УДК 316.34

КІБЕРБЕЗПЕКА В УМОВАХ ЦИФРОВОЇ НЕРІВНОСТІ: ДО ПОСТАНОВКИ СОЦІОЛОГІЧНОЇ ПРОБЛЕМИ[1]

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
korzhovga@gmail.com

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
yeninmaksym@gmail.com

У статті розглядаються теоретичні та емпіричні аспекти соціологічного вивчення поведінки у сфері кібербезпеки. Одним із релевантних соціологічних підходів до вивчення даного явища розглядається теорія трьох рівнів цифрової нерівності. В основі презентованого дослідження лежить наступна робоча гіпотеза: безпечна модель цифрової поведінки значною мірою залежить від місця користувача Інтернету в ієрархічному розподілі різноманітних соціальних, культурних і цифрових ресурсів, від місця індивіда в системі соціальної нерівності. Серед факторів, які сприяють більш відповідальній та безпечній поведінці користувачів Інтернету, важливу роль відіграє досвід користування ІКТ (частота та зміст діяльності), рівень знань про потенційні ризики та загрози, особистий досвід кіберзлочинності. Ті користувачі Інтернету, які мають більш тривалий, інтенсивний та різноманітний досвід користування Інтернетом із різними цілями, демонструють, як правило, більш обачливу настанову та більш безпечну модель поведінки в Інтернеті. Кращі знання та досвід жертви злочину роблять користувачів більш пильними та допомагають запобігати зловживанням та погрозам у майбутньому. Вік, рівень освіти, місце проживання та заняття впливають на сприйняття людьми загроз та рівня безпеки в Інтернеті, а також на їх поведінку в мережі. Дослідження підтверджує, що користувачі Інтернету змінюють свою поведінку різними способами через проблеми безпеки.

Ключові слова: кібербезпека, цифрова нерівність, цифровий капітал, мережеве спілкування, соціальні мережі, кіберзлочинність, теорія трьох рівнів цифрової нерівності, поведінка у сфері кібербезпеки, модерн, конфлікт.

Вступ. В умовах стрімкого та інтенсивного розповсюдження цифрових технологій питання безпечної та розумної поведінки в мережі Інтернет набуває особливої значущості.

У цій статті ми мали на меті розкрити соціологічні виміри вивчення кібербезпечної поведінки. Кібербезпека стала однією з найбільш обговорюваних і актуальних тем, які впливають на процеси формування політики та повсякденне життя суспільства. Злочинна діяльність у кіберпросторі розширюється з дедалі більшою швидкістю протягом останніх років. Загрози для приватних користувачів Інтернету мають багато форм і проявів: встановлення шкідливого програмного забезпечення, шахрайська електронна пошта або телефонні дзвінки, матеріали, що пропагують расову ненависть або

[1] Статтю підготовлено в рамках науково-дослідницької теми кафедри соціології КПІ імені Ігоря Сікорського «Історична соціологія конфліктів у контексті модернів та модернізацій»

релігійний екстремізм, дитяча порнографія, ворожі висловлювання, насильство в Інтернеті, шахрайство, злом соціальних мереж або облікових записів електронної пошти, використання інформації без відома та дозволу користувачів, викрадення особистої інформації, шахрайство з кредитними картками або банківськими операціями, незаконний обмін особистою інформацією про третіх осіб, незахищені онлайн-платежі, неотримання товарів або послуг, які люди купують в Інтернеті, тощо. Кіберзлочинна економіка призводить до гігантських втрат – фінансових, моральних та психологічних, вона потребує величезних ресурсів для нейтралізації численних загроз та забезпечення безпеки. Проте, незважаючи на зростання актуальності проблеми кібербезпеки та онлайн-загроз в Інтернет-просторі, у сучасній літературі бракує досліджень, пов'язаних із спробами її теоретичного осмислення. Як правило, в юридичних науках це явище розуміють як складову інформаційних прав людини та національного інформаційного законодавства, в економічній – як чинник фінансової безпеки, в управлінні – як кібернетичну функцію держави та національної безпеки в цілому, у психології – як фактор фінансової безпеки – здатність особистості проявляти самоконтроль, регулювати емоції, поведінку та бажання (Валюшко, 2016; Діордіца, 2017; Дубов, 2014; Маковець, Дрозд, 2020; Хоббі, 2020).

В соціології наразі немає обґрунтованих підходів до вивчення цього явища. **Метою статті** є обґрунтування соціологічного підходу до вивчення поведінки в сфері кібербезпеки. В першу чергу, йдеться про постановку даної проблеми в руслі вивчення цифрової нерівності, яка залишається впливовим чинником сучасної епохи. На нашу думку, предметом соціології можуть бути особливості поведінки в сфері кібербезпеки, сприйняття інтернет-користувачами загроз, з якими вони стикаються в Інтернеті, і фактори, які впливають на їх більш безпечну поведінку в Інтернеті.

Робоча гіпотеза, яка лежить в основі даного дослідження, може бути сформульована наступним чином: рівень кібербезпечної поведінки значною мірою залежить від місця користувача Інтернету в ієрархічному розподілі різноманітних соціальних, культурних і цифрових ресурсів, загалом від місця індивіда в системі соціальної нерівності. Виходячи з цього припущення, ми намагатимемось виявити основні чинники, що впливають на зміни у поведінці громадян, зокрема ті, що призводять до більш безпечного користування Інтернетом.

Завдання статті:

1) Визначити актуальність теоретичного дослідження поведінки в кібербезпеці на основі теорії цифрової нерівності.

2) Вивчити, які фактори впливають на більш безпечну поведінку в Інтернеті.

Емпірична основа статті. Стаття базується на емпіричних даних, отриманих у результаті опитування Євробарометр 87.4, проведеного серед громадян країн ЄС у 2017 році й присвяченого вивченню ставлення європейців до кібербезпеки. В його рамках досліджувалися різноманітні аспекти кіберповедінки, частота та тип використання Інтернету жителями ЄС, їхня впевненість щодо Інтернет-транзакцій, обізнаність і досвід кіберзлочинів, а також рівень занепокоєння, який вони відчувають щодо цього типу злочинів.

Практичне значення результатів дослідження. Отримані результати можуть бути використані для розробки рекомендацій щодо кібербезпекової політики та зміни поведінки користувачів Інтернету.

