УДК 316
DOI https://doi.org/10.20535/2308-5053.2021.1(49).232789

МЕРЕЖЕВА КОМУНІКАЦІЯ: РИЗИКИ ТА ПЕРСПЕКТИВИ (НА ОСНОВІ СОЦІОЛОГІЧНИХ ОПИТУВАНЬ ГРОМАДСЬКОЇ ДУМКИ В КРАЇНАХ ЄВРОСОЮЗУ)

Єнін М. Н.,
кандидат соціологічних наук,
доцент кафедри соціології
Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»
ORCID ID: 0000-0002-3835-2429

Коржов Г. О.,
кандидат соціологічних наук,
доцент кафедри соціології
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»
ORCID ID: 0000-0001-5459-0702

У статті проаналізовано основні підходи щодо перспектив розвитку практик мережевої комунікації через Інтернет. Визначено вплив розвитку цифрових технологій соціальної комунікації на процеси соціально-економічного розвитку, розширення політичної участі, розподіл влади та політичну мобілізацію. Водночас особливу увагу приділено викликам і ризикам, які несуть Інтернет-технології для особистих прав та свобод людини. Зокрема, акцент зроблено на сприйнятті самими Інтернет-користувачами загроз, з якими вони стикаються у всесвітній комп'ютерній мережі, на їхніх поведінкових реакціях на кіберзлочини, в тому числі дотримання більш безпечних моделей поведінки у віртуальному просторі. Виявлено, що з часом зростає рівень компетентності користувачів цифрових послуг, їхня обізнаність у царині кібербезпеки. Спостерігається також збільшення, іноді помітне, частки Інтернет-аудиторії, охопленої різноманітними видами послуг, які все більше переміщуються онлайн. Зроблено висновок про те, що, попри зростання масштабів небезпеки і занепокоєння самих користувачів, фактичний рівень кібервіктимізації серед мешканців країн Євросоюзу залишається більш-менш стабільним. Подібна позитивна тенденція пояснюється як ефективністю заходів із попередження та боротьби із кіберзлочинністю, що впроваджуються державними та корпоративними інститутами, так і проактивною та свідомою позицією самих користувачів. Інтернет-юзери, усвідомлюючи всю глибину та масштаби ризиків, докладають різноманітних зусиль для гарантування безпеки в мережі (періодично змінюють паролі для виходу у різні онлайн-служби, звертаються по допомогу до відповідних організацій – як державних, так і приватних).

Ключові слова: мережева комунікація, соціальні мережі, інформаційне суспільство, соціальні медіа, кіберзлочини, кібербезпека, громадська думка, Євросоюз.

Актуальність та постановка проблеми. В інформаційному суспільстві комунікативний чинник охоплює всі сфери суспільного життя, впливає на зміст і динаміку соціально-політичних, економічних процесів, трансформацію звичних форм соціального контролю. Саме тому в академічному середовищі він розглядається як один із визначальних факторів соціальному розвитку. Традиція розгляду комунікативних процесів та їх впливу на суспільні практики була характерною для канадської наукової школи теорій масової комунікації, автори якої у своїх роботах відзначали залежність матеріального та духовного прогресу, а також зміни у форматах і моделях розподілу влади від розвитку технологій соціальної комунікації [1–3].

В ряді публікацій підіймається питання ролі соціальних мереж в сучасних масових політичних процесах розвитку різних соціальних груп, спільнот та рухів. Зазначається, що віртуальна комунікація через соціальні медіа, долаючи фізичний простір, може сприяти згуртуванню людей з різних соціально-класових позицій та поселенських структур навколо тих чи інших суспільно-політичних дискурсів [4]. Суттєвою є роль соціальних мереж в організації, синхронізації та інтенсифікації масової

протестної діяльності навколо існуючих політичних груп, що перебувають при владі [5; 6]. Соціальні медіа значно зменшують можливості цензури та явної ієрархії, властивої традиційному медіасередовищу, дозволяючи користувачам бути одночасно творцями та реципієнтами інформації: «тут кожен протестуючий може також виконувати функцію дрібного журналіста, обходити державну цензуру, формувати власні наративи та взаємодіяти з традиційними ЗМІ як учасниками діалогу, а не просто пасивними одержувачами інформації» [7, с. 173–174]. Водночас потенціал соціальних мереж, а також нових програмних технологій використовується для завоювання та утримання влади політичними та економічними акторами. Так, розвиту новітніх форм соціального контролю присвячені дослідження Big Data – автоматизованих засобів реєстрації поведінки великих масивів людей [8–10].

