



МОНІТОРИНГ

ПОРУШЕНЬ ЦИФРОВИХ ПРАВ В УКРАЇНІ

Аналітичний звіт

Період моніторингу – вересень 2019 року

I. Порухення цифрових прав загального характеру (порушення, які мають вплив на необмежене коло осіб).

1. Доступ до Інтернету.

- 1) У вересні 2019 року продовжувалось блокування 240 веб-сайтів на підставі двох Указів Президента України від 15 травня 2017 року¹ та від 14 травня 2018 року², що вже відмічалось у попередніх аналітичних звітах за результатами Моніторингу порушень цифрових прав в Україні³.

Порушення носить триваючий характер і жодних покращень ситуації у вересні 2019 року не відбулось.

- 2) Продовжується блокування **17 інформаційних веб-сайтів** на підставі ухвали Печерського районного суду м. Києва у справі № 757/38387/19-к про накладення арешту на “майнові права інтелектуальної власності, які виникають у користувачів мережі Інтернет” при використанні зазначених веб-ресурсів (зазначену ухвалу прийнято у межах кримінального провадження), на що вже зверталась увага у

¹ <https://www.president.gov.ua/documents/1332017-21850>

² <https://www.president.gov.ua/documents/1262018-24150>

³ <https://www.ppl.org.ua/monitoring/monitoring-cifrovix-prav>

попередніх звітах⁴. Цією ухвалою низку великих українських Інтернет-провайдерів зобов'язано закрити доступ до таких веб-сайтів: <http://go338.top>; <https://trident-ua.info>; <https://enigma.ua>; <https://blogs.korrespondent.net>; <https://seychas.press>; <https://netadvocate.org>; <https://compromate.ws>; <https://sled-net-ua>; <https://ua-24.com>; <https://moscow-post.press>; <https://novindoosh.com>; <https://stalker-world.net>; <http://rospress.press>; <https://informer.news>; <https://ustav.press>; <https://ukrpress.info>.

Апеляційний розгляд справи відбувався 06.08.2019, 20.08.2019, 09.09.2019. Наступне судове засідання призначено на 17.10.2019⁵. Весь цей час сайти не можуть нормально працювати, поширювати інформацію і втрачають свою аудиторію.

- 3) Блокування фейсбук-сторінки вінницького сайту VinMedia соціальною мережею «Фейсбук». На думку видання це сталося через велику кількість скарг від «ботів» та «палких прихильників» політичних партій та течій, які ворожі до України⁶.

Таким чином, у вересні зафіксовано 4 (чотири) факти порушення цифрових прав загального характеру, які стосуються 258 веб-ресурсів.

2. Інтернет і виборчий процес.

Практика оприлюднення користувачами соціальної мережі «Фейсбук» фотографій своїх заповнених виборчих бюлетенів в той час, коли триває голосування на виборчих дільницях, продовжує демонструвати сталість.

У вересні 2019 року в Єдиному державному реєстрі судових рішень оприлюднено **3 (три)** судових рішення у справах про порушення обмежень щодо ведення передвиборної агітації, одна з яких стосується оприлюднення фотографії бюлетеня під час президентської передвиборчої кампанії, а дві інші - під час парламентських виборчих перегонів, а саме:

- 1) 11.09.2019 року Корольовський районний суд м. Житомира заклав провадження у справі про адміністративні правопорушення стосовно голови Житомирської обласної державної адміністрації, який 31.03.2019 на своїй сторінці «Фейсбук» виклав фото зі своїм бюлетенем під час голосування, що після цього розповсюдили засоби масової інформації. Таке рішення суду мотивоване закінченням строків накладення адміністративного стягнення⁷.

Таким чином, несвоєчасний розгляд подібних справ дає можливість уникати відповідальності за порушення правил проведення передвиборної агітації в мережі Інтернет, що не сприяє попередженню зазначених правопорушень.

- 2) Інші **дві справи** стосуються поширення матеріалів передвиборної агітації - фотографій виборчого бюлетеню з інформацією про зроблений вибір, у мережі Фейсбук під час парламентських виборів 21.07.2019 року. В обох випадках суди встановили порушення вимог виборчого законодавства та наклали на правопорушників штраф у розмірі 510,00 та 640,00 гривень відповідно, стягнувши також з кожного з них на користь держави судовий збір у розмірі 384,20 гривень.

⁴ <https://www.ppl.org.ua/monitoring/monitoring-cifrovix-prav>

⁵ <http://www.apcourtkiiev.gov.ua/CourtPortal.WebSite/Home/Sprava/51035355562>

⁶ <https://vinmedia.com.ua/posts/facebook-zablokuvav-sait-vinmedia-cherez-ataku-botiv>

⁷ <http://www.reyestr.court.gov.ua/Review/84189842>

Відповідно у вересні 2019 року зафіксовано **3 (три) порушення цифрових прав, пов'язаних із виборчим процесом.**

II. Порушення цифрових прав індивідуального характеру (порушення, які стосуються окремих осіб і не мають безпосереднього впливу на широкую аудиторію).

