



МОНІТОРИНГ ПОРУШЕНЬ ЦИФРОВИХ ПРАВ В УКРАЇНІ

Аналітичний звіт

Період моніторингу – квітень 2020 року

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

1. Доступ до інтернету та до інформації, оприлюдненої онлайн.

- 1) У квітні 2020 року продовжувалось блокування 240 веб-сайтів на підставі двох Указів Президента України від 15 травня 2017 року¹ та від 14 травня 2018 року², на що вже неодноразово зверталась увага у аналітичних звітах за результатами Моніторингу порушень цифрових прав в Україні в 2019 році³.

Коаліцією «За вільний Інтернет» було підготовлено і опубліковано юридичний аналіз Указу Президента України 2018-го року, висновки якого, в переважній більшості, є релевантними і до першого Указу⁴.

Серед основних:

- санкція, як спосіб обмеження прав і свобод людини не відповідає конституційним стандартам і вимогам і є проявом необмеженої дискреції державної влади;
- секторальний характер санкції для введення в дію потребує позитивного голосування у Верховній Раді України;
- механізм в частині блокування сайтів не відповідає національному законодавству та порушує основні конституційні права громадян;
- практика блокування сотень веб-сайтів в спосіб, який застосовано владою, не відповідає критерію «передбачено законом» в розумінні міжнародно-правових договорів та практики Європейського суду з прав людини;
- таке блокування не відповідає критерію «необхідності в демократичному суспільстві», є непропорційним визначеній законній меті.

Порушення носить триваючий характер і жодних покращень ситуації станом на квітень 2020 року не відбулось. Навпаки, від представників влади лунають заяви про необхідність продовження блокування зазначених веб-ресурсів⁵.

- 2) Заборона з боку директора середньої загальноосвітньої школи східних мов та бойових мистецтв Будокан використовувати контент дистанційної освіти, який поширюється на каналах 112, Zik та NewsOne (які транслюються в тому числі і в мережі Інтернет)

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 <https://www.ppl.org.ua/yuridichnij-analiz-ukazu-prezidenta-pro-blokuvannya-sajtiv.html>

⁵ <https://www.rnbo.gov.ua/ua/Diialnist/4597.html>

при підготовці вчителями власних стрім-уроків, тематичних презентацій та проведення on-line занять (він також не рекомендував батькам та школярам використовувати контент цих каналів для дистанційного навчання)⁶. Враховуючи, що Міністерство освіти і науки України включило зазначені канали до переліку джерел, які мають використовуватись у Всеукраїнській школі онлайн⁷, зокрема, при навчанні дітей 5-7 класів, мало місце порушення цифрових прав, зокрема права на доступ до інформації (обмеження доступу до джерел інформації) та права на освіту.

Таким чином, у звітний період **зафіксовано 3 порушення цифрових прав** у вигляді обмеження доступу до Інтернету та до інформації, оприлюдненої онлайн, які стосуються 243 веб-ресурсів.

2. Обробка персональних даних з іншою метою, ніж та, на яку особи дали згоду.

1) Мапа дотримання режиму самоізоляції від Київстар.

Компанія “Київстар” створила мапу, яка показує індекс дотримання самоізоляції, розрахований компанією за відсотком населення, який обмежив свої пересування в період самоізоляції⁸. Це свідчить про те, що персональна інформація обробляється не з тією метою, на яку абоненти надали згоду.

2) Оприлюднення Житомирською ОДА мапи з окресленням приблизної території проживання хворих на COVID-19⁹.

Створення зазначеної мапи є неможливим без обробки відповідних персональних даних хворих на коронавірусну хворобу (як про стан їх здоров'я, так і про місце їх проживання). Втім, обробка такої інформації без згоди особи з метою її публічного поширення не дозволена, вона не переслідує також і законну мету.

Поширення такої інформації окрім того, створює передумови для соціального напруження, підозр, цькування мешканців певної території проживання та поширення мови ворожнечі і може призвести до порушення прав людини індивідуального характеру.

3) Оприлюднення міською радою м. Дніпро мапи з окресленням приблизної території проживання хворих на COVID-19¹⁰.

Це порушення аналогічне вищеописаному.

