

Тема 8

Ресурси інтернету в сфері культури. Культура інтернету

8.1. Загальні особливості культури інтернету. Переваги та недоліки використання інтернету в сучасному культурному середовищі

Інтернет-культура (англ. Internet culture) – це культура подання інформації та культура спілкування користувачів у інтернеті, яка може розглядатися як вид масової та кіберкультури.

Інтернет-культура є узагальнювальним поняттям для безлічі кібер і субкультур, що входять до неї, таких, як кіберспорт, вільне програмне забезпечення, рух Вікімедіа і т. д. На базі різних видів інтернет-культур формуються спеціалізовані інтернет-спільноти, які можуть відрізнятися за масштабом.

Інтернет-культура породила такі явища, як блоги, інтернет-література, культура соціальних мереж, і багато інших. Атрибутом інтернет-культури є, серед іншого, використання «смайликів» та акронімів англійських виразів: IMHO (In My Humble / Honest Opinion – «на мою скромну думку») та RTFM (Read The Following Materials – «прочитайте наступні матеріали»). Акроніми символізують бажання носія культури скоротити в обсязі зміст повідомлень у SMS. Ці та деякі інші традиції інтернет-культури сягають, серед іншого, ранніх кіберкультур користувачів комп'ютерних мереж, відмінних від інтернету, наприклад, Фідонета та локальних мереж.

Ранні види інтернет-культур асоціювалися з екзотичними соціальними прошарками, відомими як «гіки», «фрики» тощо; згодом користування Мережею увійшло у повсякденне життя більшості, ставши фактором глобалізації. Інтернет-культура є об'єктом вивчення кіберпсихології.

Оскільки межі кіберкультури важко визначити, цей термін використовується гнучко, і його застосування до конкретних обставин може бути спірним. Як правило, він стосується щонайменше до культур

віртуальних спільнот, але поширюється на широкий спектр культурних питань, пов'язаних з кібер-topics (наприклад, кібернетика), та сприймається як прогнозована cyborgization в організмі людини і людського суспільства.

Створення інтернету позитивно вплинуло на наше суспільство, надавши можливість широкого спілкування, зберігати інформацію (таку, як файли та зображення), підтримувати наш добробут. У міру розвитку інтернету можна створювати та публікувати цифрові й аудіофайли. Він став одним із основних джерел інформації, бізнесу та розваг, що призвело до створення різних платформ соціальних мереж – Instagram, Twitter, Facebook і Snapchat.

Спілкування з іншими людьми ніколи не було таким простим. Інтернет допомагає нам підтримувати стосунки з іншими людьми, виконуючи функцію доповнення до фізичної взаємодії. Люди також можуть створювати форуми й обговорювати різні теми, що допомагає у формуванні та побудові відносин.

Взаємодія з соціальними групами в інтернеті може допомогти запобігти та навіть вилікувати депресію. Стрімкі темпи життя в нашу складну епоху впливають на поширеність психічних розладів, включно з тривогою та депресією. Дослідження 2019 р., проведене Кристо Ель Морром та іншими науковцями, показало, що студенти Йоркського університету (Торонто) були надзвичайно зацікавлені в участі в онлайн-спільноті з підтримки психічного здоров'я. Учені зауважують, що більшість студентів віддає перевагу анонімній онлайн-спільноті психіатрів перед традиційними особистими послугами, соціальна стигматизація психічних розладів. Соціальні групи, створені в інтернеті, розширюють наш кругозір; різноспрямованість їх тематики надає обширне поле для взаємодії з однодумцями та висловлювання власних поглядів на певні події і проблеми. Онлайн-спілкування з іншими людьми дає людям відчуття того, що вони потрібні і вітаються в соціальних групах.

Поряд із численними перевагами вільний доступ до інтернету створює новий тип проблем, з якими ще не стикалося людство. Залежність від Мережі набуває загрозливих масштабів, оскільки інтернет охоплює всі сфери життєдіяльності суспільства на всіх рівнях: спілкування, торгівля, освіта та ін. Психологи вичленили низку симптомів, пов'язаних із залежністю (відчуженість, занепокоєння, перепади настрою тощо).

Активна участь у соціальних групах може замінити особисте спілкування, нівелювати соціальну орієнтацію, навички та спричинити почуття самотності.