1. Факти порушення прав на свободу вираження поглядів:

1) Визнання інформації недостовірною та покладення обов'язку її спростувати без залучення належних відповідачів.

а) Рішенням Шевченківського районного суду м. Києва від 31.08.2019 у справі № 755/7693/17-ц частково задоволено вимоги позивача до веб-сайту “Українська правда” в особі його власника, веб-сайту “Центр дослідження корупції та організованої злочинності”, в особі його власника, веб-сайту Інтернет-видання “Обозреватель”, в особі власника веб-сайту Товариства з обмеженою відповідальністю “Золота середина”. Спірну інформацію визнано такою, що не відповідає дійсності, принижує честь, гідність та ділову репутацію позивача та зобов'язано веб-сайти-відповідачі її спростувати⁸.

Зазначену справу розглянуто заочно, без участі відповідачів, оскільки, як вказано у цьому рішенні, вони не з'явились у судові засідання. І це зрозуміло, оскільки відповідачі - веб-сайти не є юридичними особами і не можуть направити своїх представників у суд, а їх власники до участі у справі не притягувались. Незалучення належних відповідачів унеможливило справедливий розгляд справи, оскільки під час такого судового процесу не можна встановити дійсні обставини справи, дослідити в повному обсязі необхідні докази. Крім того, у рішенні не проведено аналізу статусу позивача та меж його допустимої критики, не розглянуто, як належить, питання суспільного інтересу до спірних відомостей та не застосовано інші стандарти у галузі свободи слова.

б) Аналогічна ситуація мала місце і у справі № 203/1876/19.

19 вересня 2019 року Кіровський районний суд м. Дніпропетровська ухвалив рішення у справі позовом ОСОБА_2 до Інтернет-порталу «ЦЕНЗОР.НЕТ» в особі головного редактора ОСОБА_3 , ОСОБА_4 , про захист честі, гідності та ділової репутації, визнання недостовірної інформації, зобов'язання спростувати недостовірну інформацію, стягнення моральної шкоди⁹. Визнавши, що інтернет-портал «ЦЕНЗОР.НЕТ» не є юридичною особою, суд все ж ухвалив рішення, яким зобов'язав цього відповідача спростувати спірну інформацію та стягнув з нього судовий збір.

Подібна судова практика є загрозливою, оскільки розгляд справ, пов'язаних із поширенням інформації без притягнення належного відповідача до участі у судовому розгляді, може стати інструментом необґрунтованого обмеження права на свободу слова, зокрема, права поширювати критичну інформацію щодо публічних осіб.

2) Залишення в силі судом апеляційної інстанції рішення про зобов'язання видалення достовірної інформації про впливового політика із Відкритого реєстру

⁸ <http://www.reyestr.court.gov.ua/Review/83975867>

⁹ <http://www.reyestr.court.gov.ua/Review/84560958>

національних публічних діячів України під приводом незаконного використання імені позивача має ознаки цензури¹⁰.

Постановою Київського апеляційного суду від 02.09.2019 у справі № 757/30830/18-ц відхилено апеляційну скаргу громадської організації «Центр протидії корупції» та залишено без змін рішення Печерського районного суду міста Києва від 11 грудня 2018 року, яким зазначену громадську організацію зобов'язано видалити із Відкритого реєстру національних публічних діячів України інформацію про відомого впливового політика, в тому числі відомості про те, що йому пред'явлено підозру у кримінальному провадженні¹¹.

Вказані судові рішення мотивовані необхідністю захисту права на використання імені позивача. При цьому суд не визнав спірну інформацію недостовірною, не аналізував наявність чи відсутність суспільного інтересу до зазначених відомостей та не розглядав питання про застосування статті 29 Закону України «Про інформацію» до спірних правовідносин. Таке рішення, на нашу думку, не відповідає критерію «необхідності у демократичному суспільстві», оскільки не враховує суспільний інтерес до спірної інформації, публічний статус особи та є непропорційним меті, що захищається, а наведені судом мотиви не можна вважати відповідними та достатніми.

3) Поширення фейкових новин шляхом зламу веб-сайтів видань.

25 вересня 2019 року на фейсбук-сторінці газети «Ратуша» було розміщено оголошення про те, що на сайті газети «Ратуша» (ratusha.lviv.ua) опубліковано новину під назвою «На навчаннях у Яворові польський військовослужбовець застрелив українського солдата». В ній також повідомлялось, що редакція газети «Ратуша» цієї інформації на сайті не розміщувала і припускає, що на сайт відбулася хакерська атака, внаслідок чого з'явилася ця фейкова новина¹².

