



МЕТОДОЛОГІЯ МОНІТОРИНГУ ПОРУШЕНЬ ЦИФРОВИХ ПРАВ

(ІЗ ЗМІНАМИ ТА ДОПОВНЕННЯМИ, ЯКІ
НАБРАЛИ ЧИННОСТІ З 01 ЧЕРВНЯ 2021
РОКУ)

ГО «ПЛАТФОРМА ПРАВ ЛЮДИНИ»

2021 РІК

ЗМІСТ

I. ВСТУП.....	2
II. МЕТА, ПРЕДМЕТ, ОБ'ЄКТ ТА МЕТОДИ МОНИТОРИНГУ.....	4
III. НОРМАТИВНО-ПРАВОВІ ЗАСАДИ ЗДІЙСНЕННЯ МОНИТОРИНГУ.....	5
IV. ВІДБІР, АНАЛІЗ, СИСТЕМАТИЗАЦІЯ ТА КЛАСИФІКАЦІЯ ІНФОРМАЦІЇ	6
Порядок внесення повідомлень до Індексу порушень цифрових прав та виключення з нього	6
Аналіз, систематизація та класифікація інформації.....	7
Інформація, яка не включається до Індексу	9
Зловживання правом на свободу слова.....	9
Цикл Моніторингу	10
V. ГЛОСАРІЙ	11

I. ВСТУП

Інтернет відіграє все більшу роль у нашому житті. Щороку його аудиторія невпинно збільшується. Лише у 2020 році кількість українських інтернет-користувачів зросла на 2 мільйони, що на 33 % більше, ніж за попередній рік. На початку 2021 року вона становила майже 30 мільйонів осіб або біля 67% населення країни. Динамічно розвивається й аудиторія соціальних мереж. У 2020 році кількість користувачів з України зросла на 7 мільйонів, досягнувши 26 мільйонів осіб¹.

Зрозуміло, що за таких умов вплив інтернету на права людини також лише посилюється, а саме дотримання цих прав набуває неабиякої актуальності.

Рада ООН з прав людини в своїй резолюції «Про сприяння, захист та здійснення прав людини в Інтернеті» від 5 липня 2012 року сформулювала надзвичайно важливий принцип, відповідно до якого «права, які людина має офлайн, мають однаковою мірою бути захищені онлайн, зокрема, свобода вираження поглядів, яка застосовується незалежно від кордонів та щодо будь-яких обраних особою ЗМІ, відповідно до статті 19 Загальної декларації прав людини та Міжнародного пакту про громадянські і політичні права». В цій резолюції визнається відкритий і глобальний характер Інтернету і міститься заклик до держав сприяти та полегшувати доступ до мережі.

Комітет міністрів Ради Європи у своїй рекомендації CM/Rec(2014)6 щодо посібника з прав людини для Інтернет-користувачів² звертає увагу на те, що держави-члени Ради Європи зобов'язані забезпечити кожному, хто знаходиться в межах їхньої юрисдикції, права та основоположні свободи, закріплені Європейською конвенцією про захист прав людини і основоположних свобод та що дія цього зобов'язання поширюється в тому числі на сферу використання мережі інтернет. Основні міжнародні стандарти у цій галузі стосуються питань доступу до інтернету та недискримінації; свободи вираження поглядів і інформації; свободи зібрань та об'єднань в інтернеті; приватного життя, права на анонімність та захист даних; права на отримання освіти, доступу до знань через інтернет; особливого захисту дітей та молоді; ефективних засобів правового захисту.

Разом з тим, в сучасних умовах масового поширення дезінформації, маніпуляцій та іншого шкідливого контенту нерідко створюються загрози для прав людини в інтернеті. Це насамперед пов'язано з тим, що органи влади, реагуючи на зазначені виклики та намагаючись обмежити обіг шкідливої інформації, нерідко забороняють чи суттєво обмежують доступ до певних веб-ресурсів. З іншого боку, існують проблеми з ефективним захистом права на приватне життя та захист персональних даних тощо.

Цей Моніторинг порушення цифрових прав в Україні (далі – Моніторинг) впроваджено з метою виявлення фактів порушення цифрових прав людини в Україні на території, яка контролюється Урядом України, з метою їх наступного

¹ <https://www.epravda.com.ua/news/2021/03/17/672023/>

² <https://rm.coe.int/16802e3e96>

узагальнення, привернення до них уваги з боку державних органів та громадськості і напрацювання подальших кроків для подолання існуючих проблем.

