Вісник Львівського університету. Серія філос.-політолог. студії. 2025. Випуск 60, с. 128–137
Visnyk of the Lviv University. Series Philos.-Political Studies. Issue 60, p. 128–137

УДК 140.8:316.774:004.056
DOI https://doi.org/10.30970/PPS.2025.60.14

СВІТОГЛЯДНІ ОСНОВИ ЦИФРОВОЇ БЕЗПЕКИ МОЛОДІ В УМОВАХ ІНФОРМАЦІЙНОГО ВПЛИВУ СОЦІАЛЬНИХ МЕРЕЖ

Ірина Ломачинська
Київський столичний університет імені Бориса Грінченка,
факультет суспільно-гуманітарних наук, кафедра філософії та релігієзнавства
вул. Левка Лук'яненка, 13-б, 04212, м. Київ, Україна

Богдан Ломачинський
Національна бібліотека України імені В. І. Вернадського
просп. Голосіївський, 3, 03039, м. Київ, Україна

Світлана Хрипко
Київський столичний університет імені Бориса Грінченка,
факультет суспільно-гуманітарних наук, кафедра філософії та релігієзнавства
вул. Левка Лук'яненка, 13-б, 04212, м. Київ, Україна

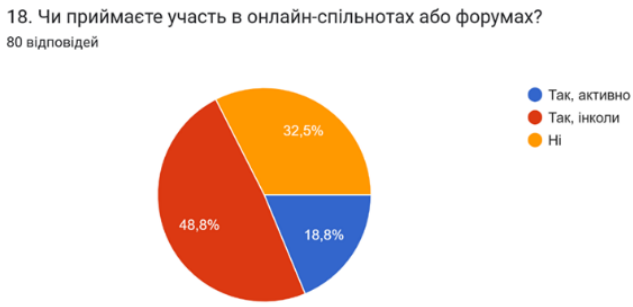
Стаття присвячена філософському осмисленню світоглядних засад цифрової безпеки молоді в умовах зростаючого інформаційного впливу соціальних мереж. В умовах цифрової доби актуалізується проблема відсутності чітких моральних і ціннісних орієнтирів у віртуальному просторі. У цьому контексті цифрова безпека постає як багатовимірне явище, що ґрунтується на усвідомленні особистої відповідальності, розвитку критичного мислення, цифрової культури та здатності до етичної взаємодії в онлайн-середовищі. Методологічну основу дослідження становить поєднання діалектичного та герменевтичного підходів, компаративного аналізу та методів збору соціологічної інформації. На підставі результатів анкетування розкрито особливості світосприйняття представників покоління зумерів, їхню комунікативну взаємодію з цифровим середовищем. Проаналізовано функціональні можливості соціальних мереж як чинників формування гнучкого, адаптивного, мобільного мислення та здатності до багаторівневої комунікації в умовах «мережевої» культури. До ключових викликів цифрової безпеки віднесено доступ до деструктивного й маніпулятивного контенту, загрозу несанкціонованого збору, обробки та використання персональних даних, а також репутаційні ризики, пов'язані з поширенням дезінформації та фальсифікованих наративів. Серед загроз соціальних мереж виокремлено кібершпигунство, кіберпереслідування, кібербулінг та масове поширення фейкових новин як складову інформаційної агресії. Наголошено, що протистояння цим викликам потребує формування високого рівня технологічної обізнаності та критичного мислення серед користувачів. Зроблено висновок, що цифрова культура, яка формується на перетині технологічного поступу та гуманітарного осмислення, постає новим світоглядним орієнтиром, здатним трансформувати уявлення про істину, свободу, суб'єктність і межі людського досвіду.

Ключові слова: цифрова доба, цифрова безпека, соціальні мережі, світогляд, цифрова культура, покоління цифрової доби, кіберзлочинність, інформаційна агресія, критичне мислення.

