

Пилипчук Володимир

доктор юридичних наук, професор, дійсний член (академік) Національної академії правових наук України, директор Державної наукової установи
«Інститут інформації, безпеки і права НАПрН України»

ГЛОБАЛЬНІ ПРОБЛЕМИ ТА ВИКЛИКИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ В КОНТЕКСТІ ЗАХИСТУ ПРАВ ТА БЕЗПЕКИ ЛЮДИНИ І СУСПІЛЬСТВА

Наприкінці ХХ століття більшість громадян України та інших держав світу ще лише починали розуміти можливості мобільного зв'язку, а тим більше – відеозв'язку та доступу до глобальних інформаційних (цифрових) технологій, зокрема Інтернету.

Нині усе це вже стало історією, а в сучасних умовах формується новітня історія цифрової трансформації та цифрового майбуття. За цих умов цілком актуальним постає питання яким саме може бути вказане майбутнє. Погляди експертів і вчених, як свідчить аналіз, надають різне бачення й оцінки, у тому числі діаметрально протилежні.

Передусім варто зосередитися на тому, які позитивні можливості й здобутки вже отримали громадяни України та інших держав світу внаслідок цифрової трансформації, зокрема:

1) завдяки згаданому мобільному та відеозв'язку мешканці різних держав та континентів отримали реальну можливість безпосереднього спілкування незалежно від відстані, часових поясів, державних кордонів чи регіонів світу. До цієї події людство рухалося декілька століть (з урахуванням технічних та інших складових цього процесу);

2) поширення інформаційно-комунікаційних технологій сприяло формуванню соціальних систем і мереж, суспільних груп і каналів для спілкування, пошуку та поширення інформації, обміну знаннями, досвідом та іншими здобутками. Зазначене також заклало підґрунтя створення інформаційного суспільства та подальшого формування суспільства знань;

3) розробка і впровадження новітніх технологічних (цифрових) продуктів (наприклад, «Дія») забезпечило формування державних реєстрів і баз даних, а також надало можливість дистанційного доступу до них у реальному часі. Це лише первинний перелік новітніх цифрових можливостей.

Поряд з цим, комплексне поєднання інформаційних та інших технологій,

зокрема штучного інтелекту та його складових, надає набагато більші можливості, наприклад: будувати так звані «розумні» будинки й міста, швидко орієнтуватися у просторі, визначати координати, маршрут руху чи місця перебування тощо. Облаштування вулиць, парків та інших публічних місць камерами спостереження надає можливість фіксувати події, які потребують надання допомоги громадянам, виявляти можливі правопорушення чи запобігати надзвичайним подіям. Розроблення і впровадження наступних поколінь штучного інтелекту згідно з наявними прогностичними оцінками має суттєво розширити і доповнити вказані можливості у різних сферах життєдіяльності людини, суспільства, держави та міжнародної спільноти.

Водночас, як свідчить аналіз, нині вже виникла проблема *пошуку балансу* між новітніми можливостями, а також реальними й потенційними ризиками і загрозами подальших цифрових трансформацій. Варто розглянути ці проблеми більш предметно.

Комплексний аналіз сучасних викликів і загроз дає змогу виокремити такі *основні групи загроз безпеці людини та суспільства*:

- *несанкціонований збір персональних даних та контроль приватного життя людини з використанням інформаційних (цифрових) технологій.* (Наочними прикладами зазначеного є несанкціонований збір і торгівля персональними даними, а також потужний спротив глобальних ІТ компаній прийняттю так званого «Пакету захисту даних ЄС», який врегульовує вказані питання);

- *створення та бурхливий розвиток нового класу зброї – інформаційної, здатної ефективно впливати на психіку і свідомість людини, критичну інфраструктуру, а також змінювати національні кордони;*

- *інформаційно-технічні загрози для людини, суспільства і держави, що виявляються у поширенні нового класу соціальних злочинів, які ґрунтуються на використанні сучасних інформаційних (цифрових) технологій (махінації з електронними грошима, кіберзлочини, кібершпигунство, кібертероризм тощо);*

- *використання інформаційних (цифрових) технологій у військово-політичних цілях, у тому числі на міжнародному рівні.*

Моделювання потенційних та реальних ризиків впровадження ШІ ускладнюються низкою актуальних причин, зокрема: *стрімкий розвиток та обмеженість інформації про фактичний стан і потенціал сучасного штучного інтелекту, вплив ШІ на зміну інформаційного середовища* (наприклад, здатний створювати аргументовані тексти, зображення, відео, поширювати дезінформацію, маніпулювати, підривати довіру до джерел інформації тощо).

