

УДК 323:351

## ЗАГРОЗИ ТА ВИКЛИКИ НАЦІОНАЛЬНИМ ІНТЕРЕСАМ УКРАЇНИ В ІНФОРМАЦІЙНІЙ СФЕРІ В УМОВАХ ГЛОБАЛІЗАЦІЇ

Конах Вікторія Костянтинівна,  
*кандидат політичних наук;*  
Лазоренко Ольга Анатоліївна

Розглянуто зміни, що виникли внаслідок глобалізації сучасного інформаційного простору. Визначено актуальні загрози та виклики національним інтересам України в інформаційній сфері нашої держави, спричинені цими процесами. Запропоновано напрями вдосконалення державної політики у сфері забезпечення інформаційної безпеки.

**Ключові слова:** глобалізація, інформаційна безпека, інформаційний простір, загрози національній безпеці.

За умов посилення глобалізаційних процесів та жорсткої міжнародної конкуренції головною ареною зіткнень і боротьби різновекторних національних інтересів держав дедалі частіше стає інформаційний простір [1]. Як наслідок, ХХІ ст. характеризується тим, що воєнна сила як засіб впливу заміщується новітніми інформаційними технологіями, які при цілеспрямованому використанні дають змогу досягати власних цілей на рівні окремих груп людей, суспільств і країн. За таких умов рівень розвитку інформаційного середовища та забезпечення інформаційної безпеки активно впливають на стан політичної, економічної та інших складників національної безпеки будь-якої держави, а отже, – потребують ґрунтовного дослідження та виваженого регулювання.

Аналізу сучасних проблем національної безпеки України та її невід’ємного складника – інформаційної безпеки присвячено робо-

ти низки українських авторів, зокрема В. Батюка, Г. Почепцова, І. Бінька, В. Горбуліна, А. Качинського, О. Дзьобаня, В. Ліпкана, В. Кормича, Д. Дубова, О. Сосніна та ін. Проте з огляду на глобалізацію інформаційного середовища, змінюються й загрози в інформаційній сфері. Тому подальше дослідження цього напрямку є вельми актуальним для України.

З огляду на зазначене **метою даної статті** є визначення актуальних загроз і викликів національним інтересам України в інформаційній сфері в умовах глобалізації та визначення основних напрямів вдосконалення державної політики у сфері забезпечення інформаційної безпеки нашої держави.

Глобалізація – це інтенсифікація та взаємопроникнення всесвітніх економічних, соціальних, технологічних, політичних і культурних явищ і зв’язків, а також вихід існуючих

процесів усередині країн за їх межі. У документах ООН глобалізація розглядається як неминучий процес формування загальних принципів облаштування суспільного життя, що є прийнятними для світової спільноти та об'єднують усі країни світу.

Ущільненню інформаційного середовища сприяли поява друкарства і пошти, телеграфу і телефону, радіо і телебачення. Проте вирішальний внесок у глобалізацію інформаційного простору внесло масове застосування в усіх сферах життєдіяльності людини сучасних інформаційно-комунікаційних технологій та інформаційних мереж. Вони сприяють прискореному переміщенню символів, знань, розширенню й водночас уніфікації різноманітних (зокрема освітніх) послуг, а отже, підвищенню загального рівня освіченості, оновленню умов праці та підвищенню її ефективності, демократизації суспільств тощо.

Однак, поряд із перевагами та досягненнями, сучасні інформаційні технології та глобальні інформаційні системи (зокрема Інтернет-мережа) створюють інформаційне середовище, де фактично відсутні державні кордони, обмеження на інформаційні впливи, на поширення інформації, на розміщення та отримання інформації тощо. Отже, глобалізація в інформаційній сфері створює передумови для різних суб'єктів інформаційних відносин несанкціоновано втручатися в інформаційний простір та актуалізує проблему забезпечення інформаційної безпеки для будь-якої держави.