Таким чином, у звітний період **зафіксовано 3 (три) факти** обробки персональних даних осіб з іншою метою, ніж та, на яку надавалась згода.

3. Інтернет і поширення чуток.

⁶<https://www.facebook.com/BudokanLviv/photos/a.152703171801001/772921236445855/?type=1&theater>

⁷<https://mon.gov.ua/ua/news/o-1000-startuye-vseukrayinska-shkola-onlajn-rozklad-i-temi-urokiv-na-tizhden-posilannya-na-youtube-mon-de-translyuvatimutsya-uroki-dlya-vsikh-klasiv>

⁸<https://kyivstar.ua/uk/covid2019-stat>

⁹<https://ms.detector.media/zakonodavstvo/post/24517/2020-04-16-chumni-kvartali-zhitomirska-oda-oprilyudnila-kartu-z-poznachkami-vulits-de-meshkayut-khvori-na-covid-19/>

¹⁰<https://ms.detector.media/zakonodavstvo/post/24566/2020-04-25-meriya-dnipra-opublikovala-na-saiti-kartu-z-poznachkami-de-viyavleno-zakhvorilikh-na-koronavirus/>

У березні 2020 року на території України введено карантин через оголошення пандемії коронавірусної інфекції¹¹. На цьому тлі з'явилося чимало різного роду повідомлень, в тому числі й неправдивих, які поширювались у соціальних мережах, зокрема у "Фейсбук". Для боротьби з фейками правоохоронні органи стали активно складати протоколи про адміністративне правопорушення, передбачене статтею 173-1 КУпАП (поширювання неправдивих чуток), що призвело до появи нової і, часом, неоднозначної практики покарання за поширення чуток в мережі Інтернет.

Зокрема за повідомленням Служби безпеки України, станом на 28 квітня 2020 року було викрито 241 особу, яка розповсюджувала неправдиву інформацію про коронавірус¹². Водночас, в квітні 2020 в Єдиному державному реєстрі судових рішень виявлено 32 постанови у справах по статті 173-1 КУпАП. З них суд:

- визнав наявність складу адміністративного правопорушення та застосував штраф у розмірі 170 грн., стягнувши судовий збір у розмірі 420 грн. 40 коп., - у **9 справах**;
- постановив рішення про наявність складу адміністративного правопорушення та про звільнення особи від відповідальності у зв'язку з малозначністю діяння, обмежившись усним зауваженням - у **5 справах**;
- прийняв рішення про відсутність події та/або складу адміністративного правопорушення, зокрема його об'єктивної сторони, і закрити провадження в **12 справах**;
- визнав необхідним повернути матеріали справи Нацполіції для приведення протоколу про адміністративне правопорушення у відповідність до вимог КУпАП - у **6 справах**.

Порушення цифрових прав зафіксовано у перших двох випадках у зв'язку з:

- 1) неповним встановлення обставин справи: нерідко суди не встановлюють повний текст повідомлення, яке стало підставою для складання адміністративного протоколу. Відтак із судового рішення неможливо зрозуміти яку інформацію аналізував суд (і чи аналізував взагалі), чи відповідає вона дійсності і чи може вона призвести до паніки або порушення громадського порядку.
- 2) відсутність належної доказової бази: нерідко не надаються докази наявності умислу на сійання паніки чи порушення громадського порядку.
- 3) відсутність оцінки спірного повідомлення судом на предмет його достовірності чи недостовірності.
- 4) відсутність обґрунтування наявності умислу посіяти паніку серед населення або порушити громадський порядок¹³.

Загалом у квітні зафіксовано **12 (дванадцять)** фактів порушення цифрових прав загального характеру, пов'язаних із поширенням чуток в мережі Інтернет.

Таким чином, загалом мало місце 18 (вісімнадцять) фактів порушення цифрових прав загального характеру, з яких: 3 (три) порушення цифрових прав у вигляді обмеження доступу до Інтернету та до інформації, оприлюдненої онлайн, які стосуються 243 веб-ресурсів; 3 (три) факти обробки персональних даних осіб з іншою метою, ніж та, на яку надавалась згода та 12 (дванадцять) фактів пов'язаних із поширенням чуток в мережі Інтернет.