Модерн, як соціально-культурна епоха, несе в собі внутрішні суперечності, що породжують конфліктну динаміку в суспільстві (Кутуєв, 2016; Fedorchenko-Kutuev, Pyholenko, Khomiak, 2023; Kutuev, Choliy, 2018). В контексті кібербезпеки, модерн виявляється через зростаючу цифрову нерівність, де доступ до інформаційних технологій і цифрового капіталу визначає здатність індивідів адаптуватися до викликів сучасності. Виникає конфлікт між тими, хто має доступ до цифрових ресурсів, і тими, хто його позбавлений, що створює нові форми соціальної стратифікації. Цифровий розрив, таким чином, є втіленням конфліктної динаміки модерну, де технологічний прогрес співіснує з соціальною нерівністю, підсилюючи як глобальну несправедливість, так і створюючи нові загрози у вигляді кіберзлочинності. Ці зміни вимагають переосмислення соціальних і культурних механізмів, які регулюють поведінку в кіберпросторі, з огляду на нові виклики і можливості, що породжує епоха модерну.

1. **Цифровий розрив, соціальна нерівність і безпечна кіберповедінка**

Початок дослідженням впливу комунікативних процесів на соціальні практики було покладено соціологами Канадської школи теорії масової комунікації в Торонто. Її представники у своїх працях відзначали залежність матеріального та духовного розвитку, а також змін моделей розподілу влади від ступеня розвинутості соціально-комунікаційних технологій (Innis, 1972; Innis, 1999; McLuhan, 1962). Ця традиція набула широкого поширення в міждисциплінарних дослідженнях, пов'язаних із цифровою нерівністю та її взаємозалежністю від становища індивідів у суспільстві, роллю соціальних мереж у масових політичних процесах та програмних технологій у соціальному контролі через Інтернет тощо (Shirky, 2011; Metzger, Tucker, 2017; Bolsover, Howard, 2017).

Повсюдність ІКТ робить кожного потенційною мішенню для посягань кіберзлочинців у різних сферах життя. Через перераховані вище численні ризики та виклики кібербезпечна модель поведінки стає необхідністю нашого часу. Однак ступінь дотримання різними особами правил безпеки в Інтернеті може суттєво відрізнятися. Чинники, які сприяють або перешкоджають цьому явищу, варіюються від особистих психологічних особливостей і соціальних характеристик через культурні норми та цінності до інституціоналізованих соціальних домовленостей.

У представленому дослідженні кібербезпечна поведінка розглядається як раціональна та цілеспрямована форма людської поведінки. Однак ми не приймаємо утилітарну версію людського актора як раціонального, автономного, егоїстичного та поінформованого. Раціональність ніколи не є константою. Люди поводяться з різним ступенем раціональності в одній і тій же ситуації. Крім того, одна й та сама особа демонструє різні рівні раціональної поведінки від ситуації до ситуації. Раціональність – це змінна, яку потрібно зрозуміти й пояснити. Це кінцева точка, де зустрічається низка різноманітних факторів. Ці фактори визначають доступ соціальних акторів до раціональних моделей поведінки, до якої відноситься, серед іншого, і безпечна кіберповедінка.

Попередні дослідження показують, що кібербезпечна поведінка пов'язана з соціальними, економічними, культурними та цифровими формами капіталу. Наприклад, результати кількісного опитування домогосподарств Словенії показують, що цифрове відчуження є результатом соціальних і культурних відмінностей і має бути проаналізовано відповідно до інших типів соціальної стратифікації (стать, вік, освіта, клас і культурний капітал) (Črnic, 2013). Кілька інших досліджень показують гендерні відмінності у прийнятті та використанні технологій на робочому місці. Вони також демонструють, що ґендерні відмінності стають більш вираженими з віком, що чоловіки мають нижчі наміри дотримуватися політики безпеки порівняно з жінками (Ifinedo, 2012; Anwar, He, Ash, Yuan, Li, 2017). Проте, ці та інші дослідження переважно стосуються мешканців окремих країн, що обмежує можливості генералізації отриманих результатів.

Одним із відповідних соціологічних підходів, який може пояснити цифрові та соціальні варіації щодо кібербезпечної поведінки, є теорія трьох рівнів цифрового розриву (digital divide)[2]. Концепція цифрового розриву стала частиною наукових досліджень наприкінці 1990-х років і замінила попередні ідеї про інформаційну нерівність та розрив. Коли термін «цифровий розрив» увійшов в офіційний дискурс, він стосувався в основному фізичного доступу до Інтернету та телекомунікаційних послуг. Ранньому етапові теоретизування на цю тему були притаманні суттєві обмеження. Так, сам термін «цифровий розрив» більше викликав непорозуміння, ніж сприяв понятійній ясності. Він апелював до жорсткої дихотомії та припускав існування абсолютної нерівності, в той час як емпіричні дані вказували на релятивний характер нерівності в доступі до комп'ютерів і цифрових технологій. На додачу, термін співзвучний ідеям технологічного детермінізму, припускаючи, що причини нерівності перебувають у сфері доступу до цифрових технологій, і, відповідно, надання такого доступу вирішить ключові проблеми з нерівністю в соціальній та економічній царинах (Van Dijk, 2006: 222).

У сучасних дискусіях перший рівень аналізу залишається центральним, але в довгостроковій перспективі слід очікувати, що важливість соціальних змінних (дохід, вік, стать, освіта, місцезнаходження), визначених у 1990-х роках як потужних предикторів доступу до фізичної інфраструктури, буде знижатися, за прикладом телебачення, яке спочатку, будучи новою та дорогою технологією, була прийнята заможними верствами, але згодом стала загальнодоступною (Hargittai, 2002: 28-33). При цьому в модернізованому варіанті цієї теорії цифровий розрив розглядається на трьох рівнях: рівень доступу до Інтернету, інформаційно-комунікаційних технологій; рівень цифрових компетенцій користувачів та цифрової грамотності; рівень соціальних переваг, які користувачі отримують від грамотного використання цифрових технологій у професійному та приватному житті (Wei, Teo, Chuan, Tan, 2011: 170–187).

