

УДК 159.9:004.056.5:316.472.4:342.721
DOI: [https://doi.org/10.17721/BPSY.2024.2\(20\).17](https://doi.org/10.17721/BPSY.2024.2(20).17)

Катерина СПРАВЦЕВА, асп.
ORCID ID: 0000-0001-5802-0344
e-mail: k.spravtseva.asp@kubg.edu.ua
Київський столичний університет імені Бориса Грінченка, Київ, Україна

ПСИХОЛОГІЧНІ АСПЕКТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ В ЦИФРОВОМУ СЕРЕДОВИЩІ

Вступ. Наголошено, що в умовах стрімкої діджиталізації суспільства та зростання кількості користувачів соціальних мереж до 5,5 мільярда осіб (67,1 % світової популяції) актуалізується проблема захисту приватності особистості в цифровому просторі. За даними Pew Research Center (2024), 79 % користувачів висловлюють занепокоєння щодо збереження персональних даних, при цьому кількість порушень приватності демонструє прогресивну динаміку. Мета дослідження – здійснити комплексний аналіз психологічних механізмів управління приватністю у соціальних мережах та розробити науково обґрунтовані стратегії захисту психологічного благополуччя користувачів.

Методи. Дослідження засновано на інтеграції системного, особистісно орієнтованого підходів та соціально-когнітивної теорії. Використано комплекс теоретичних (системний аналіз літератури, мета-аналіз емпіричних досліджень, концептуальне моделювання) та емпіричних методів (психодіагностичні методики, нейропсихологічні дослідження, лонгітюдні спостереження). Проведено мета-аналіз 166 досліджень із загальною вибіркою понад 75,000 учасників.

Результати. Емпірично підтверджено існування "парадоксу приватності" – розбіжності між декларованим занепокоєнням щодо захисту інформації та реальною поведінкою користувачів. Виявлено значущий зв'язок між порушенням приватності та погіршенням психологічного благополуччя: підвищення рівня тривожності та депресивної симптоматики. Нейропсихологічні дослідження продемонстрували активацію специфічних мозкових структур під час прийняття рішень щодо розкриття інформації. Розглянуто роботу зі шкалою цифрової резильєнтності. Ідентифіковано основні маніпулятивні стратегії в соціальних мережах: переконання (33 %), агітація (17 %), викривлення інформації (15 %).

Висновки. Установлено необхідність комплексного підходу до захисту приватності, що інтегрує розвиток цифрової компетентності, медіаграмотності та психологічної стійкості. Обґрунтовано ефективність системи медіапсихологічної підтримки через взаємопов'язані напрями медіааналітики, медіатерапії та медіаосвіти. Результати дослідження створюють теоретичне підґрунтя для розроблення програм психологічного супроводу користувачів соціальних мереж та вдосконалення систем захисту приватності.

Ключові слова: цифрова приватність, психологічна безпека, самопрезентація у соціальних мережах, кібербезпека особистості, медіакомпетентність.

Вступ

В епоху глобальної діджиталізації та стрімкого розвитку інформаційних технологій трансформація соціальних комунікацій набуває безпрецедентних масштабів. За даними Digital 2024: Global Digital Overview (2024), кількість активних користувачів соціальних мереж досягла 5,5 мільярда осіб, що становить 67,1 % світової популяції. Цей показник демонструє щорічне зростання на 6,5 %, що свідчить про подальшу інтенсифікацію діджиталізації соціальних взаємодій та формування нових патернів міжособистісної комунікації. Паралельно з розширенням цифрового простору загострюється проблематика захисту приватності особистості. Згідно з дослідженням Social Media Use in 2024 (Pew Research Center), 79 % користувачів соціальних мереж висловлюють занепокоєння щодо збереження їхніх персональних даних. При цьому статистика порушень приватності демонструє прогресивну динаміку: за даними Annual Data Breach Report, кількість витоків персональних даних у 2023 році зросла на 42 % порівняно з попереднім роком, також за даними ITRC Q3 Data Breach Analysis за другий квартал 2024 року кількість жертв становила 1,043,903,153 осіб (Identity Theft Resource Center). Ці дані актуалізують необхідність глибокого наукового аналізу психологічних механізмів управління приватністю у цифровому просторі. Теоретико-методологічною основою дослідження приватності виступає інтеграція системного підходу (Bertalanffy, 1968), що дозволяє розглядати приватність як складну багаторівневу систему взаємопов'язаних елементів, особистісно-орієнтованого підходу (Rogers, 1959), який акцентує увагу на індивідуальних особливостях сприйняття та управління приватністю, та соціально-когнітивної теорії (Bandura, 1986), що пояснює механізми формування поведінкових патернів у цифровому середовищі.