Зокрема й перед нашою державою наразі стоять загрози та виклики у сфері забезпечення інформаційної безпеки, які виникли внаслідок глобалізаційних процесів в інформаційній сфері. Ці загрози можна поділити відповідно до Доктрини інформаційної безпеки України за трьома напрямками: забезпечення технологічного розвитку, захисту інформації та інформаційно-психологічної безпеки.

Щодо *забезпечення технологічного розвитку* держави актуальною проблемою для України залишається подолання т.зв. цифрового розриву. Загалом об'єктивною тенденцією глобалізації інформаційної сфери є посилення т.зв. цифрової нерівності, яка характеризується порушенням балансу інформаційного обміну між розвиненими країнами та країнами, що розвиваються [2]. «Прогрес у галузі нових інформаційних технологій відкриває величезні можливості для вирішення найрізноманітніших економічних, соціальних проблем, однак далеко не все людство сьогодні може ними скористатися <...> безпрецедентне пришвидшення інформаційно-технологічних процесів

не лише посилює існуючий розрив між країнами так званого золотого мільярда та іншим світом, а й щодня його збільшує [3]». Перевага країн-лідерів дає їм змогу не лише в пріоритетному порядку використовувати переваги новітніх інформаційних технологій, а й коригувати і дозувати інформацію, що, на думку багатьох, ставить під сумнів об'єктивність самої тези про рівність доступу до інформації всіх людей.

У даному контексті варто зауважити, що входження України в глобальний інформаційний простір відбувається досить пасивно – як реакція на історичний виклик країнам третьої цивілізаційної хвилі. Загалом сучасний стан національного інформаційного простору характеризується наявністю слабо взаємопов'язаних по горизонталі та вертикалі галузевих, регіональних і низових підсистем, що відображає відсутність його єдності. Безсистемний розвиток інформаційних ресурсів унеможлиблює їх становлення як визначального чинника соціально-економічного зростання [2]. На цьому тлі упродовж останніх років у нашій державі актуалізувалася проблема подолання внутрішнього цифрового розриву, зумовленого відмінностями в темпах упровадження якісного швидкісного Інтернету (широкосмугового доступу (ШСД) або «бродбенду») в містах-мільйонниках (передусім у столиці) та в інформаційно-депресивних регіонах. Такий розрив також поглиблюється між різними верствами населення. Ця проблема призводить і до зростання зовнішнього цифрового розриву, причому не лише з передовими економічно розвиненими країнами світу, а й більшістю країн регіону Східної і Центральної Європи, що вельми негативно позначається на міжнародному іміджі України, інвестиційній і туристичній привабливості тощо [4]. Дається взнаки й відставання України від розвинених країн за рівнем інформатизації соціогуманітарної сфери, насамперед системи освіти, охорони здоров'я, соціального забезпечення, послуг культури.

Наступний вимір інформаційної безпеки стосується *захисту інформації*, зокрема забезпечення конфіденційності, цілісності й доступності інформації, в тому числі технічного захисту інформації в національних інформаційних ресурсах від кібернетичних атак. Тенденції останнього десятиріччя свідчать, що науково-технічний прогрес і глобалізація інформаційно-комунікаційних мереж перетворили **кіберзагрози** в одну з найактуальніших проблем у сфері безпеки особи, суспільства, держави та цивілізації загалом. Це пов'язано насамперед з особливостями застосування

кіберзброї – латентністю і транскордонністю: її легко замаскувати під інші види деструктивних інформаційних впливів, а реальне джерело й державна приналежність суб'єктів кібератак можуть бути надійно заховані в кіберпросторі (світовими лідерами здійснення кібератак на інформаційні системи є Росія й Китай, на другому місці – структури організованої злочинності); дешевиною й доступністю: вартість масованої (з використанням кількох тисяч комп'ютерів з території десятка країн) цілеспрямованої кібератаки на конкретний інформаційний ресурс може не перевищувати кількох тисяч доларів США; «псевдогуманністю»: вона не спрямована безпосередньо проти людей, що спрощує моральні аспекти ухвалення рішень про її застосування, хоча вплив кібератаки на критичну інфраструктуру за наслідками може перевершити застосування зброї масового ураження.