¹¹<https://www.kmu.gov.ua/npas/pro-zapobigannya-poshim110320rennyu-na-teritoriyi-ukrayini-koronavirusu-covid-19>

¹²<https://ssu.gov.ua/ua/news/1/category/21/view/7517#.Vz25EtDr.dpbs>

¹³ Узагальнення судової практики та детальний звіт з цього питання будуть оприлюднені орієнтовно в липні 2020 року

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

1. Факти порушення права на свободу вираження поглядів:

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

Печерський районний суд м. Києва своїм заочним рішенням від 27 лютого 2020 року задовольнив позов про захист ділової репутації та спростування недостовірної інформації, заявлений ТОВ «Новини 24 години» до керівника Головного департаменту інформаційної політики Адміністрації Президента України. Суд, визнавши, що спірна інформація поширена Адміністрацією Президента України, не притягнув її до участі у справі, як відповідача, що дає підстави сумніватись у повноті встановлених обставин цієї справи.

До того ж, судом було застосовано одразу два способи правового захисту: спростування та видалення спірної інформації із сайту, без обґрунтування потреби у їх одночасному застосуванні¹⁴.

2) Пред'явлення надмірних позовних вимог (на 5 млн. грн.) та накладення арешту на все майно відповідача в порядку забезпечення позову, що справляє «охолоджувальний ефект» на свободу слова.

Так, 6 квітня 2020 року Харківський районний суд Харківської області виніс ухвалу про забезпечення позову у справі про спростування недостовірної інформації, поширеної на Facebook-сторінці одного з користувачів, та стягнення моральної шкоди на суму 5 млн. грн., якою наклав арешт та заборонив вчиняти будь-які реєстраційні дії щодо нерухомого майна, транспортних засобів відповідача, а також наклав арешт, заборонивши відчуження його частки у статутних капіталах господарських товариств¹⁵. Пред'явлення позову на значну суму - 5 (п'ять) мільйонів гривень, а також задоволення клопотання про забезпечення позову шляхом накладення арешту на все цінне майно відповідача, - справляють «охолоджувальний ефект» на свободу слова.

3) Ухвалення рішень про спростування оціночних суджень та покладання зобов'язання вибачитись.

Рішеннями Трускавецького міського суду Львівської області від 05.03.2020 у справах №№ 457/991/18 та 457/1004/18 головного редактора газети «Джерела Трускавця» та Товариство з обмеженою відповідальністю «Редакція газети «Джерела Трускавця» суд зобов'язав оприлюднити на сайті видання текст спростування із вибаченнями перед позивачами (вибачення, як спосіб правового захисту, не передбачено законодавством України та не є спростуванням), а також спростувати не лише факти, але й оціночні судження¹⁶.

4) Напади на журналістів та блогерів, неефективне розслідування цих справ саме:

а) Майже за 2 (два) роки досудове слідство не вчинило всіх необхідних дій для притягнення до відповідальності винуватих у вчиненні нападу на журналіста

¹⁴ <http://reyestr.court.gov.ua/Review/88778487>

¹⁵ <http://reyestr.court.gov.ua/Review/88714542>

¹⁶ <http://reyestr.court.gov.ua/Review/88941545> та <http://reyestr.court.gov.ua/Review/88941130>

(блогера), що може свідчити про відсутність ефективного розслідування у справі, у зв'язку з чим готується заява до ЄСПЛ¹⁷

Так, 24 травня 2018 року стався напад на редактора інтернет-видання “Закон один для всіх” Всеволода Новохатька. Справа досі не розслідувана, кілька разів приймалися постанови про її закриття, які скасовувались судами.

б) 17 квітня 2020 року в Одесі охоронець Іллінського чоловічого монастиря Української православної церкви Московського Патріархату напав на фотокореспондентку інтернет-видання “Українська служба інформації” Владиславу Швець, яка разом із колегою готувала репортаж про підготовку до Великодня. Слідчий Нацполіції прийняв заяву про перешкоджання професійній журналістській діяльності¹⁸.