Сучасний науковий дискурс щодо приватності в соціальних мережах характеризується мультидисциплінарністю та охоплює різні аспекти проблеми. Психологічні

дослідження зосереджуються на вивченні механізмів прийняття рішень щодо розкриття інформації та аналізі психологічних наслідків порушення приватності. Нейропсихологічні дослідження розкривають нейронні кореляти процесів прийняття рішень та емоційних реакцій на порушення приватності. Соціально-психологічні дослідження аналізують групові норми, цінності та крос-культурні відмінності у ставленні до приватності. Методологія дослідження базується на комплексному застосуванні теоретичних методів (системний аналіз наукової літератури, мета-аналіз емпіричних досліджень, концептуальне моделювання) та емпіричних методів (психодіагностичні методики, нейропсихологічні дослідження, лонгітюдні спостереження, експериментальні дослідження). Така методологічна база забезпечує всебічний аналіз досліджуваного феномену.

Метою дослідження є комплексний аналіз психологічних механізмів управління приватністю у соціальних мережах та розроблення науково обґрунтованих стратегій захисту психологічного благополуччя користувачів. У межах дослідження планується систематизувати сучасні підходи до вивчення приватності, проаналізувати механізми формування парадоксу приватності, дослідити нейропсихологічні кореляти прийняття рішень та оцінити ефективність різних стратегій захисту приватності.

Завдання дослідження: систематизація та аналіз сучасних теоретичних підходів до вивчення феномену приватності, виявлення та аналіз психологічних механізмів формування парадоксу приватності, дослідження нейропсихологічних корелятів прийняття рішень щодо розкриття особистої інформації, оцінка ефективності наявних стратегій захисту приватності, розроблення комплексних рекомендацій щодо захисту психологічного благополуччя користувачів соціальних мереж.

Отримані результати можуть стати основою для подальших досліджень у галузі психології приватності та

© Справцева Катерина, 2024

розробляння практичних рекомендацій щодо безпечного користування соціальними мережами. Особлива увага приділяється розроблюванню стратегій, що враховують індивідуальні особливості користувачів та специфіку різних соціальних платформ.

Методи

Дослідження базується на інтеграції системного, особистісно-орієнтованого підходів та соціально-когнітивної теорії. Використано комплекс теоретичних (системний аналіз літератури, мета-аналіз емпіричних досліджень, концептуальне моделювання) та емпіричних методів (психодіагностичні методики, нейропсихологічні дослідження, лонгітюдні спостереження). Проведено мета-аналіз 166 досліджень із загальною вибіркою понад 75,000 учасників.

Результати

Стрімкий розвиток інформаційних технологій та соціальних мереж суттєво трансформуює розуміння приватності особистості та механізмів її захисту в цифровому просторі. Як слушно зазначає вітчизняна науковиця Дерев'янка (2024), "загрози праву на приватність походять від функціональних особливостей новітніх комунікативних й інформаційних технологій, які потребують (залучають) величезну кількість персональних даних для свого ефективного функціонування. Глобальна цифровізація також сприяла масштабуванню можливостей спостереження й нагляду за особою та її приватним життям. "Теоретичне осмислення феномену приватності в контексті соціальних мереж вимагає інтеграції класичних концепцій та сучасних емпіричних досліджень для формування цілісного розуміння психологічних механізмів її регуляції.

Фундаментальні дослідження приватності як психологічного феномену беруть свій початок у роботах А. Вестайна (Westin, 1967), який запропонував трикомпонентну модель приватності, що включає секретність, анонімність та усамітнення. Ця концепція стала основоположною для подальшого розвитку теоретичних підходів до розуміння приватності в різних контекстах соціальної взаємодії.

Значний внесок у розвиток теорії приватності зробила С. Петроніо через розробку теорії управління комунікаційною приватністю (Communication Privacy Management Theory) (Petronio, 2002). Відповідно до її досліджень, приватність розглядається як динамічний процес управління інформаційними межами, що постійно змінюються під впливом різноманітних факторів. Ця теорія набула особливої актуальності в контексті соціальних мереж, де користувачі постійно приймають рішення щодо розкриття особистої інформації.

Теорія контекстуальної цілісності (Nissenbaum, 2010) пропонує розглядати приватність через призму соціальних норм та контексту. Дослідниця наголошує на тому, що оцінка прийнятності розкриття інформації завжди залежить від конкретного контексту та відповідних соціальних конвенцій. Цей підхід особливо релевантний для аналізу поведінки користувачів у різних соціальних мережах, де контекст комунікації може швидко змінюватися.