Відсутність необхідних умов і засобів, аби забезпечити захист інформації на різних рівнях, призводить до комп'ютерних злочинів та комп'ютерного тероризму. Зазвичай пріоритетними цілями кібератак є інформаційні та телекомунікаційні ресурси: органів державної влади, насамперед вищої ланки управління, а також збройних сил і спецслужб, з метою дестабілізації соціально-політичної ситуації та погіршення керованості країною; фінансово-економічного сектору – платіжні системи, бази даних податкових і митних органів, персональних даних з метою дестабілізації економіки чи для скоєння фінансових злочинів; систем управління критично важливих галузей, насамперед енергетичної сфери, у т.ч. ядерної, газотранспортної системи, хімічної промисловості з метою здійснення техногенних аварій та катастроф із суттєвими загрозами життю і здоров'ю населення та довкіллю.

Незважаючи на те, що Україна за рівнем розвитку комп'ютерних мереж (у тому числі урядових) усе ще поступається розвиненим країнам, український урядовий сегмент залишається вразливим перед кібератаками. Якщо сфера протидії кіберзлочинності є відносно розробленою та контрольованою, то ризики для успішних атак на урядові системи та сайти зростають. Зокрема, в Україні почастишали кібератаки на сайти органів державної влади, а також акаунти відомих політичних і суспільних діячів, які здійснюються власне українцями з «ідеологічних» мотивів. Найпопулярнішими при цьому залишаються *DDOS*-атаки, які потребують мінімальної кваліфікації та фінансових ресурсів. Такий стан речей вказує на кілька тенденцій: поперше, цільовий, а отже, системно організова-

ний характер кібератак; по-друге, невідповідність забезпечення інформаційної (кібернетичної) безпеки з боку відповідних служб органів державної влади; по-третє, несерйозне ставлення до убезпеченості власних персональних даних з боку суспільно значущих осіб.

У контексті захисту інформації ще однією важливою проблемою для України на сучасному етапі є захист персональних даних. Аналіз поточної ситуації засвідчує, що як пересічні українці, так почасти і представники органів державної влади демонструють недостатній рівень розуміння сенсу та значення захисту персональних даних у сучасному світі, передусім у мережі Інтернет. Одним із яскравих підтверджень цього стали нещодавні події довкола Євромайдану, коли, з одного боку, один із народних депутатів України, а з іншого – офіцери правоохоронних і спеціальних підрозділів [5], всупереч чинному законодавству, опублікували в мережі Інтернет списки, що містили персональні дані людей, які брали участь в акціях протесту, без їхньої на те згоди. Незважаючи на те, що такі дії відповідно до чинного законодавства тягнуть за собою відповідальність, на цей інцидент ніхто в Україні, включаючи профільний наглядовий орган, не звернув жодної уваги.

Поряд із зазначеним актуальною залишається проблема захисту в глобальних мережах інтелектуальної власності – безліцензійного, контрафактного використання музичних творів, текстів, винаходів. Так, відповідно до щорічної «Спеціальної доповіді 301», яку оприлюднив 1 травня 2013 р. Офіс торговельного представника США, Україну названо найбільшим порушником авторського права, оскільки значна частина авторських творів, доступних в українському сегменті Інтернету, опинилася там із порушенням прав інтелектуальної власності. З огляду на зазначене Україну віднесено до категорії т.зв. пріоритетних зарубіжних країн (у цій категорії наша країна опинилася першою і єдиною за останні сім років). Це визначення є кульмінацією зростаючого впродовж кількох років занепокоєння з приводу вельми поширених крадіжок інтелектуальної власності, у т.ч. збільшення частоти порушень прав інтелектуальної власності, де задіяні урядові структури.

Підстав для прийняття такого рішення було три: «несправедливе, непрозоре управління» щодо організацій зі збору та розподілу авторських винагород для американських та інших правовласників, широке використання нелегального програмного забезпечення в українських державних органах, нездатність

вжити ефективних заходів для боротьби з поширеними в Інтернеті порушеннями авторських і суміжних прав в Україні [6]. Правники, які зіткнулися з цією проблемою, говорять про фактичну невразливість порушників авторських прав, їхню недосяжність для національних законодавств і судових органів. Таким чином, вдосконалення законодавчого регулювання захисту прав інтелектуальної власності в мережі Інтернет залишається дуже актуальним для нашої держави.