Мета статті – виявити основні підходи щодо перспектив розвитку практик мережевої комунікації через Інтернет та як його індивіди-користувачі сприймають загрози, з якими вони стикаються у всесвітній комп'ютерній мережі, як реагують на кіберзлочини та які фактори впливають на більш безпечну поведінку в Інтернеті.

Завдання статті:

1) визначити ключові виклики для особистих прав та свобод людини, пов'язаних із суспільно-політичним розвитком в умовах розвитку технологій мережевих комунікацій;

2) з'ясувати джерела занепокоєння громадськості щодо використання Інтернету з різними цілями, основні ризики мережевої комунікації та способи їх мінімізації (на прикладі дослідження громадян різних країн ЄС).

Емпірична база статті – дані кількох опитувань, проведених серед громадян країн ЄС. В їх рамках вивчалися частота та тип використання Інтернету мешканцями ЄС, їхня впевненість в Інтернет-транзакціях, обізнаність та досвід щодо кіберзлочинів, а також рівень стурбованості, який вони відчувають щодо цього виду злочинів.

Виклад основного матеріалу.

1. Основні підходи щодо перспектив розвитку практик мережевої комунікації через Інтернет та ключові виклики для особистих прав і свобод людини

Розроблення електронних засобів поширення інформації зумовлювалося такими особливостями європейської культури, як орієнтація на розумні принципи організації суспільства, прагнення до повноти й доступності інформації про навколишній світ, орієнтація на наукову раціональність, ліберально-демократичні інститути та цінності тощо. Більшість концепцій індустріального та інформаційного суспільства описували механізм соціального розвитку в детерміністично-прогресивних імперативах. Індустріальне і тим більше інформаційне суспільство – це суспільство участі, і, на відміну від традиційного, воно функціонує на основі демократичних норм і практик, що передбачають формування консенсусу із суспільно значущих питань. У радикальних футуристичних теоріях інформаційного суспільства обґрунтовувалася навіть необхідність заміни парламентської системи представницької демократії на демократію участі – соціальну й політичну систему, в якій переважна орієнтація на задоволення матеріальних потреб поступиться прагненню до самовдосконалення та до вирішення глобальних проблем. Децентралізоване громадянське суспільство ґрунтуватиметься на вільних інформаційних мережах, які перетинають національні кордони [11]. В академічному середовищі сформувався підхід, згідно з яким соціальні медіа є засобом звільнення від нормативного, ідеологічного й політичного контролю, що суттєвою мірою забезпечувався традиційними мас-медіа. Вільні онлайн-спільноти горизонтального типу є потенційними носіями інших групових ідентичностей, опозиційних політичних, економічних та соціальних порядків. Паралельна інформаційна реальність у соціальних мережах, яка оспорює порядок денний та картину навколишньої дійсності офіційних масових медіа, є джерелом мобілізації колективних протестних дій. З розвитком мережевих комп'ютерних технологій у дискурси науки та державного управління увійшли поняття «електронної демократії», «електронного урядування» – простори більш ефективного забезпечення політичної комунікації між органами влади та суспільством і реалізації принципів народовладдя [12; 13]. Якщо раніше популярною була думка М. Маклюена про те, що електронні ЗМІ (зокрема, телебачення) повертають нас до «глобального села», то Інтернет актуалізував іншу метафору – «кав'ярні» як простору безпосереднього спілкування.

Один із головних викликів для особистих прав та свобод людини в умовах розвитку технологій мережевих комунікацій – це проблема цифрової нерівності, нерівного доступу до інформаційно-комунікаційних каналів, технологій та ресурсів, що ставить під сумнів уявлення про Інтернет як відкритий простір рівноправних комунікацій, що має яскраво виражений потенціал демократизації, ліквідації суспільної ієрархії, цілеспрямованого росту впливу людей, які раніше були пасивними споживачами інформації. Суб'єкти інформаційно-комунікаційної активності в онлайн-просторі, залишаючи цифрові сліди й генеруючі дані своїх інформаційних, купівельних, ідейних переваг, стають об'єктами маркетингового, рекламного та політичного управління. Відповідно до можливостей використання існуючих

і створюваних масивів даних дослідники виділяють так звані data-класи. Основний клас – звичні користувачі, які генерують у великій кількості особистісні дані, на основі яких у подальшому формуються цифрові профілі з індивідуальними поведінковими та світоглядними особливостями. В акаунтах та соціальних мережах збираються цифрові персональні дані, в результаті чого формуються глобальні масиви даних. Інший клас формується з числа тих, хто має матеріально-технологічний та когнітивно-інформаційний, освітній капітал для формування Big Data (службовці та володарі крупних технологічних корпорацій, IT-індустрії). Ще один data-клас, представники якого володіють можливостями аналітичної обробки цифрових профілів і подальшого використання даних у політичних цілях, впливу на електоральні групи, а також політичні групи еліти, які на основі них здатні ставити власні політичні цілі та вибудовувати електоральні стратегії боротьби за владу [14; 15].