Модель калькуляції приватності (Dinev, & Hart, 2006) пояснює процес прийняття рішень щодо розкриття інформації через призму оцінювання потенційних ризиків та вигод. При цьому дослідники відзначають, що таке оцінювання часто відбувається на підсвідомому рівні та може бути викривлено різноманітними когнітивними упередженнями.

Особливої уваги заслуговує феномен "парадоксу приватності", детально досліджений у роботах (Baruh et al., 2017). Їхнє мета-аналітичне дослідження виявило слабку кореляцію між висловленим занепокоєнням щодо приватності та фактичним розкриттям особистої інформації онлайн, що свідчить про складність

психологічних механізмів регуляції приватності в цифровому просторі. Зокрема, вивчення безпеки самопрезентації у віртуальному просторі заслуговує окремої уваги, де користувачі соціальних мереж невимусовно трансплюють своє самосприйняття, емоційні стани, поведінкові інтенції та смисложиттєві орієнтації через символічно навантажений візуальний контент (Справцева, 2024), часто таким чином надаючи велику кількість особистої інформації несвідомо.

Нейропсихологічні дослідження (Acquisti et al., 2015) демонструють залучення специфічних нейронних мереж у процеси прийняття рішень щодо приватності, включаючи активацію областей мозку, пов'язаних з оцінюванням ризиків та емоційною регуляцією. Ці висновки підтверджуються дослідженнями Трепте і Райнеке (Trepte, & Reinecke, 2011), які додатково вивчали аспекти самопрезентації в соціальних мережах.

Професори (Boyd, & Marwick, 2011) у своєму дослідженні підлітків та їхнього ставлення до приватності в соціальних мережах виявили, що молоді користувачі розробляють складні стратегії управління своєю приватністю, які часто відрізняються від традиційних уявлень про захист особистої інформації.

Варто також зазначити, що подальший розвиток досліджень у цій сфері потребує більш глибокого теоретичного осмислення взаємозв'язків між різними аспектами приватності та психологічної безпеки. Особливу увагу, на думку автора, слід приділити розробляння інтегративних теоретичних моделей, що враховують як індивідуально-психологічні, так і соціокультурні фактори формування та підтримання психологічної безпеки в цифровому середовищі. Це дозволить не лише поглибити розуміння досліджуваних феноменів, але й розробити більш ефективні стратегії захисту приватності та забезпечення психологічного благополуччя користувачів соціальних мереж.

У контексті стрімкої цифровізації суспільства та трансформації соціальних відносин особливої актуальності набуває емпіричне дослідження приватності в соціальних мережах. Традиційне розуміння приватності, що сформувалося у доцифрову епоху, вже не відповідає викликам сучасності, де межі між приватним і публічним стають все більш розмитими.

Феномен приватності в соціальних мережах являє собою складний, багатовимірний конструкт, що інтегрує психологічні, соціальні та технологічні аспекти людської взаємодії. Емпіричне вивчення цього феномену дозволяє не лише зрозуміти механізми його функціонування, але й виявити приховані закономірності поведінки користувачів у цифровому просторі. Зокрема, мета-аналітичне дослідження, проведене Барух та співавторами (Baruh et al., 2017), охопило 166 незалежних досліджень із загальною вибіркою понад 75,000 учасників, виявивло комплексну природу взаємозв'язків між задекларованими намірами та реальною поведінкою у контексті захисту приватності.

Парадоксальність ситуації полягає в тому, що, незважаючи на рстуче занепокоєння щодо приватності, користувачі соціальних мереж часто демонструють поведінку, яка суперечить їхнім декларованим намірам щодо захисту особистої інформації. Експериментальне дослідження (Craig et al., 2020) з використанням методології повторних вимірювань протягом шести місяців показало значущий зв'язок між порушенням приватності в соціальних мережах та погіршенням показників психологічного благополуччя. Незважаючи на те, що учасники, які зазнали порушень приватності, демонстрували підвищений рівень тривожності ($d = 0.45$) та депресивної

симптоматики ($r = 0.38$), це не вплинуло на контроль власної активності в соціальних мережах.

Особливої уваги заслуговує нейробіологічний аспект прийняття рішень щодо розкриття особистої інформації. Активна специфічних мозкових структур під час оцінювання ризиків приватності свідчить про глибинну природу цих процесів та їх еволюційну значущість для людського виду. Це відкриває новий вимір у розумінні природи приватності та механізмів її регуляції. Використання методів нейровізуалізації в дослідженні (Acquisti et al., 2020) дозволило виявити специфічні патерни активації мозку під час прийняття рішень щодо розкриття особистої інформації. Зокрема, спостерігалася підвищена активність у мигдалеподібному тілі та префронтальній корі під час оцінювання потенційних ризиків розкриття інформації.

Методологічний арсенал дослідження приватності також зазнає суттєвої трансформації. Класичні методи психологічних досліджень доповнюються інноваційними підходами, що дозволяють вивчати поведінку користувачів у їхньому природному цифровому середовищі. Це створює нові можливості для розуміння реальних патернів поведінки та прийняття рішень щодо приватності. Дослідження (Distler et al., 2023), проведене з використанням методу вибірки досвіду (ESM), продемонструвало важливість відстеження поведінки користувачів у їхньому природному середовищі. Метод ESM дозволяє збирати дані про поточну ситуацію та досвід учасників у реальному часі, що підвищує екологічну валідність дослідження порівняно з лабораторними умовами.

Крос-культурне дослідження, проведене з використанням фокус-груп (Distler et al., 2023), виявило, що цей метод є недостатньо популярним, але перспективним підходом для отримання якісних глибинних даних щодо ставлення до приватності та безпеки. Фокус-групи проводилися як з пересічними користувачами, так і з експертами з безпеки, що дозволило отримати різнобічне розуміння досліджуваних питань. Експериментальне дослідження з використанням методу спільного створення (co-creation) (Distler et al., 2023) показало ефективність залучення користувачів до процесу розроблювання механізмів захисту приватності. Цей підхід розглядає користувачів як співтворців і партнерів, які є експертами у своєму життєвому досвіді, що дозволяє створювати більш релевантні та прийнятні рішення.

Психологічна безпека в контексті соціальних мереж набуває нових форм і проявів. Вона стає не просто станом захищеності від загроз, а динамічним процесом постійної адаптації до мінливого цифрового середовища. Життєстійкість особистості в цьому контексті виступає ключовим фактором успішної адаптації та збереження психологічного благополуччя. Лонгitudне дослідження Чуйко та ін. (2021) продемонструвало, що психологічна безпека є комплексним, інтегральним, динамічним явищем, яке проявляється у відчутті людиною захищеності від зовнішніх і внутрішніх загроз, контрольованості життєвих подій, упевненості у здатності зберігати стійку рівновагу та опиратися можливим загрозам. Дослідники виявили, що психологічна безпека тісно пов'язана з життєстійкістю особистості та її складниками: залученістю до життя, контролем за стресогенними ситуаціями та прийняттям ризику як життєвого виклику.

Емпіричне вивчення приватності в соціальних мережах має не лише теоретичне, але й важливе практичне значення. Розуміння механізмів регуляції приватності дозволяє розробляти більш ефективні стратегії захисту особистої інформації та підтримки психологічного благополуччя користувачів. Це особливо важливо в контексті ростучих кіберзагроз та інформаційних маніпуляцій,

наприклад, дослідження (Wisniewski et al., 2017) з використанням змішаних методів дозволило розробити та валідизувати шкалу цифрової резильєнтності, яка показала високу надійність ($\alpha = 0.89$) та конструктну валідність. Шкала демонструє значущу кореляцію з практиками захисту приватності та психологічним благополуччям користувачів.

Таким чином, емпіричні дослідження приватності в соціальних мережах є критично важливим напрямом сучасної науки, що забезпечує розуміння складних взаємозв'язків між технологічними, психологічними та соціальними аспектами цифрового життя. Вони надають необхідну емпіричну базу для розроблення ефективних стратегій захисту приватності та підтримки психологічного благополуччя користувачів у цифровому просторі.

Цифровий простір створює унікальне середовище, де традиційні механізми психологічного захисту можуть виявитися неефективними або навіть шкідливими. Важливо розуміти, що вразливість у цифровому середовищі має свої специфічні особливості та прояви, які відрізняються від традиційних форм психологічної вразливості. Це пов'язано з такими характеристиками цифрового простору, як анонімність, відсутність фізичних кордонів, швидкість поширення інформації та складність контролю власного цифрового сліду (Baruh et al., 2017).

Психологічна вразливість у цифровому просторі має кумулятивний ефект. Постійне перебування у стані психологічного напруження, викликане необхідністю захищати свою приватність, контролювати онлайн-репутацію та протистояти різноманітним формам цифрового тиску, може призводити до серйозних наслідків для ментального здоров'я. Розуміння механізмів цього процесу є критичним для розроблювання ефективних стратегій психологічної підтримки та профілактики.

Психологічні механізми вразливості в цифровому просторі включають комплекс факторів.

Когнітивні фактори:

- надмірна довірливість у віртуальному просторі;
- ілюзія контролю над персональними даними;
- недооцінка потенційних ризиків;
- схильність до необґрунтованого оптимізму щодо онлайн-безпеки Лаптев (2024).