З урахуванням зазначеного та вимог Регламенту (ЄС) 2024/1689 Європейського Парламенту і Ради від 13 червня 2024 року [1] виокремлено низку *сфер високого ризику застосування систем штучного інтелекту* – *біометричні дані, критична інфраструктура, освіта і професійна підготовка, працевлаштування, управління працівниками, доступ до самозайнятості, доступ до приватних і державних послуг та пільг*. Крім цього, до сфер високого ризику віднесено використання ШІ правоохоронними органами, в охороні державного кордону, у здійсненні правосуддя та забезпеченні демократичних процесів.

Як свідчить проведений аналіз оцінок експертів, вчених та розробників систем штучного інтелекту [2], найпопулярнішими з яких є «AI2027» [3] та «What 2026 looks like» [4], передусім варто звернути увагу на такі реальні й потенційні виклики і загрози, пов'язані з використанням ШІ:

- *ризики для персональних даних, приватного життя та безпеки людини, упередженість та посягання на основоположні права і свободи людини* (у т.ч. спроби «виховання» т.зв. «цифрової людини», залежної та керованої штучним інтелектом чи іншими цифровими технологіями);

- *неточність і неправдивість інформації, проблема «галюцинування» ШІ*, коли система вигадує дані та факти, а користувач вважає такий згенерований текст чи дані реальними фактами;

- *зростання безробіття* (поширення ШІ може реально призвести до системних трансформацій на ринку праці), *ризики деградації людини та небажання особи розвиватися* (залежність людини від ШІ може реально призвести до зміни індивідуальних когнітивних здібностей, зокрема критичного мислення, навичок розв'язання проблем, зниження мотивації до традиційних форм навчання, поверхневого рівня засвоєння знань, обмеження формування метакогнітивних навичок тощо);

- *втрата контролю над штучним інтелектом* (за оцінками фахівців наразі вже триває робота з розробки штучного інтелекту самим штучним інтелектом, що може призводити до ситуацій, коли поведінка ШІ стає непередбачуваною для операторів та розробників).

Внаслідок застосування ШІ можуть виникати й інші ризики і загрози, зокрема: *обхід автентифікації, злам корпоративної електронної пошти, шахрайство з видаванням себе за іншу особу, афери з впливовими особами, дезінформація, злам паролів тощо*.

За цих умов постає ще одна системна проблема, пов'язана з процесами глобалізації та виникненням ідей, зокрема у розробників ШІ, щодо розбудови

світової держави.

Особливий характер новітніх глобальних трансформаційних процесів, як зазначав всесвітньо відомий український вчений Б.Є. Патон, зумовлює потребу їх глибокого осмислення, метою якого є оптимізація суспільного розвитку шляхом стратегічного моделювання. Без розуміння глобальних проблем не можна кваліфіковано підійти до формування національних цілей і стратегій та сподіватись на безпечний розвиток у майбутньому.

З погляду теорії держави і права, **глобалізація** (фр. global – загальний) – це процес поширення зв'язків, залежностей, обов'язків від локального до загального та вихід за межі державних кордонів.

Термін «**глобалізація**» пов'язаний насамперед з еволюцією економіки у світовому масштабі, а також з її відбиттям у змісті внутрішньодержавної економічної діяльності (тобто має на меті економічну інтеграцію). Однак глобалізація не вичерпується однією економікою – вона поступово стає системою загальних процесів, що охоплюють усі сфери соціального життя (економічну, політичну, духовно-культурну, правову та ін.).

