Підстава має випливати з іншого юридичного механізму - санкцій, рішення у сфері безпеки, судового акта тощо.

Щодо 30 ресурсів РНБО правовий ланцюг є значно зрозумілішим: розпорядження НЦУ № 879/3680 від 18.11.2025 прямо має назву “Про реалізацію і моніторинг ефективності персональних спеціальних економічних та інших обмежувальних заходів (санкцій)”.

Щодо 39 “книжкових” вебресурсів, заблокованих за зверненням СБУ, причину блокування встановити неможливо. Хоча можна припустити, що вони створювали інформаційні загрози, зокрема, продавали заборонену продукцію.

ШАХРАЙСЬКІ, ФІШИНГОВІ ТА ІМІТАЦІЙНІ СЕРВІСИ

52 вебсайти заблоковано за зверненням Департаменту кіберполіції, 6 - СБУ.
Формально Порядок № 75 дозволяє НЦУ діяти за офіційними зверненнями керівника Національної поліції або СБУ. Але цей механізм має функціональну прив'язку до цілей оборони та безпеки держави.

Для звичайного фішингу, шахрайства з документами, імітації державних сервісів або майнового шахрайства підстав для застосування воєнно-безпекового механізму НЦУ не вбачається. Не зрозуміло, чому в цих випадках не діють звичайні кримінально-процесуальні, доменні, хостингові чи інші механізми.

ШАХРАЙСЬКІ, ФІШИНГОВІ ТА ІМІТАЦІЙНІ СЕРВІСИ

У таблицях заблокованих ресурсів немає ні номера кримінального провадження, ні характеру кіберзагрози, зв'язку з державою-агресором чи іншої фактичної ознаки, яка пояснювала б використання даного механізму.

ЛІКАРСЬКІ ЗАСОБИ ТА ОНЛАЙН-АПТЕКИ

38 онлайн ресурсів заблоковано за зверненням СБУ, 7 - Департаменту кіберполіції. Пункти 13–18 частини третьої статті 18 Закону України “Про електронні комунікації” не встановлюють окремого прямого обов'язку провайдера блокувати незаконні онлайн-аптеки.

Водночас електронна роздрібна торгівля лікарськими засобами є ліцензованою діяльністю і дозволена лише відповідним аптекам та структурним підрозділам, внесеним до спеціального переліку. Профільним органом у цій сфері є Держлікслужба. Питання прав споживачів у сфері торгівлі та послуг окремо належать до компетенції Держпродспоживслужби.

Так, у березні 2026 року Держлікслужба повідомила, що з жовтня 2025 року виявляла незаконні вебресурси, на яких здійснювалася незаконна електронна роздрібна торгівля ліками, та за результатами спільної роботи з СБУ розпорядженнями НЦУ було заблоковано 16 ресурсів.

Відповідно, у розпорядженні НЦУ № 114/3909 від 16.02.2026 щодо helsy.com.ua, pharma247.com.ua, evrofarm.com.ua, nova-pharma.com.ua та інших ресурсів зазначено, що ініціатором звернення є саме СБУ.

Проте в даному випадку знання формального “ініціатора” не показує реальної послідовності прийняття рішення. Відсутні відповіді на питання: чи підтвердила Держлікслужба відсутність належної ліцензії; чи йшлося про контрафактні або небезпечні ліки; чому до справи залучена саме СБУ; який конкретний аспект становив загрозу державній безпеці.

Більше того, доступ до сайтів add.ua, apteka-ds.com.ua, etabletka.ua, totispharma.com в подальшому був відновлений, однак без зазначення правового обгрунтування, яке стало підставою для такого розблокування.

Отже, як причини блокування, так і скасування обмеження доступу до згаданих вебресурсів залишаються прихованими від громадськості.

ШАХРАЙСЬКІ ТА ІМІТАЦІЙНІ ВЕБРЕСУРСИ

Доступ до 11 вебресурсів обмежено за зверненням Національного банку України.
Це одна з найбільш зрозумілих категорій з точки зору формальної процедури, оскільки Порядок № 75 прямо називає НБУ серед органів, на виконання рішень яких НЦУ може видавати розпорядження.

Проте навіть тут не зазначається інформація щодо предмету первинного рішення НБУ. Неможливо відрізнити, наприклад, безліцензійну фінансову діяльність від фішингу, імітації бренду банку чи іншого фінансового шахрайства.

ФІНАНСОВІ ТА КРИПТОВАЛЮТНІ СЕРВІСИ

7 вебсайтів обмежено в доступі за зверненням РНБО.
Порядок № 75 прямо передбачає можливість виконання НЦУ рішень РНБО, зокрема в рамках реалізації санкцій.

Проте у розпорядженні немає посилання на конкретне рішення РНБО або санкційну позицію. Тому не можна встановити суб'єкта санкції, строк введених ними обмежень, вид обмежувального заходу та його юридичну підставу.

СЕРВІСИ НАДАННЯ ПОСЛУГ ІНТИМНОГО ХАРАКТЕРУ

До цієї категорії віднесено sisidrivekiev.com, natashaescort.com, sexkievu.net та minuet.in.

У таблиці ініціатором зазначений Печерський районний суд м. Києва. Однак у розпорядженні НЦУ № 768/3569 від 15.10.2025 зазначено, що воно видане на звернення Київської міської прокуратури та на виконання ухвали Печерського районного суду м. Києва від 01.10.2025 у справі № 757/47917/25-к.

При цьому пункт 13 частини третьої статті 18 Закону України “Про електронні комунікації” стосується лише ресурсів, через які розповсюджується дитяча порнографія. А у розпорядженні відсутня інформація, що чотири наведені ресурси кваліфіковані саме як ресурси з дитячою порнографією.
Тому тут можливі дві принципово різні правові ситуації.
Якщо судова ухвала стосувалася дитячої порнографії, то пункт 13 статті 18 уже встановлює прямий обов'язок постачальника обмежити доступ на підставі рішення суду. У такому випадку виникає питання, навіщо необхідний ще один юридично обов'язковий акт - розпорядження НЦУ.

Якщо ж ухвала стосувалася іншого предмета кримінального провадження - наприклад, арешту майнових прав на вебресурс або припинення іншої протиправної діяльності, - пункт 13 взагалі не застосовується. Але тоді постає інше питання: Порядок № 75 у переліку ініціаторів звернень до НЦУ не називає ані суд, ані прокуратуру.
Відповідно, постають серйозні питання щодо законності таких блокувань.

ОБМІН ВАЛЮТ ТА ІНШІ ФІНАНСОВІ ПОСЛУГИ

До цієї категорії ймовірно відносяться вебресурси kyt-obmin.kyiv.ua, obmenat24.com та kytgroup.ua. У наданій таблиці всі три пов'язані з ухвалою Печерського районного суду м. Києва у справі № 757/1640/26-к та розпорядженням НЦУ № 112/3907 від 16.02.2026 року. Відповідно до зазначеної ухвали арешт накладено на майнові права інтелектуальної власності, а також зобов'язано НЦУ, НКЕК та ТОВ "Хостінг Україна" заблокувати доступ до вказаних сайтів.

З цієї ситуації так само не зрозуміло, чому для мережевого блокування використано саме судово-кримінальний механізм і чому для виконання рішення органу судової влади (суду) потрібне додаткове розпорядження органу виконавчої влади (НЦУ). Якщо це "технічний" спосіб виконання ухвали суду, то він нівелює роль судових рішень, підриває їх обов'язкову силу. Адже фактично "дозвіл" на виконання рішення суду надає орган виконавчої влади.

Можливо існує проблема виконання таких судових рішень і її намагаються подолати шляхом видачі відповідних розпоряджень НЦУ. Але такий спосіб вирішення питання є дуже сумнівним і не спирається на закон.

Аргумент про те, що суди не зазначені серед ініціаторів звернень до НЦУ є релевантним і до зазначеної ситуації.

ВИСНОВКИ

1. **В Україні паралельно існують і застосовуються галузеві і безпеково-воєнні механізми блокування вебресурсів**. Для азартних ігор, підакцизних товарів, медіа-ресурсів та фінансових послуг існують спеціальні галузеві механізми, але значна частина фактичних блокувань проходить через розпорядження НЦУ за зверненнями СБУ, БЕБ або поліції. Критерії розмежування сфер дії цих правових механізмів не визначені.
2. **Безпекова мета не обґрунтовується**. Порядок № 75 пов'язує можливість звернення за обмеженням доступу до вебресурсів для досягнення цілей оборони та безпеки держави. Однак розпорядження НЦУ не містять інформації щодо того, як саме робота відповідних вебсайтів впливає на оборону і безпеку держави.
3. Розпорядження НЦУ **не містять навіть мінімального фактичного і правового обґрунтування** необхідності обмеження доступу до вебресурсів, які блокуються.
4. "Ініціатор звернення" в розпорядженні НЦУ не завжди відображає реального організатора блокування сайтів. Наприклад, у випадку сайтів з ліками публічні матеріали Держлікслужби свідчать про її участь у виявленні порушень, але у переліку НЦУ ініціатором виступає СБУ.
5. **Судові ухвали виконуються через додаткове розпорядження НЦУ**, що підриває їх обов'язкову силу і ставить під сумнів законність таких блокувань.

ВИСНОВКИ

6. Т**ривалість обмеження доступу до вебресурсу є невизначеною**. Нерідко вона прив'язана не до моменту усунення конкретного порушення, а до припинення або скасування воєнного стану. Наприклад, так сформульовані розпорядження щодо блокування сайтів онлайн-аптек, азартних ігор і сайтів, заблокованих ухвалою суду.
7. **Причини розблокування непрозорі**. Не можна зрозуміти, чи блокування було помилковим або порушення усунуто, чи відбулась зміна власника, відпала потреба в обмеженні доступу, скасовано первинний акт абощо. Через це неможливо оцінити ефективність як механізму блокування, так і відновлення доступу до вебресурсів.
8. **IP-блокування не супроводжується оцінкою супутнього впливу на інші вебресурси**. Для 138 IP-позицій немає публічного зв'язку з доменом чи сервісом, що створює ризик надмірного блокування при використанні спільної інфраструктури.
9. **Статус онлайнмедіа не фіксується і не враховується**. Без відомостей про те, чи є конкретний вебресурс онлайн-медіа або аудіовізуальним сервісом у розумінні Закону України "Про медіа", неможливо перевірити, чи застосовано належний механізм блокування, передбачений законодавством України для Національної ради України з питань телебачення і радіомовлення, чи правомірно використано зазначений безпеко-воєнний механізм.
10. З огляду на викладене, **механізм блокування вебресурсів в Україні є непрозорим.** Для покращення прозорості блокувань необхідно чітко зазначати: мінімальну фактичну і правову підстави обмеження доступу до вебресурсу; компетентний орган звернення за блокуванням та усіх ініціаторів обмеження доступу до вебресурсу; вид і реквізити первинного акта, який є підставою для ухвалення рішення; обґрунтування використання безпеково-воєнного механізму, передбаченого Порядком № 75; технічні деталі блокування; строк блокування; дату перегляду рішення; підставу розблокування. Відсутність цієї інформації робить зазначений механізм блокування непрозорим.

V. ВИСНОВКИ І РЕКОМЕНДАЦІЇ

1. **Зростання цифрових і кіберзагроз на тлі активного розвитку штучного інтелекту та автоматизації інтернет-трафіку, що сприяє** масштабуванню кібератак, онлайн-шахрайства, дезінформаційних і дискредитаційних кампаній.

Рекомендації:

- здійснювати постійні спостереження за змінами, що відбуваються в цифровому середовищі; систематично проводити моніторинг з метою виявлення нових тенденцій, викликів і загроз, оцінки ефективності впроваджених заходів протидії цифровим і кіберзагрозам та визначення шляхів їх удосконалення, внесення, за необхідності, змін до документів публічної політики та/або законодавства України, удосконалення відповідної адміністративної та правозастосовної практики;
- налагодити міжсекторальну взаємодію органів влади, неурядових організацій та бізнесу для спільної протидії цифровим і кіберзагрозам в епоху стрімкого розвитку ШІ та автоматизації інтернет-трафіку;
- підвищувати рівень цифрової грамотності державних службовців, посадових осіб місцевого самоврядування, звичайних громадян.