Поведінкові патерни ризику:

- надмірне саморозкриття в соціальних мережах;
- нехтування налаштуваннями приватності;
- необачне поширення особистої інформації;
- ігнорування сигналів потенційної небезпеки (Довбуш та ін., 2023).

Дослідження демонструють, що ефективний захист приватності вимагає комплексного підходу, який має включати такі компоненти:

Розвиток цифрової компетентності:

- формування навичок критичного аналізу інформації;
- розуміння принципів роботи цифрових платформ;
- вміння ідентифікувати потенційні загрози.

Психологічна підготовка:

- розвиток емоційної стійкості;
- формування адекватної оцінки ризиків;
- навички протидії маніпулятивному впливу (Бутиріна, 2012).

Наразі наукова спільнота приділяє велику увагу вивченню маніпулятивних стратегій та вбачає в них особливу небезпеку (Wisniewski et al., 2017). Головною навичкою протидії маніпуляції у соціальних мережах вважається критичне мислення (Тягло, 2017) та здатність розпізнавати маніпулятивні стратегії (Dovbush et al., 2023), які можна класифікувати (табл. 1).

Таблиця 1

Маніпулятивні стратегії у соціальних мережах

Стратегія	Частота використання	Тактики реалізації
Переконання	33 %	Апеляція до авторитету (6 %) – Позитивне підкріплення (5 %) – Гра в простонародність (5.5 %) – Гіперболізація (4 %) – Апеляція до емоцій (12.5 %)
Агітація	17 %	Заклики (10 %) – Обіцянки (7 %)
Викривлення інформації	15 %	Вуалізація (4 %) – Переакцентування (4.5 %) – Сяючі узагальнення (3.5 %) – Навішування ярликів (2 %)
Дискредитації	13 %	Критика – Звинувачення – Образа – Погроза – Створення опозиції "свій-чужий"
Самопрезентації	10 %	Самопросування (3 %) – Вихвалання та екземпліфікація (7 %)
Позитиву	7 %	Підвищення значущості співрозмовника (7 %)
Ідентифікації	5 %	Солідаризація із співрозмовником (5 %)

Професор Петрунко (2011) вважає важливим аспектом розвиток медіакомпетентності, яка включає три ключові компоненти (табл. 2).

У контексті захисту психологічного благополуччя важливу роль відіграє медіапсихологічна підтримка, яка реалізується через систему взаємопов'язаних напрямів (Найдюнова, & Баришполець, 2009) (табл. 3).

Таблиця 2

Компоненти розвитку медіакомпетентності

Аналітичний компонент:	Практичний компонент:	Рефлексивний компонент:
• здатність критично оцінювати медіаконтент; • розуміння механізмів медіавпливу; • навички верифікації інформації.	• уміння налаштовувати параметри приватності; • навички безпечного користування цифровими сервісами; • здатність протидіяти кібербулінгу.	• усвідомлення власних патернів онлайн-поведінки; • розуміння своїх вразливостей; • здатність до саморегуляції в цифровому просторі.

Таблиця 3

Напрями медіапсихологічної підтримки

Медіааналітика	Медіатерапія	Медіаосвіта
• дослідження психологічних аспектів медіаконтенту; • виявлення потенційно шкідливих інформаційних впливів; • моніторинг актуальних кіберзагроз.	• розроблення методів психологічного захисту; • формування стресостійкості; • розвиток навичок психологічної саморегуляції.	• формування критичного мислення; • розвиток цифрової грамотності; • навчання методів захисту приватності.

Таким чином, захист психологічного благополуччя у цифровому просторі вимагає системного підходу, що поєднує розвиток медіакомпетентності, формування навичок критичного мислення та впровадження ефективних стратегій психологічного захисту.

Дискусія і висновки

Проведене дослідження психологічних аспектів приватності в соціальних мережах розкриває складну природу взаємодії особистості з цифровим простором та механізми регуляції приватності в умовах глобальної діджиталізації. Теоретичний аналіз продемонстрував необхідність переосмислення класичних концепцій приватності в контексті сучасних викликів цифрового суспільства. Особливо важливим виявляється розуміння динамічної природи приватності як процесу постійного балансування між потребою у саморозкритті та захистом особистих меж.

Емпірична верифікація "парадоксу приватності", підтверджена масштабними мета-аналітичними дослідженнями, свідчить про глибинну суперечність між декларованими намірами та реальною поведінкою користувачів соціальних мереж. Це явище потребує особливої уваги, оскільки демонструє обмеженість раціональних моделей прийняття рішень щодо захисту приватності та вказує на необхідність урахувати підсвідомі механізми регуляції поведінки. Підтвердженням цього є результати нейропсихологічних досліджень, які виявили активацію специфічних мозкових структур під час прийняття рішень щодо розкриття особистої інформації.