У сучасному світі зростає ефективність нормативно-правового політичного регулювання комунікації в мережевих спільнотах, суб'єктами якого переважно стають політичні та економічні інститути. Народні маси, навпаки, через кризу сучасних ідеологій та системи представницької демократії ризикують втратити свою роль свідомих, активних та впливових учасників суспільно-політичного дискурсу, а отже – здатність протидіяти несприятливим тенденціям соціального розвитку [16–18]. Це ставить питання інклюзії та зростання людських можливостей у модерному суспільстві [19].

Поширеними є випадки закриття комунікаційних мереж із боку держав, щоб не дозволити дисидентам координувати свої дії в реальному часі. Простір електронної мережевої комунікації поступово перетворився на арену політичної боротьби та конфліктів. Безпрецедентна кампанія блокування аккаунтів Д. Трампа та його прихильників з боку Facebook, Instagram, Twitter, YouTube, TikTok, Snapchat, Reddit та інших сервісів свідчить про кризу підходу, згідно з яким соціальні мережі є простором розвитку свободи та вільної, нерегламентованої комунікації. Соціальні мережі виявили себе як політичні актори, що мають свої позиції та інтереси і регулюються певними політичними інститутами та групами. В експертному середовищі з'являються думки, що в контексті цих подій можна говорити, з одного боку, про те, що всі провідні держави та корпорації створили інструменти системного впливу в середовищі соціальних медіа, а з іншого – про перспективу актуалізації міфу про мережеві онлайн-спільноти як політичні інструменти, основою діяльності яких виступає соціальний, культурний та політичний контроль за діяльністю людини на індивідуалізованому рівні. Виникає міф нової несвободи під контролем штучного інтелекту в рамках алгоритмізованих процедур повсякденної життєдіяльності [20].

Інша проблема – кібербезпека, що останні роки стала однією з найбільш гостро обговорюваних та актуальних проблем соціальних наук, що впливають на процеси вироблення політики та повсякденне життя громадськості. За останні роки злочинна діяльність у віртуальному просторі розширюється з дедалі більшою швидкістю. Загрози приватним користувачам Інтернету мають багато форм і проявів. Соціальні мережі стали каналом швидкого розповсюдження контенту екстремістського та насильницького змісту, інструментом кібербулінгу, шантажу та залякування як політичних опонентів, так і пересічних громадян [21]. Кіберзлочинна економіка приносить величезні збитки – фінансові та психологічні, примушуючи держави, корпорації та приватних осіб витрачати величезні ресурси для нейтралізації численних загроз та забезпечення безпеки.

2. Громадська думка щодо проблем кібербезпеки в країнах ЄС

Останніми роками в країнах ЄС дуже швидкими темпами розвивається цифрова інфраструктура. З кожним роком все більше і більше громадян європейських країн отримують доступ до Інтернету, а разом з тим і до різноманітних онлайн-послуг. Дослідження свідчать, що за п'ять років, з 2012 до 2017 р., помітно зросла аудиторія користувачів Інтернету, охопивши більше 81% мешканців ЄС (зростання становило більш ніж 10%). Причому майже 70% людей вдавалися до Інтернет-послуг щоденно. Менше 19% громадян не користувалося Інтернетом [22; 23]. Отже, більш ніж для двох третин громадян Євросоюзу Інтернет став повсякденною реальністю, що робить проблему безпеки їхнього доступу та використання можливостей всесвітньої павутини вкрай актуальною.

Паралельно із зростанням Інтернет-аудиторії змінюється характер та модель поведінки користувачів у мережі. По-перше, Інтернет стає рутинною і обов'язковою частиною життя для більшості сучасників. Цьому тренду посприяла зростаюча доступність різних пристроїв, що дають змогу здійснювати доступ в Інтернет, зокрема мобільних. Саме тому протягом досить короткого проміжку часу спостерігається суттєва зміна у звичках користувачів, які все більшою мірою орієнтуються на малі, мобільні пристрої для виходу у всесвітню мережу. Якщо у 2012 р. тільки 23,9% заходили в Інтернет із застосуванням смартфонів, то через 5 років цей показник зріс більш ніж утричі – до 79,3%. Ще більш помітними є зміни у використанні планшетів (від 5,9 до 40,4%, відсоток користувачів збільшився майже в 7(!) разів). Все більше людей виходять в Інтернет безпосередньо за допомогою телевізійних пристроїв (17,8% у 2017 р.) [22; 23]. Отже, змінюються моделі поведінки користувачів, роблячи Інтернет більш доступним і необхідним елементом роботи, навчання, відпочинку.

