МЕТОДОЛОГІЯ

МОНІТОРИНГУ ДОТРИМАННЯ ПРАВ ЛЮДИНИ В ІНТЕРНЕТІ ПІД ЧАС ВІЙНИ

ІЗ ЗМІНАМИ ТА ДОПОВНЕННЯМИ, ЯКІ НАБРАЛИ ЧИННОСТІ З 24 ЛЮТОГО 2022 РОКУ

ГО "ПЛАТФОРМА ПРАВ ЛЮДИНИ" 2022

ЗМІСТ

ВСТУП

24 лютого Російська Федерація після повномасштабного вторгнення почала новий етап війни проти України. Російські загарбники не тільки обстрілюють та бомбардують мирні міста й села України, а й атакують український кіберпростір. В умовах війни загроз для прав людини в інтернеті стало значно більше. Насамперед, це пов'язано з кібератаками, поширенням дезінформації, інших маніпуляцій та шкідливого контенту, які постійно здійснює ворог. На окупованих територіях та безпосередньо на лінії фронту рашисти намагаються взагалі відключити українцям доступ до інтернету. З іншого боку, ефективний спротив ворожим кібератакам та захист національної безпеки в цифровому вимірі неможливий без заборони чи суттєвого обмеження доступу до ворожих веб-ресурсів, а також, здійснення, у відповідь, атак на російські цілі у всесвітній мережі.

Метою Моніторингу дотримання прав людини в інтернеті під час війни є збір, узагальнення і аналіз даних про події, що мають вплив на цифрові права людини та привернення до них уваги з боку державних органів та громадськості, напрацювання можливих рішень для вирішення проблем, що з'явилися у цифровому вимірі.

Починаючи з 2019 року Громадська організація “Платформа прав людини” (далі - ППЛ) здійснює моніторинг дотримання цифрових прав в Україні метою якого є виявлення фактів порушення цифрових прав людини. З 24 лютого 2022 року фокус дослідження було змінено з виявлення порушень цифрових прав на збір та аналіз інформації про загрози, які відбуваються в сфері цифрових прав людини. Зміна мети, предмету та об'єкту моніторингу пов'язана із початком нового етапу війни та запровадженням 24 лютого 2022 року Указом Президента України № 64/2022 «Про введення воєнного стану в Україні» на всій території України правового режиму воєнного стану. Під час дії воєнного стану можливе тимчасове, на період його дії, обмеження, в тому числі, фундаментальних права людини, серед яких: право на свободу думки і слова, на вільне вираження своїх поглядів і переконань; право на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції; право на особисте життя. В зв'язку з тим, що законодавцями не встановлено чітких меж обмеження прав людини в умовах воєнного стану, класифікація подій, що відбуваються в сфері цифрових прав, з точки зору порушень, є досить проблематичною. Кожна подія потребує детального вивчення всіх обставин та балансування інтересів національної безпеки та відповідних прав або свобод. Саме тому на даному етапі моніторингу ППЛ не здійснює кваліфікацію подій, що стосуються цифрових прав людини як порушення, а збирає, аналізує, узагальнює інформацію про загрози для цифрових прав людини, які потенційно можуть кваліфікуватися як порушення.

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

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

Метою моніторингу є збір і аналіз інформації про загрози, які відбуваються в сфері цифрових прав під час дії правового режиму воєнного стану з метою узагальнення і визначення стану дотримання цифрових прав під час війни.

Предметом моніторингу є події, які відбуваються в сфері цифрових прав під час дії правового режиму воєнного стану та містять загрозу для цифрових прав людини.

Об'єктом моніторингу є веб-ресурси, на яких оприлюднюється інформація про події, які стосуються цифрових прав в Україні, під час дії правового режиму воєнного стану, 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.

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 події, які стосуються цифрових прав.
2. Контент-аналіз інформації, отриманої з мережі Інтернет, що дозволяє виділити події, які містять загрозу для цифрових прав людини.
3. 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 події, які стосуються цифрових прав.

ІІ. НОРМАТИВНО-ПРАВОВІ ЗАСАДИ ЗДІЙСНЕННЯ МОНІТОРИНГУ

1) Конституція України;
2) Європейська Конвенція про захист прав людини і основоположних свобод та відповідна практика Європейського суду з прав людини;
3) Цивільний кодекс України;
4) Цивільний процесуальний кодекс України;
5) Кримінальний кодекс України;
1) Кримінальний процесуальний кодекс України;
2) Кодекс України про адміністративні правопорушення;
3) Кодекс адміністративного судочинства України;
4) Закон України «Про електронні комунікації»;
5) Закон України «Про доступ до публічної інформації»;
6) Закон України «Про авторське право і суміжні права»;
7) Закону України «Про інформацію»;
8) Закон України «Про санкції»;
9) Указ Президента України від 24 лютого 2022 р. № 64/2022 «Про введення воєнного стану в Україні»;

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) Указ Президента України від 24 лютого 2022 р. № 64/2022 «Про введення воєнного стану в Україні»;
15) Закон України «Про правовий режим воєнного стану";
16) Наказ Головнокомандувача ЗСУ від 3 березня 2022 р. № 73 «Про організацію взаємодії між Збройними Силами України, іншими складовими сил оборони та представниками засобів масової інформації на час дії правового режиму воєнного стану»;
14) Постанова Кабінету Міністрів України № 263 «Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану»;
18) Інші закони України та підзаконні нормативно-правові акти з питань захисту прав людини;
19) 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);
20) Рекомендація CM/Rec(2014)6 Комітету міністрів Ради Європи державам-членам щодо посібника з прав людини для Інтернет-користувачів – пояснювальний меморандум;
22) Рекомендація CM/Rec(2018)2 Комітету міністрів Ради Європи державам-членам щодо ролі та відповідальності інтернет-посередників;
23) Інші міжнародні документи, обов'язкові до застосування на території України.