в) 29 квітня 2020 року в Києві під час прямого ефіру під Кабінетом Міністрів України працівники поліції побили і зламали техніку журналіста hromadske Богдана Кутепова, який разом зі співведучим Нікітою Мекензіним висвітлював акцію протесту підприємців, що виступали проти запроваджених під час карантину обмежень¹⁹.

Таким чином, у квітні 2020 зафіксовано **6 (шість) випадків** порушення права на свободу вираження поглядів у цифровому середовищі.

2. Приватне життя та захист даних:

1) Продаж персональних даних.

а) СБУ повідомила про те, що мешканець Івано-Франківська продавав інформацію з баз даних²⁰ Державної митної та прикордонної служб України, зокрема, дані про перетин кордону українськими громадянами та іноземцями, транспортними засобами, терміни їх перебування за кордоном. Відкрито кримінальну справу за ознаками злочину, передбаченого ч. 2 ст. 361-2 Кримінального кодексу України, щодо несанкціонованого збуту або розповсюдження інформації з обмеженим доступом, матеріали передано до суду²¹.

б) В Telegram з'явилися боти, які продавали персональні дані клієнтів, ймовірно, Приватбанку. Банк звернувся до Нацполіції у зв'язку із діяльністю ботів²².

2) Викрадення та “злив” персональних даних.

а) Прес-служба мережі готелів Marriott International повідомила про можливе викрадення даних більше п'яти мільйонів її клієнтів, що включали в себе їх імена,

¹⁷<https://helsinki.org.ua/articles/yak-politsiia-ta-prokuratura-dnipra-ta-oblasti-vzhe-dva-roky-sabotuiut-rozsliduvannia-napadu-na-aktyvistu/?fbclid=IwAR3xYO3osdCwnyofprUhfqRLtSMRnHZ6XkbqMnUHR70L2qguJk4KnGzm0mU>

¹⁸https://usionline.com/2020/04/17/v-odesse-ohrannik-tserkvi-napal-na-zhurnalistku-usi-foto-video/?fbclid=IwAR3jwHnqwKdNkToGfwdc50bjaSclmUPv3jL8_Y8PzRnRvz2vbBr2eIoLYJ0

¹⁹<https://hromadske.ua/posts/priberi-abo-zlamayemo-policiya-napala-na-zhurnalista-hromadske>

²⁰ Оскільки із повідомлення СБУ не можна зрозуміти достатньо чітко, чи мова йшла про продаж усієї бази даних, чи лише відомостей, які стосувались конкретних фізичних чи юридичних осіб, це порушення кваліфіковане, як порушення цифрових прав індивідуального характеру

²¹<https://ssu.gov.ua/ua/news/1/category/21/view/7427#.VoItFNTE.dpbs>

²²<https://ain.ua/2020/04/27/v-telegram-zarabotali-boty-kotorye-po-nomeru-vydayut-inn/>

адреси, номери телефонів, електронні адреси, дні народження, а також інформацію про їхні переваги та участі в програмах лояльності та партнерських програмах²³.

б) Оприлюднення листування заступника голови Агентства з розшуку та менеджменту активів (АРМА) Володимира Павленка без його відома²⁴.

3) Розкриття персональних даних через необачність.

Державний центр зайнятості України розіслав заявникам пароль для входу в онлайн-кабінет в листі з відкритими адресами²⁵. Тепер будь-хто може зайти в онлайн-кабінет тих осіб, які одразу не змінили пароль.

Таким чином, у квітні 2020 року мали місце **5 (п'ять)** фактів порушення права на приватне життя та захист даних у цифровому середовищі.

Загалом у квітні 2020 виявлено 11 (одинадцять) фактів порушення цифрових прав індивідуального характеру, з яких: 6 (шість) випадків порушення права на свободу вираження поглядів та 5 (п'ять) фактів порушення права на приватне життя та захист даних у цифровому середовищі.

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

- 1) **Блокування сайту.** 20 квітня 2020 року Міністерство з питань реінтеграції тимчасово окупованих територій України повідомило про те, що Роскомнагляд на вимогу Генпрокуратури РФ заблокував його сайт.