По-друге, завдяки широкій доступності Інтернету значна частина повсякденних операцій і трансакцій поступово переноситься із фізичного світу у віртуальний. Використання Інтернету для здійснення товарно-грошових операцій, спілкування, отримання інформаційних послуг, для відпочинку та розваг стало звичною справою для більшості мешканців розвинутого світу. Як свідчить рис. 1, значний набір різноманітних послуг користується попитом у більшості мешканців країн ЄС.

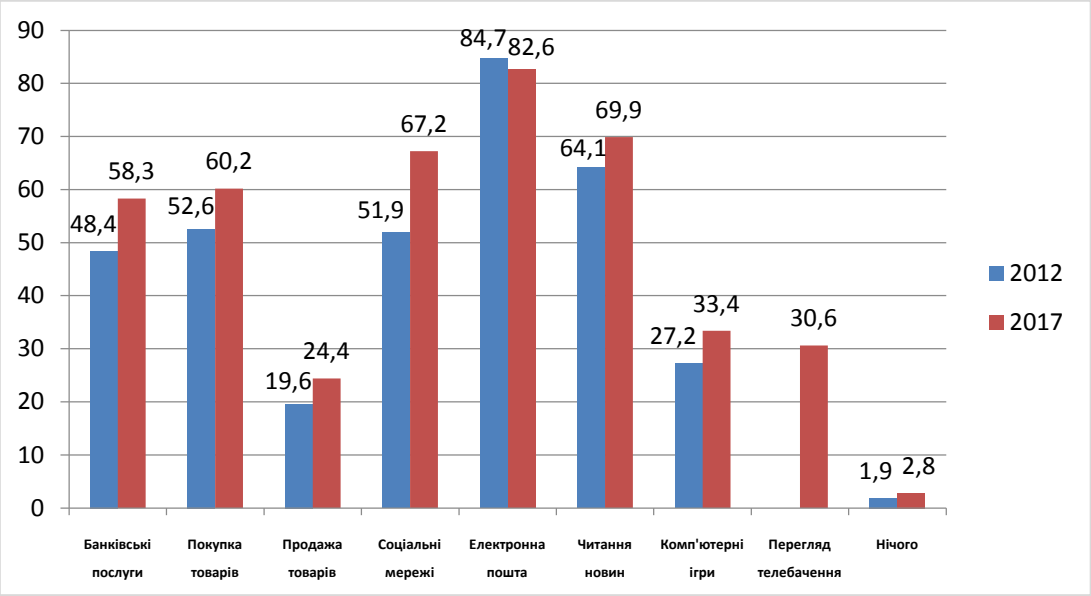

Рис. 1. Види активності в Інтернеті (%)

Джерело: Eurobarometer 77.2 (2012) [22]; Eurobarometer 87.4 (2017) [23]

Зокрема, незважаючи на невеличке зниження показника, найбільш популярною активністю в мережі залишається користування електронною поштою. По всіх інших видах діяльності спостерігається зростання, іноді помітне, частки Інтернет-аудиторії, охопленої цим видом послуг. Особливо це стосується соціальних мереж і банківських послуг, а також купівлі та продажу товарів і послуг. Зростає і сфера культурних індустрій, дозвілля та інформаційних послуг, все більше і більше переміщуючи людей у світ віртуального спілкування і розваг. Приблизно третина мешканців ЄС дивиться телебачення та грає в ігри, а більше двох третин отримує новини та суспільно-політичну інформацію із всесвітньої мережі.

По-третє, з плином часу користувачі Інтернету набувають усе більшої компетентності. Так, у 2012 році 27,1% користувачів оцінювали себе як дуже впевнених, 43,2% – впевнених, 17,4% – як не дуже впевнених і лише 12,3% – як зовсім невпевнених [22; 23]. У наступних хвилях Євробарометру це питання вже не задавалось, але про рівень компетентності споживачів онлайн-послуг можна опосередковано судити по запитаннях, що стосуються сприйняття ними власної поінформованості щодо можливих ризиків і небезпек у сфері використання інтернет-технологій.