Наступний вимір стосується *інформаційно-психологічної безпеки*, зокрема створення сприятливого психологічного клімату в національному інформаційному просторі задля утвердження загальнолюдських і національних моральних цінностей, суспільної згоди тощо. Варто зазначити, що нині внаслідок широкого застосування новітніх інформаційних технологій та інформаційно-комунікаційних мереж сформовано глобальний інформаційний простір, де фактично відсутні державні кордони, а отже – обмеження на розміщення та поширення інформації. Це створює передумови для різних суб'єктів інформаційних відносин здійснювати інформаційно-психологічні впливи на окремі суспільні групи, суспільства окремих країн чи навіть інформаційні простори цілих регіонів земної кулі, куди входять інформаційні простори власної держави, союзників, співчуваючих тощо.

Через своє важливе геополітичне розташування Україна є об'єктом інтересів багатьох держав, організацій, транснаціональних корпорацій тощо, а отже, їх інформаційно-психологічного впливу. З одного боку, розмаїття присутності вітчизняних та іноземних ЗМІ в інформаційному просторі України сприяє диверсифікації джерел інформації, розвитку внутрішнього ринку інформації і, відповідно, утвердженню принципів свободи слова в нашій державі. З іншого боку, таке проникнення робить Україну вразливою до зовнішніх інформаційно-психологічних впливів. Варто зауважити, що інтенсивність такого впливу не залежить значною мірою від політичних сил, що перебувають при владі в Україні, а зумовлена насамперед прагненням керівництва іноземних держав та міжнародних структур впливати на зовнішню та внутрішню політику нашої держави, а також має під собою політичне та економічне підґрунтя, продиктоване прагматичними підходами до забезпечення власних національних інтересів [7].

Такі інформаційно-психологічні впливи реалізуються іноземними суб'єктами як через українські, так й іноземні ЗМІ, а також мережу Інтернет. У закордонних ЗМІ та ЗМК такі

впливи здійснюються шляхом поширення викривленої, недостовірної, неповної або упередженої інформації задля формування певного (почасти негативного) іміджу України. В українських ЗМІ та ЗМК – у спосіб нав'язування потрібних оціночних характеристик, поглядів, норм поведінки тощо, здебільшого з метою маніпулювання індивідуальною, груповою та суспільною свідомістю задля досягнення власних інтересів.

Дедалі частіше зовнішні інформаційно-психологічні впливи мають тенденцію накладатися на внутрішні, з огляду на те, що сучасна українська політична еліта у своїй перманентній боротьбі не тільки створює власні інформаційні приводи, а й доволі часто використовує риторику, інспіровану ззовні. При цьому домінуючим трендом у роботі вітчизняних журналістів постає заміщення професійності політичною заангажованістю, а значна кількість традиційних журналістських форматів містить дедалі менше інформування і все більше оціночних суджень (незалежно від того, кому саме належить ЗМІ і на яких ідейних позиціях воно стоїть). Так, узагальнений моніторинг дотримання професійних стандартів у роботі інформаційних служб українських провідних телеканалів за грудень 2013 р., який здійснюється громадською організацією «Телекритика», засвідчив, що більшість із них (окрім «Першого національного») намагалися висвітлювати з достатнім рівнем дотримання стандартів журналістики протестні події в Києві та по всій країні, наслідки силового розгону Євромайдану. Водночас провідні канали подавали інші новини (традиційні звіти про пересування та заяви перших осіб держави, чиновників високого рангу тощо) з порушенням балансу думок, без належної повноти інформації, без відокремлення фактів від думок і з журналістськими оцінками<sup>1</sup>. Таким чином, журналісти, маючи майже необмежені можливості щодо розміщення інформації (зокрема, через мережу Інтернет), виходять за межі журналістики, перетворюючись на «громадських активістів» чи «пропагандистів», які