Установлений значущий зв'язок між порушенням приватності та погіршенням показників психологічного благополуччя підкреслює важливість розробляти ефективні стратегії захисту особистості в цифровому просторі. При

цьому особливого значення набуває розвиток цифрової резильєнтності як інтегративної здатності протистояти викликам онлайн-середовища. Валідизація відповідного діагностичного інструментарію створює основу для подальших емпіричних досліджень та розроблення практичних рекомендацій.

Виявлені в ході дослідження маніпулятивні стратегії в соціальних мережах та розроблена класифікація тактик їх реалізації мають важливе практичне значення для розвитку медіаграмотності користувачів. Запропонована модель медіакомпетентності, що включає аналітичний, практичний та рефлексивний компоненти, створює теоретичне підґрунтя для розроблювання освітніх програм та тренінгових методик.

Особливу цінність становить обґрунтування системи медіапсихологічної підтримки, що інтегрує напрями медіааналітики, медіатерапії та медіаосвіти. Такий комплексний підхід дозволяє не лише захищати користувачів від потенційних загроз, але й розвивати їхню здатність до свідомого та безпечного користування соціальними мережами.

Дослідження демонструє, що ефективний захист приватності вимагає комплексного підходу, який має включати такі компоненти: розвиток цифрової компетентності, зокрема формування навичок критичного аналізу інформації, розуміння принципів роботи цифрових платформ, уміння ідентифікувати потенційні загрози; та психологічну підготовку, а саме розвиток емоційної стійкості, формування адекватної оцінки ризиків, навички протидії маніпулятивному впливу.

Результати дослідження відкривають перспективи для подальшого вивчення тривалих наслідків порушення

приватності та вживання превентивних заходів захисту користувачів у цифровому просторі. Особливої актуальності набуває дослідження механізмів формування культури приватності в онлайн-середовищі та розвитку цифрової резильєнтності різних вікових та соціальних груп.

Теоретична значущість отриманих результатів полягає у поглибленні розуміння психологічних механізмів регуляції приватності в цифровому просторі та розширенні концептуального апарату психології приватності. Практичне значення дослідження визначається можливістю використання його результатів для розроблювання програм психологічного супроводу користувачів соціальних мереж, створення освітніх курсів із цифрової грамотності та вдосконалення систем захисту приватності. Подальші дослідження мають зосередитися на розроблянні та валідації конкретних інструментів оцінювання та розвитку цифрової резильєнтності, а також на вивченні крос-культурних аспектів сприйняття та захисту приватності в соціальних мережах.