Актуальність проблеми. У сучасну цифрову епоху соціальні мережі стали не лише засобом комунікації та самовираження, а й потужним інструментом впливу на формування світогляду молоді. Активна взаємодія молодого покоління з цифровим середовищем створює нові можливості для соціалізації, навчання та творчості, водночас породжуючи низку

ризиків, пов'язаних із цифровою безпекою. З огляду на виклики, спричинені глобальним поширенням соціальних мереж і зростаючим впливом цифрового контенту на свідомість молоді, дослідження світоглядних основ цифрової безпеки дозволяє не лише глибше зрозуміти природу ризиків і загроз, а й окреслити стратегічні напрямки формування цілісної, стійкої до маніпуляцій особистості, здатної безпечно й відповідально функціонувати в цифровому середовищі. **Метою дослідження** є визначення світоглядних основ формування цифрової безпеки молоді цифрової доби в контексті глобального впливу соціальних мереж.

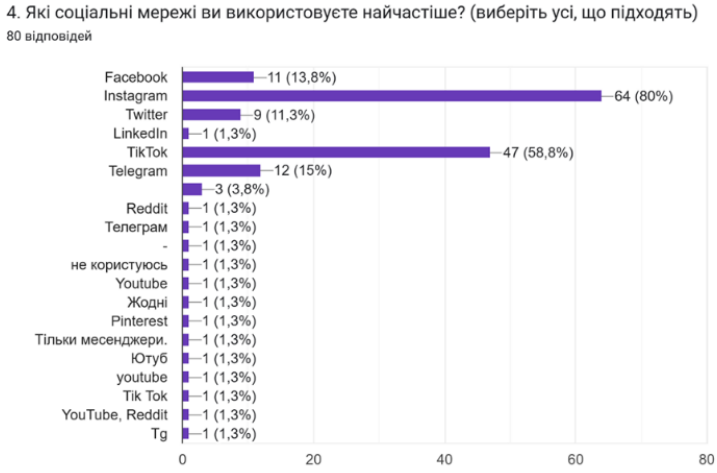
У дослідженні застосовано комплекс наукових **методів,** які забезпечили досягнення поставленої мети. Зокрема, діалектичний метод забезпечив дослідження феномену соціальних мереж у динаміці, взаємозв'язках і суперечностях; компаративний аналіз уможливив порівняння впливу соціальних мереж різних типів на світоглядні установки молоді; герменевтичний аналіз зумовив інтерпретацію смислів, що транслюються у соціальних мережах. У дослідженні використано також метод збору соціологічної інформації – електронне анкетування студентів спеціальності «Філософія» Факультету суспільно-гуманітарних наук Київського столичного університету імені Бориса Грінченка, у якому взяли участь 80 респондентів.



Основний матеріал. Світоглядні орієнтири покоління цифрової доби формуються в контексті глибинних трансформацій у способах комунікації, пізнавальної діяльності, соціалізації та самореалізації. Цифрове середовище постає не лише як технологічний фон сучасного існування, а як нова онтологічна площина, у межах якої відбувається особистісне становлення індивіда та конструювання його ціннісних орієнтирів. Представники сучасної молоді – так звані зумери – є першим поколінням, що зросло в умовах повної цифрової інтегрованості. Для них Інтернет виступає базовим середовищем комунікації, соціальної взаємодії, освіти та дозвілля. Народжені в період з 1996 по 2010 роки, ці молоді люди репрезентують покоління цифрових «аборигенів», для якого характерними є такі форми взаємодії, як текстові повідомлення, мобільні застосунки та миттєві засоби комунікації [17].

Завдяки ранньому залученню до цифрових технологій покоління зумерів демонструє специфічний тип взаємодії з реальністю, що проявляється у повсякденному використанні цифрових інструментів для виконання освітніх, професійних і соціальних завдань. Зокрема, як свідчить опитування, значну частину часу зумери проводять у соціальних мережах і на платформах потокового контенту, зокрема Instagram, TikTok, Facebook.

У сучасному науковому дискурсі [2; 4; 5] соціальна мережа трактується як інтернет-орієнтована платформа, що надає користувачам можливість створення персоналізова-



них цифрових профілів, обміну повідомленнями, зображеннями, відео та іншими видами мультимедійного контенту. Такі мережі функціонують у форматі вебресурсів або мобільних застосунків, доступ до яких здійснюється через цифрові пристрої – зокрема персональні комп'ютери, планшети, смартфони. Основні завдання соціальних мереж полягають в організації комунікативної взаємодії, поширенні інформації та забезпеченні віртуального соціального контакту.