Використовуючи онлайн-додатки, люди стають жертвами кіберзнущань. Залишаючись анонімними, кіберзалякувачі оперують негативними образами, формують атмосферу відеосорому з метою припинення гідності адресата та подальшого маніпулювання його свідомістю. Розроблена соціологами у співпраці з психологами теорія кіберзнущань містить концепт «огидності» цього явища. На жаль, найбільш уразливими в цьому плані є підлітки, оскільки ця вікова група прихильна до спілкування у соціальних групах. Грубі коментарі до їх постів знижують самооцінку, змушуючи дитину почуватися недостойною, що викликає депресійні стани.

Хоча вплив інтернету на когнітивні здатності ще не вивчений, деякі дані показують, що тривале використання вповільнює розвиток пам'яті та розбалансовує увагу, що вкрай важливо у дитячому віці. Величезний обсяг доступної інформації може спричинити інформаційне перенавантаження, знижуючи рівень її усвідомлення й оброблення. Результатом стає вповільнення ухвалення рішень, гальмування реакцій і втрата контролю за поведінкою, що є тривожним симптомом у будь-якому віці.

8.2. Взаємозв'язок інтернету, демократії та інформаційної політики

Широке застосування інтернет-комунікацій не могло не торкнутися сфери політики. Сьогодні інтернет все частіше виступає майданчиком для

політичних практик. Інтернет-комунікації та інформаційні технології впроваджуються у роботу органів державної влади, виступають інструментами для політичної мобілізації суспільства. Це сприяє виникненню нових форм участі громадян у прийнятті політико-управлінських рішень, що розширюють можливості проведення політичних кампаній. Однак потенціал інтернет-комунікацій, як і будь-якої іншої інновації у політиці, використовується політичними акторами по-різному. Так, у політичній практиці сучасних держав можна знайти багато прикладів перетворення інтернет-комунікацій на канали маніпуляції масовою свідомістю громадян, що використовуються для порушення стабільності політичних режимів і з метою розпалювання міжнаціональної ворожнечі.

Проте застосування інтернет-комунікацій дозволило створити основу для формування так званої електронної демократії.

Термін **«електронна демократія»** (далі – ЕД) має кілька різних трактувань. У найзагальнішому сенсі це – демократична політична система, в якій інформаційні системи та технології використовуються для виконання найважливіших функцій демократичного процесу: поширення інформації та комунікація, об'єднання інтересів громадян в ухваленні рішень (шляхом нарад і голосування). Електронна демократія заснована на принципі «one person – one node» (можливість підключення до мережі будь-якого користувача) та передбачає: пряме волевиявлення учасників (за аналогією з грецькою агорою); відсутність класів (рабів і рабовласників, феодалів, буржуазії); «електронне громадянство». Мова йде про участь громадян в управлінні державою, яке може здійснюватися двома шляхами: за допомогою особистої участі в ухваленні конкретних рішень (*пряма демократія*) чи виборами представників до органів законодавчої влади (*представницька демократія*).

Насправді ці явища зустрічаються не в чистому вигляді, а у різних проміжних і змішаних формах. Функціонування механізмів ЕД

проявляється в формі «електронної участі» (e-participation), за якою волевиявлення громадян здійснюється за допомогою інформаційних систем і технологій (публічні обговорення у форматі інтернет-форумів, електронне голосування, електронні вибори).

Теорія електронної демократії розроблялася низкою відомих вчених. Її основоположником вважається японський учений Єнедзі Масуда, який сформулював ідею про формування демократії участі на основі інформаційних технологій та етики спільного використання інформації.

На його думку, майбутньому суспільству належить жити в «комп-утопії», електронні комунікації тут отримають статус парламентських систем, тобто стануть технологічними. Розвиток таких інформаційних мереж передбачає проривну, революційну модель ухвалення рішень. Головною відмінністю стане наявність зворотного зв'язку, що дозволить змінювати або коригувати рішення, а швидкість передавання буде максимально скорочена. Така модель враховуватиме прагнення всіх верств населення, тому що зворотний зв'язок триватиме доти, доки не буде сформовано відповідне рішення. Це дозволить задовільнити інтереси не тільки більшості, як у сучасних демократичних країнах, а і меншин.

Існує **шість базисних принципів демократичної участі** в інформаційному суспільстві:

1) усі громадяни або принаймні переважна їх кількість мають брати участь у процесах ухвалення рішень;

2) синергія (добровільна участь у вирішенні загальних проблем) і взаємодопомога (готовність жертвувати своїми інтересами) стануть основою вироблення політичних рішень;

3) доступність широким масам населення всієї необхідної інформації для обґрунтованого ухвалення політичних рішень;

4) отримана вигода та доходи мають розподілятися між усіма громадянами;

5) вирішення політичних питань слід шукати шляхом переконування та досягнення загальної згоди;

6) ухвалене рішення має реалізовуватись шляхом спільних дій, співпраці всіх громадян.