Моніторинг здійснюється ГО «Платформа прав людини» <https://www.ppl.org.ua/> в межах спільної діяльності партнерів по коаліції «За вільний Інтернет» <https://www.facebook.com/FreeNetUkraine/>. Коаліція була створена у травні 2018 року у відповідь на постійні спроби влади обмежувати Інтернет, блокувати веб-сайти та регулювати Інтернет без врахування принципу верховенства права. Коаліція об'єднала правозахисні організації та фахівців для забезпечення дотримання стандартів прав людини в Інтернеті. Починаючи з травня 2019 року дослідження проводиться безперервно на постійній основі.

Оновлена в травні 2021 року методологія враховує існуючий досвід проведення моніторингу та відображає наявні можливості виявлення та фіксації фактів порушень прав людини в цифровому середовищі. Разом з тим, вона дозволяє давати відповідь й на нові виклики та завдання, які постають перед правозахисниками і потребують реагування. Ця методологія і надалі переглядатиметься у разі потреби з метою її осучаснення та належного реагування на нові тренди та загрози.

II. МЕТА, ПРЕДМЕТ, ОБ'ЄКТ ТА МЕТОДИ МОНІТОРИНГУ

Мету, предмет та об'єкт моніторингу можна окреслити наступним чином:

- **Метою моніторингу** є виявлення порушень цифрових прав в Україні та визначення їх кількісних і якісних характеристик.
- **Предметом моніторингу** є порушення цифрових прав в Україні³.
- **Об'єктом моніторингу** є веб-ресурси, на яких оприлюднюється інформація про випадки порушення цифрових прав в Україні у визначених цією методикою сферах, в тому числі: Єдиний державний реєстр судових рішень, офіційні веб-сайти профільних органів державної влади та неурядових організацій, онлайн видання та соціальні мережі.

Окрім того, інформацію про випадки порушення цифрових прав надають організацій-члени коаліції «За вільний Інтернет».

- **Методи, які застосовуються при проведенні Моніторингу:**
 1. **Веб-сервер-аналіз** – метод, який полягає у здійсненні експертом в режимі онлайн пошуку в мережі Інтернет інформації, яка дозволяє виявити факти порушення (або потенційного порушення) цифрових прав.
 2. **Контент-аналіз** інформації, отриманої з мережі Інтернет та від організацій-членів коаліції «За вільний Інтернет», що дозволяє виділити факти порушення (або потенційного порушення) цифрових прав та структурувати і класифікувати їх.
 3. **Інтерв'ювання** потерпілих від агресії, представників правоохоронних органів, учасників конфлікту (за можливості).
 4. **Метод спостереження** – який дозволяє встановити динаміку змін у сфері реалізації цифрових прав.

Під час Моніторингу можуть використовуватись й інші методи проведення дослідження, які дозволяють ефективно виявляти, систематизувати та класифікувати факти порушення цифрових прав.

³ Моніторинг проводиться щодо порушення цифрових прав на підконтрольній Уряду України території.

III. НОРМАТИВНО-ПРАВОВІ ЗАСАДИ ЗДІЙСНЕННЯ МОНІТОРИНГУ

- 1) Конституція України;
- 2) Європейська Конвенція про захист прав людини і основоположних свобод;
- 3) Господарський процесуальний кодекс України;
- 4) Кодекс адміністративного судочинства України;
- 5) Кримінальний процесуальний кодекс України;
- 6) Кодекс України про адміністративні правопорушення;
- 7) Цивільний кодекс України;
- 8) Цивільний процесуальний кодекс України;
- 9) Закон України «Про телекомунікації»;
- 10) Закон України «Про доступ до публічної інформації»;
- 11) Закон України «Про авторське право і суміжні права»;
- 12) Закону України «Про інформацію»;
- 13) Закон України «Про санкції»;
- 14) Інші закони України та підзаконні нормативно-правові акти з питань захисту прав людини;
- 15) Рекомендація CM/Rec(2014)6 Комітету міністрів Ради Європи державам-членам щодо посібника з прав людини для Інтернет-користувачів (ухвалена Комітетом міністрів 16 квітня 2014 року на 1197-му засіданні постійних представників міністрів);
- 16) Рекомендація CM/Rec(2014)6 Комітету міністрів Ради Європи державам-членам щодо посібника з прав людини для Інтернет-користувачів – пояснювальний меморандум;
- 17) Рекомендація CM/Rec(2018)2 Комітету міністрів Ради Європи державам-членам щодо ролі та відповідальності інтернет-посередників;
- 18) Інші міжнародні документи, обов'язкові до застосування на території України;
- 19) практика Європейського суду з прав людини.