ІІІ. ВІДБІР, АНАЛІЗ, СИСТЕМАТИЗАЦІЯ ТА КЛАСИФІКАЦІЯ ІНФОРМАЦІЇ

- **Порядок відбору інформації**

Під час моніторингу відбирається інформація, оприлюднена в мережі інтернет, в тому числі на офіційних веб-ресурсах, яка свідчить про загрозу правам людини в цифроврому середовищі в Україні, а саме:

1) Кібератак, хакерських атак;
2) Фішинг атак;
3) Поширення дезінформації;
4) Блокування веб-ресурсів;
5) Доступу до Інтернету;
6) Змін в законодавстві;
7) Свободи вираження поглядів;
8) Доступу до інформації;
9) Захисту персональних даних;
10) Іншої інформація, яка стосується цифрових прав.

Первинний збір інформації в мережі інтернет щодо загроз цифровим правам людини та її попередній аналіз щодо віднесення до тієї чи іншої категорії здійснюється спеціалістом з моніторингу, який пройшов відповідне навчання і стажування. Спеціаліст з моніторингу здійснює верифікацію інформації про подію, яка містить загрозу цифровим правам 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.

Вторинний аналіз всіх зібраних у таблиці моніторингу подій, які містять загрозу цифровим правам, здійснює юрист-аналітик, який перевіряє опис події, її верифікацію, відповідність і обґрунтованість попередньої оцінки аналітика з моніторингу.

- **Аналіз, систематизація та класифікація інформації**

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

- **Кібератаки, хакерські атаки.**

До цієї категорії відносяться повідомлення про дії кібер-зловмисників (хакерів) або шкідливих програм, метою яких є злам комп'ютерної системи чи мережі.

- **Фішинг атаки.**

До цієї категорії відносяться повідомлення про шахрайство в інтернеті з метою отримання незаконного доступу до конфіденційних даних користувачів.

- **Поширення дезінформації.**

До цієї категорії відносяться повідомлення про поширення свідомо неправдивої інформації з метою введення в оману громадськості.

- **Блокування веб-ресурсів.**

Ця категорія включає повідомлення про факти блокування чи іншого обмеження доступу до веб-ресурсів, які здійснюють як в судовому, так і позасудовому порядку.

- **Доступ до Інтернету.**

Ця категорія включає інформацію про порушення роботи електронних комунікаційних мереж України і здійснення відключення Інтернету на території України.

- **Зміни в законодавстві.**

До цієї категорії відносяться зміни в законодавстві, які стосуються цифрових прав.

- **Свобода вираження поглядів.**

До цієї категорії відноситься інформація про:
1) порушення кримінальних справ за статтями 109, 110, 111, 111-1, 111-2, 114, 114-1, 114-2, 436-2 , ст. 435-1 Кримінального кодексу України та судові вироки за даними статтями;
2) судові рішення, в тому числі про застосування заходів забезпечення позову, якими зобов’язано припинити чи обмежити доступ до інформації, оприлюдненої в мережі Інтернет;
3) 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;
4) судові рішення, в яких належним чином не розмежовано факти та оціночні судження, внаслідок чого вони суттєво обмежують свободу вираження в мережі інтернет;
5) 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;
6) 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;
7) 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;
8) інші порушення права на свободу вираження поглядів в цифровому середовищі.

- **Доступ до інформації.**

До цієї категорії відносяться повідомлення щодо:
1) порушень права на доступ до публічної інформації;
2) роботи та доступу до публічних реєстрів;
3) оприлюднення розпорядниками публічної інформації.

- **Захист персональних даних.**

До цієї категорії відносяться повідомлення щодо:
1) 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;
2) зламу сервісів, баз даних компаній /соціальних мереж/;
3) несанкціонованого (позасудового) доступу правоохоронних органів до конфіденційних персональних даних користувачів;
4) застосування та/або спроби застосування заходів загального спостереження чи перехоплення інформації (включаючи висунення законодавчих ініціатив, спрямованих на це);
5) інша інформація, яка стосується персональних даних.

- **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. Також буде збиратись інформація про порушення прав людини у цифровому середовищі, яка не охоплена іншими напрямками.

• Цикл Моніторингу

Моніторинг проводиться на постійній основі з щомісячним оприлюдненням аналітичного звіту “Війна у цифровому вимірі та права людини” (далі - Звіт). У Звіті відображається узагальнена інформація про події, які містять загрозу цифровим правам людини.

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

IV. 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. "Кібератака" - згідно Закону України "Про основні засади забезпечення кібербезпеки України"- спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту.

3. "Фішинг атака" – вид інтернет-шахрайства, метою якого є отримання доступу до конфіденційних даних користувачів. Це схема, за допомогою якої шахраї, користуючись довірливістю або неуважністю людей, змушують їх самостійно розкривати особисту інформацію про себе для наступного її використання у зловмисних цілях.

4. "Дезінформація" - інформація, яка є неправдивою та навмисно створена, щоб завдати шкоди людині, соціальній групі, організації чи країні (Звіт Ради Європи «Інформаційне безладдя: на шляху до міждисциплінарного підходу до досліджень та вироблення політик»). Кембриджський словник називає дезінформацію "неправдивою інформацією, яка поширюється з метою введення в оману людей".

5. «Кількісні характеристики порушення цифрових прав» - кількість випадків порушення цифрових прав, виявлених протягом відповідного циклу моніторингу.

6. «Якісні характеристики порушення цифрових прав» - аналіз порушень цифрових прав, визначення їх характеру (загального чи індивідуального) та виду відповідно до напрямків моніторингу.

7. 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.