На рубежі XX і XXI століть також виникла теорія «**глобальної (світової) держави**». Її родоначальник – американський економіст Р.Робертсон. Ця теорія стверджує не тільки про зближення держав, але й про стирання державних кордонів у результаті уніфікації усіх сфер життєдіяльності різних суспільств світу.

При цьому, еталоном (зразком) для всіх держав світу подається ринкова економіка, цифрова трансформація та інновації, до яких повинні «підтягуватися» (добровільно чи примусово) усі суспільства планети і на їх основі передбачається побудова світової політичної системи, світової держави («**загальної всесвітньої цивілізації**»).

Наочними у цьому контексті є висновки американського професора Збігніва Бжезинського, який ще у 1968 р. висунув тезис про необхідність створення *системи глобального планування і довгострокового перерозподілу світових ресурсів.*

Він прогнозував поступове формування все більш контрольованого і керованого світового суспільства, в якому пануватиме *глобальна еліта*, що застосовуватиме найновіші досягнення науки і техніки для впливу на поведінку суспільства. Також пророкувалося *формування наднаціональної влади* в результаті консолідації провідних індустріально розвинених країн

У контексті глобалізаційних економічних процесів вчені НАН України дали таке визначення **глобалізму** – це система абсолютної економічної і політичної

влади нових глобальних монополістичних корпорацій (відомі як ТНК – транснаціональні корпорації), які вийшли з-під контролю націй-держав свого походження і базування. Вони маневрують фінансовим капіталом, обертаючи його на світовому ринку з шаленою швидкістю, відмовляючись платити податки посилюють експлуатацію багатьох країн і регіонів, у т.ч. власних країн [5].

Подібні оцінки також є характерними для глобальних ІТ корпорацій, а їх інноваційні цифрові розробки, передусім штучного інтелекту, створюють реальні передумови для побудови керованого «цифрового суспільства», як передумови до створення вказаної «світової держави». Певні аналоги зазначеного, як свідчить аналіз, вже запроваджені в КНР в контексті цифрового контролю соціальної поведінки громадян.

Водночас, прибічниками вказаної теорії зовсім не враховується суттєва різниця між народами і державами світу (духовні, культурні, релігійні, етнопсихологічні, соціальні, економічні та інші відмінності), а також можливі негативні наслідки глобалізаційного процесу (соціальні конфлікти, конфронтації цивілізацій, загроза міжнародного тероризму та ін.).

У цьому контексті заслуговують на увагу висновки колишнього лідера Сингапуру Лі Куан Ю.: «...оскільки різні суспільства розвивалися протягом тисячоліть по-різному, то їх ідеали та суспільні норми обов'язково мають відрізнятися. Тобто, було нереальним наполягати на тому, щоб американські та європейські стандарти з прав людини кінця двадцятого століття застосувались універсально... Поступово, але беззаперечно, співдружність держав знайде баланс між невтручанням у внутрішні справи інших країн і моральним правом наполягати на більш гуманному та цивілізованому відношенні всіх урядів до їх власних народів. По мірі того, як суспільство стає більш відкритим, буде відбуватися поступове наближення поглядів різних народів і напрацювання єдиного світового стандарту на те, що є прийнятним, а що – неприйнятним, а негуманне, жорстоке або варварське відношення до людей буде засуджуватись» [6].

За нашими оцінками, які знайшли підтримку вітчизняних та іноземних вчених та експертів, новітні виклики і загрози глобального рівня в інформаційній сфері та кіберпросторі становлять реальну загрозу безпеці людства та міжнародному правопорядку. При цьому, жодна держава світу в умовах глобалізації не здатна самотійно забезпечити власну інформаційну та кібербезпеку.

Враховуючи зазначене проблема інформаційного виміру колективної

безпеки є вкрай важливою для більшості країн світу, які розвивають або формують інформаційні суспільства, у т.ч. й України. При цьому виникає низка системних проблем, що потребують комплексного опрацювання, зокрема:

– пошуку балансу між правами людини і потребою суспільства, держави та міжнародної спільноти у забезпеченні безпеки;

– перегляду принципів і механізмів міжнародних відносин та співробітництва в галузі інформаційної та кібербезпеки;

– міжнародно-правового визначення ключових понять в інформаційній сфері, зокрема, «інформаційна безпека», «кібербезпеки», «кібертероризм» та «кіберзлочинність» тощо;

– посилення міжнародно-правової відповідальності за використання в інформаційній сфері сил і засобів, які створюють загрози життю і здоров'ю людини.