4) Атаки на сайти, а саме:

а) у вересні на сайті Громадського оприлюднено повідомлення, що починаючи з 17.09.2019 здійснюється атака на зазначений сайт, яка має на меті отримання доступу до бази даних сайту¹³.

б) атаки на облікові записи Facebook українських громадських активістів та журналістів. Про це повідомила Лабораторія цифрової безпеки¹⁴. Зокрема, зазначається, що протягом останнього тижня вересня 2019 було зафіксовано щонайменше чотири атаки на облікові записи Facebook українських громадських активістів та журналістів. Переважно цілями атаки є правозахисники та журналісти, що займаються темою окупованого Криму, а також журналісти-розслідувачі. Про один із таких фактів повідомила і Олександра Матвійчук¹⁵.

¹⁰ Частина 1 статті 24 Закону України «Про інформацію» зокрема, передбачає: «Забороняється цензура - будь-яка вимога, спрямована, зокрема, до журналіста, засобу масової інформації, його засновника (співзасновника), видавця, керівника, розповсюджувача, узгоджувати інформацію до її поширення або накладення заборони чи перешкоджання в будь-якій іншій формі тиражуванню або поширенню інформації».

¹¹ <http://www.revestr.court.gov.ua/Review/84403624>

¹² https://www.facebook.com/ratusha.lviv.ua/posts/2395807443970915?_tn=-R

¹³ <https://hromadske.ua/posts/na-sajt-hromadske-namagayutsya-zdijsniti-ataku>

¹⁴ <https://www.facebook.com/cyberlabUkraine/photos/a.1573858602657653/2532933283416842/?type=3&theater>

¹⁵ <https://www.facebook.com/photo.php?fbid=10156506946217304&set=a.10150913768247304&type=3&theater>

в) триваючі потужні атаки на сервери Вікіпедії, які можуть унеможливити роботу сайту¹⁶.

г) DDOS-атаки на сайт інтернет-видання “Гордон”¹⁷.

5) **Напади на журналістів**, а саме:

а) на головного редактора вінницького інформаційного порталу “Вежа” Андрія Качора, якому погрожували прихильники проросійського відеоблогера Анатолія Шарія, про що він повідомив на своїй сторінці у Фейсбук¹⁸.

б) на редактора газети «Правдошукач», члена НСЖУ Юрія Шеляженка. Зловмисники замастили вхідні двері червоною фарбою та залишили написи з погрозами, розбили фотоапарат. Цей інцидент збігся із DDoS-атаками на сайт газети «Правдошукач»¹⁹.

Таким чином, у вересні зафіксовано 10 (десять) випадків порушення права на свободу вираження поглядів у цифровому середовищі.

2. Приватне життя та захист даних:

1) Витік персональних даних журналістів, що ставить їх у небезпечне становище.

Зокрема, 23.09.2019 року журналістка Kyiv Post Анна Миронюк на своїй сторінці у Фейсбук²⁰ повідомила про те, що після подання заявки на акредитацію, що б працювати в зоні бойових дій або #ООС, вона та ще двоє її колег отримали SMS-повідомлення від бойовиків з окупованих районів Луганської області в якому зазначалось, що їй може загрожувати від 10 років до довічного терміну ув'язнення через нібито співучасть у вчиненні таких злочинів, як “застосування заборонених засобів та методів ведення війни” та “геноцид”. Журналісти підозрюють, що витік даних відбувся після того, як вони надіслали свої документи на електронну скриньку прес-центру ООС.

Таким чином, у вересні 2019 року мав місце 1 (один) факт порушення права на приватне життя та захист даних у цифровому середовищі.

3. Потенційні загрози для свободи слова та права на приватність в Інтернеті в Україні:

1) Включення до законопроекту №1129 «Про оперативно-розшукову діяльність», ініційованого народним депутатом України Андрієм Кожем'якіним, правової норми, яка дозволяє у невідкладних випадках проводити оперативно-розшукові заходи, в тому числі знімати інформацію з транспортних телекомунікаційних мереж та з електронних інформаційних систем, контролювати кореспонденцію тощо без рішення суду лише на підставі дозволу керівника оперативного підрозділу або особи, що виконує його обов'язки, із наступним негайним повідомленням про них прокуророві.