При цьому, поки що залишається невідомо, чи заблоковано сайт Мінреінтеграції лише на території Росії або й на тимчасово окупованих територіях України. Тому наразі цей випадок включено до переліку потенційних загроз²⁶. Причина блокування - «новина про приховування хворих COVID-19 в Криму і на Донбасі»²⁷.

- 2) **Користування додатком для моніторингу дотримання режиму обсервації та самоізоляції “Дій вдома”** створює загрозу порушення цифрових прав, оскільки принципи обробки персональних даних, визначені статтею 6 Закону України “Про захист персональних даних” повністю не дотримані навіть після ухвалення закону щодо дозволу обробляти інформацію без згоди особи та постанови КМУ від 22 квітня. Зокрема, відсутня прозорість щодо порядку передачі даних, не визначено чітко обсяг даних, а саме, що відноситься до "коротких відомостей про стан здоров'я", які передаються МВС тощо. Останнє не дозволяє також до кінця оцінити чи дотримано

²³<https://ua.korrespondent.net/business/companies/4211793-velyka-merezha-hoteliv-zaiavyla-pro-vyitik-danykh-kliientiv>

²⁴<http://nashigroshi.org/2020/04/24/pavlenkoheyty-zlyv-perepysok-zamholovy-arma-i-yoho-komentari-shchodo-tsoho/?fbclid=IwAR2OTT0NpcM3saCEDlidFHUQH8FGn5-eXp4wdK3uZ3gbUpge7HXRccR-fCY>

²⁵<https://internetua.com/centr-zanyatosti-raskryl-licsnye-dannye-zayavitelei>.

<https://ms.detector.media/kiberbezpeka/post/24595/2020-04-30-cherez-neobachnist-derzhavnii-tsentr-zainyatosti-rozkriv-osobisti-dani-zayavnikiv/>

²⁶ Варто зазначити, що за це порушення Уряд України відповідальності не несе, а тому він не включається до відповідних статистичних даних. Втім, це перший випадок блокування веб-сайту органу влади України іншою державою, а тому він потребує пильної уваги.

²⁷ <https://mtot.gov.ua/ua/genprokuratura-rf-zablokuvala-sat-minreintegracii-ukraini>

вимоги про те, що склад та зміст персональних даних мають бути відповідними, адекватними та ненадмірними стосовно визначеної мети їх обробки²⁸.

Крім того, користувачі Додатку неодноразово висловлювали претензії стосовно наявності технічних проблем, пов'язаних із його функціонуванням: помилкове фіксування порушень режиму самоізоляції за відсутності таких фактів, відсутність звукового супроводження повідомлень, що не дозволяє вчасно відреагувати на них та створює штучні “порушення” режиму самоізоляції, а також неналежна технічна підтримка роботи Додатку, проблеми із зворотнім зв'язком тощо²⁹.

- 3) **Атаки на сайти та інші веб-ресурси.** Відбулась масована DDoS-атака на електронні сервіси Київської міської державної адміністрації. Це спричинило значні навантаження на систему та зовнішні канали зв'язку, що, в свою чергу, створило потенційну загрозу виникнення тимчасових обмежень доступу до е-сервісів або міських сайтів³⁰.
- 4) **Поширення фейкових новин.** У квітні 2020 виявлено **27 повідомлень про численні факти** поширення фейкових новин. В основному, вони стосувались теми коронавірусу (див., зокрема, повідомлення кіберполіції³¹, а також інформацію про розпилення дезінфікуючих засобів з вертольотів³², про створення фейкових сторінок та поширення неправдивих відомостей про ЄС та Україну під час пандемії³³ тощо)³⁴.
- 5) **Обробка даних користувачів без їх згоди.** За повідомленнями ЗМІ, компанія Фейсбук використовує мікрофон для підслуховування з метою подальшого продажу користувачам більш цілеспрямованої реклами³⁵. В той же час компанія Twitter заявила, що збиратиме більше інформації про своїх користувачів, щоб поділитися нею з рекламодавцями, і видалила зі свого мобільного додатку опцію, що дозволяла користувачам контролювати які особисті дані могли б бути відправлені діловим партнерам компанії³⁶. Такі випадки свідчать про збір і обробку персональних даних користувачів соцмережі без їх згоди, а відтак, про існування можливостей для порушення їх права на приватне життя та захист персональних даних. Оскільки цими соціальними мережами користуються і в Україні, існує загроза порушення їх права на приватність.
- 6) **Вразливості програмного забезпечення, які можуть призвести до порушення права на приватність:**