Функціональні можливості соціальних мереж охоплюють широкий спектр користувацьких запитів: надання інформаційної підтримки, соціальну верифікацію ідей через взаємодію, накопичення й активізацію соціального капіталу. Крім того, соціальні медіа сприяють конструюванню цифрової ідентичності, позиціонуванню індивіда в межах мережевої спільноти, формуванню інтересових груп, реалізації потреб у самовираженні, обміні контентом і залученні до дискусій. У контексті цифрової доби соціальні мережі функціонують як візуально-медіатизоване середовище, що посилює роль емоцій, символів та образів, трансформуючи процеси формування переконань, вірувань і цінностей. У результаті домінуючими рисами сучасного світогляду стають гнучкість, адаптивність, мобільність мислення та здатність до багаторівневої взаємодії, що потребує філософського осмислення меж свободи, відповідальності й ідентичності в умовах «мережевої» культури.

Попри численні переваги, пов'язані з використанням соціальних мереж, у науковій літературі активно висвітлюється спектр пов'язаних із цим ризиків і негативних наслідків. Зокрема, соціальні медіа формують особливий тип комунікаційного середовища – так зване «соціальне суспільство», що об'єднує індивідів із різними світоглядними позиціями, кожен з яких взаємодіє з унікальним інформаційним простором. Такий простір конструюється на основі алгоритмічного аналізу поведінки користувача, включаючи його вподобання, пошукові запити, реакції на контент тощо. Закладені в архітектуру цифрових платформ алгоритми постійно перевіряють та обробляють ці дані з метою створення персоналізованих інформаційних стрічок. У результаті алгоритмічне управління виконує не лише функцію селекції релевантного контенту, а й перетворюється на дієвий інструмент впливу на поведінкові моделі користувачів, регулюючи їхню взаємодію у межах цифрового простору [4, с. 94].

Серед ключових викликів, зумовлених такою ситуацією, особливо актуально постає проблема цифрової безпеки. Вона включає як доступ до деструктивного або маніпулятив-

ного контенту, так і загрозу несанкціонованого збору, обробки та використання персональних даних, зокрема інформації про особисте життя, сімейні зв'язки, місце проживання та індивідуальні уподобання [1, с. 154]. Зокрема, за результатами опитування, 65% респондентів не читають політики конфіденційності перед реєстрацією на нових вебсайтах, що свідчить про недостатню обізнаність щодо їх небезпек.

У сучасному цифровому середовищі соціальні мережі виступають однією з основних цілей для зловмисників, що зумовлено значним обсягом персональної інформації, яку користувачі добровільно оприлюднюють.

Завдяки особливостям функціонування соціальних медіаплатформ кіберзлочинці мають можливість здійснювати збір конфіденційних даних, що може слугувати підґрунтям для реалізації різних типів атак – зокрема поширення спаму, впровадження шпигунського програмного забезпечення, використання соціальних ботів та викрадення особистих відомостей [18]. Як свідчить опитування, найбільш поширена реакція молоді на спам чи небажані повідомлення – видалення і блокування відправника.

Крім того, соціальні мережі стають джерелом репутаційних загроз, оскільки дезінформація або фальсифіковані наративи, поширені в цифровому просторі, можуть мати тривалий негативний вплив на суспільну думку [16].

Сайти на кшталт Facebook, Instagram та інших дедалі частіше використовуються кіберзлочинцями як інструменти для незаконного отримання персональних даних, зокрема через непомітне відстеження користувацької активності. Навіть оприлюднення досвіду користування онлайн-банкінгом може надати зловмисникам важливу інформацію про типи банківських послуг чи облікових записів, що в подальшому використовується в схемах соціальної інженерії або фішингу [19, с. 6].

Науковці наголошують на важливості дотримання базових заходів кібергігієни, до яких належать: забезпечення захисту персональних даних від несанкціонованого доступу,

регулярне оновлення паролів, контроль стану банківських рахунків, а також використання лише офіційних джерел для завантаження програмного забезпечення [15]. За результатами опитування, ліцензійним програмним забезпеченням завжди або часто користується 77, 5% молоді.

Кібершпигунство у сучасному науковому дискурсі розглядається як цілеспрямоване використання цифрових технологій для несанкціонованого збору конфіденційних відомостей або інтелектуальної власності з подальшою передачею цінної інформації третім сторонам. Подібні дії часто здійснюються в контексті економічної чи військово-політичної конкуренції та можуть бути мотивовані прагненням до матеріальної вигоди або демонстрацією сили через порушення кібербезпеки. Наслідками кібершпигунства можуть стати втрата стратегічних переваг, фінансові збитки, порушення цілісності даних, а в окремих випадках – загроза життю людей.