На рис. 2 показані відповіді європейців на запитання стосовно їхніх відчуттів про власну поінформованість щодо ризиків кібер-злочинності. Як бачимо, за п’ять років відбулися помітні позитивні зрушення в цьому аспекті: користувачі з часом відчувають себе більш обізнаними, а отже, і компетентними, в царині кібербезпеки. Якщо в 2012 р. кожний четвертий європеєць сприяв себе як зовсім необізнаного в сфері кібербезпеки, то за п’ять років таких залишилося приблизно кожний п’ятий. І навпаки, частка поінформованих відчутно зросла [22; 23]. Отже, скоріш за все досвід використання Інтернету, поряд з усе зростаючими ризиками, справляє вплив на рівень компетентності споживачів цифрової інформації.

Загалом європейці серйозно ставляться до ризиків, які їх підстерігають у віртуальному просторі. Рівень їхньої стурбованості з плином часу зростає. Які саме ризики та як часто згадувались мешканцями країн Євросоюзу в цьому контексті? Дані засвідчують, що найчастіше користувачів мережі турбувала можливість зловживання їхньою персональної інформацією, використання її третьою стороною в недоброчесних або злочинних цілях, а також махінації з оплатою тих чи інших покупок в Інтернеті. Також люди надають перевагу проведенню операцій особисто, тобто коли покупець може сам перевірити продукт або спитати про нього реальну людину. Дещо нижчий рівень стурбованості

викликає ризик недоставки товарів або послуг, які індивід купує через Інтернет. По всіх вище зазначених позиціях протягом п'яти років спостерігається поступове зростання рівня занепокоєння. Водночас частка тих, кого перераховані проблеми не турбують, залишається стабільною – приблизно 20% [22; 23].

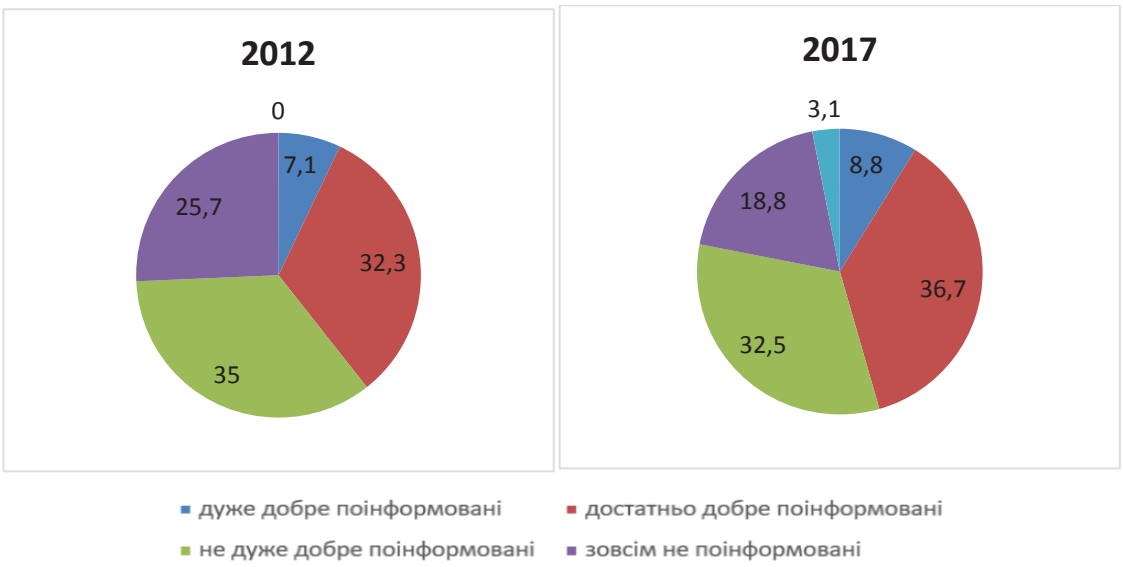

Рис. 2. Самосприйняття респондентами власної поінформованості щодо ризиків кіберзлочинності (%)

Джерело: Eurobarometer 77.2 (2012) [22]; Eurobarometer 87.4 (2017) [23]

Більш детальну інформацію щодо різноманітних проявів кібернебезпеки можна отримати з таблиці 1. Ціла низка питань мала з'ясувати, наскільки сильно турбує кожна із представлених загроз громадян європейських країн. Дані дають змогу простежити зміну настроїв європейців протягом

Таблиця 1

Сприйняття користувачами Інтернету різних видів кіберзлочинів, 2012, 2017 (%)