Список використаних джерел

- Бутіріна, М. В. (2012). Медіапсихологія: До питання формування навчальної дисципліни. *Вчені записки Таврійського національного університету ім. В. І. Вернадського*, 25(64), 85–90.
- Дерев'яно, Н. (2024). Захист права на приватність у контексті глобальної цифровізації. *Журнал інновацій та технологій в соціальній роботі і охорони*, 8(26), 591–603. [https://doi.org/10.52058/2786-6300-2024-8\(26\)-591-603](https://doi.org/10.52058/2786-6300-2024-8(26)-591-603)
- Довбуш, О., Гарасим, Т., & Скорейко-Свірська, І. (2023). Вербалізація маніпулятивних стратегій у соціальних мережах Facebook і Twitter. *Folium, Спецвип.*, 54–60. <https://doi.org/10.32782/folium/2023.3.7>
- Лаптев, С. О. (2024). Розробка моделі захисту особистих даних у соціальних мережах. *Захист інформації*, 26(1), 43–50.
- Найдьонов, Л. А., Баршполець, О. Т. (Ред.) (2009). *Медіакультура особистості: соціально-психологічний підхід*. Миленіум. <https://mediaosvita.org.ua/wp-content/uploads/2016/11/Posibnik.pdf>
- Петрунко, О. В. (2011). Агресивне медіасередовище: Якісний і змістовий дискурс. *Рідна мова*, 16, 36–43.
- Справцева, К. (2024). Психологічний аналіз структурних компонентів образу "Я" у візуальній самопрезентації. *Наукові перспективи*, 6(48), 1013–1023. [https://doi.org/10.52058/2708-7530-2024-6\(48\)](https://doi.org/10.52058/2708-7530-2024-6(48))
- Тягло, О. В. (2017). Критичне мислення в дії, або Досвід критичної рецензії. *Постметодика*, 1, 8–13.
- Чуйко, Г. В., Чаплук, Я. В., & Комисарик, М. І. (2021). Психологічна безпека особистості в нестабільному світі. *Психологічний часопис*, 7(1), 65–81. <https://doi.org/10.31108/1.2021.7.1.6>
- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2020). Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology*, 30(4), 736–758. <https://doi.org/10.1002/jcpy.1191>
- Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. Prentice-Hall.
- Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, 67(1), 26–53. <https://doi.org/10.1111/jcom.12276>
- Bertalanffy, L. von. (1968). *General system theory: Foundations, development, applications*. George Braziller.
- Boyd, D., & Marwick, A. (2011). *Social privacy in networked publics: Teens' attitudes, practices, and strategies*. Oxford Internet Institute.
- Craig, W., Boniel-Nissim, M., King, N., Walsh, S. D., Boer, M., Donnelly, P. D., ... Pickett, W. (2020). Social media use and cyber-bullying: A cross-national analysis of young people in 42 countries. *Journal of Adolescent Health*, 66(6), S100–S108. <https://doi.org/10.1016/j.jadohealth.2020.03.006>
- Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61–80. <https://doi.org/10.1287/isre.1060.0080>
- Distler, V., Fassl, M., Habib, H., Krombholz, K., Lenzini, G., Lallemand, C., Koenig, V., & Faith Cranor, L. (2023). Empirical research methods in usable privacy and security. In N. Gerber, A. Stöver, & K. Marky (Eds.), *Human factors in privacy research* (pp. 29–53). Springer.
- Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford Law Books.
- Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. State University of New York Press.
- Petrunko, O. V. (2011). Aggressive media environment: Qualitative and content discourses. *Native language*, 16, 36–43 [in Ukrainian].
- Rogers, C. R. (1959). A theory of therapy, personality, and interpersonal relationships: As developed in the client-centered framework. In S. Koch (Ed.) *Psychology: A study of a science* (Vol. 3, pp. 184–256). McGraw-Hill.
- Sprattseva, K. (2024). Psychological analysis of the structural components of the self-image in visual self presentation. *Scientific Perspectives*, 6(48), 1013–1023. [https://doi.org/10.52058/2708-7530-2024-6\(48\)](https://doi.org/10.52058/2708-7530-2024-6(48)) [in Ukrainian].
- Tiahlo, O. V. (2017). Critical thinking in action, or Experience of critical review. *Postmethodology*, 1, 8–13 [in Ukrainian].
- Trepte, S., & Reinecke, L. (2011). *Privacy online: Perspectives on privacy and self-disclosure in the social web*. Springer. <https://link.springer.com/book/10.1007/978-3-642-21521-6>
- Westin, A. F. (1967). *Privacy and freedom*. Atheneum.
- Wisniewski, P., Xu, H., Rosson, M. B., & Carroll, J. M. (2017). Parents just don't understand: Why teens don't talk to parents about their online risk experiences. In Ch. P. Lee, & S. Poltrock (Eds.) *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (pp. 523–540). Association for Computing Machinery. <https://doi.org/10.1145/2998181.2998236>

