

Моніторинг порушень цифрових прав в Україні

Аналітичний звіт

Період моніторингу – червень 2019 року

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

1. Доступ до Інтернету.

В травні 2019 року продовжується 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 аналітичному звіті Моніторингу порушень цифрових прав в Україні за травень 2019 року³. Порушення носить триваючий характер і жодних покращень ситуації у червні 2019 року не відбулось.

2. Інтернет і виборчий процес.

В Єдиному державному реєстрі судових рішень в червні 2019 оприлюднено два рішення у справах, що стосуються порушення обмежень щодо ведення передвиборної агітації. Обидві справи пов'язані із поширенням користувачами соціальної мережі «Фейсбук» фотографій бюлетеня із результатами голосування⁴. По одному із таких фактів відкрито кримінальне провадження, у зв'язку з чим матеріали справи про адміністративне правопорушення повернуті органам поліції, а в іншій - особу визнано винною у порушенні приписів частини 1 статті 212-10 КУпАП, накладено штрафу в розмірі п'ятдесяти неоподатковуваних мінімумів доходів громадян, що становить 850 (вісімсот п'ятдесят) гривень 00 копійок.

Отже, судова практика із зазначеного питання є неоднозначною. Водночас, поширення результатів особистого голосування з ознаками порушення таємниці голосування через соціальні мережі набуває популярності, що несе загрози для права на вільні вибори.

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 <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>

⁴ <http://www.reyestr.court.gov.ua/Review/82282586> та <http://www.reyestr.court.gov.ua/Review/82473796>

- 1) побитий 4 травня у Черкасах журналіст та блогер Вадим Комаров помер, не виходячи з коми⁵, що має “охолоджувальний ефект” на журналістів, які пишуть на суспільно-вагомій темі, зокрема, викривають корупцію. Черкаські журналісти почали скаржитись на те, що вони бояться надалі критикувати владу з огляду на можливість застосування до них фізичного впливу за подібні публікації;
- 2) поширення російськими пропагандистами на своїх ресурсах, а також в соцмережі Facebook фейкових скріншотів новин у стилістиці ресурсу Obozrevatel⁶;
- 3) вилучення в ході проведення обшуку у відомого українського експерта по кібербезпеці О. Галуценка окрім флеш-накопичувачів, дисків та інших носіїв інформації, “вихідників” програмного забезпечення, розробленого “ІТ-Лабораторія” протягом останніх 9 років, та майстер-ключа до нього, що, за словами О. Галуценка, не передбачено ухвалою на проведення обшуку та дає можливість для зловживань із програмним забезпеченням⁷;
- 4) DDoS-атака сайт Національного банку України⁸. Це призвело до порушень у роботі сайту;
- 5) до Богуславського районного суду Київської області пред’явлено позов про захист честі, гідності, ділової репутації, пов’язаний із поширенням інформації у соціальній мережі Facebook, і заявлено вимоги про відшкодування моральної шкоди на суму 628 000 (шістсот двадцять вісім тисяч) гривень⁹;
- 6) необгрунтоване (без наведення мотивів та норм права, як правових підстав) та непропорційне застосування судом окрім спростування спірної інформації стосовно органу державної влади, такого способу правового захисту, як видалення інформації із сайту¹⁰.

Так, рішенням Господарського суду Донецької області задоволено вимоги Департаменту капітального будівництва Донецької обласної державної адміністрації до Громадської організації "Східно - Українське патріотичне об'єднання" і **визнано недостовірною всю спірну публікацію**, а не лише низку висловлювань, які були предметом судового спору (що не тільки не ґрунтується на законі, але й є явно непропорційним). Крім того, суд окрім оприлюднення спростування, зобов'язав відповідача видалити спірну публікацію, не навівши жодного мотиву на виправдання застосування такого способу правового захисту, не обґрунтувавши необхідність його застосування та не пояснивши чому такий спосіб правового захисту, як спростування не може поновити права позивача;

- 7) судом застосовано спосіб правового захисту, який порушує авторське право в Інтернеті. Так, рішенням Господарського суду Київської області у справі № 911/238/19¹¹ відповідача зобов'язано вилучити із спірної публікації низку висловлювань, які містять недостовірну інформацію, що порушує цілісність твору. Крім того, суд поклав на відповідача обов'язок розмістити між заголовком статті та її першим абзацом текст спростування, що також порушує цілісність твору. Необхідність застосування саме такого способу захисту прав