Виокремлення другого та третього рівнів цифрового розриву передбачало включення не лише технічного (наявність технології та фізичного доступу до неї), а й соціологічного виміру аналізу. Феномен цифрового розриву передбачає відмінності в доступності цифрових технологій, диференціації навичок і результатів використання. Ця теорія постулює взаємозв'язок між компетентністю, навичками користування Інтернет, інформаційними та комунікаційними технологіями, соціально-демографічними характеристиками індивідів (вік, рівень освіти, дохід) та різними досягненнями (професійні успіхи, вищий статус у суспільстві, можливості самореалізації, участь у суспільному житті). Ван Дейк вважає цифровий розрив важливою соціальною проблемою сучасного суспільства, оскільки він призводить до уповільнення економічного зростання та інноваційного розвитку, посилення нерівності та виключення (Van Dijk, 2020). Насправді цифровий розрив є перешкодою для будь-якої програми

[2] Ґрунтовний метатеоретичний огляд проблематики цифрового розриву представлений, зокрема, в праці нідерландського дослідника Яна ван Дейка (J.A.G.M. van Dijk Digital divide research, achievements and shortcomings / Poetics 34 (2006) 221–235).

соціальної інтеграції. Відповідно до справедливого коментаря К. Спарка, якщо суспільства сьогодні частково, а в майбутньому будуть більш-менш повністю структуровані навколо Інтернету, тоді вимоги економічної ефективності, а також соціальної та політичної справедливості вимагають, щоб жодна соціальна група не була виключеною з цифрової участі (Sparks, 2013).

Загалом, із величезним поширенням Інтернету, особливо в західних суспільствах, на початку 1990-х років з'явилися дві протилежні точки зору щодо його впливу на суспільство: егалітарна та елітарна. Насправді можна стверджувати, що обидві тенденції співіснують. З одного боку, віртуальна комунікація через соціальні медіа, долаючи фізичний простір, може об'єднувати людей з різних соціальних і класових позицій навколо певних соціально-політичних дискурсів. Значною є роль соціальних мереж в організації, синхронізації та активізації масової протестної діяльності навколо існуючих при владі політичних груп. Соціальні медіа значно зменшують можливості для цензури та явної ієрархії, притаманної традиційному медіа-середовищу, дозволяючи користувачам бути як творцями, так і одержувачами інформації. Інтернет стає платформою для обміну думками та ідеями між нескінченною кількістю користувачів, самопрезентації індивідуальних і групових ідентичностей, що порушує монополію традиційних медіа на поширення інформації, формування символічної картини світу. і це створить нові простори для політичних дискусій і забезпечить громадянам прямий доступ до уряду (Коржов, Єнін, 2022: 156). З іншого боку, можна спостерігати сучасні тенденції до ефективного зростання інструментів регуляторної політики комунікації в онлайн-спільнотах, закриття комунікаційних мереж державами, формування техно-корпорацій та їх здатність придушувати, виключати цілі групи людей з громадсько-політична діяльність (як приклад, вибори у США в 2020 році).

Формування цифрового розриву тісно пов'язане з формуванням мережевого суспільства (за визначенням М. Кастельса), в якому ключові соціальні структури та діяльність його членів організовані навколо електронних комунікаційних мереж. Він стверджував, що мережі становлять нову соціальну морфологію суспільства, а впровадження мережевої логіки суттєво модифікує процеси та їхні результати в культурі (культура «реальної віртуальності»), політиці (влада, розчинена в глобальних мережах фінансів, інформації та медіа), економіка (глобальна інформаційна економіка) (Castells, 2000). У теорії мережевого суспільства представники найманої праці в соціальній структурі стратифікуються за ознакою власності на знання та інформацію. Внаслідок процесів глобалізації, ділових мереж та індивідуалізації праці слабшає соціальна організація працівників та інститути, які їх захищали, жорстка класова структура індустріального суспільства та класова солідарність найманих працівників поступово зменшуються. Зростає соціальний статус і частка в національному багатстві елітного прошарку висококваліфікованих працівників («інформаційної робочої сили»). Таким чином, рівень особистих і групових соціальних, економічних і політичних переваг, які можна отримати за допомогою Інтернету, інформаційно-комунікаційних технологій, є одним із наслідків цифрового розриву.

Отже, теорія цифрового розриву, на нашу думку, може бути продуктивною для вивчення соціальної структури, яка формується в мережевих структурах і ресурсах, які є основою її ієрархічної структури. У науковій літературі є спроби виділити так звані цифрові класи («data classes»). Модальний, найчисельніший дата-клас – звичайні користувачі, які генерують велику кількість персональних даних, на основі яких надалі формуються цифрові профілі з індивідуальними поведінковими та світоглядними особливостями. Інший клас складається з тих, хто має матеріально-технологічний, когнітивно-інформаційний та освітній капітал для формування Big Data (співробітники та власники великих технологічних корпорацій, IT-індустрії). Представники іншого дата-класу мають можливість аналітичної обробки цифрових профілів і подальшого використання даних в економічних (маркетинг, реклама) і політичних цілях, наприклад, з метою впливу на електоральні групи, а також політичні групи еліти, які здатні встановлювати власні політичні цілі та будувати виборчі стратегії владних груп (Єнін, Коржов, 2021: 23–24).

Цифровий розрив не лише відображає існуючу соціальну нерівність, притаманні їй соціальні та культурні відмінності, але є її конституюючим елементом, інструментом її відтворення та підсилення. Одним із можливих пояснень цього механізму може бути концепція різних видів капіталу – цифрового, економічного, політичного, культурного та соціального. В даній концепції до звичайних в соціологічній теорії типів капіталу додається новий – цифровий. М. Регнеда визначає цифровий капітал як «набір інтерналізованих здібностей і здатностей» (цифрові компетенції), а також «зовнішніх ресурсів» (цифрові технології), які можна історично накопичувати та передавати з однієї сфери в іншу. Цифровий капітал, яким володіє людина, впливає на якість Інтернет-досвіду (другий рівень цифрового розриву), який, у свою чергу, може бути «конвертований» в інші форми капіталу (економічний, соціальний, культурний, особистий і політичний) у соціальній сфері, що впливає на третій рівень цифрового розриву. Таким чином, цифровий капітал є мостом між життєвими шансами онлайн і офлайн, який не тільки дозволяє ефективно використовувати попередні капітали в цифровій сфері, але й підтримує їх, відтворюючи прибутки в офлайновій сфері. Реальні вигоди, які користувачі