Зокрема, соціальні мережі часто використовуються зловмисниками як інструмент соціальної інженерії для отримання чутливої інформації – наприклад, посадових обов'язків, електронної адреси тощо. Паралельно поширеним явищем є кіберпереслідування – постійне спостереження за особою через цифрові канали, що викликає психологічний дискомфорт, порушує право на приватність і супроводжується погрозами.

Для протидії подібним загрозам науковці рекомендують дотримуватися низки заходів безпеки: використовувати складні паролі, обмежувати геолокаційні сервіси, критично оцінювати запити на додавання в друзі, обачно ставитися до публікацій у мережі, а також застосовувати сучасне антивірусне програмне забезпечення [12].

Окрему увагу в науковій літературі приділяють кіберзалякуванню, яке трактується як агресивна поведінка окремих осіб чи груп, що здійснюється за допомогою цифрових медіа з метою спричинення шкоди. За результатами зарубіжних соціологічних опитувань, майже половина студентської молоді стикалася з проявами подібного насильства у соціальних мережах [14].

За результатами нашого опитування, основними реакціями студентів на негативні коментарі або критику було ігнорування супротивника.

Підтримуємо позицію українських науковців [3, с. 24] що соціальні мережі виступають не лише інструментом комунікації, але й потужним засобом маніпулятивного впливу, здатним підсилювати наявні у користувачів стереотипні уявлення. Завдяки постійному повторенню певного контенту, знижується рівень критичного осмислення, активізуються автоматизовані механізми сприйняття, що сприяє формуванню ілюзії достовірності нав'язаних суджень. Це, у свою чергу, веде до зниження когнітивної гнучкості, втрати здатності до інформаційної селекції та ослаблення критичного мислення. У результаті стереотипи трансформуються у стійкі колективні переконання, які дедалі рідше піддаються раціональному аналізу та перевірці достовірності.

Особливої гостроти в умовах сучасного інформаційного простору набуває проблема поширення дезінформації та фейкових новин у соціальних мережах [6]. Це явище стало ключовим механізмом ведення інформаційної війни, зокрема в українському контексті. Дезінформація розглядається як цілеспрямоване поширення неправдивої або маніпулятивно викривленої інформації з метою навмисного спотворення уявлень про реальність. Зазвичай вона має замовний характер і використовується окремими особами чи організованими групами для підриву суспільної довіри, формування викривленого образу окремих подій, осіб або соціальних процесів. Такі інформаційні атаки реалізуються задля досягнення політичних, економічних, пропагандистських або психологічних цілей, включаючи створення атмосфери страху, паніки та дестабілізації громадської думки.

Фейкові новини як складова інформаційної агресії мають на меті дезорієнтацію аудиторії, маніпулювання масовою свідомістю та підрив авторитету окремих інституцій чи осіб шляхом викривлення фактів, фабрикації подій або створення повністю вигаданих повідомлень. Одночасно вони можуть слугувати інструментом відволікання уваги громадськості від соціально значущих подій або проблем. У підсумку формування спотвореного інформаційного простору призводить до кризи довіри, поглиблення інформаційної дезорієнтації та руйнування цілісної картини світу в масовій свідомості користувачів цифрових платформ [10, с. 280–281].

За результатами опитування, достовірність інформації перевіряють завжди або часто 95% респондентів, що свідчить про високий рівень критичності до інформаційних повідомлень в української молоді.

Останні два роки особливого поширення в соціальних мережах набули технології маніпулювання суспільною свідомістю за допомогою штучного інтелекту. Насамперед це створення так званих дипфейків – синтетичних зображень і відео, які поєднують змодельовану візуальну та аудіоінформацію, імітуючи голос або зовнішність конкретної особи

[7]. Також поширеним є генерування візуальних образів осіб, які насправді не існують, що відкриває необмежені можливості для фабрикації та поширення будь-яких інформаційних повідомлень.