2. **Фішинг залишається однією з найпоширеніших кіберзагроз**. Розвиток штучного інтелекту робить шахрайські повідомлення, сайти та цифрові імітації дедалі переконливішими й масштабованішими.

Рекомендація: посилити інформування населення про актуальні фішингові схеми та способи їх розпізнавання; проводити адресні інформаційні кампанії для вразливих груп — військових, пенсіонерів, соціально незахищених осіб, бухгалтерів, підприємців та інших активних користувачів онлайн-сервісів.

3. В Україні сформована дієва **децентралізована екосистема протидії дезінформації**, до якої залучені державні органи, медіа, журналісти, фактчекери та громадські організації. Основними джерелами та поширювачами деструктивного контенту залишаються російські державні й пов'язані з РФ мережі. Водночас **відсутність єдиної науково обгрунтованої методології та єдиних і чітких критеріїв визначення дезінформації та маніпуляцій інформацією** створює проблеми з аналітичною і юридичною визначеністю, особливо у випадках застосування правових санкцій.

Рекомендації:

- розробити комплексну програму протидії іноземним інформаційним маніпуляціям і втручанням (FIMI), засновану на європейських підходах у зазначеній сфері;
- визначити систему органів державної влади у сфері протидії іноземним інформаційним маніпуляціям та втручанням (FIMI), наділити їх необхідними чітко визначеними повноваженнями та розмежувати зони їхньої відповідальності з метою ефективного виконання поставлених завдань;
- підготувати науково обгрунтовану методологію з питань виявлення та протидії іноземним інформаційним маніпуляціям і втручанням (FIMI); залучити до її розробки широке коло фахівців: наукову спільноту, представників медіа, фактчекерських і правозахисних організацій, фахівців із цифрових технологій та

штучного інтелекту, міжнародних експертів; зробити її загальнодоступною, принаймні в частині базових підходів до оцінювання контенту;

- уніфікувати дефініції та розширити термінологічний словник, включивши до нього не лише визначення “дезінформації” але й “міс-інформації” (misinformation), “мал-інформації” (malinformation), “маніпулювання інформацією” з урахуванням європейських підходів у цій сфері;
- уникати використання широкого терміну “дезінформація” як самостійної універсальної правової підстави для застосування правових санкцій; юридичну відповідальність за поширення шкідливої інформації вводити за конкретно визначені суспільно-небезпечні діяння (вчинення шахрайства, підбурювання до насильства, втручання у виборчий процес тощо), зокрема, як кваліфікуючі ознаки до вже наявних складів правопорушень;
- створити національний механізм координації між державою, медіа, бізнесом, фактчекерами, науковцями, громадським сектором і платформами з метою протидії іноземним інформаційним маніпуляціям і втручанням, зберігши при цьому децентралізований характер екосистеми;
- посилити механізм протидії поширенню шкідливого AI-згенерованого контенту;
- забезпечувати інформаційну стійкість суспільства шляхом проведення активної превентивної комунікації, проведення широких програм з медіаграмотності, які включатимуть розпізнавання як неправдивого контенту, так і маніпулятивних практик і скоординованих інформаційних атак;
- підготувати протоколи реагування на різні види іноземних інформаційних маніпуляцій і втручань;
- налагодити міжнародну співпрацю з питань протидії іноземним інформаційним маніпуляціям і втручанням, зокрема, з платформами спільного доступу до інформації та платформами спільного доступу до відео, міжнародними медіа, а також з міжнародними організаціями.

4. **Цифрові технології розширили можливості для свободи слова, водночас створивши й нові ризики для неї**, зокрема через цифрове стеження, онлайн-тиск, маніпуляції та непрозору модерацію контенту. В 2025–2026 роках основними загрозами стали: погрози, залякування та тиск на журналістів через їхні розслідування й публікації; дискредитаційні кампанії проти журналістів, медіа, громадських організацій і посадовців, зокрема із використанням маніпуляцій та ШІ; перешкоджання професійній діяльності журналістів і недостатньо ефективне розслідування таких випадків; гендерно зумовлене онлайн-насильство щодо жінок-журналісток; надмірне або непрозоре блокування українського контенту платформами Facebook, Instagram, YouTube та іншими; використання цифрових платформ Росією для пропаганди, контролю інформації та обмеження свободи слова на окупованих територіях.

Рекомендації:

- посилити захист журналістів і медіа, забезпечивши оперативне та ефективне розслідування погроз, нападів і перешкоджання професійній діяльності

журналістів; оновити методології розслідувань таких кримінальних правопорушень з урахуванням нових форм онлайн атак;

- розробити механізми швидкого виявлення, документування та реагування на скоординовані кампанії дискредитації журналістів і медіа та відповідну методологію; забезпечити психологічну та іншу необхідну підтримку жертвам таких кампаній;
- налагодити ефективну взаємодію з платформами спільного доступу до відео та платформами спільного доступу до інформації з метою забезпечення прозорої модерації контенту, оперативного оскарження необгрунтованих блокувань, захисту суспільно-важливих журналістських матеріалів, цифрової інформації документального характеру, особливо матеріалів про війну та воєнні злочини;
- вживати доступні заходи протидії російському інформаційному впливу на окупованих територіях України, зокрема, за можливості забезпечувати мешканцям окупованих територій доступ до незалежних українських джерел інформації; розвивати безпечні канали комунікації, які не залежать від російської цифрової інфраструктури; документувати випадки переслідування громадян за проукраїнську позицію та використовувати ці матеріали для міжнародної відповідальності Росії.

5.Стрімкий розвиток цифрових технологій та ШІ **посилює ризики для приватності та захисту персональних даних в інтернеті**, які стають об'єктом незаконного збору та використання. Зростання цифрових загроз, особливо пов'язаних із ШІ, витоками даних, цифровою ідентичністю та незаконним поширенням інтимної інформації потребує посилення захисту персональних даних в цифровому середовищі.

Рекомендації:

- посилити законодавчий захист персональних даних, ухваливши новий закон, який відповідатиме європейським стандартам в зазначеній сфері, зокрема, GDPR, та враховуватиме розвиток цифрових технологій і штучного інтелекту;
- забезпечити невідворотну відповідальність за незаконний збір, використання, передачу та поширення персональних даних;
- посилити захист особливо чутливих даних, зокрема інформації інтимного характеру та даних дітей;
- забезпечити суворий контроль за доступом посадових осіб до персональних даних і посилити їх відповідальність за незаконний збір та/або передачу інформації третім особам;
- забезпечити ефективну протидію поширенню інтимного контенту без згоди особи, зокрема, механізми швидкого блокування і видалення відповідних фото й відео; посилити відповідальність за шантаж, погрози оприлюднення інтимних матеріалів та за поширення такої інформації без згоди особи.

6. Практика **блокування онлайн-медіа та інших вебресурсів є непрозорою**, що створює ризики для свободи вираження поглядів в інтернеті.

Рекомендація: здійснювати блокування онлайн ресурсів лише на чітких законних підставах з належним фактичним і правовим обґрунтуванням ухвалених рішень; забезпечити прозору процедуру блокування та ефективні засоби правового захисту від таких обмежень.

7. Спостерігаються **системні проблеми, пов'язані із захистом цифрових прав дітей** та інших учасників освітнього процесу, зокрема: кібербулінг, образи, погрози та приниження у соціальних мережах і шкільних чатах; порушення приватності, в тому числі шляхом поширення інтимного контенту, поширення образливих висловлювань, ненормативної лексики, зйомка та розповсюдження відео насильства, небезпечних челенджів та інших шкідливих дій.

Рекомендація:

- вжити комплекс заходів, спрямованих на покращення цифрової та правової освіти дітей, розвитку у них критичного мислення, належного сексуального виховання, профілактики кібербулінгу;
- об'єднати зусилля батьків, освітян, профільних фахівців та правоохоронних органів для оперативного реагування на згадану деструктивну поведінку та розробки дієвих механізмів подолання зазначених проявів з метою створення безпечного освітнього середовища;
- посилити захист дітей від онлайн-вербування та інших форм їх інтернет-залучення до вчинення кримінальних правопорушень, зокрема, диверсій, терористичних актів тощо на замовлення спецслужб інших держав.

8. **Судова практика адаптує традиційні правові поняття до цифрового середовища:** розширюється зміст терміну **«громадське місце»**, яке вже нерідко включає соціальні мережі, чати та форуми.

Рекомендації:

- науковцям та юристам-практикам продовжувати адаптацію традиційних правових дефініцій до цифрового середовища;
- оновити термінологію Кодексу України про адміністративні правопорушення, привівши її у відповідність до реалій цифрового світу.

9. Спостерігаються спроби використання **статті 173-1 КУпАП (поширювання неправдивих чуток) для боротьби із поширенням ймовірно недостовірних відомостей про особу**, які можуть завдати шкоди її честі, гідності та діловій репутації або для протидії поширенню критичних висловлювань чи дезінформації, хоча вони не завжди не підтримуються судами. Суди застосовують низький поріг доказування можливості настання паніки або порушення громадського порядку - достатньо лише абстрактної чи гіпотетичної можливості настання таких наслідків. Це створює загрози для вільного публічного обговорення гострих чи чутливих питань. Застосовується також надто широке визначення «неправдивих чуток», яке фактично може охоплювати будь-яке повідомлення, що не відповідає дійсності. Через це стирається межа між чутками, плітками, помилковими твердженнями, критикою та іншими формами висловлювань.

Рекомендація:

- модернізувати підходи до застосування статті 173-1 КУпАП, чіткіше визначаючи характер повідомлень, які можуть кваліфікуватись як «неправдиві чутки»; встановлювати реальний, а не гіпотетичний ризик настання паніки чи порушення громадського порядку та забезпечувати належний баланс між захистом громадського порядку і свободою вираження поглядів.

10. Судова практика у справах про захист честі, гідності, а також ділової репутації, спростування недостовірної інформації рухається в бік активного застосування європейських стандартів свободи вираження поглядів. Цифрове середовище поступово формує нові правові підходи: суди враховують особливості соціальних мереж, цифрових доказів, надають правову оцінку хештегам, визначають роль гіперпосилань та встановлюють особу, відповідальну за неналежне зберігання даних облікових записів. Найбільш суперечливою є судова практика у справах, пов'язаних із порушенням презумпції невинуватості, поширенням образливих висловлювань, "спростуванням шляхом видалення", захистом права на використання імені в контексті кримінальних проваджень, а також з питань доказової сили висновків лінгвістичних експертиз.

Рекомендації:

- уніфікувати з урахуванням європейських стандартів в галузі свободи вираження поглядів судову практику розгляду спорів, пов'язаних із поширенням інформації в інтернеті, зокрема стосовно:
- *розмежування фактів та оціночних суджень;*
- *презумпції невинуватості;*
- *допустимості видалення спірної інформації;*
- *оцінки правомірності поширення образливих та принизливих висловлювань та відповідних меж допустимої критики;*
- *відповідальності за поширення гіперпосилань;*
- *доказової сили висновків лінгвістичних експертиз, зокрема, проведених експертами та експертними установами різних форм власності.*

- видалення спірної інформації застосовувати як винятковий спосіб правового захисту, виправданий лише тоді, коли немає інших ефективних засобів припинення правопорушення і поновлення прав особи; надавати пріоритет спростуванню;
- застосовувати зваженіший підхід до встановлення факту порушення презумпції невинуватості особи в цивільних провадженнях: саме лише згадування особи у зв'язку з розслідуванням кримінальних правопорушень не повинно кваліфікуватись як порушення зазначеної презумпції; правова оцінка повинна враховувати форму і зміст інформації, її контекст, джерело відомостей, існування фактичної основи тощо;
- покращити практичні навички вирішення зазначених спорів суддями, зокрема, шляхом підвищення їхньої кваліфікації із зазначених питань.