IV. ВІДБІР, АНАЛІЗ, СИСТЕМАТИЗАЦІЯ ТА КЛАСИФІКАЦІЯ ІНФОРМАЦІЇ

Порядок внесення повідомлень до Індексу порушень цифрових прав та виключення з нього

Під час моніторингу відбирається інформація, оприлюднена в мережі інтернет, в тому числі на офіційних веб-ресурсах, яка свідчить про **порушення прав людини в цифровому середовищі в Україні**. Тобто така, що вказує на реальне чи потенційне порушення прав людини в мережі інтернет на території, яку контролює Уряд України. Інші порушення прав людини (в тому числі прав на доступ до інформації, на свободу вираження поглядів, на захист приватного життя та освіти офлайн-середовищі тощо) не є предметом цього дослідження.

Первинний збір інформації в мережі інтернет щодо фактів порушень (потенційних порушень) цифрових прав та її попередній аналіз здійснюється аналітиком з моніторингу, який пройшов відповідне навчання і стажування. Аналітик з моніторингу здійснює верифікацію інформації про можливе порушення цифрових прав та заносить відповідне повідомлення до таблиці моніторингу, зазначаючи в ній джерело, опис інформації та гіперпосилання на неї.

Спірні питання стосовно внесення чи невнесення тієї чи іншої інформації до моніторингової таблиці аналітик з моніторингу узгоджує із юристом-аналітиком.

Якщо після всіх вжитих заходів перевірки, обговорення з юристом-аналітиком, залишається сумнів щодо достовірності та/чи обґрунтованості включення певного випадку до таблиці моніторингу, це питання передається на вирішення Експертної Ради коаліції «За вільний Інтернет» (далі – Експертна Рада).

Вторинний аналіз всіх зібраних у таблиці моніторингу фактів порушення цифрових прав здійснює юрист-аналітик, який перевіряє опис події, її верифікацію, відповідність і обґрунтованість попередньої оцінки аналітика з моніторингу.

Після перевірки відповідного випадку юристом-аналітиком, отримання ним у разі необхідності відповіді від Експертної Ради щодо сумнівних та/або складних випадків, за наявності підстав інформація про виявлені порушення (потенційні порушення) цифрових прав вноситься до Індексу порушень цифрових прав (далі – Індекс).

Експертна Рада коаліції «за вільний інтернет» створюється для оцінки та прийняття рішень стосовно виявлених сумнівних та/або складних випадків імовірного порушення цифрових прав, розгляду питань щодо виключення інформації з Індексу. Члени коаліції «За вільний Інтернет» делегують до Експертної Ради по одному представнику від кожної організації.

Експертна Рада ухвалює рішення щодо внесення тих чи інших фактів до Індексу або виключення з нього голосуванням, яке може проводитись в тому числі он-лайн у створеному чаті Експертної ради. Рішення приймається простою більшістю голосів членів Експертної Ради - представників організацій-партнерів.

Стосовно інцидентів, щодо яких члени Експертної Ради не змогли ухвалити рішення, для проведення консультацій можуть залучатися експерти міжнародних правозахисних місій, міжнародних організацій, що спеціалізуються на захисті цифрових прав тощо.

Аналіз, систематизація та класифікація інформації

Отримана в результаті проведення Моніторингу інформація підлягає систематизації та віднесенню до однієї з наступних категорій:

- порушення цифрових прав загального характеру;
- порушення цифрових прав індивідуального характеру;
- потенційні порушення цифрових прав.

I. Порушення цифрових прав загального характеру

До цієї категорії відносяться порушення цифрових прав, які мають вплив на необмежене коло осіб.

Зокрема, вона включатиме факти блокування чи іншого обмеження доступу до веб-ресурсів **без дотримання стандартів** частини 2 статті 10 Європейської Конвенції про захист прав людини і основоположних свобод (тобто такі, які вчинені з порушенням принципу законності (ясності та передбачуваності закону, його доступності тощо) та/або не переслідують легітимну мету та/або не є необхідними у демократичному суспільстві). Це пояснюється тим, що блокування тих чи інших веб-сайтів унеможлиблює доступ до них широкої аудиторії та робить недоступною оприлюднену на них інформацію. Отже, згадані блокування мають вплив на необмежене коло осіб, а тому відносяться до порушень загального характеру.

Сам факт недотримання органами державної влади стандартів частини 2 статті 10 Європейської Конвенції про захист прав людини та основоположних свобод є достатньою підставою для встановлення порушення цифрових прав у наведених випадках, незалежно від змісту заблокованої в такий спосіб інформації.