²⁸ <https://dslua.org/publications/chy-zahrozhuie-vykorystannia-diy-vdoma-tsyfrovym-pravam/>, а також: <https://dslua.org/publications/ne-chas-dlia-zghody-shcho-ne-tak-iz-novym-antivirusnym-zakonom/> і

<https://dslua.org/publications/kabmin-detalizuvav-umovy-zastosuvannia-diy-vdoma/?fbclid=IwAR1cELx9pTJx7P0evhjCjZwtym1KGIewqDkUBeKdc5hxf3sK-x5AgyepbDE>

²⁹ https://play.google.com/store/apps/details?id=ua.gov.diiia.quarantine&fbclid=IwAR0j7g_XZ2H8tUrOebiYEI2wdvXonJDYci1GITVv8BkSqqYrQKfUapuOkNo

³⁰ https://kyivcity.gov.ua/news/na_elektronni_servisi_kmda_zdiysnyuyetsya_kiberataka/

³¹ <https://cyberpolice.gov.ua/news/z-pochatku-karantynu-vyyavleno--faktiv-rozpozvyudzhennya-fejkiv-perevireno--povidomlennya-shhodo-mozhlyvyx-shaxrajstv-u-tomu-chysli-pry-onlajn-kupivli-zasobiv-individualnogo-zaxystu-5687/>

³² <http://www.reyestr.court.gov.ua/Review/88537270>

³³ <https://www.eurointegration.com.ua/news/2020/04/1/7108223/>

³⁴ Зазначені факти віднесено до потенційних загроз цифровим правам, оскільки на підставі лише статистичних даних без змістовного аналізу повідомлень (в тому числі судами) встановити наявність чи відсутність порушення неможливо.

³⁵ <https://internetua.com/v-facebook-priznali-csto-proslushivauat-polzovatele/>

³⁶ <https://internetua.com/twitter-teper-peredaet-reklamodatelyam-bolshe-dannyh-o-svoih-polzovatelyah>

а) ЗМІ повідомляють про ряд серйозних вразливостей, знайдених в безпеці програми Zoom, які призводять до витоку даних користувачів, крадіжки паролів з користувацьких записів Windows тощо³⁷.

б) Компанія Twitter також повідомила про існування вразливостей для користувачів соцмережі, які використовують браузер Firefox (після закриття чи виходу з Twitter особисті файли користувача залишались в кеші браузера і будь-хто може отримати до них доступ)³⁸.

в) Розробники програмного забезпечення виявили в сервісі TikTok вразливість, що дозволяє підміняти будь-які відео на чужих сторінках³⁹.

7) **Інтернет-шахрайство.** Шахраї пропонують залишити заявку і переглянути відео, однак замість цього, встановлюють на комп'ютер чи телефон шкідливу програму, що дозволяє викрасти особисті дані і отримати доступ до банківського рахунку особи⁴⁰.

8) **Спотворення інформації щодо кількості переглядів.** За повідомленнями ЗМІ російський телеканал RT накручує перегляди своїх відео на платформі Youtube і купує коментарі ботів під ними. Це призводить до спотворення інформації про відвідування сайту і потенційно може порушувати цифрові права через маніпулювання інформацією⁴¹.

9) **Ризики, які несе в собі нейромережа.** Компанія Hlab.AI повідомила про те, що вона розробила нейромережу, яка дозволяє ідентифікувати осіб, що не носять захисних масок⁴². Це становить потенційну загрозу праву людини на захист приватного життя та персональних даних.

10) **Стеження за користувачами соціальних мереж.** Викрито намагання компанії Facebook влаштувати масове стеження за своїми користувачами, які мають смартфони iPhone. З цією метою компанія намагалась придбати спеціальне шпійське програмне забезпечення у ізраїльської компанії NSO Group⁴³.

Такі дії потенційно загрожують праву людини на захист приватного життя та персональних даних.

