

УДК 342.951:004

**Л.С. Гулак,**

кандидат юридичних наук,  
доцент, доцент кафедри адміністративного та інформаційного права  
Національного університету «Львівська політехніка»

**Р.І. Радейко,**

кандидат юридичних наук,  
асистент кафедри адміністративного та інформаційного права  
Національного університету «Львівська політехніка»

## **БЛОКУВАННЯ, ФІЛЬТРАЦІЯ ТА ВИДАЛЕННЯ КОНТЕНТУ В СОЦІАЛЬНИХ МЕРЕЖАХ: ПОРІВНЯЛЬНО-ПРАВОВИЙ АСПЕКТ**

**Анотація.** У статті розглянуто зміст права доступу до Інтернету; визначено особливості міжнародного досвіду управління Інтернетом; проаналізовано досвід іноземних держав у сфері блокування доступу до інтернет-контенту. Крім цього, розкрито умови використання державами технологій блокування або фільтрації інтернет-контенту у відповідності до міжнародно-правових норм.

**Ключові слова:** Інтернет, свобода слова, доступ до Інтернету, блокування інтернетконтенту, фільтрація інтернет-контента.

**Постановка проблеми.** Ерік Шмідт і Джерард Коен з компанії Google, прогнозують, що «кожна держава спробує регулювати Інтернет ... всі країни — від найбільш демократичних до авторитарних — намагаються спроектувати закони з реального світу на світ віртуальний» [9, с. 91]. Ці тенденції прослідковуються у багатьох сучасних країнах (Велика Британія, Ізраїль, Китай, Німеччина, Росія, США, Україна) Уряди цих держав почали збільшувати свій контроль над кіберпростором і демонструють готовність втрутитися в комунікацію між користувачами в Інтернеті.

В останні роки зростає кількість випадків використання програмного забезпечення для управління контентом, з метою обмеження або контролю доступу до його вмісту. Це перш за

все використовується для фільтрації матеріалів, переданих через Інтернет, електронну пошту, соціальні мережі або інші онлайн-засоби. Чимало установ використовують блокування доступу до інтернет-сайтів, щоб обмежити можливість працівників користуватися соціальними мережами у робочий час, а також спостерігається тенденція до впровадження фільтрації в Інтернеті для захисту дітей від шкідливих матеріалів і зменшення доступу порнографії. Деякі держави блокують доступ до інтернет-контенту, з метою «забезпечення прав інтелектуальної власності», «захисту національної безпеки», «збереження культурних норм і релігійних цінностей».

**Аналіз останніх досліджень і публікацій.** Деякі питання блокування доступу до інтернет-контенту

досліджували В.В. Архипов, О.А. Баранов, О.О. Золотар, В.Г. Пилипчук, О.Д. Рябоконт та інші. Незважаючи на чималий доробок у цій сфері та впровадження нових методів і способів блокування доступу до інтернет-сайтів, існує нагальна потреба детального дослідження цього питання з урахуванням досвіду різних країн світу.

**Метою статті** є з'ясування особливостей блокування, фільтрація та видалення контенту в соціальних мережах.

**Викладення основного матеріалу.** Блокування — це заходи, що використовуються з метою попередження надходження певного контенту до кінцевого користувача. До них належать: закриття для користувачів доступу до конкретних веб-сайтів, адрес інтернет-протоколу і доменних зон, видалення веб-сайтів з веб-сервера, на яких вони розміщені, або використання технологій фільтрації, що перешкоджають появи сайтів, які можуть містити матеріали, ключові слова або інший контент. Механізми, які використовують для управління інформацією і цензури в Інтернеті, стають все більш технічно складними із застосуванням багаторівневих систем контролю, часто прихованих від користувачів [17].

Не заважаючи на існування технічної можливості блокувати інтернет-контент [14], у світі сформувалися дві правові моделі регулювання блокування, фільтрації та видалення інтернет-контенту.

Перша модель полягає у відсутності в держав законодавства з питань блокування, фільтрації та видалення інтернет-контенту (Австрія, Великобританія, Ірландія, Нідерланди, Німеччина, Польща, Чехія та Швейцарія). Тобто, у наведених кра-

їнах не існує законодавчо визначних умов і процедур, які повинні дотримуватися суб'єкти, що беруть участь у блокуванні, фільтрації та видаленні інтернет-контенту.

Наприклад, у Великій Британії відсутні конкретні нормативно-правові норми щодо блокування сайтів. Так, для блокування інформації про жорстоке поводження з дітьми та непристойного контенту для дорослих, британські інтернет-провайдери впроваджують технічну систему, розроблену British Telecom під назвою «Система очищення» (список URL-адрес і доменних імен, який підтримується галузевим регуляторним органом «Internet Watch Foundation»). Система передбачає двоетапну переадресацію IP-адрес і систему блокування URL-адрес на основі DPI, здатна блокувати веб-сайти, розміщені на загальних IP-адресах, без блокування інших сайтів, розміщених за тією ж адресою. Такий же метод використовується для блокування матеріалів, які заохочують терористичну діяльність. Для блокування наклепницького контенту та контенту, що порушує авторські права, торгові марки або закони про конфіденційність, інтернет-провайдери повинні застосовувати конкретні методи, викладені у відповідному судовому рішенні, прийнятому Високим судом Лондона [10]. У Нідерландах та Німеччині повноваження щодо блокування інтернет-контенту покладено на муніципальні суди, з метою забезпечення балансу між свободою вираження поглядів та захистом інших основних прав людини [10].

Друга модель об'єднує країни в яких законодавство передбачає юридичні підстави, відповідно до яких може бути застосовано блокування або видалення контенту адміністративними чи судовими органами, які

мають компетенцію приймати належні заходи і процедури, яких слід дотримуватися.

Загалом, у даній групі держав блокування доступу до інтернет-ресурсів застосовується відповідно до ч. 2. ст. 10 Конвенції про захист прав людини і основоположних свобод, а саме з метою: захисту національної безпеки, територіальної цілісності або громадської безпеки, для запобігання заворушенням чи злочинам, для охорони здоров'я чи моралі, для захисту репутації чи прав інших осіб, для запобігання розголошенню конфіденційної інформації [3]. Однак деякі держави законодавчо розширили підстави для блокування доступу до інтернет-ресурсів. Для попередження та уникнення жорстокого поводження з дітьми, тероризму, злочинності (зокрема злочинів на ґрунті ненависті) і національної безпеки у деяких державах прийняті норми, що регулюють питання блокування інтернет-контенту та забезпечують термінове блокування таких матеріалів без необхідності прийняття судового рішення. Така практика існує в таких країнах, як Росія, Франція і Туреччина. Адміністративним або правоохоронним органам надано повноваження прийняття рішення про блокування доступу до інтернет-контенту без судового рішення. Зазвичай такі рішення передбачають здійснення блокування провайдером інтернет-доступу протягом 24 годин і без будь-якого повідомлення постачальника контенту [10].

У деяких країнах формується тенденція до тимчасового блокування з метою позбавлення користувачів можливості отримувати та розповсюджувати інформацію в політично значимі періоди, такі як вибори, соціальні протести або святкування

річниця важливих історичних подій. У цей час заблоковано доступ до соціальних мереж, таких як «Twitter» і «Facebook», як це було в період протестів у країнах «Арабської весни» у 2010-2011 рр. (Алжир, Бахрейн, Єгипет, Ємен, Йорданія, Ірак, Кувейт, Ліван, Лівія, Мавританія, Марокко, Оман, Саудівська Аравія, Сирія, Судан, Туніс) та під час військового перевороту в Туреччині у липні 2016 р.

Прогнозуючи розвиток блокування доступу до зв'язку та Інтернету, Е. Шмідт і Дж. Коен зазначають, що авторитарні країни недовго думатимуть пережити тим, як заборонити одно-ранговий зв'язок або взяти його під контроль. А от демократичні країни діятимуть помірковано перед застосуванням будь-яких обмежень у цій сфері. Так, під час масових заворушень у Великобританії в серпні 2011 р., протестувальники вимагали відновити справедливість у справі Марка Деггана, якого застрелили працівники поліції в Тоттенгемі. Через декілька днів протести переросли в сутички, внаслідок яких завинувало п'ятеро людей і пошкоджено майна на суму 300 мільйонів фунтів стерлінгів. На думку уряду Великобританії, цьому найбільше посприяли такі засоби комунікації, як Twitter, Facebook і особливо BlackBerry. Коли протести припинилися, британський Прем'єр-міністр Девід Кемерон виступив у парламенті та повідомив про можливість блокування цих соціальних сервісів в певних ситуаціях, зокрема тоді, «коли відомо, що люди задумують розбій, безпорядки та злочини» [9, с. 81].

У авторитарних державах поширена практика довгострокового блокування або обмеження доступу до соціальних мереж: Венесуела (Twitter), Іран (Facebook, Twitter), Китай (Facebook, Twitter, Instagram), Па-

кистан (Facebook), Російська Федерація (LinkedIn, Telegram), Саудівська Аравія (Facebook), Туркменістан (Facebook, Twiter, Instagram). Наприклад, політика уряду Китаю щодо соціальних мереж полягає в блокуванні міжнародних сайтів (Google Plus; Facebook; Twitter; Instagram) і створенні виключно «китайських» цензурованих соціальних мереж. Замість Twitter, в Китаї функціонує Weibo (<http://tw.weibo.com/>), а замість Facebook є Renren (<http://www.renren.com/>).

В Україні сформувалася окрема практика блокування доступу до деяких російських соціальних мереж. Так, з метою «формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни» [6], 25 лютого 2017 р. Президент України Указом №47/2017 ввів у дію рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. «Про Доктрину інформаційної безпеки України» [6]. У цьому документі визначено, що для забезпечення інформаційної безпеки, слід законодавчого врегулювати не лише механізму блокування, але й виявлення, фіксації та видалення з українського сегмента мережі Інтернет, інформації, яка загрожує життю, здоров'ю громадян України, пропагує війну, національну та релігійну ворожнечу, зміну конституційного ладу насильницьким шляхом або порушення територіальної цілісності України, загрожує державному суверенітету, пропагує комуністичний та/або націонал-соціалістичний (нацистський) тоталітарні режими та їхню символіку [6].

15 травня 2017 р. Президент України підписав Указ щодо засто-

сування персональних спеціальних економічних та інших обмежувальних заходів (санкції), зокрема, до ТОВ «Мэйл.РУ ГРУП», ТОВ «Вконтакте», ТОВ «Вконтакті», ТОВ «Мейл.РУ Україна» у формі заборони Інтернет-провайдерам надання послуг з доступу користувачам мережі Інтернет до ресурсів сервісів «Mail.ru» та соціальних мереж «Вконтакте» та «Одноклассники» [5]. Однак в цьому Указі не зазначено причин та механізму блокування доступу до цих інтернет-сервісів, що зумовило неоднозначні оцінки експертів та широкої громадськості. Проте блокування даних інтернет-сервісів, слід розглядати крізь призму «забезпечення національної безпеки» [1], а не «обмеження свободи слова». Особливої значущості ця теза набуває в контексті зміни політики соціальної мережі Facebook після виявлення створення Росією фейкових акаунтів, для поширення у соціальній мережі політичної реклами під час виборів президента США у 2016 р. [8].

На початку червня 2017 р. даний Указ Президента України [5] оскаржено до Вищого адміністративного суду України в частині блокування доступу до інтернет-ресурсів. Позивач вказав, що оскаржуваний Указ у зазначеній частині прийнятий всупереч вимогам Закону України «Про санкції», порушує права на свободу вираження поглядів у відповідності зі ст. 10 Конвенції про захист прав людини та основоположних свобод, а також порушує право позивача на свободу доступу до інформації.

Однак Вищий адміністративний суд України відмовив у задоволенні позовних вимоги через відсутність правових підстав, мотивуючи свою позицію тим, що у даному випадку спірним є не користування мережею в цілому, а лише заборона Інтернет-про-

вайдерам на певний період здійснювати надання послуг з доступу користувачам мережі Інтернет до ресурсів певних сервісів, яка, у свою чергу, не створює перешкод для користування будь-якими іншими сервісами. Крім цього, на думку суддів Вищого адміністративного суду України, спірним Указом позивача не обмежено у виборі форм і джерел одержання інформації. Окремі перешкоди, які можуть виникнути в процесі використання заблокованих інтернет-ресурсів, не обмежують права громадян на використання цих ресурсів, а спричинені виключно необхідністю створення негативних наслідків для осіб, щодо яких застосовано спеціальні економічні та інші обмежувальні заходи (санкції) [4].

Зважаючи на відсутність правового механізму блокування доступу до інтернет-ресурсів в Україні, слід закріпити процедуру формування списків веб-сайтів з обґрунтуванням необхідності блокування кожного конкретного сайту. Будь-яке рішення про те, який контент необхідно блокувати, повинен приймати судовий орган.

Окрім блокування доступу до соціальних мереж, застосовується фільтрація онлайн-контенту. Найбільш яскравим прикладом фільтрації контенту в Інтернеті та соціальних мережах є «Проект Золотий Щит» (The Golden Shield Project), також відомий як «Великий китайський файрвол» (Great Firewall of China). Проект стартував у 2003 р. та є системою серверів на інтернет-каналі між провайдерами і міжнародними мережами передачі інформації, що фільтрує інформацію. Китай реалізував найскладнішу фільтрацію інтернет-контенту, що здатна ефективно фільтрувати контент з використанням безлічі методів регулювання і технічного контролю (блоку-

вання IP-адрес і фільтрація контенту; фільтрація DNS і URL; скидання з'єднання тощо).

Фільтрація поширюється на «ключові слова», які внесені до «національного чорного списку» («демократія», «права людини», «диктатура», «пригнічення», «червоний терор», «Далай-лама»), які заблоковані під час запитів місцевих користувачів до іноземних пошукових систем.

Постачальники інтернет-послуг зобов'язані видаляти контент відповідно до вказівок цензорів. Так, у червні 2016 р. заборона на незалежний збір або розповсюдження оригінальних новин була поширена на всі додатки для соціальних мереж, в той час як в липні 2016 р. пекінський підрозділ адміністрації Китаю прийняв норми, що забороняють китайським інтернет-порталам створювати будь-які оригінальні новини, обмежуючи їх контентом, наданим невеликою кількістю дозволених «офіційних» джерел. Керівництво сайтів новин повинно цілодобово відстежувати зміст заміток і статей, щоб не допустити фактичних, стилістичних та інших помилок.

У серпні 2016 р. Кіберпростір адміністрації Китаю (Cyberspace of Administration of China) встановив нові жорсткі вимоги до цензури для інтернет-провайдерів, в тому числі запроваджено постійний моніторинг вмісту новин і персональну відповідальність головних редакторів сайтів за контент.

З метою посилення державного контролю над Інтернетом, у листопаді 2016 р. Всекитайськими зборами народних представників ухвалено новий закон «Про кібербезпеку». Згідно з цим законом, фізичні особи та організації Китаю не мають права «шкодити безпеці, честі та інтересам держави» в інтернеті. Також законом заборо-

няється діяльність в Інтернеті, спрямована на «повалення соціалістичної системи, розкол нації, підрих національної єдності, захист тероризму та екстремізму» [15].

Механізми, що використовуються для фільтрації інформації та цензури в онлайн-просторі, стають все більш технічно складними із застосуванням багаторівневих систем контролю, часто прихованих від користувачів.

Окрім блокування доступу до соціальних мереж та фільтрації їх контенту, також застосовується видалення вмісту в пошукових сервісах і соціальних мережах, які постійно отримують від різних осіб вимоги щодо видалення певної інформації з їх сервісів.

Основними причинами видалення вмісту в сервісах Google наступні:

1) *видалення вмісту через порушення авторських прав*. Згідно з внутрішніми правилами, корпорація Google, реагує на чіткі повідомлення про ймовірні порушення авторських прав. Веб-форма сповіщення відповідає зразку в законі США «Про захист авторських прав у цифрову епоху» (DMCA) [11] і забезпечує простий та ефективний механізм для власників авторських прав у всьому світі. Щоб розпочати процедуру видалення вмісту з результатів пошуку в Google, власник авторських прав, який вважає, що URL-адреса перепрямовує на правопорушний вміст, надсилає запит корпорації Google на видалення такого ймовірно правопорушного матеріалу. Отримавши запит на видалення, представники Google перевіряють його на повноту та наявність інших проблем. Якщо повідомлення повне, і не знайдено інших проблем, представники Google видаляють URL-адресу з результатів пошуку Google;

2) *запити на видалення вмісту від державних установ*. Корпорація Google регулярно отримує від органів державної влади різних країн вимоги видалити з його сервісів такі матеріали, як записи в блогах, відео на YouTube або результати пошуку [2].

Google отримує запити на видалення вмісту різними шляхами та від державних установ усіх рівнів. Це ухвали суду, письмові запити від центральних і місцевих державних установ, правоохоронних органів тощо. Іноді запити на видалення вмісту від державних установ надходять через користувачів (наприклад, скаржник долучає ухвалу суду як доказ того, що певний вміст заборонений). У деяких запитах просять видалити одразу кілька матеріалів або, навпаки, можуть надходити кілька запитів на видалення того самого матеріалу.

Однак не усі запити підлягають задоволенню, оскільки вони мають бути подані у письмовій формі, якомога точніше описувати вміст, який потрібно видалити, і пояснювати, чому цей вміст є незаконним. Не підлягає задоволенню запит, надісланий неналежним чином.

Google можемо відмовити у видаленні вмісту з різних причин. Деякі запити не містять точної інформації про елементи, які державний орган просить видалити (наприклад, у запиті не вказано URL-адресу). В інших випадках Google отримує скарги на наклеп, оформлені у вигляді офіційних листів від державних установ, а не ухвал суду. Приймаючи рішення про те, чи є повідомлення наклепницьким згідно з місцевим законодавством, Google зазвичай покладається на рішення суду.

Іноді письмових звернень від органів недостатньо й потрібна ухвала суду. Зазвичай Google покладається

на рішення суду щодо того, чи повідомлення вважається наклепом згідно зі законодавством держави. Представник Google здійснюють перевірку законності отриманих документів, і якщо виявиться, що ухвала суду є фальшивою, не виконує її.

3) *видалення результатів пошуку відповідно до закону про конфіденційність користувачів із ЄС.* Згідно з рішенням Суду Європейського Союзу від травня 2014 р. [13], користувачі мають право надсилати в пошукові системи, як-от Google, запити на видалення результатів пошукових запитів на основі імені людини. Пошукова система повинна видалити ці посилання, якщо вони «неадекватні, недоречні, неактуальні або надмірні», беручи до уваги чинники суспільного інтересу, зокрема роль людини в житті громадськості. Сторінки видаляються з результатів пошуку лише у відповідь на запити, які стосуються імені особи. Google видаляє URL-адреси з усіх європейських результатів пошуку Google (для користувачів з Іспанії, Німеччини, Франції тощо) і використовує дані геолокації, щоб обмежувати доступ до URL-адреси в країні, звідки надійшов запит на видалення.

4) *контроль відповідності правилам спільноти YouTube.* Google виявляє на YouTube вміст, що не відповідає його внутрішнім правилам (порнографія, заклики до насильства, переслідування чи ворожі висловлювання), за допомогою спеціальних алгоритмів, а також завдяки скаргам, які надсилають користувачі. Скарги можуть надходити від систем автоматичного виявлення, учасників програми позначення невідповідних відео (неурядових організацій, державних установ і фізичних осіб) або користувачів спільноти YouTube.

5) *видалення відповідно до Закону про регулювання вмісту в соціальних мережах.* Так, в Німеччині 1 жовтня 2017 р. набрав чинності Закон про регулювання вмісту в соціальних мережах (NetzDG) [12]. Відповідно до п. 2. § 1 цього Закону, соціальні мережі, у яких зареєстровано понад 2 мільйони користувачів із Німеччини, мають локально видаляти «очевидно незаконний» вміст (напр., публікацію, зображення, відео) упродовж 24 годин після отримання сповіщення. Якщо законність важко визначити одразу, постачальник має розглянути запит упродовж семи днів. Цей процес може тривати довше лише в порядку виключення, наприклад, якщо залучено авторів вмісту або рішення приймає спільний галузевий орган чи установа регульованого саморегулювання. Щоб підлягати видаленню відповідно NetzDG, вміст має порушувати один із 22 законів Кримінального кодексу Німеччини, на який посилається NetzDG.

24 квітня 2018 р. адміністрація Facebook опублікувала внутрішні рекомендації, які використовуються для ухвалення рішень про видалення контенту в цій соціальній мережі [16]. Якщо модератори Facebook зафіксують порушення цих правил користувачами соціальної мережі, останнім можуть заборонити публікувати дописи, а згодом — відключать профіль. Facebook використовує комбінацію штучного інтелекту та звіти від осіб для визначення відео, зображень та іншого контенту, який порушує стандарти соціальної мережі.

У Стандартах соціальної мережі Facebook [7] визначено перелік умов видалення дописів, якщо вони містять інформацію про:

— *насильство* (реальне насильство; небезпечних осіб та організацій,

які здійснюють: терористичну діяльність; організоване ненависництво; масові чи серійні вбивства; торгівля людьми; організоване насильство чи злочинна діяльність; пропагування, реклама злочинності та координування заподіяння шкоди;

– *безпеку* (пропагування, заохочення, координація чи надання вказівки щодо: самогубства; самоушкодження; харчових порушень; дитяча нагота й сексуальна експлуатація дітей /дорослих/; порушення конфіденційності та прав на конфіденційність зображень);

– *вміст, що підлягає запереченню* (пропаганда ненависті; насильство та графічний вміст; оголеність і сексуальна активність дорослих; жорстокість і нечуйність);

– *цілісність та автентичність* (спам; введення в оману; неправдиві новини);

– *контент, який порушує авторські права та права на торговельну марку*.

Зазвичай дописи видаляють після того, як на них скаржаться інші користувачі. Після отримання скарги, допис відправляється на модерацию.

Наслідки порушення Стандартів спільноти Facebook залежать від тяжкості порушення та історії користувача на платформі. Наприклад, Facebook може попередити користувача про перше порушення. Якщо користувач продовжить порушувати Стандарти соціальної мережі, то модератори можуть скасувати дозвіл на публікацію дописів у Facebook чи заблокувати профіль особи.

Отже, до інформації, що може бути обмежена в соціальних мережах, належить: дитяча порнографія (для захисту прав дітей), підбурювання до ненависті (для захисту прав вразливих категорій осіб), дифамація (для

захисту прав і репутації інших осіб від незаконних нападів), пряме і публічне підбурювання до здійснення геноциду (для захисту прав інших осіб), будь-який виступ на користь національної, расової чи релігійної ненависті, що являє собою підбурювання до дискримінації, ворожнечі або насильства (для захисту прав людини) [17]. Однак постає питання про межі допустимості держава і корпорацій у сфері блокування, фільтрації та видалення певних видів контенту.

Нажаль часто органи державної влади намагаються законодавчо обмежити, контролювати, обробляти і цензурувати контент, який розповсюджується через інтернет-ресурси, без будь-яких законних підстав або на основі суперечливих законів, що не обґрунтовуючи такі дії, і/або здійснюють це непропорційно до заявленої мети. Такі дії явно не сумісні зі зобов'язаннями держав, передбачених міжнародними нормами у сфері прав людини, і часто ще більше перешкоджають реалізації права на свободу слова.

**Висновки.** Використання державами і корпораціями технологій блокування, фільтрації та видалення онлайн-контенту часто є порушенням їхніх зобов'язань щодо гарантування права на свободу слова, адже:

1) конкретні підстави для блокування, фільтрації та видалення інтернет-контенту не закріплені в законодавстві, або вони вкрай широко і нечітко прописані в законах, що створює небезпеку довільного і надмірного їх застосування;

2) блокування, фільтрація та видалення інтернет-контенту не завжди спрямоване на виконання цілей, передбачених в ч. 2. ст 10 Конвенції про захист прав людини і основоположних свобод та ч. 3 ст. 19 Міжнародного пакту про громадянські і політичні



права, а списки сайтів, які підлягають блокуванню зазвичай не розголошуються, що ускладнює оцінку того, чи є обмеження доступу до контенту законним;

3) навіть у випадку обґрунтування заходів блокування, фільтрації та видалення інтернет-контенту, вони є зайвими і непропорційними досягненню

поставленої мети, оскільки часто є неналежно обґрунтованими і зумовлюють закриття доступу до більшого обсягу контенту, ніж той, який вважається незаконним;

4) контент часто блокують без участі судового або незалежного органу або без можливості перегляду відповідного рішення цими органами.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Відповідь Президента України на електронну петицію № 22/036543-еп “Отменить блокировку интернет-ресурса Вконтакте”, розміщену на веб-сайті Офіційного інтернет-представництва Президента України 16.05.2017 громадянином А.А.Ткаченком <https://petition.president.gov.ua/petition/36543>
2. Запити на видалення вмісту від державних установ. URL: <https://transparencyreport.google.com/government-removals/overview?hl=uk>
3. Конвенція про захист прав і свобод людини і громадянина від 04.11.1950 р. URL: [http://zakon5.rada.gov.ua/laws/show/995\\_004](http://zakon5.rada.gov.ua/laws/show/995_004)
4. Постанова Вишого адміністративного суду України від 14 червня 2017 р. у справі № 800/198/17. URL: <http://reyestr.court.gov.ua/Review/67196698>
5. Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»: Указ Президента України від 15 травня 2017 р. № 133/2017. Офіційний вісник України. 2017. № 41. Ст. 1276.
6. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25 лютого 2017 р. № 47/2017. Офіційний вісник України. 2017 р. № 20. Ст. 554.
7. Стандарти спільноти Facebook. URL: <https://www.facebook.com/communitystandards/introduction>
8. Цукерберг: Facebook виявив докази активності РФ в соцмережі і змінить алгоритми. URL: <https://hromadske.ua/posts/tsukerberh-facebook-vyiyaviv-dokazy-aktyvnosti-ri-v-sotsmerezhi-i-zminyt-alhorytmy>
9. Шмідт Е. Коен Дж. Новий цифровий світ / Пер. з англ. Ганна Ленів. — Л.: Літопис, 2015. С. 91.
10. Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content, prepared by the Swiss Institute of Comparative Law, commissioned by the Council of Europe, 20 December 2015, Lausanne. URL: <https://www.coe.int/en/web/freedom-expression/studyfiltering-blocking-and-take-down-of-illegal-content-on-the-internet>.
11. Digital Millennium Copyright Act. 10,28,1998, Public Law No: 105-304. URL: <https://www.congress.gov/bill/105th-congress/house-bill/2281/text>
12. Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken. Ausfertigungsdatum: 01.09.2017. URL: <https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html>
13. Google Spain SL Google Inc. V Agencia Española de Protección de Datos (AEPD) Mario Costeja González Judgment of the Court (Grand Chamber) in Case C-131/12, 13 May 2014. URL: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageId=dex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=794833>
14. Internet Society Perspectives on Internet Content Blocking: An overview. Internet Society, March 2017. URL: <https://www.internetsociety.org/wpcontent/uploads/2017/03/ContentBlockingOverview.pdf>.

15. Paul Mozur. China's Internet Controls Will Get Stricter, to Dismay of Foreign Business. URL: <https://www.nytimes.com/2016/11/08/business/international/china-cyber-security-regulations.html>

16. Publishing Our Internal Enforcement Guidelines and Expanding Our Appeals Process By Monika Bickert, Vice President of Global Policy Management Facebook. URL: <https://newsroom.fb.com/news/2018/04/comprehensive-community-standards/>

17. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. 16 May 2011. URL: [http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27\\_en.pdf](http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf)

**Гулак Л.С., Радейко Р.И.**

**Блокировка, фильтрация и удаление контента в социальных сетях: сравнительно-правовой аспект.**

**Аннотация.** В статье рассмотрены содержание права доступа к Интернету определены особенности международного опыта управления Интернетом; проанализирован опыт иностранных государств в сфере блокировки доступа к интернет-контенту. Кроме этого, раскрыто использование государствами технологий блокировки или фильтрации интернет-контента в соответствии с международно-правовых норм.

**Ключевые слова:** Интернет, свобода слова, доступ к Интернету, блокировки интернет-контента, фильтрация интернет-контента.

**L. Hulak, R. Radeiko**

**Blocking, filtration and disposal of the content in social networks: comparative aspects.**

**Summary.** In the article the contents of the right of access to the Internet are considered, the features of the international experience of Internet governance are determined; The experience of foreign countries in the field of blocking access to Internet content is analyzed. In addition, the use of state-of-the-art technologies for blocking or filtering Internet content is disclosed in accordance with international legal norms.

**Keywords:** Internet, freedom of speech, access to the Internet, blocking of Internet content, filtering of Internet content.