<sup>1</sup> Зокрема, з ознаками замовності (або цензури) на «Першому національному» було розміщено 46 новин, на «Інтері» – 29, на «1+1» – 27, на каналі «Україна» – 20, на СТБ – 15, ICTV – 13, на «Новому каналі» – 10, на «5 каналі» – 8, на ТВі – 7. Також спостерігалася значна кількість замовчань важливих тем, думок, фактів або бекграундів, зокрема на «Першому національному» – 276, на «Інтері» – 242, на «1+1» – 221, на каналі «Україна» – 266, на СТБ – 260, на ICTV – 247, на «Новому каналі» – 277, на «5 каналі» – 276, на ТВі – 277 [8].

своєю діяльністю дедалі частіше провокують суспільне напруження.

Узагальнюючи викладене, можна зробити висновок, що глобалізація поставила перед нашою державою низку проблем, які потребують нагального вирішення задля всебічного забезпечення інформаційної безпеки держави, суспільства і громадян. При цьому сучасні виклики інформаційній безпеці України зумовлені як внутрішніми, так і зовнішніми чинниками. Внутрішні – найбільшою мірою пов'язані з відсталістю інформаційних технологій в Україні від провідних країн світу, недостатньою дієвістю органів державної влади та законодавства в інформаційній сфері, а також байдужістю, низьким рівнем розуміння та професійної відповідальності як окремих груп, так і громадян, що нині провадять свою діяльність в інформаційному просторі України. Зовнішні – з намаганнями іноземних суб'єктів впливати на світовий та вітчизняний інформаційний простір з метою забезпечення власних інтересів.

Варто зазначити, що забезпечення інформаційної безпеки нашої держави гарантується низкою нормативно-правових актів України. Так, ст. 17 Конституції наголошує, що забезпечення інформаційної безпеки – «одна з найважливіших функцій держави, справа всього українського народу» [9], а Закон України «Про Концепцію Національної програми інформатизації» проголошує, що «інформаційна безпека є невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки» [10]. У ст. 13 Закону України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» зазначається, що «інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» [11].

Концептуальні засади забезпечення інформаційної безпеки визначаються Доктриною інформаційної безпеки України, в якій відзначено особливу роль інформаційної безпеки в системі забезпечення національної безпеки, а саме двоєдиної сутності інформаційної безпеки як невід'ємного складника кожної зі сфер забезпечення національної безпеки і як важливої самостійної сфери забезпечення національної безпеки [12].

На інституціональному рівні забезпеченням окремих напрямів інформаційної безпеки опікується низка установ, зокрема Державна служба спеціального зв'язку та захисту інформації України, Державне агентство з питань науки, інновацій та інформатизації України, Національна рада України з питань телебачення і радіомовлення, Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації, Державний комітет з телебачення та радіомовлення України, Служба безпеки України, Служба зовнішньої розвідки України, Генеральне управління розвідки Міністерства оборони України, Міністерство внутрішніх справ України, Міністерство закордонних справ України.

Таким чином, в Україні наразі закладено концептуальні, нормативно-правові та інституціональні основи забезпечення інформаційної безпеки. Проте наявні загрози та виклики у сфері забезпечення інформаційної безпеки й неспроможність держави їм протистояти за сучасних умов вказують на необхідність подальшого вдосконалення державного регулювання на означеному напрямі.

## Висновки

Процеси інформаційної глобалізації поряд із значними перевагами ставлять перед кожною державою низку новітніх викликів та загроз.

Для України актуальні загрози та виклики в інформаційній сфері можна розмежувати за трьома напрямками: забезпечення технологічного розвитку – посилення внутрішнього цифрового розриву; захисту інформації – вразливість до кібератак (зокрема на органи державної влади), незаконне поширення персональних даних, а також поширення інформації з порушенням авторських прав; інформаційно-психологічної безпеки – широке застосування інформаційно-психологічних впливів зовнішніми та внутрішньодержавними суб'єктами інформаційних відносин на масову свідомість громадян.