11. Судова практика у справах, пов'язаних із захистом права на використання (оприлюднення) імені особи у зв'язку з підозрою чи обвинуваченням її у вчиненні адміністративного чи кримінального правопорушення залишається суперечливою і не забезпечує належного балансу між презумпцією невинуватості, правом на приватність і повагу до честі, гідності, ділової репутації, з одного боку, та правом суспільства на інформацію - з іншого.

Рекомендації:

- застосовувати балансуючий тест Європейського Суду з прав людини, описаний, зокрема, в рішеннях у справах "Axel Springer AG v. Germany (no. 2)", (пункт 57), "Редакція газети "Гривна» проти України"(пункт 97) та інших;
- підготувати методичні рекомендації з питань застосування вказаного балансуючого тесту;
- покращити практичні навички застосування зазначеного тесту під час розгляду справ та підготовки судових рішень.

12. Судова практика в кримінальних справах, пов'язаних із поширенням інформації в інтернеті, залишається сталою; нерідко судовий розгляд таких справ завершується угодами про визнання винуватості та призначенням умовного покарання; суди, яік і раніше, не покладають на засуджених обов'язок видалити незаконний контент, доля останнього залишається невизначеною. Проблемою правозастосовчої практики є надто широке тлумачення Верховним Судом поняття «засіб масової інформації», що може призводити до безпідставного посилення кримінальної відповідальності за поширення інформації в інтернеті.

Рекомендації:

- узгодити зміст терміну "засіб масової інформації", що використовується для цілей кримінального провадження, з відповідною термінологією Закону України "Про медіа";
- внести зміни до КК України, привівши зазначену термінологію у відповідність до дефініцій Закону України "Про медіа" та/або адаптувавши цю термінологію з урахуванням ролі соціальних мереж у сучасному світі;
- підготувати навчальні матеріали, посібники та інші роз'яснення щодо особливостей поширення інформації в інтернеті, ролі і правового статусу різних учасників інформаційних відносин, розподілу між ними відповідальності, забезпечення балансу між захистом національних інтересів держави та свободою вираження поглядів;
- систематично підвищувати кваліфікацію суддів із зазначених питань.

VI. ДОДАТКИ

У Додатках 1–3 представлено підсумки експертних обговорень профільних тем. Матеріали підготовлено із використанням інструментів штучного інтелекту (Whisper та ChatGPT) та фіналізовано фахівцями ГО «Платформа прав людини». Організація здійснювала ретельну перевірку й редагування текстів та несе повну відповідальність за їхній зміст.

Додаток 1

ЗВІТ ЗА РЕЗУЛЬТАТАМИ ПРОВЕДЕННЯ ЕКСПЕРТНОЇ ЗУСТРІЧІ НА ТЕМУ: “ЗАХИСТ ВІД ІНФОРМАЦІЙНИХ ОНЛАЙН-АТАК”

1. Загальний контекст і мета зустрічі

Експертна зустріч була присвячена проблемі скоординованих інформаційних онлайн-атак, спрямованих проти журналістів, медіа, громадських діячів та інших осіб, які працюють із суспільно значущими темами. У центрі дискусії перебували не поодинокі конфлікти навколо окремих публікацій, а системні кампанії, що використовують мережі анонімних вебресурсів, Telegram-каналів, ботів і троль-акаунтів, платну рекламу, відео та аудіоматеріали, створені із застосуванням штучного інтелекту, а також інструменти офлайн-тиску.

Головним результатом зустрічі стало спільне розуміння, що чинна модель захисту є структурно слабшою за модель атаки. Кампанія дискредитації може бути запущена швидко, відносно дешево і масштабована через десятки або сотні каналів. Натомість документування порушень, встановлення власників ресурсів, фіксація цифрових доказів, підготовка адвокатських запитів, звернення до правоохоронних органів та судовий захист потребують значних фінансових, часових і психологічних ресурсів. Юридична відповідь часто настає тоді, коли первинна хвиля вже досягла своєї мети: підірвала довіру, виснажила атаковану особу або створила охолоджувальний ефект для інших журналістів.

Учасники погодилися, що ефективна протидія не може будуватися навколо одного інструменту. Потрібна комплексна модель, у якій правовий захист поєднується з технічною аналітикою, оперативною взаємодією з платформами, кризовою комунікацією, психологічною підтримкою, професійною солідарністю та публічним документуванням верифікованих атак. Окремо було наголошено на необхідності залучення правоохоронних органів до розслідування випадків незаконного впливу на журналістів і на потребі застосовувати кримінально-правові механізми там, де кампанія безпосередньо пов’язана з професійною діяльністю медійника.

Разом із тим дискусія не дала універсальної відповіді на питання, чи потрібно публічно реагувати на кожну атаку. Публічне спростування може підтримати потерпілу особу, позначити маніпуляцію та пояснити аудиторії механіку впливу. Водночас воно може збільшити охоплення маловідомого ресурсу, повторити шкідливий наратив і надати анонімному каналу додаткової легітимності. Тому одним із ключових фіналізованих висновків стала потреба у процедурі аналізу, яка дозволить оцінювати масштаб, швидкість, аудиторію, походження та потенційну шкоду кампанії до вибору публічної тактики.

Зустріч також засвідчила, що проблема виходить за межі репутаційного захисту окремої людини. Системна дискредитація журналістів послаблює здатність суспільства отримувати перевірену інформацію, створює сприятливе середовище для зовнішніх інформаційних маніпуляцій і може використовуватися для втручання у виборчі процеси. Саме тому подальша робота має розглядати такі кампанії не лише як приватні спори, а як загрозу свободі слова, демократичному контролю та інформаційній стійкості.

2. Опис перебігу обговорення

На початку зустрічі було зафіксовано зростання кількості повідомлень про дискредитаційні кампанії проти журналістів і медіа. Йшлося про випадки, коли публічна критика не була спрямована на зміст журналістських матеріалів і не мала ознак добросовісної дискусії, а концентрувалася на особі журналіста, його приватному житті, родині, політичних або нібито кримінальних зв'язках. Такі матеріали часто поширювалися через анонімні Telegram-канали та вебсайти без прозорої редакційної структури, власників, адреси або реальних контактів.

Було підкреслено, що аналогічні технології застосовуються не лише проти медіа. Об'єктами кампаній можуть ставати кандидати на керівні посади, судді, університетські керівники, громадські активісти, правозахисники, представники державних інституцій і військові. Це свідчить про універсальність інструменту: його можна використовувати для тиску, усунення конкурента, помсти за публічну діяльність, політичної боротьби або формування потрібного ставлення до суспільно важливої теми.

Окрема увага була приділена міжнародному контексту та практикам FIMI - зовнішнього інформаційного маніпулювання та втручання. Дискусія показала, що внутрішні кампанії дискредитації можуть використовувати подібну інфраструктуру, методи та логіку поширення: спочатку повідомлення виникає на маловідомому ресурсі, потім підхоплюється мережею вторинних каналів, набуває вигляду «множинного підтвердження», поширюється через соціальні мережі та зрештою може бути використане більшими медіа або іноземними пропагандистськими ресурсами.

VI. ДОДАТКИ

На основі обговорених кейсів було реконструйовано типову послідовність дій. Вона не є універсальною для кожної кампанії, однак дозволяє побачити повторювану структуру:

- поява первинного матеріалу на маловідомому або новоствореному ресурсі, який не має прозорої редакційної відповідальності;
- передрукування або переказ матеріалу іншими сайтами, завдяки чому створюється ілюзія кількох незалежних джерел;
- поширення через Telegram-канали, сторінки в соціальних мережах і троль-акаунти, які імітують органічну суспільну дискусію;
- підсилення платною рекламою, штучними переглядами, купленими акаунтами та ботами;
- розвиток наративу від окремої претензії до повної дискредитації особи: сумніви у професійності, звинувачення у шахрайстві, роботі на ворога, загрозі національній безпеці або інших тяжких порушеннях;
- використання згенерованих відео, дипфейків, клонованих сторінок або підроблених документів для створення сильнішого емоційного ефекту;
- перенесення кампанії в офлайн через заяви до поліції, спроби ініціювати провадження, контакти з роботодавцями, публічні заходи чи інші форми тиску;
- повторне використання вже опублікованих матеріалів у наступних хвилях або під час нових суспільно-політичних подій.

Учасники звернули увагу, що кампанії часто поєднують неправдиву інформацію з реальними фактами. Маніпулятори можуть розміщувати в одному каналі достовірні повідомлення, офіційні матеріали державних органів, справжні випадки порушень і свідомо викривлені звинувачення проти конкретної особи. Такий підхід підвищує довіру до ресурсу та ускладнює спростування. У дискусії цей механізм був описаний як поєднання фейків із «малінформацією» - правдивими або частково правдивими даними, що використовуються поза контекстом для заподіяння шкоди.

Один із детально розглянутих кейсів стосувався журналістського розслідування про знищення екологічних природних систем на полонинах Карпат. Після публікації матеріалів проти авторки та пов’язаних із нею громадських діячів протягом кількох місяців поширювалися дискредитаційні статті, коментарі троль-акаунтів і згенеровані відео. Кампанія доповнювалася платною рекламою та заявами до поліції. Для юридичної фіксації епізодів потрібно було опрацювати понад два десятки ресурсів, направити значну кількість адвокатських запитів та зберегти великий масив цифрових доказів. Ідентифікувати власників вдалося лише для незначної частини ресурсів.

Інший тип кейсів був пов’язаний зі створенням Telegram-каналів, які позиціонували себе як громадські рухи або інформаційні платформи навколо гострої суспільної теми. Вони публікували частину якісного або офіційного контенту, але одночасно систематично атакували окремих журналістів і публічних осіб. Значна кількість підписників, низьке співвідношення переглядів до аудиторії та синхронізоване

поширення матеріалів через інші великі канали вказували на можливе штучне нарощування охоплення.

Також було наведено приклади клонування сторінок громадських організацій і використання впізнаваних облич журналістів або ведучих у дипфейк-відео. З'ясувалося, що сучасні інструменти детекції не дають гарантованого результату: різні сервіси можуть по-різному оцінювати один і той самий матеріал, а системи модерації платформ інколи не розпізнають навіть очевидно маніпулятивний контент.
Окремий блок стосувався тиску, який формально маскується під правові дії. Йшлося про позови, підроблені заяви, заяви до поліції та інші процесуальні інструменти, які можуть використовуватися не стільки для захисту законних інтересів, скільки для виснаження журналіста, створення додаткових ризиків і формування в аудиторії враження, що проти особи існують обґрунтовані претензії.

Правова частина дискусії показала, що чинне законодавство дає певний набір інструментів: позови про захист честі, гідності та ділової репутації; заяви про встановлення фактів, що мають юридичне значення; звернення щодо незаконного поширення персональних даних; кримінальні провадження у зв'язку з перешкоджанням журналістській діяльності. Однак кожен із цих інструментів має суттєві обмеження.

Цивільний процес потребує встановлення відповідача або принаймні ретельного доказування факту анонімності поширювача інформації. Анонімність ресурсів, захист даних доменних реєстраторів, іноземна юрисдикція та відсутність відповіді на адвокатські запити значно ускладнюють підготовку справи. Навіть коли позов або заява є перспективними, рішення може бути отримане через рік, два або пізніше. Воно може допомогти у відновленні репутації, але не зупиняє первинну хвилю.

Кримінально-правовий шлях потенційно краще відповідає природі скоординованого впливу. Якщо метою кампанії є втручання у творчу діяльність журналіста, примушування його відмовитися від теми або створення системного тиску у зв'язку з професійною діяльністю, учасники вбачали підстави для застосування статті 171 Кримінального кодексу України. Водночас практична ефективність залежить від готовності поліції та прокуратури бачити в цифровій кампанії не просто конфлікт, а комплексну операцію впливу.

Особливо критично оцінювалася низька оперативність слідчих дій. Учасники зазначали, що навіть відносно прості дії із збереження відео, встановлення відправника заяви або отримання даних можуть не проводитися вчасно. Тому було запропоновано не лише вдосконалювати норми, а й створювати спеціалізацію слідчих і прокурорів, забезпечувати постійний процесуальний контроль та підтримувати регулярний діалог між правоохоронними органами і медійними організаціями.

VI. ДОДАТКИ

Технологічна частина обговорення продемонструвала, що інфраструктура атак стала доступною як послуга. Домени можна масово реєструвати через іноземних реєстраторів; акаунти соціальних мереж, поштових сервісів і рекламних платформ продаються великими пакетами; інструменти генерації відео й аудіо постійно вдосконалюються. Це різко знижує вартість запуску кампанії.
Платформи мають формальні механізми скарг, однак вони часто орієнтовані на окремі порушення, а не на мережеву координацію. У практичній роботі можуть допомагати скарги щодо шахрайства, порушення авторських прав, клонування сторінок, видавання себе за іншу особу або порушення правил спільноти. Проте результат залежить від якості доказів, доступу до каналів пріоритетної комунікації та політики конкретної платформи.

Дискусія також виявила конфлікт інтересів платформ: боти, штучні акаунти та висока активність можуть збільшувати формальні показники аудиторії. Це не означає, що платформи свідомо підтримують атаки, але свідчить про обмеженість саморегулювання. Відтак потрібні механізми довірених скаржників, прозорі процедури оцінки скоординованої поведінки та міжнародна співпраця з провайдерами послуг.

Однією з найскладніших тем стала публічна реакція. Традиційна порада «не годувати тролів» може бути виправданою, коли йдеться про одиничний допис із низьким охопленням. Проте вона перестає працювати, коли інформація системно поширюється великими каналами, переходить у традиційні медіа, впливає на партнерів або створює реальні юридичні та фізичні ризики.

Публічне спростування має кілька можливих функцій: підтримати атаковану особу, надати партнерам перевірену позицію, зафіксувати наявність кампанії, попередити аудиторію та зменшити ефект повторного поширення. Однак буквальне повторення фейку може закріпити його в пам’яті, а пряма полеміка з анонімним каналом - підвищити його статус. Тому учасники схилялися до рефреймінгу: пояснювати механіку атаки, підмінювати нав’язану рамку власною та фокусуватися на перевірених фактах без зайвого цитування шкідливих формулювань.

Окремо було наголошено на сегментації аудиторій. Професійний юридичний аналіз потрібен правоохоронцям, партнерам і редакціям, але він не досягає масової аудиторії, яка споживає короткі відео та емоційні повідомлення. Тому комунікаційна відповідь має включати короткі формати для соціальних мереж, зрозумілі візуальні пояснення, готові тези для партнерів і докладний доказовий матеріал для фахівців.

3. **Висновки**

3.1. Скоординовані атаки слід розглядати як інфраструктурну загрозу.

Повторюваність методів, наявність мережі ресурсів, синхронізоване поширення, платне підсилення та перехід від онлайн-дискредитації до юридичного або офлайн-тиску свідчать, що проблема не зводиться до недобросовісної публікації. Йдеться про інфраструктуру, яка може бути багаторазово використана різними замовниками. Відповідно, захист не повинен щоразу починатися з нуля навколо окремого потерпілого. Потрібні постійні інституційні спроможності, база знань, контакти платформ, стандарти доказування та механізм швидкого залучення фахівців.

3.2. Основна перевага атакувальника - асиметрія швидкості та вартості.

Запустити десятки публікацій, тиражувати їх ботами та купити рекламу значно простіше, ніж юридично зафіксувати кожний епізод. Ця асиметрія є центральною причиною неефективності виключно судового підходу. Система захисту має мінімізувати вартість повторюваних дій: використовувати готові шаблони, автоматизоване архівування, спільну технічну інфраструктуру, централізовану юридичну допомогу та колективні канали взаємодії з платформами.

3.3. Юридичний захист потрібен, але його функція має бути правильно визначена.

Судове рішення може підтвердити недостовірність інформації, створити репутаційний доказ або відкрити доступ до даних власника ресурсу. Проте воно не є інструментом миттєвого кризового реагування. Тому правовий трек має працювати паралельно з комунікаційним і технічним, а не замінювати їх. На ранньому етапі пріоритетом є збереження доказів і зупинення поширення; на середньому - встановлення мережі та організаторів; на довгому - судова оцінка і відповідальність.

3.4. **Стаття 171 КК України потребує активнішого та спеціалізованого застосування.**

Коли атака очевидно пов’язана з професійною діяльністю журналіста та спрямована на зміну його поведінки, відмову від теми або дискредитацію результатів роботи, її доцільно розглядати як можливий незаконний вплив на журналіста. Для цього правоохоронцям необхідно бачити не окремий допис, а повну картину координації. Саме тому якісно підготовлений аналітичний пакет, який демонструє хронологію, мережу поширення, повторюваність тез і зв’язок із журналістською діяльністю, може мати більше значення, ніж десятки непов’язаних скарг.

3.5. **Потрібна процедура аналізу, а не автоматичне спростування.**

Не кожен негативний допис є кампанією, і не кожен фейк потребує публічної відповіді. Рішення має враховувати реальне охоплення, темп зростання, наявність координації, статус ресурсів, ризик виходу в офлайн, чутливість теми, вразливість особи та ймовірність того, що мовчання буде інтерпретоване як підтвердження. Аналіз дозволить зменшити хаотичні реакції й уникнути ситуації, коли спростування саме створює інформаційну подію.

3.6. **Найкраща комунікація пояснює механіку, а не повторює звинувачення.**
Класичне спростування часто змушене цитувати фейк і тим самим закріплює його. Ефективнішим може бути пояснення ознак кампанії: анонімність першоджерела, однакові формулювання, синхронність, штучне охоплення, відсутність доказів, поєднання правди з маніпуляцією. Такий рефреймінг переводить увагу з нав'язаного звинувачення на спосіб впливу та допомагає аудиторії самостійно оцінювати майбутні повідомлення.

3.7. **Професійна солідарність є функціональним елементом безпеки.**
Публічна підтримка колег зменшує ізоляцію, демонструє замовнику обмеженість залякування та надає аудиторії альтернативний сигнал довіри. Вона також може бути психологічно важливою для людини, яка змушена протягом місяців повторно переглядати образливі матеріали, збирати докази й спілкуватися з правоохоронними органами. Водночас заяви підтримки мають спиратися на верифікацію, щоб механізм солідарності не став інструментом захисту від добросовісної критики.

3.8. **Технологічна експертиза має бути вбудована з першого дня.**
Юрист або комунікаційник не завжди може визначити, чи можливо технічно встановити зв'язок між каналами, зберегти метадані, підтвердити клонування або виявити штучну активність. Пізнє залучення технічного фахівця може означати втрату доказів. Тому первинний протокол має включати цифрове архівування, перевірку доменів, фіксацію рекламних оголошень, збір ідентифікаторів контенту.

3.9. Детектори штучного інтелекту не можуть бути єдиним доказом.
Інструменти виявлення згенерованого контенту відстають від генеративних технологій і можуть давати суперечливі результати. Тому висновок про дипфейк має спиратися на сукупність ознак: походження файлу, невідповідності з першоджерелами, технічний аналіз, контекст публікації, поведінку мережі та експертну оцінку. Автоматичний індикатор може бути сигналом для перевірки, але не остаточною підставою для публічного звинувачення.

3.10. Підготовка до виборів має початися до старту кампанії.
Учасники очікують, що доступність ШІ-аватарів, дипфейків, ботів і мереж анонімних каналів зробить виборчий період особливо вразливим. Після офіційного старту кампанії буде пізно створювати контакти, методології й правила реагування. Необхідно заздалегідь узгодити критерії верифікації, механізми міжорганізаційного обміну інформацією, протоколи публічних заяв і способи взаємодії з платформами.

3.11. Центральною мішенню є довіра, а не окремий факт.
Навіть успішне спростування одного твердження не обов'язково відновлює довіру, якщо кампанія створює загальне враження моральної сумнівності або професійної ненадійності особи. Саме тому атаки часто використовують велику кількість різних

пізвинувачень, частково правдивих деталей та емоційних асоціацій. Стратегія захисту повинна працювати з репутаційною рамкою в цілому, а не лише з кожною фразою окремо.

3.12. **Відповідь має захищати свободу слова, не створюючи механізм цензури.**
Будь-які пропозиції щодо блокування, встановлення обов'язкової ідентифікації або державного визначення дезінформації несуть ризик зловживань. Анонімність може використовуватися для атак, але також захищає джерела, викривачів і людей у небезпечних середовищах. Тому регуляторні рішення мають бути вузькими, процедурно захищеними, заснованими на доказах координованої поведінки та доступними для незалежного оскарження.

4**. Підсумки**
Зустріч продемонструвала, що інформаційні онлайн-атаки проти журналістів і медіа стали простим та доступним інструментом впливу. Їхня сила полягає не лише у неправдивості окремих повідомлень, а в мережевій природі, швидкості, емоційності та здатності поєднувати цифрову дискредитацію з юридичним і офлайн-тиском. Саме тому традиційне розуміння репутаційного спору є недостатнім.

Фіналізована позиція, що випливає з дискусії, полягає в необхідності перейти від реакції на окремі публікації до управління інформаційним інцидентом. Такий підхід вимагає координатора, швидкого аналізу, належної фіксації доказів, технічного аналізу, правового захисту, роботи з платформами, комунікаційної стратегії та підтримки людини. Успіхом слід вважати не лише судову перемогу, а й зменшення шкоди, збереження здатності журналіста продовжувати роботу, недопущення переходу атаки в фізичну площину та формування суспільного розуміння маніпулятивної технології.

Водночас запропонована система повинна бути побудована так, щоб не підмінити захист журналістики цензурою. Критичність до влади, бізнесу, медіа або громадських організацій є законною частиною демократичного процесу. Об'єктом протидії мають бути не незручні позиції, а верифіковані ознаки скоординованого переслідування, підробки, прихованої мережевої поведінки, незаконного використання персональних даних, погроз та втручання у професійну діяльність.

Найважливішим практичним наслідком зустрічі має стати перехід від обміну кейсами до створення операційної спроможності. Без визначеного координатора, строків, ресурсів і першого спільного продукту навіть якісна аналітична дискусія не змінить становище атакованих осіб. Першим таким продуктом доцільно зробити короткий протокол реагування протягом 24–72 годин, доповнений методологією документування та переліком перевірених контактів.

Отже, захист від інформаційних онлайн-атак слід розглядати як один із компонентів інформаційної безпеки та захисту демократичних інституцій. Чим раніше професійна спільнота створить спільні правила, тим менше ресурсів потребуватиме кожний наступний кейс і тим складніше буде використовувати дискредитацію як дешевий спосіб примусити журналіста або медіа до мовчання.

Додаток 2

ЗВІТ ЗА РЕЗУЛЬТАТАМИ ПРОВЕДЕННЯ ЕКСПЕРТНОЇ ЗУСТРІЧІ НА ТЕМУ: “ПРОТИДІЯ ПОШИРЕННЮ ДЕЗІНФОРМАЦІЇ ТА МАНІПУЛЯТИВНОЇ ІНФОРМАЦІЇ”

1. Загальний контекст і мета зустрічі

Експертна зустріч була присвячена пошуку збалансованого підходу до протидії дезінформації, маніпулятивній інформації, чуткам, скоординованим інформаційним операціям та новим технологічним формам впливу. Вихідною точкою дискусії стало визнання того, що свобода вираження поглядів є однією з фундаментальних суспільних цінностей, а тому будь-яке державне втручання в інформаційну сферу має відповідати вимогам законності, необхідності, пропорційності та правової визначеності.

Актуальність теми зумовлена одночасною дією кількох факторів: повномасштабною війною, тривалими операціями впливу з боку держави-агресора, швидким розвитком генеративного штучного інтелекту, поширенням діпфейків і синтетичних медіа, домінуванням соціальних платформ у розповсюдженні інформації, підготовкою до майбутніх повоєнних виборів, а також появою законодавчих і стратегічних ініціатив, у яких уже використовується термін «дезінформація».