11) **Використання соцмереж, додатків, а також певних продуктів інтернет-гігантів, зокрема, Apple та Google, з метою боротьби з пандемією коронавірусу.**

³⁷<https://www.buzzfeednews.com/article/pranavdixit/google-bans-zoom>, <https://mind.ua/news/20209799-google-zaboroniv-svoyim-spivrobotnikam-vikoristovuvati-zoom>, <https://www.bleepingcomputer.com/news/security/zoom-lets-attackers-steal-windows-credentials-run-programs-via-unc-links/>

³⁸<https://internetua.com/twitter-sohranyal-lichsnye-soobsxeniya-polzovatelei-v-keshe-brauzera>

³⁹<https://internetua.com/uyazvimost-v-tiktok-pozvolyaet-podmenyat-video-na-csujih-stranica>

⁴⁰<https://www.obozrevatel.com/economics/fea/dostatochno-zajti-v-internet-moshenniki-v-razgar-koronavirusa-ostavlyayut-ukraintsev-bez-kopejki.htm>

⁴¹<https://ms.detector.media/manipulyatsii/post/24442/2020-04-03-kanal-rt-nakruchue-milionni-pereglyadi-v-youtube-cherez-pornosaiti-rozsliduvannya/>, <https://navalny.com/p/6325/?fbclid=IwAR3qQ2CpsGNS6JFgYoGf44tQSqgm8ExJzyFms6mVNVsUwpJS7B45zZf87E>

⁴²<http://hlab.ai/covid-mask-detection>

⁴³<https://internetua.com/facebook-pytalas-kupit-shpionskoe-po-dlya-slejki-za-polzovateljami-iphone>

ЗМІ повідомляють, що Facebook буде відслідковувати переміщення користувачів з метою протидії поширенню COVID-19⁴⁴, а також про співпрацю компаній Apple та Google у розробці програмного забезпечення, спроможного сприяти скороченню можливостей для поширення хвороби⁴⁵. Окрім цього, КМДА повідомила про можливість використання додатку Telegram для дистанційного контролю за дотриманням киянами режиму самоізоляції⁴⁶.

Потенційно це може призвести до порушення цифрових прав осіб, особливо в частині збирання, зберігання та використання їх персональних даних.

12) Розсилка фішингових повідомлень, що становлять загрозу цифровій безпеці осіб.

Компанія Google повідомила про блокування 18 мільйонів фішингових листів про коронавірус, надісланих користувачам нібито від Всесвітньої організації охорони здоров'я (ВООЗ)⁴⁷.

Таким чином, у квітні 2020 зафіксовано 12 (дванадцять) 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 квітні 2020 року дозволив виявити:

- **18 (вісімнадцять) фактів порушення цифрових прав загального характеру, з яких:**
 - 3 порушення цифрових прав у вигляді обмеження доступу до Інтернету та до інформації, оприлюдненої онлайн, які стосуються 243 веб-ресурсів;
 - 3 факти обробки персональних даних осіб з іншою метою, ніж та, на яку надавалась згода;
 - 12 фактів пов'язаних із поширенням чуток в мережі Інтернет.
- **11 фактів порушення цифрових прав індивідуального характеру, з яких:**
 - 6 випадків порушення права на свободу вираження поглядів у цифровому середовищі;
 - 5 фактів порушення права на приватне життя та захист даних у цифровому середовищі.

Виявлено також **12 потенційних загроз** для для свободи слова та права на приватність в Інтернеті в Україні.

⁴⁴<https://www.segodnya.ua/world/usa/big-brother-facebook-budet-sledit-za-peremeshcheniem-polzovateley-v-ramkah-borby-s-pandemiyey-koronavirusa-1426746.html>, <https://internetua.com/facebook-predlagauat-ispolzovat-dlya-poiska-zarajennyh>

⁴⁵<https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/>, <https://www.blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology/>

⁴⁶https://kyivcity.gov.ua/news/u_stolitsi_zapustili_telegram-bot_dlya_dstantsiyynogo_kontrolyu_za_dotrimannyam_kiyanami_rezhimu_samoizolyatsi/

⁴⁷<https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond>