Вісник Київського національного університету імені Тараса Шевченка
Державне управління, 1(17), 28-37
УДК 351.86:004:321.64
DOI: https://doi.org/10.17721/2616-9193.2023/17-5/7

Володимир Литвиненко, канд. наук із соціальних комунікацій,
директор Центру комунікацій
Київський національний університет імені Тараса Шевченка, Київ, Україна
https://orcid.org/0000-0003-1156-105X
email: vollyt@knu.ua

Олександр Кантур, асп.
Київський національний університет імені Тараса Шевченка, Київ, Україна
https://orcid.org/0000-0001-8351-6210
email: oleksandr.kantur@knu.ua

"БАЛКАНІЗАЦІЯ ІНТЕРНЕТУ" ЯК ІНСТРУМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АВТОРИТАРНИХ ДЕРЖАВ

Досліджено особливості та проблематика фрагментації глобальної мережі Інтернет державами, у яких панують авторитарні режими. Зокрема, здійснено спробу узагальнити трактування дефініції "балканізація інтернету", вивчено принципи роботи китайської розробки "Золотий щит" як державної системи цензури в кіберпросторі, проаналізовано особливості впровадження "Національної інформаційної мережі" в Ірані та суверенного інтернету в Росії, а також розглянуто північнокорейський досвід реалізації проєкту "Кванмьон".

За результатами проведеного аналізу нормативно-правових актів, публікацій у ЗМІ та інших відкритих джерел з'ясовано, що найчастіше уряди держав пояснюють такі рішення захистом національної безпеки. Водночас на практиці балканізація інтернету нівелює і без того обмежену свободу слова в країнах, де інші джерела інформації так чи інакше перебувають під державним контролем, а також призводить до більшої інформаційної, культурної, наукової, економічної автаркії суспільств.

Ключові слова: інформаційна безпека, держава, інформаційно-комунікаційні технології, інтернет, цифровий авторитаризм, балканізація інтернету.

Актуальність теми. Глобальний розвиток інформаційно-комунікаційних технологій та їх повсюдне поширення закріпили за глобальною мережею Інтернет статус відносно вільного від контролю середовища. Водночас завдяки глибокій інтеграції в усі сфери життєдіяльності людини Інтернет став потужним інструментом впливу на геополітичні конфлікти, зокрема, шляхом втручання у внутрішні справи інших держав, підриву національної безпеки, дестабілізації фінансових систем та атаки на критично важливі об'єкти інфраструктури.

Паралельно з отриманням соціальних та економічних переваг, що надає глобальна мережа, світова спільнота також постає і перед новими загрозами, які Інтернет створює для національної безпеки. У сучасному світі простежуються дві окремі тенденції таких загроз: для демократичних режимів – це кібератаки; підрив довіри до державних і соціальних інститутів через поширення ворожої пропаганди, а також інші інформаційні впливи з боку авторитарних країн, що призводять до послаблення держав і суспільств. Для авторитарних, напівавторитарних і тоталітарних – доступ до альтернативних джерел інформації, що загрожує контролю над суспільною думкою, створює передумови для появи плюралізму думок, поширення медіаграмотності та формування у споживачів інформації критичного мислення.

У відповідь на ці загрози держави починають посилювати свої інтернет-кордони шляхом спроб розбудови власних інформаційних мереж, а також створювати додаткові інформаційні інструменти, що можуть використовуватися як засіб стримування конфліктів і поширення ворожих впливів. Потенційним недоліком такого втручання у діяльність глобальної мережі з боку авторитарних і напіваторитарних держав є гальмування їхнього розвитку та появи інновацій, яким традиційно сприяв Інтернет, та обмеження свободи слова. З іншого боку, ті ж інновації та свобода слова не можуть процвітати в умовах невизначеності та в середовищі з підвищеним рівнем злочинності та відсутністю правил, норм і етики. Зважаючи на це, національні політики досить часто стикаються з проблемою досягнення балансу між регулюванням і потенційною вседозволеністю в Інтернеті. Відтак держави вдаються до низки інструментів забезпечення інформаційного порядку, зокрема і до спроб фрагментації інтернет-простору, що наразі можна вважати однією із визначальних рис "цифрового авторитаризму", який є притаманним країнам із відповідним політичним режимом.

Аналіз досліджень. Проблематика механізмів забезпечення інформаційної безпеки держави перебуває в центрі уваги Т. Перуна, С. Домбровської, В. Пашковського, Є. Кобко, В. Шемчука. Питання фрагментації глобальної мережі Інтернет частково відображено у працях Е. Бриньольфссона, П. Сагави, М. Мюллера, К. Кунера, К. Мілларда. Однак у переважній більшості наукових розвідок наголошується на комплексному характері цього явища. Водночас окремого дослідження потребує явище "балканізації Інтернету" як одного з інструментів забезпечення інформаційної безпеки держави, що і зумовлює актуальність нашого дослідження.

Мета статті полягає у детальному розгляді та вивченні особливостей використання авторитарними державами інструменту фрагментації глобальної мережі Інтернет шляхом створення внутрішньодержавної комп'ютерної мережі.

Виклад основного матеріалу. Протягом останніх років у багатьох країнах світу спостерігається тенденція щодо посилення контролю над доступом до інформації у мережі. Здійснення подібних заходів найчастіше мотивується зміцненням інформаційної безпеки держави, збереженням традиційних цінностей чи способів життя. Водночас такий контроль здійснюється не лише завдяки обмеженню доступу до певної інформації чи блокуванню окремих інтернет-ресурсів, а і через спроби державами "балканізувати" інтернет-середовище.

За даними "Великої української енциклопедії" дефініція "балканізація" – це геополітичний термін, яким характеризується процес розпаду багатонаціональних держав певного регіону на частини; атомізація регіо-

ISSN 1728-3817

ну [2]. Однак Л. Велію стверджує, що термін "балканізація" не має чіткого визначення. На думку науковиці, поняття найчастіше використовувалося для описання широкого кола складних і проблемних ситуацій, людей і подій [36]. Згідно з тлумаченням Британської енциклопедії, термін "балканізація" сьогодні використовують для пояснення розпаду деяких багатонаціональних держав і їх перетворення на режим диктатури, етнічних чисток та громадянської війни [41].

До того ж останніми роками в професійному дискурсі дедалі частіше трапляється словосполучення "балканізація Інтернету" або ж поділ (спліт) Інтернету. Уперше цей термін використав дослідник Клайд Уейн Крюс з американської неполітичної дослідницької організації Інститут Катона (*Cato Institute*) у 2001 році. На його думку, поняття характеризує концепцію паралельних інтернет-мереж, які працюватимуть як автономні [35]. Інше трактування терміна використовує Д. Шаршаткін, який визначає балканізацію Інтернету як "регіоналізацію режимів управління Інтернетом" [18].

Водночас ми здійснюємо спробу узагальнення трактувань поняття "балканізація Інтернету" та окреслюємо його ***як процес, у результаті якого відбувається фрагментація простору глобальної мережі на окремі частини (за однією чи кількома ознаками), які не залежать одна від одної. Такий поділ призводить до виокремлення суверенних національних чи регіональних сегментів Інтернету. Їхні межі можуть бути цілком ідентичні кордонам держав або ж не збігатися з ними.*** В основі логіки фрагментації Інтернету є переконання щодо унеможливлення зовнішнього інформаційного впливу, що є одним зі складників інформаційної безпеки держави. Задля її забезпечення держави дедалі частіше намагаються встановити власні правила гри в тій частині інформаційного простору, яку вони вважають своєю, запроваджуючи власні проєкти з реалізації внутрішньодержавного Інтернету. Дослідники із правозахисної організації Freedom House визначили три основні складники фрагментації Інтернету: 1) запровадження обмежень щодо новинних потоків та інформації загалом; 2) централізований державний контроль над інтернет-інфраструктурою; 3) створення бар'єрів для транскордонного передавання даних користувачів [24].

Щорічно обмеження в інтернеті застосовують дедалі більше країн. Зокрема, у 2022 році із 70 країн, які відстежує Freedom House, у 47 державах було запроваджено ті чи інші обмеження щодо джерел інформації, які розміщені за межами їхніх кордонів [24]. У переважній більшості випадків до таких кроків вдаються лідери авторитарних держав у прагненні стримати інакодумство в мережі, обмежуючи доступ до джерел інформації, які розташовані в країнах з вищим рівнем свободи слова. Бажання отримати абсолютний контроль над цифровою сферою підштовхує автократії до впровадження масштабних ініціатив із фрагментації інформаційного простору (табл. 1.).

***Таблиця* 1**

"Обмеження інтернет-простору у світі"
(за даними порталу Freedom House) [24]

Країна	Кількість використаних засобів управління Інтернетом	Блокування соціальних мереж або комунікаційних платформ	Блокування політичного, соціального або релігійного контенту	Навмисно виведені з ладу мережі ІКТ	Провладні коментатори маніпулюють онлайн-дискусіями	Ухвалено новий закон або директиву, що посилює цензуру або покарання	Ухвалено новий закон або директиву, що посилює нагляд або обмежує анонімність	Арешт або ув'язнення осіб за створення чи поширення цензурованого контенту	Фізичний напад або вбивство блогера чи користувача ІКТ	Технічні атаки проти критиків уряду або правозахисних організацій	Загальна оцінка у 2022 році	Загальний статус доступу до Інтернету
Китай	9							X			10	Обмежений
М'янма	8							X			12	Обмежений
Іран	7							X			16	Обмежений
Куба	8							X			20	Обмежений
В'єтнам	6							X			22	Обмежений
Росія	7							X			23	Обмежений
Саудівська Аравія	7							X			24	Обмежений
Пакистан	9							X			26	Обмежений
Єгипет	6							X			27	Обмежений
Ефіопія	5							X			27	Обмежений
Узбекистан	6							X			27	Обмежений
Білорусь	6							X			28	Обмежений
ОАЕ	7							X			28	Обмежений
Бахрейн	4							X			29	Обмежений
Судан	6							X			29	Обмежений
Венесуела	6							X			30	Обмежений
Казахстан	6							X			32	Обмежений
Туреччина	7							X			32	Обмежений
Руанда	4							X			37	Обмежений
Азербайджан	7							X			38	Обмежений
Таїланд	4							X			39	Обмежений

Закінчення табл. 1

Країна	Кількість використаних засобів управління Інтернетом	Блокування соціальних мереж або комунікаційних платформ	Блокування політичного, соціального або релігійного контенту	Навмисно виведені з ладу мережі ІКТ	Провладні коментатори маніпулюють онлайн-дискусіями	Ухвалено новий закон або директиву, що посилює цензуру або покарання	Ухвалено новий закон або директиву, що посилює нагляд або обмежує анонімність	Арешт або ув'язнення осіб за створення чи поширення цензурованого контенту	Фізичний напад або вбивство блогера чи користувача ІКТ	Технічні атаки проти критиків уряду або правозахисних організацій	Загальна оцінка у 2022 році	Загальний статус доступу до Інтернету
Ірак	6							X			42	Ускладнений
Бангладеш	5							X			43	Ускладнений
Камбоджа	5							X			43	Ускладнений
Лівія	5							X			44	Ускладнений
Нікарагуа	4							X			45	Ускладнений
Йорданія	4							X			47	Ускладнений
Шрі-Ланка	7							X			48	Ускладнений
Індонезія	6							X			49	Ускладнений
Зімбабве	4							X			49	Ускладнений
Уганда	5							X			50	Ускладнений
Індія	7							X			51	Ускладнений
Ліван	5							X			51	Ускладнений
Марокко	4							X			51	Ускладнений
Киргизстан	6							X			53	Ускладнений
Сінгапур	4							X			54	Ускладнений
Республіка Гамбія	1							X			56	Ускладнений
Малаві	2							X			57	Ускладнений
Нігерія	5							X			57	Ускладнений
Замбія	3							X			58	Ускладнений
Малайзія	3							X			59	Ускладнений
Україна	7							X			59	Ускладнений
Ангола	1							X			61	Ускладнений
Мексика	4							X			61	Ускладнений
Туніс	5							X			61	Ускладнений
Колумбія	4										64	Ускладнений
Еквадор	2										64	Ускладнений
Гана	3							X			64	Ускладнений
Бразилія	3							X			65	Ускладнений
Філіппіни	4							X			65	Ускладнений
Південна Корея	1										67	Ускладнений
Кенія	2										68	Ускладнений
Угорщина	3										69	Ускладнений
Аргентина	1										71	Вільний
Сербія	3							X			72	Вільний
Південна Африка	1							X			73	Вільний
Вірменія	4							X			74	Вільний
Італія	1										75	Вільний
Австралія	3										76	Вільний
Франція	3										76	Вільний
США	2							X			76	Вільний
Німеччина	3										77	Вільний
Японія	0										77	Вільний
Грузія	1										78	Вільний
Тайвань	2							X			79	Вільний
Велика Британія	1										79	Вільний
Канада	0										87	Вільний
Коста-Ріка	0										88	Вільний
Естонія	1										93	Вільний
Ісландія	0										95	Вільний

Як відомо, одним із найбільш згадуваних подібних проєктів у світі є "Золотий щит", що наразі функціонує в Китайській Народній Республіці. Через популярність цієї розробки Китай почали називати країною, яка "найбільш нахабно" керує інтернетом удома і навчає світ цифровому авторитаризму [4]. Розроблення "Золотого щита" розпочалося ще в 1998 році, а вже у 2003 р. його було введено в експлуатацію. Першочергово проєкт

ISSN 1728-3817

створювався для підвищення мережевої безпеки, але згодом його почали використовувати і як інструмент цензури та відстежування. Розробка також вміщує і "Великий китайський фаєрвол", який дозволяє відфільтровувати контент в інтернеті та обмежувати доступ до цілої низки сайтів, у тому числі релігійної, політичної чи філософської тематики. Таким чином іноземні соціальні мережі, такі як Facebook, Twitter чи YouTube у Китаї заблоковані, унаслідок чого китайські громадяни використовують локальні аналоги, зокрема Youku чи Sina Weibo, де цензура і пропаганда легко може бути посилена державою. За даними дослідження, проведеного у 2021 році, китайська влада блокує доступ до близько 311 тисяч сайтів, з яких 270 тисяч заблоковано цілеспрямовано, а 41 тисяча потрапила під заборону помилково [29]. Окрім безпосередньо блокування вебсайтів, окремий контент на інтернет-ресурсах також піддається цензурі за низкою ознак, зокрема за тематикою, яка, на думку влади, є політично чутливою. Здійснюється обмеження доступу до коментарів, що містять критику Комуністичної партії Китаю, репортажі іноземних ЗМІ про Китай, міжнародну політику, а також конкретні внутрішньополітичні події, які держава прагне "приховати" від суспільства [25].

Посилення мережевого контрою у КНР здійснюється також і через функціонування регуляторних відомств. Наприклад, у 2014 році було створено Адміністрацію кіберпростору Китаю – центральний орган регулювання Інтернету в Республіці. Вона перебуває під прямою юрисдикцією Керівної групи ЦК КПК з інформатизації та безпеки в Інтернеті – партійної установи, підпорядкованої Центральному комітету Комуністичної партії Китаю. Наразі керівну групу очолює Сі Цзіньпінь, діючий Голова Китайської Народної Республіки та Генеральний секретар Центрального комітету Комуністичної партії Китаю.

Із моменту свого заснування, Адміністрація кіберпростору розширює законодавчу базу для контролю над онлайн-контентом та особистими даними. Найбільш важливим законодавчим актом, який контролює функціонування інтернету в Китаї, вважають Закон про кібербезпеку, ухвалений Постійним комітетом Всекитайських зборів народних представників 7 листопада 2016 року. З 1 червня 2017 року Закон регулює всю онлайн-діяльність у КНР та зобов'язує постачальників інтернет-послуг перевіряти справжні імена користувачів, наприклад, на форумах чи в коментарях, а мережевих операторів – контролювати створений користувачами контент і перевіряти наявність у ньому інформації, яку заборонено публікувати чи передавати стороннім особам. Таким чином влада, крім порушення приватності та конфіденційності користувачів в Інтернеті, ще й посилює персональну відповідальність та перекладає провину з медіа та компаній безпосередньо на користувачів [44].

Щоб ефективно фільтрувати контент, мережеві оператори вимушені збільшувати власні спроможності. Ідеться про нарощування обсягів людських і технологічних ресурсів, що дозволяють здійснювати перевірки контенту та допомагають з видаленням контенту як превентивно, так і постфактум.

Зазвичай цензуру в Китаї розглядають як монолітну систему контролю, що має свою структуру і послідовність. Про це свідчить розвинена законодавча база, наявність цілої мережі державних регуляторних органів та арсенал технологічних інструментів, які дозволяють владі виявляти небажаний контент. Протягом останніх років китайський уряд справді доклав чимало зусиль, щоб посилити свій контроль над Інтернетом та іншими медіа, а також централізувати контроль, який раніше здійснювався кількома різними структурами. Водночас влада в організації системи контролю частково покладається на приватні компанії та зобов'язує їх виконувати свої директиви, що часом призводить до суперечливих результатів.

Зрештою, комуністичний режим досить ефективно контролює китайське суспільство. Більшість великих засобів масової інформації або перебувають у державній власності, або ж перебувають під наглядом влади. Міжнародні новини вибірково редагуються та фільтруються, щоб користувачі могли отримувати цензурований контент. Одним з ілюстративних прикладів цього є дослідження, що проведене компанією Citizen Lab, у якому йдеться про те, що зображення, якими обмінюються користувачі в китайському месенджері WeChat, автоматично піддаються цензурі в режимі реального часу [22].

Влада Китаю стверджує, що такі обмеження спрямовані на підтримку суспільного порядку і забезпечення національної безпеки. Слід додати, що. окрім політичних цілей, "Великий китайський фаєрвол", на думку влади, також стимулює внутрішні економічні процеси в країні. Сьогодні Китай є однією із небагатьох країн світу, де лідером інтернет-пошуку є зовсім не Google, а місцевий проєкт-аналог Baidu. Окрім самих інтернет-користувачів, які вимушені користуватися локальними сервісами, на поступки також змушені йти і світові корпорації, що бажають залишитися присутніми на ринку китайських інформаційних послуг та уникнути блокування. До прикладу, у 2016 році китайські регулятори змусили компанію Apple заблокувати доступ до сервісів Apple iBooks Store та iTunes [23]. Корпорація також згодилася виконувати китайське законодавство на предмет розташування серверів на території Китаю, розмістивши власні дата-центри у провінціях Гуйчжоу та Внутрішній Монголії [15]. Зберігши власну присутність на китайському ринку, що становить 20 % світового, Apple вдалося отримати лідерські позиції з продажів власних продуктів, зокрема, у жовтні 2021 року iPhone став найбільш продаваним смартфоном у КНР. Це дозволило компанії отримати 68 млрд доларів – 19 % від загального прибутку з продажів [15].

Інший приклад – робота пошуковика Bing від компанії Microsoft, який сьогодні є чи не єдиною іноземною пошуковою системою, що функціонує на території Китаю. Компанії вдається залишатися на ринку завдяки дотриманню вимог китайського законодавства. Таким чином, у грудні 2021 року в Microsoft заявили, що тимчасово призупиняють функцію автоматичних пропозицій у пошуковику Bing через звернення "відповідної державної установи" [37].

Водночас критики запевняють, що впровадження "Великого китайського фаєрволу" зображає параною влади щодо потенціалу інтернету поширювати опозиційні матеріали щодо комуністичного режиму. У Китаї існує окрема група користувачів соціальних мереж, яка, за попередніми підрахунками, публікує близько 500 млн провладних коментарів у мережі на рік. До того ж задля проведення цензурування контенту наразі з владою співпрацює близько 50 тисяч осіб, які обмежують доступ до вебсайтів або ж змушують пошукові системи фільтрувати інформацію, яку влада вважає шкідливою [20].

Комуністична партія Китаю, побоюючись втратити монополію на владу в разі політичної лібералізації, вибудувала в країні повноцінну мережу тотального державного електронного стеження та комплексну систему інтернет-цензури, щоб виявляти та припиняти

будь-яку несанкціоновану критику. Побутує також думка, що надмірна регуляція кіберпростору обмежує державу в економічному секторі, стримуючи розвиток інновацій, а також унеможливлює взаємообмін важливими ідеями та розробками.

У результаті Китай у 2022 році посів перше місце серед 70 країн у рейтингу правозахисної організації Freedom House за рівнем інтернет-цензури [26].

Ще однією країною, де намагаються впровадити національний інтернет, є Ісламська Республіка Іран. Розроблення Національної інформаційної мережі розпочалася там ще у 2005 році. Проєктом визначено створення на території Ірану національного "умовно безпечного" інтернету, який відповідає критеріям "ісламського контенту", що означає блокування або фільтрацію інформації за політичними, культурними чи релігійними критеріями.

Перший етап запуску мережі відбувся у серпні 2016 року. Він передбачав відкриття доступу для користувачів до електронних державних послуг, внутрішніх цифрових сервісів і контенту. Запуск другої фази включав міграцію онлайн-сервісів на локальний хостинг, що розташовувався на території Ірану. На третьому етапі реалізовано доступ до всіх електронних державних сервісів за допомогою національної інформаційної мережі [42].

Принциповою відмінністю цієї розробки від її китайського аналога є те, що іранська національна мережа базується на локальній мережі, яка забезпечує зв'язок між різноманітними службами всередині країни, при цьому вона є повністю незалежною від глобальної мережі. Водночас для того, аби нівелювати попит інтернет-користувачів на міжнародні соціальні сервіси, Іран також активно розвиває власні аналогічні онлайн-ресурси. Зокрема, іранські телекомунікаційні компанії запустили соціальні мережі Cloob Facekoob, Facenama, а також Soroush, iGap, BisPhone Plus, Wispi, Esom, Saina. Також створено відеохостинговий сайт Aparat – аналог YouTube, інтернет-сервіси обміну повідомленнями та медіафайлами Mobogram та TD Messenger [19]. Влада країни також заохочує людей користуватися місцевими послугами за допомогою порушення мережевого нейтралітету: поділу місцевого та міжнародного трафіку. Наприклад, якщо користувач прагне споживати локальні сервіси, то він має доступ до швидшої мережі та дешевшого трафіку, ціна якого майже удвічі нижча. Відповідно, якщо користувач споживає міжнародний трафік – обмін даними буде повільнішим і дорожчим [30].

На думку колишнього президента держави Хасана Рухані, необхідність реалізації проєкту викликана питаннями захисту національної автономії. За його словами, звичайним користувачам більше не знадобляться іноземні мережі для задоволення їхніх потреб, а сама мережа дозволить забезпечити високошвидкісні комунікації всередині країни [21].

Утім, західні експерти зазначають, що одним з основних недоліків іранських національних сервісів, зокрема електронної пошти, є необхідність вказувати під час реєстрації, окрім адреси, особистий ідентифікаційний номер і проходити обов'язкове звіряння вказаних реєстраційних даних з оригіналами документів [32]. Очевидно, що такий крок дозволяє владі Ірану ретельніше відстежувати діяльність користувачів у мережі задля подальшої протидії поширенню альтернативної інформації та посиленню тотальної цензури усередині країни.

Окрім експертного середовища, проєкт піддався критиці й з боку урядовців. Колишній Міністр зв'язку та інформаційних технологій Ірану (2005–2009) Мохаммад Солеймані в інтерв'ю іранській студентській агенції новин "ISNA" зазначив, що ізоляція від глобального інтернету стала б санкцією, накладеною Іраном на самого себе, і це було б нелогічно [27].

На тлі масових демонстрацій, які розпочалися у вересні 2022 року, іранська влада у спробі придушення протестного руху майже повністю вимкнула Інтернет в країні, а також обмежила доступ до таких платформ, як Instagram і WhatsApp. Остання, зокрема, використовувалась іранськими компаніями для здійснення експорту своїх товарів. За підрахунками експертів, загальні збитки для країни через вимкнення Інтернету вже сягають понад 3 млрд доларів [11]. Попри те, що Організація Об'єднаних Націй визнає доступ людини до Інтернету її базовим правом [40], влада Ірану продовжує провадити політику інформаційної ізоляції держави та її громадян. Із цією метою у 2012 році в країні створено Вищу раду у справах кіберпростору, яку технічно очолює чинний президент Ібрагім Райсі, який, по суті, підпорядковується Верховному лідеру – Алі Хаменеї. Рада має право, зокрема, видавати директиви, що стосуються регуляції інтернет-простору, які не є законами, але залишаються обов'язковими до виконання на території країни [33].

У 2022 році регулятор розпочав реалізацію окремих положень нового закону про захист кіберпростору. Міжнародні технологічні компанії зобов'язуються мати законного представника в Ірані для того, аби контролювати дотримання законодавства компанією та співпрацювати з владою у питаннях цензури інтернет-простору і нагляду за користувачами мережі. Якщо така платформа не виконує норми законодавства чи взяті на себе зобов'язання, до неї спочатку застосують обмеження у вигляді зниження швидкості доступу до її інформаційних ресурсів. Така санкція буде діяти, доки в Національній інформаційній мережі не буде створено внутрішнього ресурсу-аналогу. Відтак, коли він запрацює, доступ до міжнародної платформи буде повністю заблоковано.

Таким чином закон спонукає іранських інтернет-користувачів використовувати місцеві служби або міжнародні, що відповідають вимогами законодавства. До того ж документ забороняє приватним компаніям регулювати пропускну здатність підключення пристрою до Інтернету. Подібні обмеження сприяють централізації комунікаційної мережі Ірану, зменшують приватні інвестиції в інформаційну інфраструктуру та послуги, а також посилюють цифрову диспропорцію між Ісламською Республікою Іран та іншими країнами.

Окрім регуляції інформаційного середовища, закон також має на меті криміналізувати розроблення, застосування та продаж технічних засобів, які маскують місце перебування користувачів Інтернету і дають змогу користувачам переглядати заблоковані вебсайти. Ідеться, наприклад, про проксі-сервіси чи віртуальні приватні мережі (VPN). Якщо факт належності до таких інструментів буде доведено, користувача можуть ув'язнити на строк до двох років.

Зі статей документа також випливає, що контроль над ключовою комунікаційною інфраструктурою в країні, зокрема і міжнародними шлюзами, буде делеговано спеціальному державному регулятору, який контролюється іранськими військовими та службами безпеки. У результаті обмежувати доступ до Інтернету стане ще простіше, а сама методика здійснення цих дій не буде прозорою. Водночас подальша централізація комунікаційної інфраструктури також спрощує провадження політики цензури [28].

Безумовно, через призму стратегії розбудови інформаційного суспільства дії іранської влади спрямовані насамперед на захист панівного режиму від процесів, які можуть становити загрозу його існуванню. Контроль над глобальною мережею, а також створення власного національного інтернету, безперечно, можна вважати однією з основоположних ознак авторитарних країн. Цю тезу підтверджує також і третє місце серед 70 країн у рейтингу правозахисної організації Freedom House за рівнем інтернет-цензури [26].

Політика Російської Федерації у сфері цифровізації також є додатковим прикладом реалізації внутрішньодержавного інтернету. У 2014 році Президент РФ Владимир Путін зазначив, що вважає глобальну мережу Інтернет проєктом ЦРУ, у зв'язку з чим він закликав росіян "боротися за власні інтереси у кіберпросторі" [17]. Відтак тривалий час реалізація російського "суверенного інтернету" перебувала на стадії обговорення. У 2018 році Всеросійський центр вивчення громадської думки провів опитування, згідно з яким 36 % росіян підтримали пропозицію Радбезу РФ про незалежний інтернет усередині країн-членів БРІКС, який був би незалежним від США [6].

Утім, перший вагомий крок у цьому напрямі було зроблено у 2019 році, коли Держдума РФ ухвалила в третьому, останньому, читанні закон № 608767-7 "Про внесення змін до Федерального закону "Про зв'язок" і Федеральний закон "Про інформацію, інформаційні технології та про захист інформації", що відомий під неформальною назвою "Закон про суверенний інтернет" [9]. Метою його ухвалення, згідно з офіційною версією, є створення незалежної інфраструктури для безперебійного функціонування Інтернету в Росії. Водночас, як зазначається на офіційному сайті Держдуми, "документ розроблено з урахуванням агресивного характеру ухваленої у вересні 2018 року Стратегії національної кібербезпеки США" [12]. Зокрема, закон пропонує такі зміни:

- оператори зв'язку зобов'язані встановити державне обладнання на точках обміну інтернет-трафіком для аналізу і фільтрації трафіку всередині країни і на лініях зв'язку, що перетинають кордони Російської Федерації;
- оператори зв'язку зобов'язуються вносити до реєстру і використовувати виключно ці точки обміну (порядок визначає Уряд);
- Роскомнагляд реалізує "централізоване управління" російським сегментом Інтернету;
- Роскомнагляд реалізує обмеження доступу до заборонених у Російській Федерації інтернет-ресурсів;
- для здійснення процедур будуть проводити навчання;
- створюється національна система доменних імен (DNS) [9].

Ухвалення цього закону дозволяє Росії досягнути принаймні трьох різних цілей. По-перше, створення механізму відстежування в інтернеті в межах своїх кордонів. З цією метою поправка "про обов'язкове встановлення державного обладнання" сприяє посиленню державного контролю інформації і дозволить запобігти її поширенню в разі такої потреби. Для прикладу, реалізація нового законодавства дозволяє російській владі зменшити активність опозиції в соціальних мережах. Водночас, навіть якщо цю поправку подекуди буде складно реалізувати з технологічного погляду, сам закон є частиною стратегії режиму правління Володимира Путіна і впливатиме на російське суспільство.

По-друге, держава прагне стати ключовим регулятором Інтернету в Росії. Отримання Роскомнаглядом повноважень щодо управління російським сегментом Інтернету є спробою ізолювати національну мережу від глобальної мережі. Відтак влада зможе не лише відкривати й закривати "цифрові кордони", а і визначати потоки інформації всередині на свій розсуд.

По-третє, Росія прагне поширити таку державну модель інтернету на міжнародному рівні. Поправка, яка стосується створення національної системи доменних імен (DNS), допоможе створити власний російський сегмент Інтернету, який буде існувати паралельно з глобальною мережею, або ж бути несумісним із нею. Цим кроком РФ не стільки бажає відмежувати себе від світу, а радше створює прецедент для інших країн. Адже якщо інші держави виявлять бажання використовувати російський інтернет-ринок, то вони будуть вимушені співпрацювати, аби розвивати власні технології, та координувати свою інтернет-політику на міжнародному рівні.

На думку віцепрезидента з досліджень та аналізу міжнародної правозахисної неурядової організації Freedom House Адріана Шахбаза, закон сприяє звуженню простору свободи висловлення думок у Росії. "Суверенний інтернет" є ще однією цеглиною у прагненні російської влади створити "Великий фаєрвол". На відміну від Китаю, який запровадив високий рівень обмежень в Інтернеті одразу з моменту його появи в країні у 1990-х роках, офіційна Москва намагається встановити контроль над онлайновим інформаційним середовищем [8].

Водночас викладач Університету Джорджа Вашингтона Девід Саконьї вважає, що Росія, імовірно, рухається у бік "китайської моделі" щодо цензури інтернету. "Ми маємо справу зі своєрідними заходами безпеки, які російська влада вживатиме в тому разі, якщо якісь події будуть виходити з-під контролю. Вони хочуть мати ці заходи на законодавчому рівні, але я не вважаю, що їх насправді буде вжито в короткостроковій перспективі, а якщо і буде, то вони виявляться неефективними. Сьогодні ми не маємо справу з "китайською моделлю", але той факт, що Російська Федерація має такі інструменти, як цей закон, у результаті може призвести до того, що Росія стане більш схожою на Китай, ніж на країни Східної Європи" [8].

Повномасштабне вторгнення Росії в Україну у 2022 році також стало каталізатором для тоталітарних настроїв російської влади в питанні використання Інтернету всередині країни та її бажанні контролювати внутрішній інформаційний простір. Інтернет-платформи стали важливим майданчиком розвінчування російської пропаганди. Задля того, аби приховати злочини російської армії, а також ускладнити доступ до правдивої інформації громадян, Уряд РФ почав вживати додаткових кроків для регулювання інформаційного простору та продовження реалізації проєкту з упровадження суверенного інтернету. Зокрема, 6 березня 2022 року білоруський телеграм-канал NEXTA опублікував урядову телеграму до федеральних органів виконавчої влади, згідно з якою пропонується:

- перевірити доступи до особистих кабінетів реєстраторів доменних імен для публічних ресурсів у мережі інтернет;
- оновити та ускладнити парольну політику;
- перейти на сервери DNS, що розміщені на території РФ;

- видалити з шаблонів сторінок HTML весь код Javascript, що завантажується з іноземних ресурсів (зокрема й рекламні банери та лічильники);
- у разі використання іноземного хостингу перемістити розміщені на ньому ресурси на російський хостинг;
- ресурси, не розміщені в доменній зоні .ru, перенести до неї [38].

Окрім цього, у Росії розпочалося блокування низки інтернет-сервісів, зокрема Роскомнагляд обмежив доступ до Instagram [14], Facebook, Twitter [16] та TikTok [43]. За даними групи Top10VPN, яка займається питаннями цифрових прав і конфіденційності, з початку російсько-української війни в Росії було заблоковано 960 новинних доменів [13]. Загалом у російській громадській організації, яка провадить діяльність у сфері захисту цифрових прав і розширення цифрових можливостей "Роскомсвобода", заявили, що після початку повномасштабного вторгнення Росії в Україну Роскомнагляд заблокував понад 3 тисячі сайтів [5].

Уже в червні 2022 року спеціальний представник президента Російської Федерації із цифровізації Дмітрій Пєсков заявив, що Росія не планує самостійно від'єднуватись від глобальної мережі, але якщо країну відімкнуть ззовні, то РФ готова до такого сценарію. "Ми підготувалися так, щоб російський Інтернет продовжив існування, навіть якщо його в нас вимкнуть. […] Якщо нам його вимкнуть ззовні, то ми виживемо: локальні ресурси працювати будуть, а конектори до світового інтернету ми добудуємо" [3].

Попри це Росія планує витрати 1,2 млрд рублів протягом 2023–2024 років на створення новітньої системи контролю трафіку в Інтернеті, яка дозволить контролювати передавання даних між усіма операторами і провайдерами зв'язку. Її розроблення покладено на створений у межах закону "Про суверенний інтернет" Центр моніторингу і управління мережею зв'язку загального користування [7].

Такі дії призвели до того, що за рейтингом правозахисної організації Freedom House у 2022 році Росія посідає 6-те місце серед 70 країн за рівнем інтернет-цензури [26].

Принагідно також варто згадати про досвід Північної Кореї у питанні фрагментації інформаційного простору. Інтернет в КНДР з'явився у 2000 році у вигляді внутрішньої мережі "Кванмьон". В основу її роботи закладено досить простий принцип: користувач має доступ до певного набору сайтів, водночас існують жорсткі обмеження на завантаження інформації із зовнішніх мереж. Сьогодні мережа налічує, за різними підрахунками, від 1000 до близько 5500 вебресурсів партійного чи освітнього спрямування [1].

Окрім власне північнокорейських сайтів, у "Кванмьон" розміщуються і вебресурси із "зовнішнього" Інтернету, переважно технічної чи довідкової тематики (маловідомі китайські та південнокорейські, деякі статті з Вікіпедії). Перед публікацією сайти вивантажує Корейський комп'ютерний центр – основний дослідницький центр інформаційних технологій, який також здійснює цензурну перевірку, фільтруючи контент на предмет наявності шкідливої інформації, і лише потім розміщує ресурси в національній мережі [34].

Варто зазначити, що у 2013 році доступ до "Кванмьон" мав вичерпний перелік користувачів. Під'єднатися до мережі можна було лише за умови використання комп'ютерів спеціалізованих установ, які розташовувалися у великих містах, а отже жителі провінцій не мали доступу до мережі. Наразі в КНДР офіційно дозволено використовувати "Кванмьон" звичайним громадянам, на відміну від глобальної мережі, адже доступ до неї можуть отримати лише організації після отримання офіційного дозволу від влади. У 2019 році кількість дозволених для під'єднання до глобальної мережі IP-адрес становила лише 1024. Така можливість надається зазвичай партійним діячам, пропагандистам, представникам Міністерства закордонних справ чи іноземних установ, деяким науковим та освітнім організаціям [39].

Прикметним також є той факт, що до 2017 року в КНДР існував лише один інтернет-провайдер – китайська компанія China Unicom, а з 01 жовтня 2017 року понад половина північнокорейських інтернет-з'єднань встановлюються через мережі російської компанії "Трансгелеком", яка є дочірньою структурою ВАТ "Російські залізниці" [10].

З огляду на те, що країна фактично закрита для зовнішнього світу, вона рідше потрапляє до різних рейтингів. Це пов'язано і неможливістю отримати ті чи інші дані, що потрібні для здійснення аналізу. Ті ж показники, які вдається отримати, свідчать про вкрай негативні тенденції в країні. Наприклад, у Світовому індексі свободи преси КНДР посіла 180 позицію зі 180 країн [31].

Висновки. Кіберпростір стає дедалі більш затребуваним комунікаційним середовищем, зважаючи на повсюдний процес інформатизації. Інтеграція інтернет-технологій у суспільне життя надає не лише переваги їхнім користувачам, а і зумовлює появу нових викликів для інформаційної безпеки як демократичних, так і авторитарних держав: зовнішній вплив на суспільства та роботу державних інституцій, кібератаки, шпіонаж, поширення пропаганди та дезінформації, загроза для контролю над інформацією, створення передумов для політичного плюралізму тощо.

У зв'язку з цим виникає необхідність регулювання Інтернету. Однією із найпоширеніших таких практик є його балканізація. На наш погляд, це поняття слід трактувати *як процес, у результаті якого відбувається фрагментація простору Глобальної мережі на окремі частини (за однією чи декількома ознаками), які не залежать одна від одної. Такий поділ призводить до виокремлення суверенних національних чи регіональних сегментів Інтернету. Їхні межі можуть бути цілком ідентичні кордонам держав або ж не збігатися з ними.*

Як видається, балканізація Інтернету є центральною частиною політики недемократичних держав у галузі цифрового авторитаризму і дозволяє таким політичним режимам вирішувати цілу низку питань. Для прикладу, у Китаї, Росії, Ірані та Північній Кореї вона виступає як один із важливих інструментів внутрішньої і зовнішньої легітимізації влади, механізм моніторингу суспільних настроїв або тотального стеження за громадянами. Серед іншого, фрагментований інтернет-простір вищезазначених країн підлягає тотальному контролю з боку влади через діяльність відповідних державних регуляторів: Центральної комісії з питань кіберпростору у Китаї, Вищої ради у справах кіберпростору в Ірані, Роскомнагляду в Росії та Корейського комп'ютерного центру в КНДР. Спираючись на розгалужену законодавчу систему та мережу державних інституцій влади, авторитарні країни намагаються укорінити систему інтернет-контролю та цензуру. Повсюдний характер подібного державного втручання ефективно нівелює і без того обмежену свободу слова в цих державах, а також призводить до більшої інформаційної, культурної, наукової, економічної автаркії суспільств.

ISSN 1728-3817

Варто зазначити, що балканізація Інтернету може бути також економічним інструментом, що в короткостроковій перспективі здатен стимулювати розвиток внутрішнього ринку інформаційно-комунікаційних послуг, але в довгостроковій – загрожує непропорційно більшими негативними наслідками через проблеми, які породжує ізоляція від решти світу. Це може бути підвищений рівень кіберзлочинності, підґрунтям для якого стане поява нових інформаційних загроз, що вражатимуть дедалі більше держав, адже важливою умовою ефективної протидії інформаційним впливам є консолідація і співпраця міжнародної спільноти.

Реалізація закликів до створення відокремлених мереж інтернету в межах певних міжнародних організацій (наприклад, БРІКС) може призвести до виникнення біполярного інтернет-простору на планеті. Такі зміни повністю підірвали б основну роль Інтернету як інструменту вільної комунікації людства. Окрім цього, наслідком поділу світової мережі стала б поява чітко розмежованих паралельних інформаційних просторів. Сепаровані інтернет-кордони здатні сповільнити не лише глобалізаційні процеси, а і розвиток цивілізації загалом – через ускладнення або унеможливлення безперешкодної комунікації, меншу конкуренцію ідей, відсутність обміну інноваціями та доступу до знань.

Список використаних джерел

1. 15 заборон і обмежень, які є тільки в Північній Кореї. *Творчість. Свобода. Життя.* URL: https://social.org.ua/5806-15-zaboron-i-obmezhen-yaki-ie-tilki-v-pivnichniy-koreyi.html (дата звернення: 12.01.2023).
2. *Каменецький М. С.* Балканізація. *Велика українська енциклопедія*. URL: https://vue.gov.ua/Балканізація (дата звернення: 23.11.2022).
3. В Кремле заявили о невозможности отключения России от интернета. *РБК.* 27 июня 2022. URL: https://www.rbc.ru/rbcfreenews/62b926289a79477950215f92 (дата звернення: 25.01.2023).
4. *Ваннек Л.* Freedom House: наступ на свободу в інтернеті під гаслом боротьби з "фейковими новинами". *Радіо Свобода.* 01 листопада 2018. URL: https://www.radiosvoboda.org/a/freedom-on-the-net-2018/29575606.html (дата звернення: 19.01.2023).
5. Военной цензуре подверглось более 3000 сайтов. Роскомсвобода. *Роскомсвобода. 5 мая 2022.* URL: https://roskomsvoboda.org/post/voennaya-cenzura-3000-saytov/ (дата звернення: 03.01.2023).
6. ВЦИОМ: треть россиян хотят "суверенный" и независимый от США интернет. *Настоящее Время.* 29 января 2018. URL: https://www.currenttime.tv/a/29004253.html (дата звернення: 25.01.2023).
7. Роскомнадзор создаст новую систему контроля интернет-трафика за 1,2 млрд рублей. *Настоящее Время*. 7 ноября 2022. URL: https://www.currenttime.tv/a/roskomnadzor-sozdast-novuyu-sistemu-kontrolya-internet-trafika/32119010.html (дата звернення: 15.01.2023).
8. *Егисман В., Владимиров В.* "Суверенный интернет" в России: технология и политика. *ГОЛОС АМЕРИКИ*. 16 апреля 2019. URL: https://www.golosameriki.com/a/russian-sovereign-internet--last-reading/4878381.html (дата звернення: 12.01.2023).
9. Законопроєкт № 608767-7. URL: https://sozd.duma.gov.ru/bill/608767-7 (дата звернення: 15.01.2023).
10. *Коріновська Н.* Компанія з РФ стала другим інтернет-провайдером у КНДР. *Громадське телебачення*. 04 жовтня 2017. URL: https://hromadske.ua/posts/kompaniia-z-rf-stala-druhym-internet-provaiderom-u-kndr (дата звернення: 25.01.2023).
11. Потери Ирана из-за ограничения интернета превысили 3 млрд долларов. *Oxu.Az.* 24 октября 2022. URL: https://ru.oxu.az/world/656527 (дата звернення: 10.01.2023).
12. Принят закон о "суверенном интернете". *Государственная Дума.* 16.04.2019. URL: http://duma.gov.ru/news/44551/ (дата звернення: 25.01.2023).
13. Росія блокує навіть сайти про котиків, щоб приховати правду про війну, – дослідження. *Texty.org.ua.* 2022-05-09. URL: https://texty.org.ua/fragments/106620/rosiya-blokuye-navit-sajty-pro-kotykiv-shob-pryhovaty-pravdu-pro-vijnu-doslidzhennya/ (дата звернення: 25.11.2022).
14. Роскомнадзор ограничит доступ к Instagram из-за призывов к насилию в отношении россиян. *Роскомнадзор*. 11 марта 2022. URL: https://rkn.gov.ru/news/rsoc/news74176.htm (дата звернення: 17.01.2023).
15. *Сапітон М.* З'ясувалося, що Apple підписала у Китаї угоду на $275 млрд задля збереження ринку. Як домовляється з КНР найдорожча компанія планети. *Forbes.ua.* 08 грудня 2021. URL: https://forbes.ua/news/vyyasnilos-chto-apple-podpisala-v-kitae-sdelku-na-275-mlrd-radi-sokhraneniya-rynka-kak-dogovarivaetsya-s-knr-samaya-dorogaya-kompaniya-planety-08122021-2931 (дата звернення: 18.11.2022).
16. *Свобода Р.* У більшості росіян перестали відкриватися Facebook, Twitter, а також сайти Радіо Свобода, "Медузи" та інші. *Радіо Свобода.* 4 березня 2022. URL: https://www.radiosvoboda.org/a/news-rosija-cenzura/31734943.html (дата звернення: 25.01.2023).
17. Суверенный интернет – новый проєкт российской власти *BBC News Русская служба.* 29 апреля. 2014. URL: https://www.bbc.com/russian/society/2014/04/140429_cheburashka_russian_internet (дата звернення: 11.01.2023).
18. *Шаршаткін Д. Ю.* Теоретичні основи дослідження інформаційних війн та інформаційної безпеки держави. *International Scientific Journal "Internauka.* URL: https://www.inter-nauka.com/uploads/public/15495684476315.pdf (дата звернення: 18.02.2023).
19. *Shahbazian Armen*. Iran. BBC Monitoring. 2023. URL: https://monitoring.bbc.co.uk/product/c20041be (дата звернення: 09.11.2022).
20. The Great Firewall of China. *Bloomberg*. 6 ноября 2018. URL: https://www.bloomberg.com/quicktake/great-firewall-of-china (date of access: 11.01.2023).
21. Boom D. V. Iran's internet freedom is on life support. *CNET*. Dec. 8, 2019. URL: https://www.cnet.com/tech/services-and-software/irans-president-plans-to-cut-countrys-internet-off-from-the-rest-of-the-world/ (date of access: 22.01.2023).
22. *Knockel Jeffrey and Xiong Ruohan*. Can't Picture This 2: An Analysis of WeChat's Realtime Image Filtering in Chats. *The Citizen Lab*. July 15, 2019. URL: https://citizenlab.ca/2019/07/cant-picture-this-2-an-analysis-of-wechats-realtime-image-filtering-in-chats/ (date of access: 22.01.2023).
23. *Carsten P.* Apple's book, film services go dark in China. *Reuters*. APRIL 22, 2016. URL: https://www.reuters.com/article/us-apple-china-idUSKCN0XJ0CD (date of access: 09.11.2022).
24. *Shahbaz Adrian, Funk Allie, Vesteinsson Kian*. Countering an Authoritarian Overhaul of the Internet. *Freedom House*. 2022. URL: https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet (date of access: 25.01.2023).
25. *Cunningham Laura*. Countering Chinese Censorship. *USAGM*. August 8, 2019. URL: https://www.usagm.gov/2019/08/08/countering-chinese-censorship/ (date of access: 07.11.2022).
26. Countries. Freedom House. URL: https://freedomhouse.org/countries/freedom-net/scores?sort=asc&order=Total%20Score%20and%20Status (date of access: 25.01.2023).
27. *Сейфи Фарназ, Бушуев Михаил*. *И*ран ограждает себя "национальным интернетом" *Deutsche Welle.* 27.09.2012. URL: https://www.dw.com/ru/иран-ограждает-себя-от-мира-национальным-интернетом/a-16266264 (дата звернення: 07.11.2022).
28. *Esfandiari G.* Iran Accused Of Secretly Implementing Controversial Draft Internet Bill. *RadioFreeEurope/RadioLiberty*. September 09, 2022 URL: https://www.rferl.org/a/iran-internet-bill-controversy-secretly-implementing/32026313.html (date of access: 07.11.2022).
29. *Hoang Nguyen Phong, Niaki Arian Akhavan, Dalek Jakub at all*. How Great is the Great Firewall? Measuring China's. *Cornel University*. 3 Jun 2021. URL: https://arxiv.org/abs/2106.02167 (дата звернення: 09.11.2022).
30. *Bushwick Sophie*. How Iran Is Using the Protests to Block More Open Internet Access. *Scientific American*. October 13, 2022. URL: https://www.scientificamerican.com/article/how-iran-is-using-the-protests-to-block-more-open-internet-access/ (date of access: 25.01.2023).
31. 2022 PRESS FREEDOM INDEX. *Reporters sans frontières. RSF*. URL: https://rsf.org/en/index (date of access: 21.01.2023).
32. Indigenous E-Mail Service Remains an Outsider. *Financial Tribune*. September 22, 2017 URL: https://financialtribune.com/articles/economy-sci-tech/72827/indigenous-e-mail-service-remains-an-outsider (date of access: 22.01.2023).
33. Iran: Cyberspace authorities 'silently' usher in draconian internet bill. *ARTICLE 19*. SEPTEMBER 09, 2022. URL: https://www.article19.org/resources/iran-draconian-internet-bill/ (date of access: 22.01.2023).
34. Korea Computer Center. *DBpedia*. URL: https://dbpedia.org/page/Korea_Computer_Center (date of access: 13.01.2023).
35. *Kumar A.* Libertarian, or Just Bizarro?. *WIRED*. APR 25, 2001. URL: https://www.wired.com/2001/04/libertarian-or-just-bizarro/ (date of access: 13.01.2023).
36. *Liridona V.* Balkanization. *SpringerLink*. 14 October 2019. URL: https://link.springer.com/referenceworkentry/10.1007/978-3-030-11795-5_34-1 (date of access: 02.01.2023).
37. Microsoft's Bing suspends auto suggest function in China at government's behest. *Reuters*. December 17, 2021. URL: https://www.reuters.com/technology/microsoft-bing-says-suspended-auto-suggest-function-china-government-behest-2021-12-17/ (date of access: 02.01.2023).
38. NEXTA. #Russia began active preparations for disconnection from the global Internet No later than March 11, all servers and domains must. *Twitter*. Mar 6, 2022. URL: https://twitter.com/nexta_tv/status/1500553480548892679 (date of access: 25.01.2023).
39. North Korea ASN summary – IP addresses and networks by country – IPInfo.io. Comprehensive IP address data, IP geolocation API and database – IPinfo.io. 2023 URL: https://ipinfo.io/countries/kp (date of access: 25.01.2023).

40. *La Rue Frank*. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. *United Nations A/HRC/17/27 General Assembly*. 16 May 2011. URL: https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf (дата звернення: 19.01.2023).

41. *Pringle R. W.* Balkanization. *Encyclopedia Britannica*. URL: https://www.britannica.com/topic/Balkanization (date of access: 17.01.2023).

42. *Sheikhi M.* Iran launches National Information Network. *Mehr News Agency*. Aug 28, 2016. URL: https://en.mehrnews.com/news/119304/Iran-launches-National-Information-Network (дата звернення: 09.11.2022).

TikTokComms. 3/ We will continue to evaluate the evolving circumstances in Russia to determine when we might fully resume our services. *Twitter*. Mar 6, 2022. URL: https://twitter.com/TikTokComms/status/1500535440205836288 (date of access: 19.01.2023).

43. 中华人民共和国网络安全法-中共中央网络安全和信息化委员会办公室. 中共中央网络安全和信息化委员会办公室. *Cyberpace Administration of China*. URL: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm (дата звернення: 11.11.2022).

References

1. 15 zaboron i obmezhen, yaki ye tilky v Pivnichnii Korei. Tvorchist. Svoboda. Zhyttia. – Retrieved from: https://social.org.ua/5806-15-zaboron-i-obmezhen-yaki-ie-tilki-v-pivnichniy-koreyi.html

2. Balkanizatsiia. VUE. – Retrieved from: https://vue.gov.ua/Балканізація

3. V Kremle zayavili o nevozmozhnosti otklyucheniya Rossii ot interneta. RBK. – Retrieved from: https://www.rbc.ru/rbcfreenews/62b926289a79477950215f92

4. Vannek L. Freedom House: nastup na svobodu v interneti pid haslom borotby z "feikovymy novynamy". Radio Svoboda. – Retrieved from: https://www.radiosvoboda.org/a/freedom-on-the-net-2018/29575606.html

5. Voennoy tsenzure podverglos bolee 3000 saytov. Roskomsvoboda. – Retrieved from: https://roskomsvoboda.org/post/voennaya-cenzura-3000-saytov

6. Vremya N. VTsIOM: tret rossiyan hotyat "suverennyiy" i nezavisimyiy ot SShA internet. Nastoyaschee Vremya. – Retrieved from: https://www.currenttime.tv/a/29004253.html

7. Vremya N. Roskomnadzor sozdast novuyu sistemu kontrolya internet-trafika za 1,2 mlrd rubley. Nastoyaschee Vremya. – Retrieved from: https://www.currenttime.tv/a/roskomnadzor-sozdast-novuyu-sistemu-kontrolya-internet-trafika/32119010.html

8. Egisman V., Vladimirov V. "Suverennyiy internet" v Rossii: tehnologiya i politika. GOLOS AMERIKI. – Retrieved from: https://www.golosameriki.com/a/russian-sovereign-internet--last-reading/4878381.html

9. Zakonoproekt № 608767-7. – Retrieved from: https://sozd.duma.gov.ru/bill/608767-7.

10. Kompaniia z RF stala druhym internet-provaiderom u KNDR. Hromadske telebachennia – Ostanni novyny dnia, vsi nadzvychaini novyny v Ukraini. – Retrieved from: https://hromadske.ua/posts/kompaniia-z-rf-stala-druhym-internet-provaiderom-u-kndr

11. Poteri Irana iz-za ogranicheniya interneta prevyisili 3 mlrd dollarov. Oxu.Az. – Retrieved from: https://ru.oxu.az/world/656527

12. Pryniat zakon o "suverennom ynternete". Hosudarstvennaia Duma. – Retrieved from: http://duma.gov.ru/news/44551

13. Rosiia blokuie navit saity pro kotykiv, shchob prykhovaty pravdu pro viinu, – doslidzhennia. Texty.org.ua – statti ta zhurnalistyka danykh dlia liudei – Teksty.org.ua. – Retrieved from: https://texty.org.ua/fragments/106620/rosiya-blokuye-navit-sajty-pro-kotykiv-shob-pryhovaty-pravdu-pro-vijnu-doslidzhennya

14. Roskomnadzor ogranichit dostup k Instagram iz-za prizyivov k nasiliyu v otnoshenii rossiyan. Roskomnadzor. – Retrieved from: https://rkn.gov.ru/news/rsoc/news74176.htm

15. Sapiton M. Ziasuvalosia, shcho Apple pidpysala u Kytai uhodu na $275 mlrd zadlia zberezhennia rynku. Yak domovliaietsia z KNR naidorozhcha kompaniia planety – Forbes.ua. Forbes.ua | Biznes, miliardery, novyny, finansy, investytsii, kompanii. – Retrieved from: https://forbes.ua/news/vyyasnilos-chto-apple-podpisala-v-kitae-sdelku-na-275-mlrd-radi-sokhraneniya-rynka-kak-dogovarivaetsya-s-knr-samaya-dorogaya-kompaniya-planety-08122021-2931

16. Svoboda R. U bilshosti rosiian perestaly vidkryvatysia Facebook, Twitter, a takozh saity Radio Svoboda, "Meduzy" ta inshi. Radio Svoboda. – Retrieved from: https://www.radiosvoboda.org/a/news-rosija-cenzura/31734943.html

17. Suverennyiy internet – novyiy proekt rossiyskoy vlasti – BBC News Russkaya sluzhba. BBC News Russkaya sluzhba. – Retrieved from: https://www.bbc.com/russian/society/2014/04/140429_cheburashka_russian_internet

18. *Sharshatkin D. Yu.* Theoretical foundations for the investigation of information wars and information security of the state. International Scientific Journal *Internauka*. URL: https://www.inter-nauka.com/uploads/public/15495684476315.pdf (date of entry: 02/18/2023)

19. BBC Monitoring – Essential Media Insight. BBC Monitoring – Essential Media Insight. – Retrieved from: https://monitoring.bbc.co.uk/product/c20041be

20. Bloomberg – Are you a robot?. Bloomberg – Are you a robot?. – Retrieved from: https://www.bloomberg.com/quicktake/great-firewall-of-china

21. Boom D. V. Iran's internet freedom is on life support. CNET. – Retrieved from: https://www.cnet.com/tech/services-and-software/irans-president-plans-to-cut-countrys-internet-off-from-the-rest-of-the-world

22. Can't Picture This 2: An Analysis of WeChat's Realtime Image Filtering in Chats – The Citizen Lab. The Citizen Lab. – Retrieved from: https://citizenlab.ca/2019/07/cant-picture-this-2-an-analysis-of-wechats-realtime-image-filtering-in-chats

23. Carsten P. Apple's book, film services go dark in China. U.S. – Retrieved from: https://www.reuters.com/article/us-apple-china-idUSKCN0XJ0CD

24. Countering an Authoritarian Overhaul of the Internet. Freedom House. – Retrieved from: https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet

25. Countering Chinese Censorship. USAGM. – Retrieved from: https://www.usagm.gov/2019/08/08/countering-chinese-censorship

26. Countries. Freedom House. – Retrieved from: https://freedomhouse.org/countries/freedom-net/scores?sort=asc&order=Total%20Score%20and%20Status

27. Deutsche Welle. Iran ograzhdaet sebya "natsionalnyim internetom" – DW – 27.09.2012. dw.com. – Retrieved from: https://www.dw.com/ru/иран-ограждает-себя-от-мира-национальным-интернетом/a-16266264

28. Esfandiari G. Iran Accused Of Secretly Implementing Controversial Draft Internet Bill. RadioFreeEurope/RadioLiberty. – Retrieved from: https://www.rferl.org/a/iran-internet-bill-controversy-secretly-implementing/32026313.html

29. How Great is the Great Firewall? Measuring China's DNS Censorship. arXiv.org. – Retrieved from: https://arxiv.org/abs/2106.02167

30. How Iran Is Using the Protests to Block More Open Internet Access. Scientific American. – Retrieved from: https://www.scientificamerican.com/article/how-iran-is-using-the-protests-to-block-more-open-internet-access

31. Index. Bienvenue sur le site de Reporters sans frontières | RSF. – Retrieved from: https://rsf.org/en/index

32. Indigenous E-Mail Service Remains an Outsider. Financial Tribune. – Retrieved from: https://financialtribune.com/articles/economy-sci-tech/72827/indigenous-e-mail-service-remains-an-outsider

33. Iran: Cyberspace authorities 'silently' usher in draconian internet bill – ARTICLE 19. ARTICLE 19. – Retrieved from: https://www.article19.org/resources/iran-draconian-internet-bill

34. Korea Computer Center. DBpedia. – Retrieved from: https://dbpedia.org/page/Korea_Computer_Center

35. Kumar A. Libertarian, or Just Bizarro?. WIRED. – Retrieved from: https://www.wired.com/2001/04/libertarian-or-just-bizarro

36. Liridona V. Balkanization. SpringerLink. – Retrieved from: https://link.springer.com/referenceworkentry/10.1007/978-3-030-11795-5_34-1

37. Microsoft's Bing suspends auto suggest function in China at government's behest. Reuters. – Retrieved from: https://www.reuters.com/technology/microsoft-bing-says-suspended-auto-suggest-function-china-government-behest-2021-12-17

38. NEXTA. #Russia began active preparations for disconnection from the global Internet No later than March 11, all servers and domains must. Twitter. – Retrieved from: https://twitter.com/nexta_tv/status/1500555480548892679

39. North Korea ASN summary – IP addresses and networks by country – IPInfo.io. Comprehensive IP address data, IP geolocation API and database – IPinfo.io. – Retrieved from: https://ipinfo.io/countries/kp

40. OHCHR Homepage. – Retrieved from: https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

41. Pringle R. W. Balkanization. Encyclopedia Britannica. – Retrieved from: https://www.britannica.com/topic/Balkanization

42. Sheikhi M. Iran launches National Information Network. Mehr News Agency. – Retrieved from: https://en.mehrnews.com/news/119304/Iran-launches-National-Information-Network

43. TikTokComms. 3/ We will continue to evaluate the evolving circumstances in Russia to determine when we might fully resume our services. Twitter. – Retrieved from: https://twitter.com/TikTokComms/status/1500535440205836288

44. Network Security Law of the People's Republic of China – Office of the Central Committee of the Communist Party of China for Network Security and Informatization. Office of the Central Committee of the Communist Party of China for Network Security and Informatization. – Retrieved from: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm.

Отримано: 14.11.22
Ухвалено до друку: 19.12.22
Опубліковано: 30.01.23

Bulletin of Taras Shevchenko National University of Kyiv
Public Administration, 1(17), 28-37
UDC 351.86:004:321.64
DOI: https://doi.org/10.17721/2616-9193.2023/17-5/7

Volodymyr Lytvynenko, PhD in Social Communication,
Communication Office
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
https://orcid.org/0000-0003-1156-105X
email: vollyt@knu.ua

Oleksandr Kantur, postgraduate student of the Department of Global and National Security
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
https://orcid.org/0000-0001-8351-6210
email: oleksandr.kantur@knu.ua

"INTERNET BALKANIZATION" AS AN INSTRUMENT OF INFORMATION SECURITY OF AUTHORITARIAN STATES

The article examines the peculiarities and problems of fragmentation of the global network "Internet" by the states dominated by authoritarian regimes. An attempt was made to generalize the interpretation of the definition of the "Balkanization of the Internet", the principles of the Chinese development of the "Golden Shield" as a state system of censorship in cyberspace were studied, the peculiarities of the implementation of the "National Information Network" in Iran and the sovereign Internet in Russia were analyzed, and the North Korean experience of the "Kwangmyong" project was considered.

Based on the results of the analysis of legal acts, open data sources and publications in the media, it was found that most often governments justify such decisions by protecting national security. At the same time, in practice, the Balkanization of the Internet levels out the already limited freedom of speech in countries where other sources of information are somehow under state control, and leads to greater information, cultural, scientific, economic autarky of societies.

Keywords: information security, state, information and communication technologies, Internet, digital authoritarianism, Balkanization of the Internet.