	Дуже стурбований		Досить стурбований		Не дуже стурбований		Зовсім не стурбований		Разом	
	2012	2017	2012	2017	2012	2017	2012	2017	2012	2017
Крадіжка особистих даних	24,7	**32,9**	37,5	**36,6**	26,6	**22,2**	11,2	**8,3**	100	100
Шахрайський електронний лист	15,9	**26,2**	32,8	**34,7**	33,6	**25,8**	17,7	**13,2**	100	100
Шахрайство при купівлі товарів	14,5	**22,1**	35,5	**37,2**	33,5	**28,1**	16,5	**12,6**	100	100
Екстремістські матеріали	13,2	**21,5**	28,3	**30,2**	37,5	**30,1**	21,0	**18,2**	100	100
Кібератаки	12,6	**22,6**	31,5	**35,3**	36,5	**28,4**	19,5	**13,7**	100	100
Дитяча порнографія	24,5	**27,7**	27,2	**26,5**	28,8	**26,4**	19,5	**19,4**	100	100
Зламування акаунту	-	**27,7**	-	**36,4**	-	**24,8**	-	**11,2**	100	100
Банківське шахрайство в Інтернеті	-	**32,4**	-	**35,1**	-	**21,0**	-	**11,5**	100	100
Шантаж	-	**25,8**	-	**30,4**	-	**28,2**	-	**15,6**	100	100
Шкідливе програмне забезпечення	-	**29,4**	-	**40,9**	-	**21,7**	-	**8,1**	100	100
Середнє	*17,6*	***26,8***	*32,1*	***34,3***	*32,8*	***25,7***	*17,6*	***13,2***		

Джерело: Eurobarometer 77.2 (2012) [22]; Eurobarometer 87.4 (2017) [23]

п'ятирічки. Загальна тенденція виглядає досить очевидно: ризики наростають, стурбованість підвищується. Причому ця тенденція є всебічною, охоплює всі сторони діяльності людей в Інтернеті та презентує різноманітні прояви кіберзлочинності – від шахрайства та крадіжки особистих даних до дитячої порнографії та шантажу. Більше того, останні роки принесли нові небезпеки, про які майже не було відомо або які не являли серйозної загрози в 2012 р. Але незабаром, через декілька років, вони стало предметом помітного занепокоєння, оскільки набули загрозливих масштабів. Йдеться, приміром, про зламування персонального акаунта, шахрайство під час проведення банківських платежів, шантаж, використання шкідливого програмного забезпечення тощо. По всіх позиціях в обидва періоди часу, коли проводилося дослідження, частка стурбованих цими загрозами споживачів переважала тих, хто не відчував особливого занепокоєння. А ті, хто взагалі не відчував жодних ризиків в Інтернет-просторі, складали малий відсоток – від 8,1 до 19,4% (в середньому 13,2%). Отже, наряду з усе більш активним і широким залученням публіки до активності у віртуальному просторі зростає небезпека, яку самі користувачі відчувають усе гостріше. І це відчуття зумовлене реальним досвідом людей, а не тільки відображенням створеної засобами масової інформації атмосфери підвищеної уваги та пильності щодо кібербезпеки (табл. 1).

Інтернет-простір все частіше стає ареною різноманітних атак, загроз, зловживань і злочинних посягань. Розширюється спектр загроз, вони стають усе більш прихованими та складними до розпізнання. Привертає увагу той факт, що в своїй більшості Інтернет-користувачі мали змогу безпечно користатися благами цифрової цивілізації та не ставали мішенями кіберзлочинної активності. Найбільш розповсюдженими видами кіберзлочинів були використання шкідливого програмного забезпечення та надсилання шахрайських електронних листів (від них потерпали тією чи іншою мірою відповідно 43 та 38,4% європейців). Решта різновидів зустрічалися значно рідше – від 7,8 до 18,2% [22; 23]. Проте, зважаючи на постійне вдосконалення та експансію цього типу злочинності, можна очікувати поступове наростання вже існуючих і виникнення нових загроз.