¹⁶ <https://ms.detector.media/web/cybersecurity/u/vikipedii/zayavili-pro-masshtabnu-ataku-na-sayt-entsiklopedii/>

¹⁷ <https://www.facebook.com/alesia.batsman/posts/10217997613763513>

¹⁸ <https://zmina.info/news/cze-vy-pro-shariya-pysaly-vinnyczkogo-zhurnalista-vakomu-pogrozhuvaly-prvyhlynyky-odioznogo-blogera-pobyly-nevidomi/> та <https://www.facebook.com/andriy.kachor/posts/2672134949476765>

¹⁹ <http://nsju.org/index.php/article/view/8231>

²⁰ <https://www.facebook.com/photo.php?fbid=2514082801990506&set=a.794967737235363&type=3&theater>

Якщо за неї проголосують парламентарі, це може призвести до здійснення контролю інтернет-трафіку користувачів та їх прослуховування без рішення суду²¹.

- 2) Надсилання інформації про власників смарт-телевізорів та медіаплеєрів цими пристроями стороннім компаніям та сервісам, навіть тим, у яких користувачі не зареєстровані. Дослідники дізналися, що сторонні компанії отримують мінімальну інформацію про пристрій, який використовує людина, її місце розташування та години роботи пристрою. Так можна з'ясувати, коли людина зазвичай буває дома, кажуть експерти. Більшу частину даних «розумні» пристрої відправляють у зашифрованому вигляді²². Чи поширювались у такий спосіб персональні дані українців наразі невідомо.
- 3) Низка додатків (зокрема, Maya від Plackal Tech (5 мільйонів завантажень на Google Play), MIA від Mobapp Development Limited (1 мільйон завантажень) та My Period Tracker від Linchpin Health (понад 1 мільйон завантажень), серед яких календарі розрахунку місячних циклів для жінок, збирали дані та передавали їх компанії «Фейсбук» для кращого налаштування контекстної реклами²³.
- 4) Деякі додатки Google Play можуть таємно отримувати доступ до особистих даних користувачів²⁴.
- 5) Наявність вразливостей в сервісах Gmail і «Гугл Календарі»²⁵.
- 6) Пості в інстаграмі, які користувачі закрили для широкого загалу налаштуваннями приватності, можуть поширюватись будь-кому підписниками чи друзями юзера²⁶.
- 7) Фейки, створені за допомогою штучного інтелекту, можуть становити ще більшу небезпеку, ніж вважали раніше. Незабаром можуть виникнути серйозні фінансові та юридичні наслідки від розповсюдження фото, відео або аудіо, створених за допомогою штучного інтелекту. Зокрема, повідомляється, що керівника енергетичної компанії у Великій Британії обманули і примусили перевести на рахунки нібито угорського постачальника 200 000 євро. Йому зателефонували і, зімітувавши голос реального партнера-постачальника, попросили це зробити²⁷.
- 8) Протиправне отримання персональних даних користувача через фейкові повідомлення про блокування сторінки в Instagram²⁸.

Таким чином, у вересні 2019 зафіксовано 8 (вісім) фактів наявності потенційних загроз для свободи слова та права на приватність в Інтернеті в Україні.

Підсумовуючи викладене необхідно зазначити, що моніторинг порушень цифрових прав в Україні у вересні 2019 року дозволив виявити **18 порушень цифрових прав, а саме:**

²¹ <https://internetua.com/nardery-hotyat-razreshit-proslushku-i-kontrol-internet-trafika-bez-resheniya-suda>

²² https://ms.detector.media/web/cybersecurity/smarttelevizori_peredayut_dani_pro_vlasnikov_kompaniyam_facebook_ta_netflix_d_oslidzhennya/

²³ https://ms.detector.media/web/cybersecurity/nizka_dodatkov_peredavala_feysbuku_informatsiyu_pro_seksualne_zhittya_koristuvachiv/

²⁴ https://ms.detector.media/web/IT_companies/dodatki_google_mozhut_taemno_otrimuvati_dostup_do_osobistikh_danikh_forbes/

²⁵ https://ms.detector.media/web/cybersecurity/gugl_viznala_vrazlivist_gmail_i_gugl_kalendarja_do_shakhrayskikh_div/

²⁶ https://ms.detector.media/web/cybersecurity/privatni_posti_v_instagrami_ne_e_povnistyu_privatnimi_buzzfeed/

²⁷ https://ms.detector.media/web/cybersecurity/shakhray_vimanyuyut_koshiti_u_biznesu_za_dopomogoyu_glibinnikh_feykiv_wsji/

²⁸ <https://internetua.com/eksperty-nashli-novyi-sposob-vzlatat-akkaunt-v-instagram>

7 порушень цифрових прав загального характеру, з яких **4 факти** стосуються 258 веб-ресурсів та **3** порушення цифрових прав, пов'язане із виборчим процесом; **11 фактів порушень цифрових прав індивідуального характеру**, з яких **10** випадків стосуються порушення права на свободу вираження поглядів, а **1** - порушення права на приватне життя та захист даних у цифровому середовищі.

Виявлено також **8 загроз** для свободи слова та права на приватність в Інтернеті в Україні.