Іншим важливим інструментом є розробка детальних психологічних портретів користувачів соціальних мереж на основі аналізу їхніх профілів, що дозволяє значно підвищити точність і результативність маніпулятивного впливу. Крім того, активно використовуються чат-боти для поширення інформаційного контенту певного ідеологічного або політичного спрямування, що забезпечує масштабне охоплення аудиторії при мінімальних витратах. Важливу роль також відіграє контент-аналіз інформаційного трафіку в Інтернеті, зокрема аналіз тональності повідомлень (sentiment analysis), який здійснюється на основі великих обсягів даних із блогів, форумів, статей, опитувань тощо. На основі такого аналізу можливо здійснювати прогнозування можливих наслідків і сценаріїв розвитку суспільних настроїв або інформаційного впливу [9, с. 63].

Для ефективного протистояння подібним маніпулятивним практикам необхідним є розвиток технологічної обізнаності та критичного мислення серед користувачів. Ці навички мають формуватися як складова цифрової медіаграмотності, що, своєю чергою, сприятиме усвідомленому споживанню інформації, підвищенню рівня відповідальності у використанні соціальних мереж і слугуватиме дієвим інструментом протидії поширенню фальсифікованого контенту [8].

О. Гоцур акцентує увагу на поширенні у соціальних мережах таких феноменів, як тролінг і функціонування бот-акаунтів, зокрема в рамках цілих ботомереж або так званих «ботоферм», які істотно впливають на формування громадської думки та суспільних настроїв з різноманітних питань [5, с. 200]. Боти, як правило, є акаунтами неіснуючих осіб, створених для автоматизованого поширення заданого інформаційного контенту, що дозволяє здійснювати цілеспрямоване інформаційне маніпулювання на масовому рівні.

На відміну від ботів, троль – це учасник комунікаційного процесу, який імітує зацікавленість у спілкуванні, однак його справжньою метою є дестабілізація дискусії, порушення комунікативної взаємодії, а також провокування емоційної напруги, фрустрації та роздратування серед інших користувачів. Тролінг часто слугує інструментом мережевих провокацій або знущань, що здійснюються в межах цифрової комунікації.

Додаткову загрозу становлять атаки із використанням зламаних акаунтів, у межах яких зловмисники отримують контроль над профілями реальних користувачів і застосовують їх для здійснення шкідливих дій. Це може включати поширення дезінформації через публікації на сторінці, розсилку шкідливих посилань у приватних повідомленнях, участь у фейковій активності (наприклад, штучні вподобання комерційних сторінок) тощо. Подібна діяльність не лише порушує конфіденційність і безпеку особистих даних, але й сприяє посиленню інформаційного впливу шляхом використання довіри до справжніх профілів [13].

Ключовим чинником, що визначає формування нових світоглядних орієнтирів молоді в умовах функціонування соціальних мереж, виступає цифрова культура. Вона сприяє трансформації комунікативних практик, розвитку медіаграмотності та здатності орієнтуватися в умовах зростаючих інформаційних загроз. Саме в цій культурі зосереджується потенціал для подолання інформаційного нігілізму, маніпулятивного спотворення реальності та духовного спустошення, характерних для доби постправди й цифрової симуляції. Варто зазначити, що в українському законодавстві поняття «цифрова культура» не має прямого визначення, однак у «Концепції розвитку цифрових компетентностей» цифрова компетентність розглядається як інтегративне поєднання знань, умінь, установок, стра-

тегій мислення й особистісних характеристик, що забезпечують ефективне застосування інформаційно-комунікаційних і цифрових технологій у професійній, освітній та соціальній діяльності [11]. Цей підхід охоплює не лише технічні навички роботи з цифровими інструментами, а й регулює поведінкові аспекти взаємодії в інформаційному просторі, включно з відповідальним, етичним і безпечним використанням цифрового контенту. Цифрові компетенції, які включають навички критичного мислення, оцінки та фільтрації інформації, стають основними для здатності адаптуватися до інформаційного суспільства, яке потребує не лише технологічної обізнаності, але й етичної відповідальності. Тому покоління цифрової доби потребує переосмислення традиційних підходів до формування світогляду. У центрі мають бути інтеграція гуманістичних цінностей, розвиток критичного мислення, цифрової етики, що дозволить зберегти цілісність людини в умовах цифрової трансформації.