References

- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2020). Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology*, 30(4), 736–758. <https://doi.org/10.1002/jcpy.1191>
- Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. Prentice-Hall.
- Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, 67(1), 26–53. <https://doi.org/10.1111/jcom.12276>
- Bertalanffy, L. von. (1968). *General system theory: Foundations, development, applications*. George Braziller.
- Boyd, D., & Marwick, A. (2011). *Social privacy in networked publics: Teens' attitudes, practices, and strategies*. Oxford Internet Institute.
- Butyrina, M. V. (2012). Media psychology: To the question of formation of educational discipline. *Scientific notes of V. I. Vernadsky Taurida National University*, 25(64), 85–90 [in Ukrainian].
- Chuiiko, H. V., Chaplук, Y. V., & Komisaryk, M. I. (2021). Psychological security of personality in an unstable world. *Psychological Journal*, 7(1), 6–81 [in Ukrainian]. <https://doi.org/10.31108/1.2021.7.1.6>
- Craig, W., Boniel-Nissim, M., King, N., Walsh, S. D., Boer, M., Donnelly, P. D., ... Pickett, W. (2020). Social media use and cyber-bullying: A cross-national analysis of young people in 42 countries. *Journal of Adolescent Health*, 66(6), S100–S108. <https://doi.org/10.1016/j.jadohealth.2020.03.006>
- Derevianko, N. (2024). Protection of the right to privacy in the context of global digitalization. *Journal of Innovation and Technologies in Social Work and Education*, 8(26), 591–603 [in Ukrainian]. [https://doi.org/10.52058/2786-6300-2024-8\(26\)-591-603](https://doi.org/10.52058/2786-6300-2024-8(26)-591-603)
- Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61–80. <https://doi.org/10.1287/isre.1060.0080>
- Distler, V., Fassl, M., Habib, H., Krombholz, K., Lenzini, G., Lallemand, C., Koenig, V., & Faith Cranor, L. (2023). Empirical research methods in usable privacy and security. In N. Gerber, A. Stöver, & K. Marky (Eds.), *Human factors in privacy research* (pp. 29–53). Springer.
- Dovbush, O., Harasym, T., & Skoreiko-Svirskaya, I. (2023). Verbalization of manipulative strategies in social networks Facebook and Twitter. *Folium, Special Issue*, 54–60 [in Ukrainian]. <https://doi.org/10.32782/folium/2023.3.7>
- Laptev, S. O. (2024). Development of personal data protection model in social networks. *Information Protection*, 26(1), 43–50 [in Ukrainian].
- Naidonova, L. A., & Baryshpolets, O. T. (Eds.). (2009). *Media culture of personality: socio-psychological approach*. Milenium [in Ukrainian].
- Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford Law Books.
- Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. State University of New York Press.
- Petrunko, O. V. (2011). Aggressive media environment: Qualitative and content discourses. *Native language*, 16, 36–43 [in Ukrainian].
- Rogers, C. R. (1959). A theory of therapy, personality, and interpersonal relationships: As developed in the client-centered framework. In S. Koch (Ed.) *Psychology: A study of a science* (Vol. 3, pp. 184–256). McGraw-Hill.
- Sprattseva, K. (2024). Psychological analysis of the structural components of the self-image in visual self presentation. *Scientific Perspectives*, 6(48), 1013–1023. [https://doi.org/10.52058/2708-7530-2024-6\(48\)](https://doi.org/10.52058/2708-7530-2024-6(48)) [in Ukrainian].
- Tiahlo, O. V. (2017). Critical thinking in action, or Experience of critical review. *Postmethodology*, 1, 8–13 [in Ukrainian].
- Trepte, S., & Reinecke, L. (2011). *Privacy online: Perspectives on privacy and self-disclosure in the social web*. Springer. <https://link.springer.com/book/10.1007/978-3-642-21521-6>
- Westin, A. F. (1967). *Privacy and freedom*. Atheneum.
- Wisniewski, P., Xu, H., Rosson, M. B., & Carroll, J. M. (2017). Parents just don't understand: Why teens don't talk to parents about their online risk experiences. In Ch. P. Lee, & S. Poltrock (Eds.) *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (pp. 523–540). Association for Computing Machinery. <https://doi.org/10.1145/2998181.2998236>

Отримано редакцією журналу / Received: 28.08.24

Прорецензовано / Revised: 19.11.24

Схвалено до друку / Accepted: 15.12.24

Kateryna SPRAVTSOVA, PhD Student
ORCID ID: 0000-0001-5802-0344
e-mail: k.spravtsova.asp@kubg.edu.ua
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine

PSYCHOLOGICAL ASPECTS OF SECURITY AND PRIVACY IN THE DIGITAL ENVIRONMENT

Background. *In the era of rapid digitalization and the increase in social network users to 5.5 billion people (67.1 % of the global population), safeguarding personal privacy in the digital realm has become increasingly significant. According to Pew Research Center (2024), 79 % of users are concerned about personal data protection, while privacy violations are showing a worrying upward trend. The study aims to conduct a comprehensive analysis of the psychological mechanisms of privacy management in social networks and to develop evidence-based strategies for safeguarding users' psychological well-being.*

Methods. *The research employs a combination of systemic and person-centered approaches along with social cognitive theory. A diverse range of theoretical methods (systematic literature review, meta-analysis of empirical research, conceptual modeling) and empirical methods (psychodiagnostic techniques, neuropsychological studies, longitudinal observations) were utilized. A meta-analysis of 166 studies, encompassing over 75,000 participants, was conducted.*

Results. *The existence of the "privacy paradox" — the gap between stated privacy concerns and actual user behavior — has been empirically verified. A significant correlation was found between privacy violations and a decline in psychological well-being, indicated by increased levels of anxiety and depressive symptoms. Neuropsychological studies revealed the activation of specific brain structures during decision-making related to information disclosure. The research also examined the digital resilience scale and identified the primary manipulative strategies employed in social networks: persuasion (33 %), agitation (17 %), and information distortion (15 %).*

Conclusions. *The need for a comprehensive approach to privacy protection that combines the development of digital competence, media literacy, and psychological resilience has been established. The effectiveness of a media psychological support system through interconnected areas of media analytics, media therapy, and media education has been substantiated. The research findings provide a theoretical basis for designing psychological support programs for social network users and enhancing privacy protection systems.*

Keywords: *digital privacy, psychological safety, social media self-presentation, personal cybersecurity, media competence.*

Автор заявляє про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The author declares no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.