Слід зазначити, що по тих видах кіберзлочинів, щодо яких проводилися заміри протягом проаналізованого періоду, Інтернет-юзери загалом піддавалися приблизно одному і тому ж самому рівню загроз і атак. Це, скоріше за все, свідчить про поступову адаптацію Інтернет-користувачів до ситуації різноманітних викликів і зростаючої небезпеки. Отже, попри зростання масштабів небезпеки і занепокоєності самих користувачів, фактичний рівень кібер-віктимізації серед мешканців країнах Євросоюзу залишається більш-менш стабільним. Подібна позитивна тенденція пояснюється як ефективністю заходів із профілактики та боротьби із кіберзлочинністю, що впроваджуються державними та корпоративними інститутами, так і проактивною та свідомою позицією самих користувачів. Публіка стає більш поінформованою, пильною, озброєною різними засобами нейтралізації ризиків та боротьби з кіберзагрозами. Самі користувачі, усвідомлюючи всю глибину та масштаби ризиків, докладають різноманітних зусиль для гарантування безпеки в мережі. Дослідження демонструють, що все більше користувачів в якості превентивної міри змінюють паролі для виходу у різні онлайн-служби, зокрема для користування електронною поштою, соціальними мережами, здійснення онлайн-покупок, отримання банківських послуг тощо. Якщо у 2012 р. частка тих, хто змінив пароль протягом останнього року, становила 45,1%, то через п'ять років вона вже досягла 61,8% [22; 23]. Користувачі, які стали жертвами кіберзлочинів, усе активніше звертаються по допомогу до різних організацій – як державних, так і приватних, примушуючи останні докладати додаткових зусиль із створення безпечного Інтернет-середовища.

Висновки. Розвиток технологій комунікації в інтернет-просторі може мати неоднозначні наслідки. З одного боку, вони дозволяють розвивати демократичні інститути та зворотні зв'язки між владою і суспільством, все більше людей отримують можливість висловлювати свою позицію в публічному просторі. З іншого, стає можливим використання інформації для досягнення різних політичних, економічних цілей шляхом маніпулювання суспільною свідомістю, приховування інформації або обмеження доступу до неї. Процес інтерпретації політичних явищ в онлайн-просторі може формувати нові ціннісно-смислові орієнтири, що не завжди збігається з політичними цінностями традиційних медіаканалів трансляції інформації. Це явище може ставати одним із факторів дестабілізації політичної системи. Закономірно, що аналіз ціннісних орієнтирів інтернет-простору для ефективної взаємодії з громадськістю є одним із необхідних завдань влади для збереження стабільного функціонування політичної системи. Тому для того, щоб функціонувати та ефективно управляти суспільством, інститутам влади необхідно формувати в масовій свідомості свій образ та порядок денний, в тому числі через інтернет-простір, вчитися вибудовувати горизонтальні зв'язки. Звідси проблема регулювання Інтернету, введення його в правове поле набуває особливої гостроти.

Технологічний розвиток не має свідомо встановлених соціальних ефектів, щодо яких можна передбачати, чи будуть вони приносити благо, тому детермінізм образу майбутнього суспільства є фальшивим. Відмова від нього означає, що поняття інформаційного суспільства повинне бути

відкритим для вільної дискусії з метою обговорення майбутніх альтернатив. Питання соціальних цілей, оцінка етичних і культурних вимірів нових технологій та засобів їх нормативно-правового регулювання, встановлення кордону (балансу) між правом громадян на особистий простір, приватністю життя і правом на цифровий контроль за ними з боку держави, різних політичних, економічних суб'єктів повинні бути пріоритетними в соціальних дослідженнях.

Yenin M., Korzhov H. Online communication: risks and prospects (on the basis of sociological study of public opinion in the EU countries)

The article analyzes the main approaches to the prospects for the development of network communication practices via the Internet. The influence of the development of digital technologies of social communication on the processes of socio-economic development, expansion of political participation, distribution of power and political mobilization is explored. At the same time, special attention is paid to the challenges and risks posed by Internet technologies for personal rights and freedoms. In particular, the emphasis is on the perception by Internet users of threats they face in the global computer network, on their behavioral responses to cybercrime, including safer patterns of behavior in cyberspace. Over time the level of competence of Internet users, their awareness in the field of cybersecurity is constantly increasing. There is also a growth, sometimes noticeable, in the share of the Internet audience utilizing various types of online services. The research illuminates that despite the growing scale of danger and concern of users themselves, the actual level of cyber-victimization among residents of EU countries remains quite stable. Such a positive trend is explained by both the effectiveness of measures to prevent and combat cybercrime implemented by government and corporate institutions and proactive and conscious position of the users themselves. The latter, being aware of the depth and scale of the risks, make various efforts to ensure network security (they periodically change passwords to access various online services, seek help from relevant organizations – both public and private).

Key words: network communication, social networks, information society, social media, cybercrime, cybersecurity, public opinion, European Union.