Висновки. Аналіз зазначених аспектів цифрової комунікації та соціальної взаємодії в мережевому середовищі свідчить про складну й амбівалентну роль соціальних медіа у формуванні сучасної інформаційної культури. З одного боку, цифрові платформи створюють широкі можливості для самовираження, реалізації інтелектуального та творчого потенціалу, розширення доступу до знань, розвитку медіа- і цифрової грамотності, а також формування цифрового капіталу як ресурсу соціального й економічного зростання. З іншого – вони дедалі частіше стають інструментами маніпулятивного впливу, поширення дезінформації, деструктивного контенту, цифрових злочинів, що спричиняють фрустрацію, втрату критичного мислення, формування стереотипів і навіть загострення суспільної нестабільності. Особливу загрозу становить використання штучного інтелекту: створення дипфейків, фальшивих акаунтів, ботів, тролів і таргетованих інформаційних впливів, що базуються на психологічному профілюванні користувачів. У цьому контексті визначальною умовою протидії інформаційним загрозам є розвиток цифрової культури як нової світоглядної парадигми, що не лише забезпечує функціональне користування цифровими інструментами, а й сприяє формуванню критичного мислення, етичної відповідальності, інформаційної безпеки та соціальної стійкості. Цифрова культура має стати основою сучасної освіти, державної політики в інформаційній сфері та особистісної стратегії сучасної молоді.

Список використаної літератури

1. Асєєва Ю. О. Кіберкомунікативна залежність від соціальної мережі Instagram як проблема сучасної молоді. *Габітус*. 2020. № 14. С. 152–157. URL: https://repo.odmu.edu.ua:443/xmlui/handle/123456789/8327 (дата звернення: 17.12.2024).
2. Бірюкова М.В. Технології самопросування в соціальних мережах. *Соціальні технології: актуальні проблеми теорії та практики*. 2021. Вип. 89. С. 138–145.
3. Була С.П., Свідерська О.І. Соціальні мережі як інструмент політичної маніпуляції. Науковий журнал «Політикус». 2020. вип. 4. С. 21–25.
4. Гаврилюк О., Гнатюк А. Взаємовплив соціальних мереж і масової культури: роль і значення алгоритмів. *Питання культурології.* 2023. № 42, С. 90–101.
5. Гоцур О. Соціальні мережі та блоги як інструменти реалізації PR-кампанії. *Вісник Львівського університету. Серія Журналістика*. 2021. Вип. 50. С. 196–204.
6. Ломачинська І.М., Гришина Ю.О. Інтернет-покоління і консцієнтальні війни сучасності. Вісник Львівського університету. Серія філос.-політолог. студії. 2024. 52. С. 161–168. DOI https://doi.org/10.30970/PPS.2024.52.19
7. Ломачинська І.М., Ломачинський Б.Г. Роль медіакультури в інформаційних війнах сучасності. *SKHID*. 2022. 3(3). С. 66–73. DOI: https://doi.org/10.21847/1728-9343.2022.3 (3).268297