У зв'язку з необхідністю нейтралізації цих загроз потребує вдосконалення державна політика у сфері забезпечення інформаційної безпеки. Зокрема, така політика на напрямі технологічного розвитку має бути скерованою на розбудову та інноваційне оновлення національних інформаційних ресурсів, впровадження новітніх технологій створення, обробки та поширення інформації, подолання «цифрової нерівності»; щодо захисту інформації – на подальше удосконалення системи захисту інформаційного простору

та інформаційних ресурсів (передусім тих, доступ до яких здійснюється з використанням мережі Інтернет), а також посилення відповідальності й контроль за незаконним поширенням інформації; щодо інформаційно-психологічної безпеки – на своєчасне

виявлення, запобігання, відвернення, ліквідацію, мінімізацію чи нейтралізацію інформаційно-психологічних впливів, а також визначення відповідальності як для іноземних, так і вітчизняних суб'єктів інформаційних відносин за здійснення таких впливів.

### Список використаних джерел

1. *Информационные ресурсы власти и формирование новой постклассической картины политического мира XXI в.* // Вестн. Моск. ун-та. – 2004. – № 2. – С. 26–37. – Сер. 12. Политические науки.
2. *Добровольська А.* Глобалізація інформаційного простору: адаптація України до загальносвітових тенденцій / А. Добровольська [Електронний ресурс]. – Режим доступу: <http://soskin.info/ea/2005/9-10/20050918.html>
3. *Чернов А.* Становление глобального информационного общества: проблемы и перспективы / А. Чернов. – М. : Издательско-торговая корпорация «Дашков и К<sup>о</sup>», 2003. – 232 с.
4. *Дубов Д. В.* Створення в Україні «Фонду цифрової солідарності» як перспективний напрям подолання внутрішнього цифрового розриву : аналіт. записка / Д. В. Дубов, М. А. Ожеван. – К. : НІСД [Електронний ресурс]. – Режим доступу: <http://www.niss.gov.ua/articles/1157/>
5. *Разгон* Євромайдана: опубліковані списки задержаних [Електронний ресурс]. – Режим доступу: <http://glavred.info/politika/razgon-evromaydana-opublikovany-spiski-zaderzhannyh-264781.html> ; *В сети* опубліковані оперативные данные о «Правом секторе» [Електронний ресурс]. – Режим доступу: <http://www.politarena.org.ua/?newsid=62365>
6. *У США* Україну назвали «піратом номер один» // ТВІ. – 2013. – 23 травня [Електронний ресурс]. – Режим доступу: [http://tvi.ua/new/2013/05/02/u\\_ssha\\_ukrayinu\\_nazvaly\\_piratom\\_nomer\\_odyn](http://tvi.ua/new/2013/05/02/u_ssha_ukrayinu_nazvaly_piratom_nomer_odyn)
7. *Конах В. К.* Зовнішні інформаційно-психологічні впливи на Україну та можливі шляхи їх нейтралізації / В. К. Конах, П. Д. Рогов // Сучасна українська політика. – 2013. – Вип. 29. – С. 135.
8. *Про що мовчали* новини у грудні-2013 // MediaSapiens. – 2014. – 1 серпня [Електронний ресурс]. – Режим доступу: <http://osvita.mediasapiens.ua/material/26525>
9. *Конституція* України : прийнята на п'ятій сесії Верховної Ради України 28.06.1996 р. // Відомості Верховної Ради України. – 1996. – № 30. – С. 141.
10. *Про Концепцію* Національної програми інформатизації : закон України від 4.02.1998 р. № 75/98-ВР // Відомості Верховної Ради України. – 1998. – № 27–28. – С. 182.
11. *Про основні засади* розвитку інформаційного суспільства в Україні на 2007–2015 роки : закон України від 9.01.2007 р. № 537-V [Електронний ресурс]. – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/537-16>
12. *Про Доктрину* інформаційної безпеки України : указ Президента України від 8.07.2009 р. № 514/2009 [Електронний ресурс]. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/514/2009>