Література:

1. Innis H.A. Empire and Communications. Toronto, University of Toronto Press, 1972. 288 p.
2. Innis H.A. The Bias of Communication. Toronto, University of Toronto Press, 1999. 227 p.
3. Маршалл Мак-Люэн. Галактика Гутенберга. Становление человека печатающего. URL: https://royallib.com/read/maklyuen_marshall/galaktika_gutenberga.html#0.
4. Breuer A. (2012) The Role of Social Media in Mobilizing Political Protest. Evidence from the Tunisian Revolution. Discussion Paper. No. 10. Bonn: German Development Institute.
5. Атанесян А. Влияние социальных сетей на протестное поведение (на примере Армении). *Социс*. 2019. № 3. С. 73–84.
6. Shirky Clay. The political power of social media. *Foreign affairs.* 2011. № 1. С. 28–41.
7. Metzger M.M., Tucker J.A. (2017) Social Media and EuroMaidan: A Review Essay. *Slavic Review.* Vol. 76. No.1 (Spring): 169–191. DOI: 10.1017/slr.2017.16.
8. Одинцов А.В. Социология общественного мнения и вызов Big Data. *Мониторинг общественного мнения: экономические и социальные перемены*. 2017. № 3. С. 30–43.
9. Bolsover G., Howard P. Computational Propaganda and Political Big Data: Moving Toward a More Critical Research Agenda. In: Big Data, 2017, vol. 5, no 4, pp. 273–276.
10. Gourley S. Get ready for the robot propaganda machine. URL: http://www.wired.co.uk/article/robot-propaganda.
11. Masuda Y. The Information Society as Postindustrial Society. Wash.: WorldFutureSoc., 1983.
12. Концепція розвитку електронного урядування в Україні / За ред. А.І. Семенченко. Київ, 2009. 16 с.
13. Розпорядження від 20 вересня 2017 р. № 649-р Кабінету Міністрів України Про схвалення Концепції розвитку електронного урядування в Україні. URL: https://www.kmu.gov.ua/npas/250287124.
14. Manovich L. The Science of Culture? *Social Computing, Digital Humanities and Cultural Analytics.* URL: http://manovich.net/content/04-projects/088-cultural-analytics-social-computing/cultural_analytics_article_final.
15. Володенков С.В. Digital-технологии в системе традиционных институтов власти: политический потенциал и современные вызовы. URL: https://cyberleninka.ru/article/n/digital-tehnologii-v-sisteme-traditsionnyh-institutov-vlasti-politicheskiy-potentsial-i-sovremennye-vyzovy/viewer.

16. Єнін М. Еліта і народні маси в суспільстві другого модерну. *Вісник Харківського національного університету імені В.Н. Каразіна.*2010. № 891. С. 50–55.
17. Єнін М. Ідеологічні трансформації в суспільстві другого модерну. *Сучасні суспільні проблеми у вимірі соціології управління: Збірник наукових праць ДонДУУ.* Т. XIII. Вип. 217. *Серія «Соціологія»*. Донецьк, 2012. С. 165–171.
18. Єнін М., Віхров М. Ідеологічні ідентичності та можливість групових рухів солідарності в сучасній Україні. *Вісник Луганського національного університету імені Тараса Шевченка (соціологічні науки).* 2013. № 23. С. 222–236.
19. Кутуєв П., Чолій С. Мобілізація на пострадянському просторі: між імперативами модернізації та загрозами демодернізації. *Ідеологія і політика.* 2018. № 2 (10). С. 4–24.
20. Щербина В. Социальные медиа как пространство альтернативного политического действия: смерть мифа. URL: https://sg-sofia.com.ua/socialniye-media-kak-prostor-alt-polit-detviya.
21. Грег-Обі О., Лилик І., Коржов Г., Бучинська О. Прояви насильства щодо жінок в онлайн просторі під час виборів в Україні: аналітичний огляд IFES. Київ: Міжнародна фундація виборчих систем, 2019. 32 с. URL: https://ifesukraine.org/wp-content/uploads/2019/ 11/IFES-Ukraine-Manifestations-of-violence-against-women-online-during-elections-v1-2019-11-25-Ukr.pdf.
22. European Commission (2014): Eurobarometer 77.2 (2012). TNS OPINION & SOCIAL, Brussels [Producer]. GESIS Data Archive, Cologne. ZA5598 Data file Version 4.0.0, https://doi.org/10.4232/1.12032.
23. European Commission, Brussels (2019): Eurobarometer 87.4 (2017). TNS opinion, Brussels [producer]. GESIS Data Archive, Cologne. ZA6924 Data file Version 1.0.0, https://doi.org/10.4232/1.13207.