Учасники прагнули відповісти не лише на питання, як описати дезінформацію, а насамперед на питання, яке саме суспільно небезпечне явище потребує правового реагування, які цінності мають бути захищені, де проходить межа між допустимим висловлюванням і шкідливою інформаційною операцією та які інструменти дадуть змогу протидіяти загрозам без створення надмірних обмежень для журналістики, політичної дискусії, критики влади, сатири, прогнозів або добросовісних помилок.

Зустріч мала діагностичний і концептуальний характер. Її завданням було не ухвалення готової законодавчої моделі, а систематизація проблем, зіставлення правових, комунікаційних, безпекових, технологічних і виборчих перспектив та визначення напрямів, у яких доцільно продовжити роботу.

2. Опис перебігу обговорення

Центральною дилемою стало питання, чи потрібно закріплювати в законодавстві України єдине юридичне визначення дезінформації. З одного боку, без спільної термінології державним органам, регуляторам, правоохоронцям, виборчим інституціям, платформам і громадським організаціям складно координувати дії. З іншого боку, надто широке визначення може перетворитися на інструмент довільного обмеження свободи слова, особливо якщо воно стане самостійною підставою для блокування ресурсів, видалення контенту, адміністративної або кримінальної відповідальності.

VI. ДОДАТКИ

У дискусії послідовно розмежовувалися щонайменше три рівні використання терміна. Перший - дослідницький і комунікаційний, де поняття може бути широким та охоплювати фейки, маніпуляції, пропаганду, оманливі наративи й інші форми викривлення інформації. Другий - стратегічний, де визначення використовується для опису загроз, цілей державної політики та координації між інституціями. Третій - юридичний, де кожен елемент визначення має бути достатньо точним, передбачуваним і доказовим, оскільки його застосування може спричиняти втручання у права та свободи.

Саме змішування цих трьох рівнів створює найбільший ризик. Формулювання, придатне для стратегії або фактчекінгового дослідження, не обов'язково придатне для санкційної норми. У правовій площині необхідно встановити, хто визначає неправдивість, яким є стандарт доказування, як доводиться умисел, що вважається суспільною шкодою, яким має бути причинний зв'язок між повідомленням і наслідками та як захищаються особи, які поширили інформацію добросовісно.

Було відзначено, що в Україні різні державні органи, медійні організації, фактчекінгові команди користуються власними класифікаціями. Одні розрізняють фейк, маніпуляцію, напівправду, неправду та помилку; інші використовують ширше поняття дезінформації; у медійному просторі дедалі частіше будь-який сумнівний або небажаний контент називають «ІПСО». Відсутність прозорої спільної методології призводить до того, що однакове повідомлення може отримати різну кваліфікацію залежно від установи або експертної команди.

Для досліджень така множинність підходів сама по собі не є критичною. Проблема виникає тоді, коли непублічна або нечітка методологія використовується для ухвалення рішень про обмеження діяльності медіа, блокування ресурсів, притягнення до відповідальності чи інших владних рішень. У таких випадках суб'єкт має розуміти критерії, за якими його поведінку визнано шкідливою, мати доступ до доказів і можливість ефективного оскарження.

Значну увагу було приділено відмінності між чутками та організованою дезінформацією. Чутки були описані як актуальна неперевірена інформація, що поширюється між людьми в умовах невизначеності та сприймається ними як корисна для пояснення подій або подолання психологічної загрози. Її поширення не обов'язково має зловмисний намір, автор часто невідомий, зміст змінюється під час передачі, а шкода може бути ненавмисною.

Натомість дезінформаційна операція зазвичай передбачає свідоме конструювання або викривлення повідомлення, наявність певної мети, кероване поширення та очікуваний шкідливий ефект. Однак на практиці межа між цими явищами розмивається: первинний вкид може бути навмисним, а подальше масове поширення здійснюють люди, які щиро повірили в повідомлення. Тому проста формула «намір є -

це дезінформація, наміру немає - це місінформація» не відображає мережеву природу сучасних кампаній.

Було також підкреслено, що велика частина агресивних і дискредитаційних чуток не піддається оперативній перевірці. Вони можуть стосуватися закритої військової інформації, внутрішніх мотивів посадових осіб, прогнозів, оцінок або припущень. У таких ситуаціях правова модель, побудована виключно на доведенні фактичної неправдивості, буде малоефективною.

Учасники звернули увагу, що неправдиві висловлювання виконують різні соціальні функції. Частина з них є побутовою, сатиричною, рекламною, художньою або жартівливою інформацією, яка не створює значної загрози. Водночас правдивий факт може бути використаний маніпулятивно - вибірково, поза контекстом, у критичний момент або в межах скоординованої кампанії, спрямованої на розпалювання ворожнечі, паніки чи недовіри.

Звідси випливає, що істинність повідомлення є важливим, але не єдиним і не завжди центральним критерієм. Для оцінювання ризику необхідно враховувати контекст, спосіб поширення, масштаб, цільову аудиторію, час, фінансування, рівень координації, авторитет мовця, наявність технологічного підсилення та характер можливої шкоди.

Однією з найстійкіших ліній дискусії стало зміщення фокусу з пошуку універсальної «правди» на аналіз шкоди. Йдеться про шкоду національній безпеці, громадському порядку, здоров'ю населення, правам інших осіб, демократичним інституціям, виборчому процесу, соціальній згуртованості та довірі до критично важливих суспільних систем.

Водночас категорія шкоди також потребує конкретизації. Необхідно розрізняти фактичну шкоду, безпосередній ймовірний ризик та віддалений кумулятивний вплив. Для кримінальної відповідальності вимоги до доказування мають бути особливо високими. Для системних обов'язків платформ може застосовуватися превентивний ризик-орієнтований підхід, за якого оцінюється не вина за окрему публікацію, а здатність архітектури сервісу сприяти масштабним суспільним загрозам.

Обговорення прикладів із судової і адміністративної практики показало, що наявні норми іноді застосовуються до ситуацій, для яких вони не були призначені. Зокрема, механізми протидії неправдивим чуткам можуть використовуватися замість цивільно-правового захисту честі, гідності або ділової репутації, а негативні оцінки діяльності посадовців можуть помилково трактуватися як суспільно небезпечна неправдива інформація.

Водночас значна частина явно небезпечного контенту вже охоплюється чинним правовим регулюванням, яке забороняє заклики до насильства або вчинення актів тероризму, пропаганду війни, розпалювання ворожнечі, посягання на права дітей, шахрайство, незаконний обіг товарів, окремі форми колабораціонізму тощо. Це підтримує висновок, що проблема часто полягає не у відсутності ще одного широкого складу правопорушення, а у якості кваліфікації, розслідування, доказування й судового контролю.

Окремим викликом є швидке стирання межі між шкідливим діпфейком і легітимним ШІ-аватаром. Синтетичне зображення або голос можуть використовуватися в освіті, творчості, сервісах, політичній комунікації чи доступності контенту. Водночас ті самі технології можуть створювати фіктивні заяви, дебати без участі реальної особи, підроблені звернення або матеріали, що неправомірно використовують зовнішність і персональні дані.

Автоматичні детектори ШІ-контенту не дають достатньо надійних результатів і можуть помилятися в обидва боки. Тому вони не можуть бути єдиною доказовою підставою для застосування санкцій. Більш перспективними названо прозоре маркування синтетичного контенту, створення правил використання образу людини, вимог до політичної реклами, збереження даних про походження матеріалу та спеціальні гарантії для виборчого періоду.

У дискусії сформувалося розуміння, що головним середовищем масштабування дезінформації є не традиційні зареєстровані медіа, а соціальні мережі, відеоплатформи, месенджери, анонімні канали, мережі фейкових акаунтів та кросплатформні екосистеми. Саме там відбуваються алгоритмічне підсилення, мікротаргетинг, прихована реклама, координація, масове дублювання та перенесення повідомлень між різними аудиторіями.

Європейський підхід, відображений у регулюванні цифрових послуг і штучного інтелекту, був розглянутий як приклад зміщення уваги з окремої одиниці контенту на функціонування інфраструктури. Він передбачає оцінку системних ризиків, прозорість рекламних і рекомендаційних механізмів, підзвітність великих платформ, належні процедури повідомлення та оскарження, доступ до даних і спеціальні заходи під час криз або виборів.

Одночасно було зафіксовано, що критерії скоординованої неавтентичної поведінки, які використовують самі платформи, є недостатньо прозорими й не завжди збігаються з оцінками українських дослідників. Складність зростає через кросплатформність: різні автори можуть формально не бути пов'язаними між собою, але працювати в межах спільної наративної або організаційної парасольки. Учасники неодноразово зверталися до концепції боротьби з FIMI - іноземними інформаційними маніпуляціями і втручаннями. перевага полягає в тому, що об'єктом аналізу стає

не просто неправдиве повідомлення, а комплексна діяльність: зовнішній вплив, маніпулятивне використання інформації, скоординована неавтентична поведінка та шкідливі наслідки для захищених суспільних цінностей.

Така рамка потенційно є точнішою за універсальну заборону дезінформації, особливо для протидії операціям держави-агресора та втручанню у вибори. Водночас вона не вирішує автоматично питання внутрішніх авторів, які поширюють подібні наративи без доведеного іноземного фінансування або прямої координації. Також термін залишається новим і потребує подальшої операціоналізації, тобто визначення чітких і вимірюваних індикаторів, зрозумілих не лише міжнародним експертам, а й національним інституціям, судам та громадськості.

Майбутні повоєнні вибори були визначені як період, у якому інформаційні операції можуть безпосередньо впливати на вільне формування волі виборця. Загроза полягає не лише в неправдивих заявах кандидатів, а у прихованому іноземному фінансуванні, непрозорій онлайн-рекламі, використанні персональних даних для мікротаргетингу, синтетичних матеріалах, ботомережах, масовому поширенні дискредитаційних наративів та нерівному доступі до платформних інструментів.

Було наголошено, що правове регулювання має захищати не тільки свободу вираження кандидатів та медіа, а й право громадян на власне, неупереджене та вільне волевиявлення. Для цього потрібні спеціальні правила виборчого періоду, оновлення законодавства про агітацію й політичну рекламу, координація між виборчими, медійними та безпековими інституціями та визначення процедур швидкого реагування.

Важливим завершальним акцентом стало застереження, що джерелом неправдивої або маніпулятивної інформації можуть бути не лише анонімні мережі, іноземні суб'єкти, медіа чи користувачі платформ, а й органи державної влади, посадові особи та політичні діячі. Високий статус мовця збільшує охоплення, легітимність і потенційний вплив повідомлення, тому модель регулювання не повинна автоматично надавати державній комунікації презумпцію достовірності.

З цього випливає вимога нейтральності: однакові принципи доказовості, прозорості, спростування та відповідальності мають застосовуватися незалежно від того, хто є джерелом повідомлення. Будь-які спеціальні повноваження держави щодо взаємодії з платформами повинні супроводжуватися незалежним контролем, фіксацією підстав, прозорими процедурами та ефективним оскарженням.

3. Висновки

3.1. Не запроваджувати поспішно універсальне каральне визначення дезінформації.

Загальне визначення, яке одночасно охоплює неправдивість, маніпулятивність, умисел і шкоду, неминуче залишатиме значний простір для суб'єктивної оцінки. Воно може бути доречним у стратегії, але є ризикованим як безпосередня підстава для санкцій.

3.2. Розділити стратегічну термінологію та юридичні склади правопорушень.

Стратегічні документи можуть описувати явище широко. Норми, що обмежують права, мають бути чіткими, вузько сформульованими, конкретними і прив'язаними до точно визначеного діяння, способу поширення інформації, захищеної цінності та визначеного рівня шкоди.

3.3. Регулювати передусім шкідливу поведінку та інфраструктуру.

Найбільш перспективними об'єктами правового регулювання є скоординована неавтентична поведінка, ботоферми, приховане фінансування, алгоритмічне підсилення, мікротаргетинг, масове створення фейкових акаунтів, незаконне використання образу людини та відсутність маркування синтетичного контенту.

3.4. Використовувати шкоду як ключовий, але не абстрактний критерій.