В контексті зазначеного вкрай актуальною постає потреба реалізації вимог ст. 17 Конституції України згідно з якою забезпечення інформаційної безпеки визнається однією з основних функцій держави і справою усього Українського народу.

Відповідно, потребують прийняття такі першочергові закони України: «Про внесення змін до Закону України «Про національну безпеку України» щодо забезпечення інформаційної безпеки», «Про кіберсили», «Про штучний інтелект», «Про забезпечення інформаційної безпеки». Зазначене, як видається, сприятиме захисту прав і безпеки людини та суспільства, а також розвитку систем національної, інформаційної та кібербезпеки в сучасних умовах війни та глобальних цифрових трансформацій.

Список використаних джерел:

1. Європейський Союз. Регламент (ЄС) 2024/1689 Європейського Парламенту та Ради від 13 червня 2024 року, що встановлює гармонізовані правила щодо штучного інтелекту (Акт про штучний інтелект) : офіційний вебсайт. URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (дата звернення: 28.06.2026).

2. Пилипчук В. Г. Новітні виклики і загрози у сфері інформаційної та кібернетичної безпеки в контексті цифрової трансформації та розвитку штучного інтелекту. Протидія загрозам суспільству і державі в умовах інформаційної та кібервійни рф проти України : збірник матеріалів наук.-практ. семінару (м. Київ, 2026 р.). Київ : НА СБУ, 2026. С. 13–16.

3. AI 2027: Global Summit on Artificial Intelligence Developments : official website. URL: <https://ai-2027.com/> (дата звернення: 28.06.2026).

4. What 2026 Looks Like : analytical platform. LessWrong. URL: <https://www.lesswrong.com/posts/6Xgy6CAf2jqNhynHL/what-2026-looks-like> (дата звернення: 28.06.2026).

5. Білорус О. Проблеми політичної економії глобалізму. Глобалізм як світова система імперіалістичної інтеграції. Матеріали науково-практичної конференції. С. 7.

6. Lee Kuan Yew. The Singapore Story: 1965–2000. From third world to first. New York : Harper Collins Publishers, 2000. P. 345.

Петрикова Анастасія

здобувач вищої освіти спеціальності D3 Менеджмент
Вінницького державного педагогічного університету
імені Михайла Коцюбинського

Науковий керівник: Посвалюк О. А.

асистент кафедри фундаментальних і приватно-правових дисциплін
Вінницького державного педагогічного університету
імені Михайла Коцюбинського

**ПОВЕДІНКОВІ ДОСЛІДЖЕННЯ МОЛОДІ В УМОВАХ ЦИФРОВОГО
СУСПІЛЬСТВА**

Ключові слова: молодь, цифрове суспільство, соціальні мережі, поведінка, цифрові технології, інформаційне середовище, кібер простір.

Сучасне цифрове суспільство суттєво трансформує поведінкові моделі молодого покоління. Розвиток інформаційно-комунікаційних технологій, поширення соціальних мереж і цифрових платформ зумовлюють зміну способів комунікації, навчання та соціалізації молоді. Актуальність дослідження полягає у необхідності комплексного аналізу поведінкових змін молоді в умовах цифровізації суспільства.

Метою дослідження є аналіз поведінкових особливостей молоді в умовах цифрового суспільства та визначення їх впливу на суспільні процеси. Однією з ключових характеристик цифрового середовища є активне використання соціальних мереж. Згідно з міжнародними дослідженнями, понад 95% підлітків користуються онлайн-платформами, а значна частина проводить у цифровому середовищі значну частину свого часу [3, с. 1-2].

Це сприяє формуванню нових моделей поведінки, зокрема віртуалізації спілкування та зменшенню безпосередніх соціальних контактів. Дослідження