отримують від використання Інтернету, базуються на їхніх попередніх капіталах плюс їх взаємодії з цифровим капіталом, як під час, так і після онлайн-досвіду [Ragnedda, 2018: 2367]. Цифровий капітал – це продукт отриманої інформації та знань, ресурсів і навичок, набутих під час онлайн- та офлайн-діяльності. У свою чергу, цей вид капіталу можна перетворити на зовнішньо спостережувані статусні характеристики: вищий соціальний статус, більш престижну роботу, практики споживання та дозвілля, соціальні зв'язки тощо. Він є сукупною похідною від інших ресурсів (капіталів), їх наслідком і, водночас ресурсом, який дозволяє реінвестувати їх для накопичення та зростання. Тому обмежений доступ до Інтернету, інформаційно-комунікаційних технологій є одним із основних джерел соціальної нерівності в сучасному суспільстві. Тип соціалізації, соціальний статус і культурний капітал сім'ї, тип і рівень освітніх закладів впливають не тільки на доступ до цифрових технологій і відповідний рівень цифрової грамотності та компетентності (перший і другий рівні цифрового розриву), але й на можливість конвертувати це в різні соціальні винагороди. І навпаки, ті особи, які вже мають потужний освітній, економічний, політичний, соціальний капітал, можуть надалі його нарощувати за рахунок використання цифрових ресурсів. Інтернет-маркетинг, ведення та розширення бізнесу, політичні спільноти та багато інших повсякденних видів активності нині здебільшого базуються на цифрових платформах. У цьому контексті важливим завданням соціологічних досліджень є вивчення можливостей створення та впровадження цифрових рішень і програм для незахищених верств населення, оскільки поглиблення їх цифрової нерівності призводить до посилення соціальної нерівності (Єнін, Кухта, 2022: 218).

Водночас наявність цифрового та інших видів капіталу може пояснювати модель кіберповедінки – більш чи менш безпечної. Наша загальна робоча гіпотеза передбачає, що рівень кібербезпечної поведінки залежить від різних типів ресурсів і їх кількості, якими володіє людина. Особи, які володіють більшою кількістю відповідних ресурсів, швидше за все, поводитимуться більш безпечно і, таким чином, матимуть вищий рівень безпеки в Інтернеті. Таким чином, ступінь ризику стати жертвою кіберзлочинців залежить від соціального становища та ресурсних характеристик індивідів.

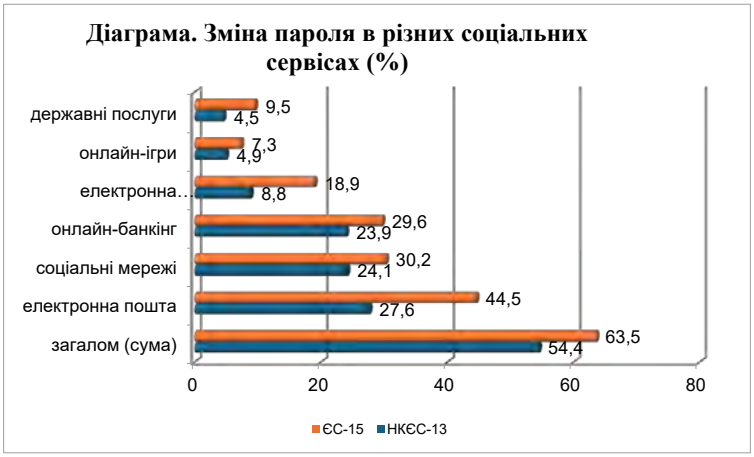
У наступному розділі статті представлено початковий емпіричний аналіз Інтернет-активності мешканців країн ЄС, їх уявлень про ризики та виклики, пов'язані з використанням різноманітних онлайн-сервісів та ресурсів, а також чинників, що сприяють та перешкоджають безпечній поведінці в Інтернеті.

2. Фактори, що сприяють безпечній поведінці в Інтернеті: попередній емпіричний аналіз

Ми досліджували різну діяльність мешканців країн ЄС в Інтернеті, їх уявлення про ризики та виклики, пов'язані з використанням різноманітних онлайн-сервісів і ресурсів, а також модель безпеки, якої вони віддають перевагу у своїй цифровій діяльності. Ми прагнули краще зрозуміти, що спонукає людей бути більш обережними щодо кіберризиків і злочинної діяльності, а також які фактори сприяють більш безпечній поведінці в Інтернеті. Як проксі для безпечної поведінки в Інтернеті ми використовували індикатор, який визначає, чи змінював респондент свій пароль для доступу до облікового запису(-ів) для будь-якої з різних онлайн-служб протягом останніх 12 місяців (електронна пошта, соціальні мережі в Інтернеті, веб-сайти для покупок, онлайн-банкінг, онлайн-ігри, веб-сайти державних послуг). Даний індикатор вже неодноразово використовувався в Євробарометрі і може розглядатись як показник, що свідчить про тип поведінки в кіберпросторі – безпечною чи, навпаки, ризикованої. Ми пропонуємо вважати тих, хто змінив пароль хоча б в одному сервісі протягом року, такими, що практикують безпечну модель поведінки в Інтернеті, а хто не змінив – небезпечну. Очевидно, що даний показник можна використовувати більш диференційовано, зокрема, підраховуючи кількість сервісів, в яких індивід робить подібні зміни. Проте, для цілей нашого аналізу достатньо його використовувати в узагальнюючому контексті: чи вдавався взагалі користувач до такого запобіжного заходу чи ні.

Перш ніж аналізувати фактори, що сприяють безпечній поведінці в Інтернеті, детальніше розглянемо частоту зміни паролів у різних соціальних службах (див. Діаграму) у двох групах країн: тих, що формують ядро ЄС (15 «старих» членів Євросоюзу, ЄС-15), і тих, котрі приєдналися до європейського об'єднання протягом останніх 20 років (нові члени спільноти, НКЄС-13).

Як показують дані, є три сфери онлайн-активності, які змушують користувачів поводитися більш обережно та частіше від інших форм діяльності змінювати паролі як засіб запобігання кібератакам. Це електронна пошта, соціальні мережі та банківські операції. Саме цим сферам громадськість в обох регіонах ЄС приділяє найбільшу увагу. Проте можна виявити значні відмінності серед користувачів у ЄС-15 та нових країнах ЄС (НКЄС-13): у всіх сферах діяльності, проаналізованих в опитуванні, без виключення, користувачі Інтернету у країнах, що формують ядро ЄС, виявляють більш виражену схильність до безпечної моделі поведінки. Водночас, громадяни держав-нових членів ЄС поводяться не так обережно: лише 54,4 % проти 63,5% в країнах ядра змінювали пароль як мінімум в одному онлайн-сервісі. Пояснення даної різниці може стати предметом окремого дослідження.



Одначе, виходячи з проблематики презентованого дослідження, можемо тільки висувати попередні припущення про різний за обсягом і наповненням ресурсний потенціал користувачів із різних частин ЄС: більший та змістовніше багатший в розвиненішій частині Європи. Верифікація даної гіпотези може стати предметом подальших наукових розвідок.

Повертаючись до даних із Діаграми, зазначимо, що в багатьох сферах цифрової активності навіть в країнах ЄС-15 існує великий потенціал для зростання. Наприклад, в онлайн-іграх або у відносно новій сфері державних послуг менше 10% користувачів в обох регіонах змінили паролі протягом минулого року.

Щоб з'ясувати вплив різних факторів на безпечну онлайн-активність, ми порівняли між собою різні групи та категорії споживачів інтернет-сервісів. Залежна змінна, що вимірює зміни пароля в будь-якій із зазначених вище соціальних служб протягом останніх 12 місяців, є дихотомічною і кодується як 1 для «змінений пароль» і 0 – для «не змінений». Незалежні змінні – чинники впливу на модель онлайн-поведінки – були обрані з кількох індикаторів, використаних у Спеціальному Євробарометрі 464a (2017) відповідно до теоретичних припущень дослідження. Вибір незалежних змінних визначався двома міркуваннями: їхньою відповідністю теоретичним припущенням та практичною доступністю.

Попередній аналіз обмежується тільки мешканцями НКЄС-13 і не включає громадян т. з. «старої Європи». Вибір даної групи країн обумовлений низкою чинників. Більшість країн – нових членів ЄС – за рівнем свого економічного та технологічного розвитку поступаються «старій Європі». З цієї причини ІКТ та цифрова інфраструктура в цих суспільствах також менш розвинута, а фізичний доступ громадськості до Інтернету – більш обмежений. Крім того, користувачі Інтернету можуть бути більш уразливими до різних ризиків і небезпек під час перебування в Інтернеті, оскільки вони менш досвідчені та менше занепокоєні ними, а законодавча база й інституційні запобіжники проти кіберпорушень менш розвинені. Завдяки вищезазначеним обставинам ми очікуємо більшу диференціацію поведінкових практик серед населення, що досліджується, в залежності від різних типів ресурсів, або капіталу, що створюватиме кращі можливості для емпіричного тестування теоретичних гіпотез.

До нашому аналізі ми включили чотири аналітичні моделі, і відповідно, соціальні виміри, кожен з яких відповідає певному типу ресурсів або капіталу, які потенційно можуть впливати на модель онлайн-поведінки. Перший вимір базується на використанні аскриптивних ресурсів, пов'язаних зі статтю, віком, місцем проживання, національністю (етнічною групою), расою або будь-яким іншим атрибутом, приписаним при народженні або прийнятим мимоволі, іншим, ніж ті, котрі є результатом індивідуальних досягнень чи заслуг. У нашому випадку деякі з цих показників або недоступні (національність), або нерелевантні (раса для країн відповідного регіону) для аналізу. Як показує попередній аналіз, стать залишається амбівалентним чинником: в деяких дослідженнях виявлено, що жінки частіше обирають безпечнішу модель поведінки, ніж чоловіки. Таким чином, ми включили дві змінні – вік і місце проживання. Як доводять багато попередніх досліджень, вік є впливовим предиктором багатьох аспектів цифрової поведінки, включаючи частоту використання Інтернету, форми Інтернет-діяльності. Як правило, молодші користувачі більш активні, проводять більше часу в Інтернеті та користуються різноманітними соціальними сервісами. Отже, варто очікувати більшу обізнаність молодого сегменту Інтернет-споживачів з приводу безпеки поводження в мережі, а отже, і більш безпечної поведінки. Водночас, існують чинники, котрі грають проти даного припущення: молоді люди мають невеликий соціальний досвід і почуття відповідальності, гірше контролюють емоційну сферу і легше піддаються маніпуляціям, в т.ч. і кіберзлочинним. Відповідно, їх модель онлайн-поведінки

може бути менш раціональною та більш ризикованою. Щодо мешканців міст, слід відзначити, що вони краще обізнані про використання Інтернет-технологій і пов'язані з цим ризики, тому вони, швидше за все, поводитимуться в Інтернеті більш обережно.

Друга модель походить від ідеї соціального капіталу або рівня соціальної інтеграції. Як індикатори соціальної інтеграції можна використовувати дві змінні: сімейний стан і приналежність до соціального класу. Одружені люди та представники вищих соціальних класів зазвичай вважаються більш соціально інтегрованими. Ці категорії, цілком імовірно, більше орієнтовані на безпечний тип поведінки в Інтернеті.

Третя модель передбачає схильність до безпечної поведінки за рахунок наявності більш потужного людського капіталу, тобто знань, навичок і кваліфікації людей. У нашому випадку використовуються два показники, а саме рівень освіти, який вимірюється віком завершення освіти, та рівень поінформованості про ризики кіберзлочинності. Очевидно, що чим вище кожен із цих параметрів, тим безпечнішою можна очікувати поведінку людини.

Нарешті, четверта модель оцінює роль так званого цифрового, або кіберкультурного капіталу (ресурсів ІКТ). Емпіричні показники капіталу ІКТ наступні: частота використання Інтернету, індекс занепокоєння кіберзлочинністю, індекс досвіду кіберзлочинності та онлайн-діяльність з бізнес-цілями. Очікується, що люди, які мають більш тривалий та більш інтенсивний досвід використання Інтернету, будуть більш обережними під час перебування в Інтернеті. Вищий рівень занепокоєння щодо кіберзлочинів гіпотетично пов'язаний із вищою потребою перебувати у безпеці та з відповідними запобіжними заходами, яких має вживати особа під час перебування в Інтернеті. Цілком імовірно, що користувачі, які зазнали більшої кількості атак з боку кіберзлочинців, з більшою ймовірністю поводитимуться безпечно в Інтернеті. Окрім того, очікується, що люди, які користуються Інтернетом з діловими, службовими, професійними цілями, а не виключно для розваг, частіше змінюватимуть свій пароль у соціальних службах.

Результати попереднього аналізу вище обґрунтованих гіпотез можна побачити в Таблиці. В ній містяться перелік незалежних змінних і частотний розподіл залежної змінної (у % або середніх значеннях) за категоріями незалежних. Цей розподіл дає дослідникам попереднє розуміння того, наскільки та чи інша змінна може відіграти істотну роль в поясненні безпечної кіберповедінки.

Таблиця 1

Розподіл залежної змінної за категоріями незалежних змінних (%, середні значення*)

Незалежні змінні		**Залежна змінна (1 – зміна паролю)**
Аскриптивні характеристики		
Стать	Чоловік	54,2
	Жінка	54,6
Вік	15–24 років	59,6
	25–39 років	58,3
	40–54 років	52,9
	55 років і старше	44,6
Місце проживання	Сільська місцевість	49,4
	Малі міста та пригороди	54,4
	Великі міста	58,6
Соціальний капітал (ступінь соціальної інтеграції)		
Соціальний клас	Робочий клас	40,9
	Нижній середній клас	59,7
	Середній клас	57,6
	Вищий середній та вищий класи	71,5
Шлюбний статус	Поза шлюбом	58,8
	У шлюбі	52,6
Людський капітал		
Роки навчання	До 15 років	33,9
	16–19	50,0
	20 років і більше	60,0

Продовження таблиці 1

Наскільки добре ви поінформовані про ризики кіберзлочинності	Дуже добре	70,3
	Досить добре	61,2
	Не дуже добре	48,9
	Зовсім не поінформований	37,6
Кіберкультурний або цифровий капітал (ІКТ-ресурси)		
Частота користування Інтернетом	(Майже) щоденно	56,6
	2-3 рази на тиждень	49,6
	Один раз на тиждень	34,0
	2-3 рази на місяць	33,3
	Рідше	35,0
Занепокоєність кіберзлочинністю (індекс)*	Не змінили пароль	1,20
	Змінили пароль	1,51
Кібервіктимізація (індекс)*	Не змінили пароль	0,74
	Змінили пароль	2,31
Онлайн-активність з службовими, професійними, діловими цілями (фактор)*	Не змінили пароль	-0,524
	Змінили пароль	-0,117

* Середні значення залежної змінної. В інших випадках наводяться відсоткові показники.

Джерело: European Commission, Brussels (2022)

В результаті проведеного аналізу можна побачити наступні тенденції. В першій моделі стать не впливає на безпечну онлайн-поведінку: чоловіки та жінки демонструють однакову частоту використання зміни пароля як запобіжника ускладнень та загроз. Проте, це не виключає того, що всередині окремих національних спільнот можуть спостерігатися істотні крос-ґендерні відмінності. Два інших показники – вік і місце проживання – помітно диференціюють користувачів. Загалом, люди молодших вікових груп і містяни, особливо мешканці великих урбаністичних центрів, в середньому частіше змінюють пароль в мережі, а отже демонструють більш зважену поведінку.

В другій моделі очікувано більш безпечно поводяться онлайн представники більш високих класів. Водночас, всупереч нашим попереднім очікуванням люди, які не перебувають у шлюбі (за виключенням овдовілих), частіше за одружених вдаються до зміни паролю.

В третій моделі попередні припущення отримали підтвердження: людський капітал у вигляді більш високого рівня освіти та більшої поінформованості про ризики кіберзлочинності позитивно впливає на безпечну поведінку в Інтернеті.

Нарешті, цифровий капітал виявися також значущим фактором, що дозволяє прогнозувати безпечне поводження користувачів у мережі. Частота перебування онлайн, тобто досвід користування ІКТ, і зокрема, застосування Інтернету з професійними та діловими цілями, веде до позитивних наслідків, спонукаючи людей приділяти більше уваги безпековим питанням. В той же час негативний досвід, такий як більш високий рівень занепокоєння проблемами кіберзлочинності або власний досвід перебування в ролі жертви кіберзлочинного посягання, також може посприяти зміні в поведінці людей, використанню більш безпечних практик.

Висновки. Модерн, як епоха глибоких соціальних і технологічних змін, призводить до виникнення нових форм нерівності та конфліктів у суспільстві. Одним із проявів цього є цифровий розрив, що поглиблює соціальну стратифікацію та створює нові виклики для кібербезпеки. Пробне дослідження, представлене в статті, демонструє, що більш безпечна модель поводження в мережі залежить від наявності певних ресурсів, або різновидів капіталу – особистого, соціального, людського та цифрового. Як було показано в нашому емпіричному дослідженні, серед факторів, котрі сприяють більш відповідальній та безпечній поведінці онлайн-користувачів, важливу роль відіграє досвід користування Інтернетом (частота та змістовна наповненість діяльності, зокрема, зосередженість на вирішенні службових, професійних і бізнес-завдань), рівень знань про потенційні ризики та загрози, а також особистий досвід кіберзлочинності. Існують також соціально-демографічні відмінності в цифровій поведінці. Вік, рівень освіти, місце проживання та професія впливають на сприйняття людьми загроз та рівень безпеки в Інтернеті. Тому важливо з'ясувати, як пов'язані цифрова та соціальна нерівності, як нерівність у компетенціях та навичках роботи з інформаційно-комунікаційними технологіями трансформується в різноманітні досягнення.

Водночас, виявлення інших, додаткових факторів, котрі потенційно впливають на вибір людьми більш безпечної моделі поведінки в мережевих комунікаціях, потребує більш глибокого та детального аналізу. Маємо з'ясувати ступінь відносної впливовості кожного із виокремлених чинників і характер

взаємозв'язку між ними. Крім того, представлений аналіз обмежувався однією групою країн. Розширення географічного охоплення за рахунок включення країн інших регіонів ЄС може суттєво покращити наші уявлення про тенденції кіберповедінки у більш розвинутих суспільствах Західного світу і порівняти їх з менш технологічно та економічно просунутими регіонами світу. І наостанок, узагальнюючий аналіз для окремого регіону варто доповнити крос-національною перспективою, більш детальним поглядом всередину національних держав, їх порівнянням між собою, виявленням і поясненням схожості та відмінностей. Це надасть додатковий імпульс дослідженням у важливій з теоретичної та прикладної точок зору царині суспільних відносин, сприяючи розповсюдженню більш безпечного патерну кіберповедінки.

Korzhov H., Yenin M. Cybersecurity in conditions of digital inequality: defining the sociological problem

The article deals with theoretical and empirical aspects of the sociological study of behaviour in the field of cybersecurity. One of the relevant sociological approaches to the study of this phenomenon is the theory of three levels of digital inequality. The main hypothesis of the presented research is: a secure model of digital behaviour largely depends on the Internet user's position in the hierarchical distribution of various social, cultural, and digital resources, on individual's place in the overall system of social inequality. Among the factors that contribute to more responsible and secure behaviour of Internet users, the experience of using ICT (frequency and content of activities), the level of knowledge about potential risks and threats, and personal experience of cybercrime play an important role. Those Internet users who have longer, more intensive, and more varied experiences of using the Internet with different purposes tend to exhibit more prudent guidance and a securer pattern of Internet behaviour. Better knowledge and experiences of the victim of crime make users more vigilant and help prevent abuse and threats in the future. Age, education level, place of residence and occupation influence people's perception of threats and level of safety on the Internet, as well as their online behaviour. The research confirms that Internet users are changing their behaviour in various ways due to security concerns.

Key words: cybersecurity, digital inequality, digital capital, online communication, social networks, cybercrime, theory of three levels of the digital inequality, cybersecurity behaviour, modern, conflict.

Література:

1. Валюшко І. Кібербезпека України: наукові та практичні виміри сучасності. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право*. 2016. № 3-4. С. 117–124.
2. Діордіца І. Система забезпечення кібербезпеки: сутність та призначення. *Інформаційне право*. 2017. № 7. С. 109–116.
3. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва: монографія / Д. В. Дубов. К.: НІСД, 2014. 328 с.
4. Єнін М., Коржов Г. Мережева комунікація: ризики та перспективи (на основі соціологічних опитувань громадської думки в країнах Євросоюзу). *Вісник Національного технічного університету України «Київський політехнічний інститут». Політологія. Соціологія. Право: зб. наук. праць. Київ; Одеса*: Видавничий дім «Гельветика», 2021. № 1 (49). С. 22–29.
5. Єнін М., Кухта М. Цифровий розрив та вразливі у цифровому аспекті соціальні групи в Україні [Електронний ресурс]. *Соціокультурні трансформації та геополітичні виклики в умовах багатополярного світу*: тези доп. Всеукр. наук.-практ. конф. (Київ, 24 листоп. 2022 р.) / відп. ред. А. Кравченко. Київ: Держ. торг.-екон. ун-т, 2022. С. 216–220.
6. Коржов Г., Єнін М. Соціологічні виміри кібербулінґу: сутність, наслідки, стратегії подолання. *Соціологія: теорія, методи, маркетинг*. 2022. № 4. С. 156–173.
7. Кутуєв П. В. Трансформації модерну: інституції, ідеї, ідеології : монографія / П.В. Кутуєв. Херсон: Видавничий дім «Гельветика», 2016. 516 с.
8. Fedorchenko-Kutuev P., Pygolenko P., Khomiak A. Ukrainian State Between the Imperatives of Democracy and Post-War Modernization. *Ideology and Politics Journal*. 2023. № 1 (23). P. 148–171.
9. Маковець О., Дрозд І. Кібербезпека як фактор фінансової безпеки підприємства. *Економіка. Фінанси. Право*. 2020. № 5. С. 31–35.
10. Хоббі Ю. Право людини на кібербезпеку: проблеми визначення та гарантування. *Юридичний вісник*. 2020. № 2. С. 37–43.

11. Anwar M., He Wu, Ash I., Yuan X., Li L. Gender Difference and Employees' Cybersecurity Behaviour s. *Computers in Human Behaviour* . 2017, Vol. 69. P. 437–443.
12. Bolsover G., Howard P. Computational Propaganda and Political Big Data: Moving Toward a More Critical Research Agenda. *Big Data.* 2017. Vol. 5, No. 4. P. 273–276.
13. Castells M. The Rise of The Network Society: The Information Age: Economy, Society and Culture. John Wiley & Sons, 2000. 624 p.
14. Črnic T. O. Slovenians Offline: Class and Cultural Aspects of Digital Exclusion. *Sociologický časopis/ Czech Sociological Review*. 2013. Vol. 49, No. 6. P. 927–949.
15. Chen H., Beaudoin C. E., Hong T. Securing Online Privacy: An Empirical Test on Internet Scam Victimization, Online Privacy Concerns, and Privacy Protection Behaviours. *Computers in Human Behaviour*. 2017, Vol. 70. P. 291–302.
16. European Commission, Brussels. Eurobarometer 87.4. (2017). GESIS, Cologne. ZA6924 Data file Version 2.0.0. URL: https://www.unidata.unimib.it/wp-content/pdf/SI369_NM_CB_eng.pdf
17. Hargittai E. Second level digital divide: Differences in people's online skills. *First Monday*. 2002. Vol. 7, No. 4.
18. Ifinedo P. Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory. *Computers & Security*. 2012. Vol. 31, No. 1. P. 83–95.
19. Innis H. A. Empire and Communications. Toronto: University of Toronto Press, 1972. 288 p.
20. Innis H. A. The Bias of Communication. Toronto: University of Toronto Press, 1999. 227 p.
21. Kutuev P., Choliy S. (2018). Mobilization in post-socialist spaces: between imperatives of modernization and threats of demodernization. *Ideolology and politics.* № 2 (10). P. 4–22.
22. McLuhan M. The Gutenberg Galaxy: The Making of Typographic Man. Toronto: University of Toronto Press, 1962. 293 p.
23. Metzger M. M., Tucker J.A. Social Media and EuroMaidan: A Review Essay. *Slavic Review*. 2017. Vol. 76, No. 1 (Spring). P. 169–191.
24. Ragnedda M. Conceptualizing digital capital. *Telematics and Informatics.* 2018. Vol. 35. P. 2366–2375.
25. Shirky C. The political power of social media. *Foreign Affairs*. 2011. No. 1. P. 28–41.
26. Sparks C. What is the «Digital Divide» and why is it Important? *Javnost - The Public: Journal of the European Institute for Communication and Culture*. 2013. Vol. 20, No. 2. P. 27–46.
27. Van Dijk J. Digital divide research, achievements and shortcomings. *Poetics.* 2006. Vol. 34, No. 4–5. P. 221–235.
28. Van Dijk J. The Digital Divide. Cambridge; Medford: Polity Press, 2020. 208 p.
29. Wei K., Teo H., Chuan H., Tan B. Conceptualizing and Testing a Social Cognitive Model of the Digital Divide. *Information Systems Research*. 2011. Vol. 22, No. 1. P. 170–187.