Необхідно заздалегідь визначити захищені суспільні цінності, рівні ризику, вимоги до причинного зв'язку та різні стандарти для кримінальних санкцій, адміністративного реагування, цивільного захисту і системних обов'язків платформ.

3.5. Не покладати на державний орган функцію остаточного арбітра правди.

Рішення, що спричиняють блокування, видалення або відповідальність, мають бути перевірюваними, мотивованими та оскаржуваними. Для найбільш істотних втручань необхідний незалежний, переважно судовий контроль.

3.6. Провести аудит чинного законодавства і практики його застосування.

До введення в законодавство України правових норм, що регулюватимуть нові види правопорушень, слід встановити, які загрози вже охоплюються чинним законодавством, де існують реальні прогалини, а де проблема спричинена неправильною кваліфікацією діянь, слабким розслідуванням, відсутністю науково-обгрунтованих методологій чи іншими факторами.

3.7. Розвивати вузьку рамку FIMI для протидії зовнішньому втручанню.

Концепція FIMI дає можливість комплексно поглянути на проблему і врахувати одразу кілька вимірів: зовнішнє походження впливу, маніпулювання інформацією та поширення дезінформації, скоординованість дій і шкоду. Водночас її застосування

має бути достатньо чітким і вузьким, щоб, з одного боку, ефективно захищати демократичний лад від шкідливого іноземного втручання, а з іншого - забезпечити дотримання прав людини, зокрема, право на свободу вираження та інформації.

3.8. Створити законну і підзвітну модель взаємодії з платформами.
Правила мають визначати підстави запитів, строки, компетенцію органів, порядок збереження доказів, критерії терміновості, прозорість, захист журналістського контенту та можливість оскарження.

3.9. Запровадити спеціальні гарантії для виборчого періоду.
Потрібні правила прозорості політичної реклами, іноземного фінансування, таргетингу, використання персональних даних, ШІ-контенту та швидкого реагування на скоординовані операції, що загрожують вільному волевиявленню.

3.10. Не криміналізувати звичайне поширення чуток і добросовісні помилки.
Більшість учасників мережевого поширення інформації можуть не знати про первинний зловмисний задум. Правове реагування має відрізняти організаторів, замовників, інфраструктурних посередників, професійних поширювачів і пересічних користувачів.

3.11. Поєднувати правові заходи з кризовою комунікацією та медіаграмотністю.
Чутки виникають і масштабуються в умовах невизначеності та дефіциту довіри. Своєчасна, конкретна й послідовна комунікація держави є не додатковим, а центральним засобом зменшення інформаційної вразливості.

3.12. Забезпечити нейтральність майбутньої моделі.
Державні органи, посадовці й політики також можуть поширювати неправдиві або маніпулятивні повідомлення. Їхній статус не повинен звільняти їх від стандартів прозорості, доказовості та відповідальності.

3.13. Оцінювати операції за сукупністю ознак, а не за одним маркером.
Практичне розпізнавання скоординованих інформаційних операцій часто базується на комбінації повторюваних наративів, синхронності мережевої поведінки, штучного охоплення, джерел фінансування, кросплатформного перенесення та спрямованості на конкретні вразливості.

3.14. Зробити протидію превентивною і ризик-орієнтованою.
Держава та платформи мають працювати не лише після появи окремого фейку, а виявляти системні вразливості, мережі поширення, технологічні механізми та суспільні теми, які можуть бути використані для масштабної маніпуляції.

4. Підсумки

Результати зустрічі свідчать, що ефективна політика протидії дезінформації не може бути побудована навколо одного універсального визначення або одного карального інструменту. Сучасні інформаційні загрози є мережевими, технологічними, кросплатформними та часто базуються не на повністю вигаданих фактах, а на змішаних повідомленнях, маніпулятивних інтерпретаціях, емоційному таргетингу й довготривалому просуванні наративів.

Найбільш збалансованою видається модель, яка поєднує вже існуючі вузькі правові заборони на поширення незаконного контенту, спеціальні механізми протидії іноземному втручанню, системні обов'язки платформ, прозорість політичної реклами та фінансування, правила для синтетичного контенту, якісне правозастосування, незалежний контроль і сильну кризову комунікацію. У центрі цієї моделі має бути не право держави встановлювати єдину істину, а обов'язок захищати конкретні суспільні цінності від доведених і пропорційно визначених ризиків.

Для України пріоритетними є три взаємопов'язані завдання. Перше - підготуватися до інформаційних ризиків майбутніх виборів. Друге - створити правову основу підзвітної взаємодії з глобальними платформами. Третє - перевести накопичений експертний досвід розпізнавання інформаційних операцій у прозорі, вимірювані й перевірювані критерії, придатні для правового та інституційного застосування.

Додаток 3

ЗВІТ ЗА РЕЗУЛЬТАТАМИ ПРОВЕДЕННЯ ЕКСПЕРТНОЇ ЗУСТРІЧІ НА ТЕМУ: “СТАН ЗАБЕЗПЕЧЕННЯ ПРАВА НА ДОСТУП ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ В ЦИФРОВОМУ СЕРЕДОВИЩІ УКРАЇНИ”

1. Загальний контекст і мета зустрічі

Експертна зустріч була присвячена оцінці того, наскільки в Україні забезпечується право на доступ до публічної інформації у цифровому середовищі. Вихідною точкою стала презентація результатів моніторингу, що охоплював повідомлення медіа, судову практику, законодавчі ініціативи та практику розпорядників інформації. Водночас дискусія свідомо вийшла за межі одного дослідження: учасники розглядали системні причини погіршення доступу до публічної інформації, поточні ризики для відкритих даних, доступ до судових рішень, проблеми документування та обліку інформації, а також можливі моделі спільної адвокації.

Предметом обговорення стала не лише формальна наявність законодавчих гарантій, а й реальна спроможність громадян, журналістів, дослідників, бізнесу та громадських організацій отримувати повну, своєчасну й придатну для використання інформацію. Особливу увагу було приділено тому, що цифрова трансформація не означає автоматичного підвищення відкритості. За відсутності належного інформаційного менеджменту цифрові інструменти можуть лише відтворювати старі бар’єри в новій формі або навіть посилювати їх.

Учасники прагнули відповісти на кілька практичних запитань: чи потрібні зміни до базового Закону України «Про доступ до публічної інформації»; як коректно імплементувати європейські вимоги щодо повторного використання публічної інформації; як не допустити використання безпекових та євроінтеграційних аргументів для невиправданого звуження доступу до публічної інформації; які заходи - моніторингові, навчальні, аналітичні чи адвокаційні - мають бути пріоритетними і якою має бути організаційна модель постійної спільної роботи.

2. Опис перебігу обговорення

На початку було представлено загальну оцінку стану доступу до публічної інформації у цифровому середовищі. Було відзначено, що Україна, попри повномасштабну війну та значні безпекові виклики, зберегла базову законодавчу рамку доступу до інформації. Це було оцінено як важливе досягнення. Водночас практика застосування цієї рамки демонструє сталі та повторювані проблеми, які існували ще до 2022 року і за воєнних умов стали помітнішими та небезпечнішими.

Серед найбільш типових порушень називалися ненадання відповідей на запити, неправомірне перекваліфікування запиту на інформацію у звернення громадян, формальні відписки, посилання на відсутність компетенції за наявності самої

інформації, а також обмеження доступу до інформації без належного застосування трискладового тесту. Особливо критично оцінювалася практика ненадання інформації, що має значний суспільний інтерес і може безпосередньо стосуватися безпеки людей, використання публічних коштів або контролю за діяльністю органів влади.

Окремий блок дискусії стосувався стану офіційних вебсайтів та внутрішнього документообігу. Було підкреслено, що значна частина сайтів центральних органів влади перетворилася на інформаційні вітрини або PR-ресурси. Вони містять новини про діяльність органу, але не дають зрозуміти, якими документами орган володіє, як ці документи обліковуються, де розміщені реєстри, які набори даних створюються та яким є механізм доступу до них. Відсутність систем обліку публічної інформації фактично унеможливлює якісне виконання обов'язків розпорядника.

Учасники приділили значну увагу доступу до судових рішень. Закриття рішень, які раніше перебували у відкритому доступі, відсутність зрозумілого механізму перегляду таких обмежень і паралельна доступність тих самих матеріалів у комерційних сервісах були охарактеризовані як дисбаланс, що підриває рівність доступу, антикорупційний контроль і свободу журналістської діяльності. Питання було визнано окремим стратегічним напрямом, який потребує скоординованої роботи.

Найбільш гостра частина обговорення стосувалася відкритих даних та законодавчих ініціатив. Було відзначено велику кількість змін до постанов, базових законів та непрофільних нормативних актів, які прямо або опосередковано впливають на доступ до інформації. Системний моніторинг таких змін практично відсутній, через що регрес може відбуватися непомітно, через десятки дрібних рішень.

У центрі критики опинився підхід, за якого імплементація Директиви ЄС про повторне використання публічної інформації використовується як підстава для внесення змін, що руйнують загальну логіку Закону України «Про доступ до публічної інформації». Учасники наголошували, що доступ до інформації та її повторне використання є взаємопов'язаними, але юридично різними сферами. Директива має імплементуватися через точкові зміни до спеціального законодавства та технічного регулювання відкритих даних, а не через створення нових підстав для відмови у доступі до інформації або розмивання базових понять.

Водночас дискусія не зводилася до повного заперечення будь-яких змін. Було визнано, що окремі сфери - архіви, бібліотеки, музеї, наукові дані, державні підприємства, цифрові масиви для навчання моделей штучного інтелекту - справді потребують сучаснішого регулювання. Ключовою умовою має бути точна і секторальна імплементація, яка не знижує вже досягнутий в Україні рівень гарантій.
Наприкінці зустрічі обговорення перейшло до організаційних рішень. Було визнано, що наявна експертна реакція переважно є кризовою: спільнота мобілізується, коли

з'являється особливо небезпечний законопроєкт, але не має ресурсу для щоденного моніторингу. Тому сформувалася підтримка ідеї створити невелике робоче ядро, розподілити напрями відповідальності, підготувати спільний меморандум, визначити потенційних донорів і провести окрему стратегічну сесію. Ширше коло організацій має забезпечувати суспільну та адвокаційну підтримку, тоді як повсякденну аналітичну роботу повинна виконувати компактна професійна команда.

3. Висновки

3.1. Правова основа доступу до інформації зберігається, але її практична ефективність поступово знижується.

Українська система доступу до публічної інформації все ще спирається на сильний базовий закон і значний масив судової практики. Сам факт збереження цієї рамки в умовах війни є суттєвим досягненням. Проте формальна стабільність закону не означає збереження реального рівня відкритості. Практичне право на інформацію послаблюється через неналежне застосування правових норм, широкі винятки, прийняття підзаконних актів, внутрішніх інструкцій, закриття реєстрів, скорочення складу відкритих наборів даних та адміністративну поведінку, орієнтовану на уникнення відповіді. Тому для оцінювання стану реалізації цього права лише тексту базового закону недостатньо. Потрібно аналізувати всю екосистему: нормативні акти різного рівня, технічну архітектуру державних інформаційних систем, реальну практику надання відповідей, проактивне оприлюднення публічної інформації, ефективність судового захисту і доступність даних у машинозчитуваному форматі.

3.2. Основна загроза має характер поступової, фрагментарної ерозії.

Дискусія засвідчила, що найбільш небезпечним сценарієм є не одноразове скасування права на доступ, а накопичення численних дрібних обмежень. Кожна окрема зміна може подаватися як технічна, тимчасова, безпекова або вузькосекторальна. Проте сукупний ефект таких змін здатний радикально змінити систему. Обмеження можуть з'являтися у законах, які формально не стосуються доступу до інформації, у постановах уряду, наказах центральних органів виконавчої влади, правилах функціонування реєстрів та технічних умовах доступу. За відсутності постійного моніторингу ці зміни стають видимими лише тоді, коли вони вже прийняті або почали застосовуватися. Отже, захист інформаційних прав має перейти від реагування на окремі резонансні проєкти до системи раннього виявлення регуляторних ризиків.