II. Порушення цифрових прав індивідуального характеру

До цієї категорії відносяться порушення цифрових прав, які стосуються окремих осіб і не мають безпосереднього впливу на широку аудиторію. Сюди можуть відноситись факти погроз та нападів на журналістів інтернет-видань, їх редакції, пов'язані із здійсненням професійної журналістської діяльності онлайн, випадки цькування журналістів з використанням мережі інтернет, неправомірне використання тих чи інших засобів правового захисту у справах про захист репутації, неналежне розмежування фактів і оціночних суджень та покладення обов'язку спростувати достовірну інформацію, поширену в мережі інтернет, інформація про протиправне поширення в інтернеті відомостей про приватне життя особи, в тому числі її персональних даних, факти тиску на органи саморегуляції журналістів, пов'язані з оприлюдненням в інтернеті їх рішень та заяв тощо.

III. Потенційні порушення цифрових прав

До цієї категорії відносяться факти виявлених порушень, які можуть мати негативні наслідки в майбутньому (наприклад, факти реєстрації в парламенті проєктів законів, що обмежують права людини в інтернеті) та такі, де на момент проведення Моніторингу існують потенційні ризики порушення цифрових прав користувачів інтернету в Україні, проте точно визначити чи вплинули вони на українських інтернет-користувачів за наявною інформацією неможливо або неможливо встановити реальних жертв таких загроз (відомості про поширення фішингових листів, витік або загроза витоку персональних даних, атаки на веб-сайти та збої в роботі останніх тощо).

Хакерські та інші атаки на веб-ресурси будуть кваліфікуватись як порушення цифрових прав у разі, якщо вони призвели до зупинки чи значних ускладнень в роботі сайтів. Разом з тим, якщо зазначені наслідки не настали, а самі атаки мали місце, такі дії будуть кваліфікуватись як потенційні порушення цифрових прав.

Під час Моніторингу інформація буде збиратись, зокрема, за наступними напрямками⁴:

1. Доступ до Інтернету:

а) факти обмеження (заборони) доступу до веб-ресурсів, в тому числі їх блокування.

2. Свобода вираження поглядів та інформації в Інтернеті:

а) напади на журналістів, блогерів, громадських активістів та інших медіа-учасників та/або на редакції онлайн видань у зв'язку із здійсненням ними журналістської діяльності в інтернеті;

б) цькування журналістів та інших медіа-учасників з використанням мережі інтернет та цифрових технологій;

в) судові рішення, в тому числі про застосування заходів забезпечення позову, якими зобов'язано припинити чи обмежити доступ до інформації, оприлюдненої в мережі Інтернет;

г) судові рішення, якими на учасника справи покладено обов'язок, не передбачений законом (наприклад, зобов'язано вибачитись) або такий, що не відповідає іншим стандартам в галузі свободи слова в інтернеті, визначеним практикою Європейського суду з прав людини;

ґ) судові рішення, в яких належним чином не розмежовано факти та оціночні судження, внаслідок чого вони суттєво обмежують свободу вираження в мережі інтернет;

д) судові рішення у справах по статті 173-1 КУпАП щодо поширювання неправдивих чуток в інтернеті, які ухвалюються без дотримання міжнародних стандартів в галузі свободи слова;

е) факти подачі позовів до журналіста, блогера, фрілансера та/чи ЗМІ щодо інформації, оприлюдненої в мережі Інтернет, де позивачем заявлено надмірні позовні вимоги, які можуть мати «охолоджувальний ефект» для свободи слова;

є) обшуки та/або тимчасовий доступ до речей і документів із вилученням у дата-центрах, редакціях он-лайн видань серверів, комп'ютерів та іншої техніки, яка використовувалась для поширення інформації в мережі інтернет; силове блокування роботи провайдерів, редакцій тощо;

ж) хакерські та інші атаки на веб-сайти, внаслідок яких веб-ресурси припинили роботу чи їх робота значною мірою ускладнилась;

з) інші порушення права на свободу вираження поглядів в цифровому середовищі.

⁴ Цей перелік не є вичерпним.

3. Приватне життя та захист даних:

- а) факти витоку та/або оприлюднення конфіденційних персональних даних в мережі Інтернет без згоди особи чи володільця цих даних та за відсутності суспільного інтересу до них або спроби вчинити зазначені дії;
- б) факти зламу сервісів, баз даних компаній /соціальних мереж/;
- в) факти несанкціонованого (позасудового) доступу правоохоронних органів до конфіденційних персональних даних користувачів;
- г) застосування та/або спроби застосування заходів загального спостереження чи перехоплення інформації (включаючи висунення законодавчих ініціатив, спрямованих на це).