⁵ <http://nsju.org/index.php/article/view/8028>

⁶ https://ms.detector.media/ethics/manipulation/obozrevatel_zayaviv_scho_rosiyski_propagandisti_pos_hiryuyut_feyki_vid_yogo_imeni/

⁷ <https://internetua.com/u-vedushego-ukrainskogo-specialista-po-kiberbezopasnosti-iz-yali-tehniku-i-programmnoe-obespechenie?fbclid=IwAR3GwqwI8CXplVUjeRKlaOz5mul59DToSUZhM5iht0u-Jz06SaENzXkZ7U8>

⁸ <https://internetua.com/hakeri-zdiisnili-potujnu-ddos-ataku-na-sait-nbu>

⁹ <http://www.reyestr.court.gov.ua/Review/82262641#>

¹⁰ <http://www.reyestr.court.gov.ua/Review/82335661>

¹¹ <http://www.reyestr.court.gov.ua/Review/82600370#>

позивача і неможливість поновлення його прав без надмірного втручання у права відповідача судом не мотивована.

2. Приватне життя та захист даних:

- 1) збір та поширення конфіденційної інформації про абонентів оператором мобільного зв'язку, зокрема, про регулярність його візитів до лікаря, його спосіб життя, звички, рівень доходів тощо¹².
- 2) надання надмірного і непропорційного доступу до інформації про споживача послуг з доступу до Інтернету на підставі ухвали Галицького районного суду м. Львова від 26.04.2019¹³, якою надано тимчасовий доступ до речей і документів, а саме **всієї наявної інформації** по вказаній IP адресі на паперових та цифрових носіях.

3. Потенційні загрози для свободи слова в Інтернеті в Україні:

- 1) загроза блокування трансляції на відеохостингу YouTube матеріалів супутникового телеканалу «ATR Т» (ТОВ «ТК «Атлант-СВ») через вимогу Федеральної служби з нагляду у сфері масових комунікацій і зв'язку (Роскомнагляду) Російської Федерації, яка стверджує, що розміщені матеріали порушують російське законодавство про інформацію, інформаційні технології та про захист інформації¹⁴;
- 2) хакерам вдалося зламати 10 мобільних операторів по всьому світу і отримати доступ до записів «років» телефонних розмов їхніх клієнтів¹⁵;
- 3) продовжується практика направлення слідчими до суду клопотань про накладення арешту на майнові права інтелектуальної власності, які “виникають у користувачів мережі Інтернет при використанні” того чи іншого веб-ресурсу, як підстави для закриття доступу до такого веб-сайту інтернет-провайдером¹⁶. І хоча у справі № №766/11086/18 суд це клопотання не задовольнив, надавши строк на усунення недоліків, вважаємо за необхідне звернути увагу на зазначену проблему як таку, що має потенційну загрозу для свободи слова в Інтернеті, оскільки надумані підстави використовуються для блокування доступу до Інтернету.

Загалом в результаті моніторингу у червні 2019 року виявлено **13 порушень цифрових прав**, а саме: **4** порушення цифрових прав **загального характеру**, з яких 2 стосуються доступу до Інтернету, 2 - порушення законодавчих обмежень щодо ведення передвиборної агітації, а також **9** порушень цифрових прав **індивідуального характеру**, з яких 7 порушень права на свободу вираження поглядів та 2 - права на приватне життя та захист даних. Крім того, виявлено 3 загрози для для свободи слова в Інтернеті в Україні.

¹²https://ms.detector.media/web/cybersecurity/ukrainskiy_mobilniy_operator_rozpoviv_yaki_dani_zbir_ae_pro_svoikh_klientiv/

¹³ <http://www.reyestr.court.gov.ua/Review/82174339>

¹⁴<https://www.nrada.gov.ua/ukrayinskyj-regulyator-zvernuvsya-google-shhodo-vykorystannya-jogo-dochirnoyi-kompaniyi-youtube-u-gibrydniy-vijni-rosiyi-proti-ukrayiny/>

¹⁵Про те, що до цього переліку потрапили мобільні оператори України не повідомляється, однак цього не можна виключити. Тому зазначений факт включено до переліку потенційних загроз: https://ms.detector.media/web/cybersecurity/khakeri_zlamali_10_mobilnikh_operatoriv_ta_otrimali_dostup_do_telefonnikh_rozmov/.

¹⁶ <http://www.reyestr.court.gov.ua/Review/82695854#>