3.3. Коренева причина багатьох порушень - слабкий менеджмент офіційної інформації.

Проблеми із відповідями на запити, проактивним оприлюдненням інформації і формуванням відкритих даних мають спільне джерело: органи влади часто не управляють інформацією як системним ресурсом. Документи можуть зберігатися в різних підрозділах, не мати зрозумілої класифікації, єдиного обліку, належних метаданих або визначеного відповідального. За таких умов навіть добросовісний

працівник не завжди здатний швидко знайти документ і надати його. Водночас слабкість внутрішньої системи створює зручний простір для формальних відмов: розпорядник може стверджувати, що інформація не створена у потрібній формі, не належить до його компетенції або потребує додаткового узагальнення. Тому довгострокове покращення доступу неможливе без реформи електронного документообігу, систем обліку публічної інформації та внутрішніх процедур пошуку й оприлюднення документів.

3.4. Офіційні вебсайти не виконують функцію повноцінного інтерфейсу доступу.

Чимало державних сайтів побудовані навколо новин, повідомлень про заходи та позитивної презентації діяльності органу. Натомість користувачу складно встановити, які рішення прийняті, які документи перебувають у володінні органу, де оприлюднені нормативні акти, звіти, бюджети, переліки інформації, системи обліку та відкриті набори даних. Такий підхід суперечить логіці проактивного доступу. Вебсайт має бути не лише каналом комунікації органу із громадськістю, а структурованим каталогом його офіційної інформації. Розвиток цифрових послуг без реформування інформаційної архітектури сайтів не вирішить проблему. Потрібні мінімальні стандарти структури, пошуку, метаданих, доступності архівних версій, стабільних посилань і машинозчитуваних форматів.

3.5. Відкриті дані мають бути результатом системи, а не додатковим ручним обов'язком.

Наявна модель часто передбачає, що працівники органу окремо готують набори даних для оприлюднення, паралельно із виконанням основних функцій. У такій конструкції відкриті дані сприймаються як додаткове навантаження, яке можна відкласти через брак ресурсу, кадрові зміни або безпекові причини. Стратегічно правильним є інший підхід: дані мають формуватися автоматично у процесі здійснення повноважень органу. Якщо інформаційна система правильно структурована, очищений і безпечний для оприлюднення набір повинен генеруватися без повторного ручного введення. Це підвищить якість, регулярність оновлення та економічну цінність даних, а також зменшить можливість довільного закриття або вибіркового вилучення полів.

3.6. Безпекові обмеження мають бути конкретними, доказовими та пропорційними.

Повномасштабна війна об'єктивно створила нові ризики, які можуть виправдовувати обмеження доступу до окремих відомостей. Проте загальне посилання на воєнний стан не може замінити оцінку конкретної шкоди. Практика вилучення цілих категорій інформації про всіх суб'єктів, незалежно від їхнього зв'язку з обороною або критичною інфраструктурою, суттєво знижує цінність реєстрів і відкритих наборів. Учасники дійшли висновку, що обмеження повинні бути адресними, строковими,

переглядатися через визначені інтервали і ґрунтуватися на трискладовому тесті. Важливо також пояснювати суспільству логіку обмеження: якій саме шкоді запобігає закриття інформації, чому не можна застосувати менш обмежувальний захід і коли доступ буде відновлено.

3.7. Інформація значного суспільного інтересу потребує посиленого режиму захисту.

Інформація про безпеку укриттів, використання бюджетних коштів, закупівлі, діяльність критично важливих установ, стан довкілля або інші питання, що безпосередньо впливають на життя та безпеку людей, не може розглядатися як звичайний запит. Для таких категорій інформації потрібні прискорені внутрішні процедури, визначені відповідальні посадові особи та підвищений стандарт обґрунтування будь-якої відмови. В умовах війни ціна затримки може вимірюватися не лише якістю громадського контролю, а й людськими життями. Отже, органи влади мають навчитися розрізняти звичайні інформаційні запити і випадки, коли суспільний інтерес вимагає максимально швидкого та повного розкриття.

3.8. Формальна відсутність компетенції не повинна використовуватися для уникнення надання відповіді по суті.

На практиці поширеною є ситуація, коли орган фактично володіє документом або даними, але відмовляє у їх наданні, посилаючись на те, що питання не належить до його компетенції. Такий підхід переносить центр аналізу з факту володіння інформацією на відомчий розподіл повноважень і створює можливість нескінченного переспрямування запитувача між установами. Узгоджений висновок полягає в тому, що добросовісний розпорядник має виходити з наявності інформації та обов'язку сприяти доступу. Навіть коли інший орган є основним відповідальним за певну сферу, наявна публічна інформація не повинна приховуватися лише через формальну невідповідність компетенції.

3.9. Розмежування запиту на інформацію і звернення громадян потребує повторного навчального акценту.

Незважаючи на тривалу практику застосування закону про доступ до публічної інформації та сформовані судові підходи, розпорядники продовжують перекваліфіковувати запити у звернення. Це дозволяє застосовувати довші строки, вимагати додаткові реквізити або відповідати не по суті. Повторюваність проблеми свідчить не лише про окремі помилки, а про втрату інституційної пам'яті та недостатнє навчання нових працівників. Потрібні прості методичні матеріали, типові приклади, внутрішні чеклісти та регулярне підвищення кваліфікації. Водночас навчання буде недостатнім, якщо керівництво органу не створює стимулів до відкритості і не оцінює якість відповідей.

3.10. Доступ до судових рішень є важливим антикорупційним інструментом та невід'ємним елементом демократії.

Доступ до судових рішень забезпечує можливість перевірки єдності судової практики, дозволяє досліджувати діяльність правоохоронних і судових органів, виявляти корупційні ризики та готувати журналістські розслідування. Закриття доступу до рішень, проголошених у відкритих судових засіданнях, або до тих, що вже перебували у публічному доступі, підриває принцип правової визначеності. Особливо проблематичною є ситуація, коли офіційний реєстр більше не дає доступу до матеріалу, але той залишається доступним у платному комерційному продукті. Це створює нерівність між користувачами та фактично приватизує доступ до суспільно значущої інформації. Рішення про закриття доступу до судових рішень повинні мати законні підстави і бути публічно доступними, а також періодично переглядатись і за необхідності - оскаржуватись.

3.11. Доступ до інформації та повторне використання даних не можна змішувати.

Право отримати публічну інформацію відповідає на питання, чи має людина доступ до документа або даних. Повторне використання регулює подальше застосування вже доступної інформації, включно з технічними форматами, ліцензіями, API, оплатою граничних витрат, високовартісними наборами та умовами масового завантаження.

Змішування цих рівнів створює ризик, що технічні правила повторного використання перетворяться на нові підстави для відмови у первинному доступі. Фіналізований висновок полягає в тому, що імплементація європейських вимог має відбуватися без послаблення права знати. Необхідні зміни слід вносити до спеціальних законів і підзаконних актів, а будь-яке втручання у базовий закон має бути мінімальним, обґрунтованим і захищеним від додавання сторонніх обмежень.

3.12. Євроінтеграція повинна підвищувати, а не знижувати український стандарт.

Україна в окремих компонентах доступу до інформації та відкритих даних уже має регулювання, яке перевищує мінімальні стандарти деяких держав ЄС. Тому формальне перенесення положень директив без оцінки національного контексту може призвести до регресу. Справжня імплементація означає досягнення цілей європейського права, узгодження різних актів і збереження сильніших національних гарантій. Політична позначка «євроінтеграційний законопроєкт» не повинна звільняти проєкт від якісної правової експертизи, консультацій та оцінки впливу на основоположні права. Експертна спільнота має пропонувати не блокування інтеграції, а точнішу та повнішу модель виконання зобов’язань.

3.13. Сектор архівів, бібліотек, музеїв і наукових даних потребує окремого модернізованого регулювання.

Дискусія показала, що зміна статусу документів після передачі їх до архіву, умови оцифрування культурної спадщини, доступ до великих масивів даних, питання авторського права та можливість використання матеріалів для навчання моделей штучного інтелекту утворюють складний окремий блок. Такі проблеми не варто вирішувати шляхом загального звуження Закону про доступ до публічної інформації. Необхідний секторальний аналіз: які матеріали вже є публічними, які обмеження випливають із захисту персональних даних або авторських прав, як забезпечити недискримінаційний доступ, чи можуть державні установи надавати одному приватному суб'єкту масив даних, недоступний іншим, і якими мають бути технічні умови передачі великих обсягів даних.

3.14. Інституційна пам'ять у сфері доступу суттєво послабилася.

Зміна кадрів у державних органах призводить до того, що нові працівники не знають історії підготовки закону, досягнутих компромісів, відповідної судової практики та міжнародних стандартів. Через це до порядку денного повертаються пропозиції, які раніше вже були відхилені як небезпечні або концептуально помилкові. Аналогічна проблема існує і в громадському секторі: після перших успішних років імплементації увага донорів та організацій переключилася на інші теми. В результаті зменшилася кількість фахівців, які постійно стежать за системою. Відновлення інституційної пам'яті потребує бази правових позицій, попередніх законопроєктів, систематизованої судової практики, навчальних курсів і передачі досвіду новим посадовцям та експертам.

3.15. Ефективна адвокація має поєднувати принциповість, професійність і робочі канали комунікації.

Учасники визнали, що надмірно конфронтаційна комунікація може призвести до закриття неформальних каналів взаємодії, особливо у середовищі, де критика сприймається персонально. Водночас прагнення зберегти доступ до посадовців не повинно перетворюватися на самоцензуру або легітимізацію шкідливих рішень. Потрібна двоканальна модель. Перший канал - закрита предметна робота з текстами, аргументами та компромісними варіантами. Другий - готовність до публічної коаліційної кампанії, якщо змістовний діалог не дає результату. Комунікація має бути зосереджена на правових наслідках і практичних альтернативах, а не на персоналізації конфлікту.

3.16. Усередині держави існують потенційні інституційні союзники.
Зустріч продемонструвала, що державний сектор не є монолітним. Окремі інституції поділяють занепокоєння щодо регресивних змін, готують офіційні зауваження, залучають експертні ради та готові надавати організаційну підтримку. Це відкриває можливість формувати міжінституційні коаліції, де громадська експертиза поєднується з офіційними механізмами погодження, парламентського контролю та формування державної політики.
3.17. Найкраща організаційна модель - компактне робоче ядро та широке коло підтримки.
Широка коаліція забезпечує репутаційну вагу, видимість і можливість швидко мобілізувати підписи. Проте щоденний аналіз текстів, підготовка альтернатив, переговори та моніторинг не можуть ефективно здійснюватися десятками організацій одночасно. Тому доцільно сформувати невелику професійну групу з чітко розподіленими напрямами: законодавство, відкриті дані, судова практика, документообіг, навчання, комунікація та міжнародна взаємодія. Ширше коло партнерів має отримувати регулярні оновлення, погоджувати ключові публічні позиції та долучатися до адвокаційних кампаній. Така дворівнева структура дозволить поєднати швидкість і легітимність.

3.18. Конструктивна альтернатива сильніша за суто оборонну позицію.
Відмова від шкідливого законопроєкту може зупинити один ризик, але не вирішує питання імплементації європейських вимог, модернізації архівної сфери або відкриття високовартісних наборів даних. Якщо експертна спільнота лише критикує, органи влади можуть стверджувати, що вона блокує необхідні реформи. Тому стратегічно важливо підготувати власну альтернативу, яка підвищить переговорну позицію і дозволить перейти від захисту статус-кво до формування кращої політики.