4. Інші порушення цифрових прав

За цим напрямком збирається та узагальнюється інформація про порушення цифрових прав на мирні зібрання та участь у інтернет-спільнотах, про порушення права на освіту через мережу інтернет та щодо інших видів порушень цифрових прав.

Крім того, сюди відноситься інформація, яка стосується порушень цифрових прав, що мають місце в особливий період, такий як вибори, пандемія тощо.

Наприклад, під час виборів, а також у певний проміжок часу до та після них можуть мати місце порушення виборчих прав через поширення спотвореної інформації в мережі інтернет, зокрема, шляхом підробки інтернет-сайтів чи сторінок відомих соціологічних компаній та поширення через них неправдивих результатів соціологічних досліджень з метою впливу на виборців, або поширення фотографій виборчих бюлетенів у день виборів, що прирівнюється до агітації, яка в цей період заборонена.

За цим напрямком також буде збиратись інформація про порушення прав людини в цифровому середовищі, яка не охоплена іншими напрямками.

Інформація, яка не включається до Індексу

До Індексу порушень цифрових прав за загальним правилом не включається інформація про випадки шахрайства із використанням мережі інтернет.

Разом з тим, повідомлення про відсутність належного реагування на зазначені випадки з боку органів влади та невчинення дій щодо протидії кіберзлочинності може бути підставою для включення відповідних відомостей до Індексу.

Порушення права на доступ до публічної інформації журналістів, інших працівників онлайн видань та інших медіа-учасників (блогерів, лідерів думок тощо) зазвичай не вважається порушенням цифрових прав, за винятком випадків, коли порушення стосується ненадання інформації в електронній (цифровій) формі через мережу інтернет.

Зловживання правом на свободу слова

Під час моніторингу можуть виявлятися факти зловживання правом на свободу слова, зокрема, поширення дезінформації, шкідливої та/або хибної інформації та маніпуляцій, використання ботів, тролів тощо.

Збір та узагальнення зазначеної інформації не є метою цього моніторингу. Зазвичай зазначені зловживання викривають організації-фактчекери, повідомляючи про них громадськість та готуючи відповідні аналітичні звіти.

Втім, у разі виявлення зазначених фактів, якщо буде доцільно, може прийматись рішення про їх включення до Індексу в окремому підрозділі «Зловживання правом на свободу слова».

Цикл Моніторингу

Моніторинг проводиться на постійній основі з щомісячним оприлюдненням Індексу порушень цифрових прав. В Індексі відображаються виявлені під час Моніторингу факти порушення (потенційного порушення) цифрових прав.

Раз на рік, а за можливості – частіше (раз на півроку, раз на квартал тощо) на основі щомісячних Індексів порушення цифрових прав готуються аналітичні звіти, в яких узагальнюється стан дотримання цифрових прав в Україні, звертається увага на існуючі види порушень цифрових прав, їх динаміку, фактори, які сприяють їх вчиненню та пропозиції щодо покращення захисту цифрових прав в Україні.

V. ГЛОСАРІЙ

1. **«Цифрові права»** для цілей цього дослідження – це права людини в он-лайн середовищі, які включають, зокрема, право на доступ до Інтернету, право на свободу висловлювання, право на захист приватності та інші права людини, реалізація яких відбувається за допомогою цифрових технологій.
2. **«Кількісні характеристики порушення цифрових прав»** - кількість випадків порушення цифрових прав, виявлених протягом відповідного циклу моніторингу.
3. **«Якісні характеристики порушення цифрових прав»** - аналіз порушень цифрових прав, визначення їх характеру (загального чи індивідуального) та виду відповідно до напрямків моніторингу.
4. **Надмірні позовні вимоги, що можуть мати «охолоджувальний ефект»** - це позовні вимоги, які відповідають одному чи декільком нижченаведеним критеріям:
 - а) вимоги про стягнення надмірної суми відшкодування шкоди;
 - б) вимоги про видалення інформації, яка має суспільний інтерес;
 - в) вимоги про спростування інформації у формі оціночних суджень;
 - г) вимоги про обмеження доступу до веб-ресурсу, на якому оприлюднено спірну інформацію.

При оцінці позовних вимог враховується контекст, в якому викладено спірну інформацію, особа позивача, особа відповідача, публічність осіб та межі їх дозволеної критики, суть позовних вимог, сума позову тощо.