8. Ломачинська І.М., Рихліцька О.Д. Виклики соціальних мереж у формуванні ціннісних орієнтирів українського інтернет-покоління. Вісник Національного юридичного університету імені Ярослава Мудрого. 2025. № 1 (64). С. 147–158. DOI: https://doi.org/10.21564/2663-5704.64.324580
9. Пєвцов Г.В., Залкін С.В., Ревін О.В., Сідченко С.О., Хударковський К.І., Методологічний підхід до підготовки і проведення інформаційної (психологічної) операції у соціальних мережах. *Системи обробки інформації*. 2022. Вип. 2 (169). С. 58–65.
10. Предместніков О., Хотмірова В. Соціальні мережі як майданчик для порушення прав людини: можливості та загрози. *Scientific Collection «InterConf»*. 2023. № 156. С. 276–284.
11. Розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації» від 3 березня 2021 р. № 167-р. URL: https://smartlawin.ndipzir.org.ua/normatyvno-pravovi-akty-didzhytalizacziya/ (дата звернення: 27.04.2025).
12. Jain A.K., Sahoo S.R., Kaubiyal J. Online social networks security and privacy: comprehensive review and analysis. Complex & Intelligent Systems. 2021. Vol. 7, Issue 5. P. 2157–2177. https://doi.org/10.1007/s40747-021-00409-7
13. Kayes I., Iamnitchi A. Privacy and security in online social networks: A survey. Online Social Networks and Media. 2017. Vol. 3–4, P. 1–21. https://doi.org/10.1016/j.osnem.2017.09.001Get rights and content
14. Masrom M., Busalim A.H., Abuhassna H., Nik Mahmood N.H. Understanding students' behavior in online social networks: a systematic literature review. International Journal of Educational Technology in Higher Education. 2021. Vol. 18. https://doi.org/10.1186/s41239-021-00240-7
15. Miranda M.E.I., Sánchez N.F.F., Portilla Paguay R.E., González Caballero E. Preserving Freedom in the Digital Age: A Neutrosophic Exploration of Online Privacy and Security Measures. Neutrosophic Sets and Systems. 2024. Vol. 62, Issue 1. URL: https://digitalrepository.unm.edu/nss_journal/vol62/iss1/6
16. Narasimha Rao B., David V., Kalyani V. A Study on Positive and Negative Effects of Social Media on Society. Journal of Science and Technology . Vol.7, Issue 10. P. 46–54.
17. Nicholas A.J. Preferred learning methods of Generation Z. Faculty and Staff – Articles & Papers. 2020. Vol. 74. URL: https://digitalcommons.salve.edu/fac_staff_pub/74
18. Mehraj, H., Jayadevappa, D., Abdul Haleem, S. L., Parveen, R., Madduri, A., Ayyagari, M. R., & Dhabliya, D. Protection motivation theory using multi-factor authentication for providing security over social networking sites. Pattern Recognition Letters, 2021, Vol. 152, P. 218–224. https://doi.org/10.1016/j.patrec.2021.10.002
19. Sinnathambi S.A.P., Zukarnain Z.A. Online Identity Theft, Security Issues and Reputation Damage. Preprints, 2021. DOI: 10.20944/preprints202102.0082.v1.

WORLDVIEW FOUNDATIONS OF DIGITAL SECURITY OF YOUTH IN THE CONTEXT OF INFORMATION INFLUENCE OF SOCIAL NETWORKS

Irina Lomachinska
Borys Grinchenko Kyiv Metropolitan University,
Faculty of Social and Human Sciences, Department of Philosophy and Religious Studies
Levko Lukianenko str., 13-B, 04212, Kyiv, Ukraine

Bohdan Lomachynskyi
National Library of Ukraine named after V. I. Vernadsky
Holosiivskyi Ave., 3, 03039, Kyiv, Ukraine

Svitlana Khrypko
Borys Grinchenko Kyiv Metropolitan University,
Faculty of Social and Human Sciences, Department of Philosophy and Religious Studies
Levko Lukianenko str., 13-B, 04212, Kyiv, Ukraine

The article is devoted to the philosophical comprehension of the worldview foundations of youth digital security in the context of the growing informational influence of social networks. In the digital age, the lack of clear moral and value-oriented guidelines in the virtual space becomes particularly relevant. Within this framework, digital security is interpreted as a multidimensional phenomenon grounded in the awareness of personal responsibility, the development of critical thinking, digital culture, and the ability to engage in ethical interaction within online environments. The methodological foundation of the study combines dialectical and hermeneutic approaches, comparative analysis, and methods of collecting sociological data. Based on the results of a survey, the article reveals the specific features of Generation Z's worldview and their communicative interaction with the digital environment. The functional capabilities of social networks are analyzed as factors fostering flexible, adaptive, and mobile thinking, as well as the ability for multi-level communication in the context of "networked" culture. Key challenges to digital security include exposure to destructive and manipulative content, the threat of unauthorized collection, processing, and use of personal data, and reputational risks posed by the dissemination of disinformation and fabricated narratives. Among the threats posed by social networks are cyber espionage, cyberstalking, cyberbullying, and the proliferation of fake news as a component of informational aggression. The article emphasizes that effective resistance to such manipulative practices requires the development of technological awareness and critical thinking among users. It concludes that digital culture, emerging at the intersection of technological advancement and humanistic reflection, represents a new worldview paradigm capable of transforming traditional conceptions of truth, freedom, subjectivity, and the boundaries of human experience.

Key words: digital age, digital security, social networks, worldview, digital culture, digital generation, cybercrime, informational aggression, critical thinking.