4. Підсумки
Зустріч засвідчила, що право на доступ до публічної інформації в Україні має гарну правову базу, але перебуває під тиском різноманітних практичних, інституційних, технологічних і законодавчих чинників. Найбільша небезпека полягає у тому, що регрес може відбутися не через ухвалення окремого рішення, а внаслідок поступового накопичення винятків, скорочення наборів даних, зміни технічних правил, втрати інституційної пам’яті і компетентності та відсутності постійного зовнішнього контролю.
Водночас ситуація не є безвихідною. Експертна спільнота зберігає високий рівень знань, здатна швидко мобілізувати широку коаліцію та має потенційних союзників усередині державної системи. Європейська інтеграція, за умови правильної інтерпретації, може стати інструментом модернізації, а не обмеження.
Ключова умова подальшого прогресу - перехід від епізодичної реакції на виклики до постійної організованої роботи. Потрібен механізм, який відслідковує можливі зміни до їх ухвалення, швидко оцінює ризики, готує альтернативи, підтримує робочий діалог із владою та здатний проводити публічну адвокацію. Створення такої спроможності є найважливішим практичним результатом, до якого має призвести ця зустріч.

Додаток 4

ВІДПОВІДЬ ЦПД ПРИ РНБО ЩОДО МЕТОДОЛОГІЇ ТА СИСТЕМИ ОЦІНКИ ІНФОРМАЦІЙНИХ ЗАГРОЗ

РАДА НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

ЦЕНТР ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ

бульвар Лесі Українки, 26, м. Київ, 01133, e-mail: cpd@rnbo.gov.ua, сайт: www.cpd.gov.ua,
код ЄДРПОУ 44176573

_____ № _____ На № _____ від _____

ГО «Платформа прав людини»

Соломії ЯРЕМЕНКО

ел. адреса: law@ppl.org.ua

Про відповідь на звернення

Шановна пані Соломіє!

Центр протидії дезінформації за результатами опрацювання Вашого запиту, який надійшов на електронну пошту Центру 13.11.2025 року (вх. № Я-10/0-25 від 13.11.2025), повідомляє.

Відповідно до ч. 1 ст. 1 Закону України «Про доступ до публічної інформації» (далі - Закон), публічна інформація – це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом.

Згідно з ч. 1 ст. 19 цього Закону, запит на інформацію – це прохання особи до розпорядника інформації надати публічну інформацію, що знаходиться у його володінні.

Відповідно до ч. 1 ст. 13 Закону, розпорядниками інформації для цілей цього Закону визнаються:

1) суб'єкти владних повноважень - органи державної влади, інші державні органи, органи місцевого самоврядування, органи влади Автономної Республіки Крим, інші суб'єкти, що здійснюють владні управлінські функції відповідно до законодавства та рішення яких є обов'язковими для виконання;

2) юридичні особи, що фінансуються з державного, місцевих бюджетів, бюджету Автономної Республіки Крим, – стосовно інформації щодо використання бюджетних коштів;

СЕД АСКОД
Центр протидії дезінформації
№ 1249/1.2-6/2025 від 18.11.2025
Підписувач Сербін Євген Леонідович
Сертифікат 10CC9C
Дійсний з 16.02.2024 14:19:49 по 16.02.2026 14:19:49

Додаток 4

ВІДПОВІДЬ ЦПД ПРИ РНБО ЩОДО МЕТОДОЛОГІЇ ТА СИСТЕМИ ОЦІНКИ ІНФОРМАЦІЙНИХ ЗАГРОЗ

3) особи, якщо вони виконують делеговані повноваження суб'єктів владних повноважень згідно із законом чи договором, включаючи надання освітніх, оздоровчих, соціальних або інших державних послуг, - стосовно інформації, пов'язаної з виконанням їхніх обов'язків;

4) суб'єкти господарювання, які займають домінуюче становище на ринку або наділені спеціальними чи виключними правами, або є природними монополіями, - стосовно інформації щодо умов постачання товарів, послуг та цін на них;

5) юридичні особи публічного права, державні/комунальні підприємства або державні/комунальні організації, що мають на меті одержання прибутку, господарські товариства, у статутному капіталі яких більше 50 відсотків акцій (часток, паїв) прямо чи опосередковано належать державі та/або територіальній громаді, - щодо інформації про структуру, принципи формування та розмір оплати праці, винагороди, додаткового блага їх керівника, заступника керівника, особи, яка постійно або тимчасово обіймає посаду члена виконавчого органу чи входить до складу наглядової ради.

З урахуванням інформації, щодо якої Центр виступає розпорядником публічної інформації, та змісту питань, викладених у Вашому запиті, він не є запитом на отримання публічної інформації, тож його розглянуто відповідно до Конституції України та Закону України «Про інформацію».

Відповідно до Положення про Центр протидії дезінформації (далі – Положення), затвердженого Указом Президента України від 07.05.2021 № 187/2021, Центр протидії дезінформації (далі – Центр) є робочим органом Ради національної безпеки і оборони України, утвореним відповідно до рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації», уведеного в дію Указом Президента України від 19 березня 2021 року № 106.

Згідно з частиною другою п. 1 Положення, Центр забезпечує здійснення заходів щодо протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері, забезпечення інформаційної безпеки України, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою.

Відповідно до підпункту другого п. 6 Положення, Центр виявляє та вивчає поточні і прогнозовані загрози інформаційній безпеці України, чинники, які впливають на їх формування, прогнозує та оцінює наслідки для безпеки національних інтересів України.

Згідно з п. 2.1. Переліку відомостей, що становлять службову інформацію в Центрі протидії дезінформації, затвердженого наказом Центру від 25.12.2023 № 76, відомості щодо методології та системи оцінки інформаційних загроз та оперативного реагування на них, віднесено до відомостей, що становлять службову інформацію.

Додаток 4

ВІДПОВІДЬ ЦПД ПРИ РНБО ЩОДО МЕТОДОЛОГІЇ ТА СИСТЕМИ ОЦІНКИ ІНФОРМАЦІЙНИХ ЗАГРОЗ

Відкрита інформація щодо діяльності Центру, зокрема щодо повідомлень та інформаційних джерел, що містять дезінформацію, фейки та маніпуляції, оприлюднюється на каналах комунікації Центру (офіційний вебсайт, платформи Telegram, Instagram, Facebook,, YouTube, TikTok, Viber, X; зокрема, загальне охоплення протягом запитуваного періоду становить 2, 681 млрд, загальна кількість підписників – 611 тис.).

З повагою

Перший заступник керівника Центру **Євген СЕРБІН**

Додаток 5

ВІДПОВІДЬ НПУ ЩОДО РОЗБЛОКУВАННЯ ВЕБРЕСУРСУ У ВЕРЕСНІ - ЛИСТОПАДІ 2025 РОКУ

АДМІНІСТРАЦІЯ ДЕРЖСПЕЦЗВ'ЯЗКУ

НАЦІОНАЛЬНИЙ ЦЕНТР ОПЕРАТИВНО-ТЕХНІЧНОГО УПРАВЛІННЯ ЕЛЕКТРОННИМИ КОМУНІКАЦІЙНИМИ МЕРЕЖАМИ УКРАЇНИ

НЦУ

вул. Солом'янська, 13, м. Київ, 03110, тел. (044) 281-67-12,
e-mail: ncu@cip.gov.ua, web: cip.gov.ua
Код ЄДРПОУ 42980729

від_____20__р. № _____ На №_____від_____20___р.

ГО «Платформа прав людини»

Соломії ЯРЕМЕНКО

e-mail: law@ppl.org.ua

Пані Соломіє!

Національним центром оперативно-технічного управління електронними комунікаційними мережами України (далі - НЦУ) опрацьовано в межах компетенції Ваш запит на доступ до публічної інформації від 09.12.2025 (вх. № 917/68-2025 від 09.12.2025) про надання переліку веб ресурсів, до яких на підставі розпоряджень НЦУ постачальники електронних комунікаційних мереж та/або послуг (далі – постачальники) зобов'язані припинити здійснення обмеження доступу (блокування доступу).

За результатами розгляду повідомляємо про те, що згідно із частиною 8 статті 32 Закону України «Про електронні комунікації» та Порядку створення та діяльності системи оперативно-технічного управління електронними комунікаційними мережами загального користування та Національного центру оперативно-технічного управління електронними комунікаційними мережами України для цілей оборони та безпеки держави в умовах надзвичайної ситуації, надзвичайного або воєнного стану, затвердженого постановою Кабінету Міністрів України від 24.01.2025 № 75, НЦУ, що входить до загальної структури Державної служби спеціального зв'язку та захисту інформації України, з метою оперативно-технічного управління електронними комунікаційними мережами загального користування видає розпорядження, які є обов'язковими для виконання постачальниками.

Розпорядження НЦУ, які є обов'язковими для виконання всім постачальниками електронних комунікаційних мереж та/або послуг (далі – постачальники) опубліковуються на офіційному веб сайті Державної служби спеціального зв'язку та захисту інформації України «https://cip.gov.ua/» в розділі «Діяльність».

За період з 01.09.2025 по 30.11.2025 НЦУ було видано 1 розпорядження від 01.11.2025 № 834/3635 ««Про скасування обмеження доступу до ресурсу Інтернет»», яким постачальникам належало припинити здійснення обмеження доступу (блокування доступу) на власних рекурсивних DNS-серверах до доменного імені https://warontherocks.com, а також його піддоменів.

Начальник Національного центру Олександр ТИТАРЕНКО

42980729 - НЦУ
№68/02-600/2025 від 11.12.2025
КЕП (Підписання): Титаренко О. В.
11.12.2025 13:07
3FAA9288358EC0030400
0000F7FD2B00E946D600
Сертифікат дійсний з 05.07.2024 10:07 до 05.07.2026 10:07

Владислав МІСАНЬ 044-281-67-13

Додаток 6

ПЕРЕЛІК РЕСУРСІВ ІНТЕРНЕТУ, ЩОДО ЯКИХ ВІДПОВІДНО ДО РОЗПОРЯДЖЕНЬ НЦУ ПОСТАЧАЛЬНИКАМ НАЛЕЖАЛО ПРИПИНИТИ ОБМЕЖЕННЯ ДОСТУПУ ЗА ПЕРІОД З 01.01.2026 ПО 31.05.2026

№ з/п	Ресурс Інтернету	Ініціатор рішення або звернення	№ розпорядження НЦУ	Дата розпорядження НЦУ
1	specznak.ua	ДК НПУ	11/3786	08.01.2026
2	avtovin.com.ua	ДК НПУ	11/3786	08.01.2026
3	znaj.ua	ДК НПУ	37/3812	19.01.2026
4	ucavtoshkola.com.ua	ДК НПУ	53/3828	23.01.2026
5	rozvytok-avto.com	ДК НПУ	53/3828	23.01.2026
6	add.ua	ДК НПУ	252/4047	09.02.2026
7.	apteka-ds.com.ua	ДК НПУ	252/4047	09.02.2026
8.	etabletka.ua	ДК НПУ	252/4047	09.02.2026
9.	totispharma.com	ДК НПУ	252/4047	09.02.2026
10	smartpeople.com.ua	СБУ	213/4008	04.04.2026

Додаток 7

ІНФОРМАЦІЯ ПРО ЗАБЛОКОВАНІ ВЕБРЕСУРСИ

Повний перелік вебресурсів, заблокованих рішеннями НЦУ протягом вересня 2025 - травня 2026 року, доступний за посиланнями:

ВЕРЕСЕНЬ 2025

https://ppl.org.ua/wp-content/uploads/2026/08/dodatok-do-vidpovidi_veresen-2025.docx.docx.pdf

ЖОВТЕНЬ 2025

https://ppl.org.ua/wp-content/uploads/2026/08/dodatok-do-vidpovidi_zhovten-2025.docx.docx.pdf

ЛИСТОПАД 2025

https://ppl.org.ua/wp-content/uploads/2026/08/dodatok-do-vidpovidi_lystopad-2025.docx.docx.pdf

ГРУДЕНЬ 2025

https://ppl.org.ua/wp-content/uploads/2026/08/dodatok-do-vidpovidi_gruden-2025.docx.docx.pdf

СІЧЕНЬ 2026

https://ppl.org.ua/wp-content/uploads/2026/08/dodatok-1-sichen-2026.docx.docx.pdf

ЛЮТИЙ - ТРАВЕНЬ 2026

https://ppl.org.ua/wp-content/uploads/2026/08/dodatok-1-lyutyj-traven-2026.docx.pdf