References:

1. Valyushko, Í. (2016). Kiberbezpeka Ukraina: nauchnyye i prakticheskiye vozmozhnosti. *Vísnik NTUU «KPÍ». Politologiya. Sotsiologiya. Pravo*, (3-4), 117–124. [in Ukrainian].
2. Díorditsa, Í. (2017). Sistema bezpecheniya priznaniya kberbezpeki: sutníst' ta priznatel'nost'. *Informatsionnoye pravo*, (7), 109–116. [in Ukrainian].
3. Dubov, D. V. (2014). Kiberprostír kak novyy vimír geopoliticheskogo supernitstva: monografiya / D. V. Dubov. K.: NÍSD. 328 s. [in Ukrainian].
4. Yenin, M., Korzhov, H. (2021). Merezheva komunikatsiya: ryzyky ta perspektyvy (na osnovi sotsiolohichnykh opytuvan' hromads'koyi dumky v krayinakh Yevrosoyuzu). *Visnyk Natsional'noho tekhnichnoho universytetu Ukrayiny «Kyyivs'kyy politekhnichnyy instytut». Politolohiya. Sotsiolohiya. Pravo: zb. nauk. prats'*. Kyyiv; Odesa: Vydavnychyy dim «Hel'vetyka» (1), (49), 22–29. [in Ukrainian].
5. Yenin, M., Kukhta, M. (2022). Tsyfrovyy rozryv ta vrazlyvi u tsyfrovomu aspekti sotsial'ni hrupy v Ukrayini [Elektronnyy resurs]. *Sotsiokul'turni transformatsiyi ta heopolitychni vyklyky v umovakh bahatopolyarnoho svitu*: tezy dop. Vseukr. nauk.-prakt. konf. / vidp. red. A. Kravchenko. Kyyiv: Derzh. torh.-ekon. un-t, 216–220. [in Ukrainian].
6. Korzhov, H., Yenin, M. (2022). Sotsiolohichni vymiry kiberbulingu: sutnist', naslidky, stratehiyi podolannya. *Sotsiolohiya: teoriya, metody, marketynh*. (4), 156–173. [in Ukrainian].
7. Kutuev, P. V. (2016). Transformatsii moderna: institutsii, idei, ideologii: monografiya / P. V. Kutuyevym. Kherson: Izdatel'skiy dom «Gel'vetika». 516 s. [in Ukrainian].
8. Fedorchenko-Kutuev, P., Pyholenko, I., Khomiak, A. (2023). Ukrainian State Between the Imperatives of Democracy and Post-War Modernization. *Ideology and Politics Journal*, (1), (23), 148–171. [in Ukrainian].

9. Makovets', O., Drozd, I. (2020). Kiberbezpeka yak faktor finansovoyi bezpeky pidpryyemstva. *Ekonomika. Finansy. Pravo*, (5), 31–35. [in Ukrainian].
10. Khobbi, Yu. (2020). Pravo lyudyny na kiberbezpeku: problemy vyznachennya ta harantuvannya. *Yurydychnyy visnyk*, (2), 37–43. [in Ukrainian].
11. Anwar, M., He, Wu, Ash, I., Yuan, X., Li, L. (2017). Gender Difference and Employees' Cybersecurity Behaviour s. *Computers in Human Behaviour* , 69, 437–443. [in English].
12. Bolsover G., Howard P. (2017). Computational Propaganda and Political Big Data: Moving Toward a More Critical Research Agenda. *Big Data*, 5 (4), 273–276. [in English].
13. Castells, M. (2000). The Rise of The Network Society: The Information Age: Economy, Society and Culture. John Wiley & Sons. 624 p. [in English].
14. Črnic, T. O. (2013). Slovenians Offline: Class and Cultural Aspects of Digital Exclusion. *Sociologický časopis/Czech Sociological Review*, 49 (6), 927–949. [in English].
15. Chen, H., Beaudoin, C. E., Hong, T. (2017). Securing Online Privacy: An Empirical Test on Internet Scam Victimization, Online Privacy Concerns, and Privacy Protection Behaviours. *Computers in Human Behaviour*, (70), 291–302. [in English].
16. European Commission, Brussels. Eurobarometer 87.4. (2017). GESIS, Cologne. ZA6924 Data file Version 2.0.0. URL: https://www.unidata.unimib.it/wp-content/pdf/SI369_NM_CB_eng.pdf [in English].
17. Hargittai, E. (2002). Second level digital divide: Differences in people's online skills. *First Monday*, 7 (4). [in English].
18. Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory. *Computers & Security*, 31 (1), 83–95. [in English].
19. Innis, H. A. (1972). Empire and Communications. Toronto: University of Toronto Press, 288 p. [in English].
20. Innis, H. A. (1999). The Bias of Communication. Toronto: University of Toronto Press, 227 p. [in English].
21. Kutuev, P., Choliy, S. (2018). Mobilization in post-socialist spaces: between imperatives of modernization and threats of demodernization. *Ideolology and politics*, 2 (10), 4–22. [in English].
22. McLuhan, M. (1962). The Gutenberg Galaxy: The Making of Typographic Man. Toronto: University of Toronto Press, 293 p. [in English].
23. Metzger, M. M., Tucker, J. A. (2017). Social Media and EuroMaidan: A Review Essay. *Slavic Review*, 76 (1), 169–191. [in English].
24. Ragnedda, M. (2018). Conceptualizing digital capital. *Telematics and Informatics,* 35, 2366–2375. [in English].
25. Shirky, C. (2011). The political power of social media. *Foreign Affairs*, 1, 28–41. [in English].
26. Sparks, C. (2013). What is the «Digital Divide» and why is it Important? *Javnost - The Public: Journal of the European Institute for Communication and Culture*, 20 (2), 27–46. [in English].
27. Van Dijk, J. (2006). Digital divide research, achievements and shortcomings. *Poetics*, 34 (4–5), 221–235. [in English].
28. Van Dijk, J. (2020). The Digital Divide. Cambridge; Medford: Polity Press, 208 p. [in English].
29. Wei, K., Teo, H., Chuan, H., Tan, B. (2011). Conceptualizing and Testing a Social Cognitive Model of the Digital Divide. *Information Systems Research*, 22 (1), 170–187. [in English].

Стаття надійшла до редакції 25.09.2024
Стаття рекомендована до друку 30.09.2024