Положення про право вільного доступу громадян до державної інформації у сучасних розвинених демократіях уже отримало повсюдне поширення та закріплено в законодавстві.

Поширенню електронної демократії дала поштовх та обставина, що інтернет став зручним місцем зустрічей для різних груп за інтересами, професійними спільнотами, споживчими асоціаціями тощо. Інтернет-спільноти виникають навколо певних електронних ресурсів та експлуатують природне прагнення людей до спілкування з однодумцями. Відмітними рисами інтернет-спільнот вважаються:

регулярна відвідуваність досить стабільними аудиторіями мережевого ресурсу, навколо якого створюється співтовариство;

наявність зворотного зв'язку завдяки інтерактивним можливостям ресурсу;

створення власної субкультури з усіма обов'язковими атрибутами: ієрархією, етичними та поведінковими нормами, рольовими іграми, спільною участю в online-/offline-заходах.

Синонімами електронної демократії можна вважати також поняття мережевої демократії, Демократії 3.0, вікідемократії та плинної (рухомої) демократії (Liquid Democracy).

Мережева демократія означає широку участь громадянського суспільства в процесі ухвалення політичні рішення через інтернет. Демократія 3.0 наголошує на використанні найсучаснішої інтерактивної платформи Web 3.0 для реалізації концепції «**мережевої демократії**».

«Вікідемократія» включає модель прямої електронної демократії, заснованої на поєднанні принципів спільної роботи громадян над рішеннями (як у Вікіпедії) та загального голосування з усіх спірних питань (як за прямій демократії). Люди можуть вносити будь-які пропозиції щодо рішень і поправки в них, але прийнятими вважаються лише ті пропозиції, які підтримані більшістю голосів.

Поточна (рухлива, хмарна) демократія – це найбільш гнучкий варіант мережевої демократії, симбіоз прямої та представницької демократій. Її сутність полягає в тому, що, оскільки окремо взятий громадянин не може однаково добре розумітися на всіх проблемах, він має право з будь-якого питання делегувати свій голос іншим учасникам голосування, зокрема експертам (фахівцям чи політикам від різних партій, а також безпартійним).

На окрему увагу заслуговує концепція **електронного уряду** (далі – ЕУ), яка не тотожна поняттю електронної демократії. Відповідно до визначення Європейської комісії, електронний уряд передбачає використання у державних структурах інформаційно-телекомунікаційних технологій на тлі проведення організаційних реформ і формування у державних службовців навичок, спрямованих на покращення функціонування держструктур і підвищення рівня надаваних ними послуг. З цього випливає, що основна мета застосування ЕУ – підвищення ефективності роботи державних служб.

Індекс розвитку електронного уряду (EGovernment Development Index, EGDI) складається раз на два роки Департаментом економічного і соціального розвитку ООН (UN DESA, United Nations Department of

Economic and Social Affairs). Містить три підіндекси, що характеризують стан ІКТ-інфраструктури, людського капіталу й онлайнових державних послуг.

З погляду електронної демократії, створення ЕУ має найважливіше значення, оскільки відкриває доступ громадськості до інформації державної

ваги, тим самим сприяючи транспарентності державної влади та створення системи громадського контролю за її діяльністю через інтернет.

Спроби створення подібних систем на основі різних телекомунікаційних засобів регулярно робилися у промислово розвинених країнах у другій половині XX ст. Але саме інтернет виявився найбільш зручним і, що важливо, дешевим засобом, за допомогою якого ці ідеї перейшли у практичну сферу. Мережа розглядається як можливість заміщення розриву між керівними та керованими системами.

Виділяють чотири умовні напрями взаємодії між органами державного управління, громадянами та суб'єктами комерційної діяльності:

держава – бізнес / бізнес – держава (Government-to-Business/ Business-to-Government, G2B/B2G);

держава – держава (Government-to-Government, G2G);

держава – громадяни / громадяни – держава (Government-to-Citizen/Citizen-to-Government, G2C/C2G);

держава – службовці (Government-to-Employees, G2E).

Хоча найчастіше названі функції виконуються тими самими електронними урядовими структурами, цілі у цих напрямів різні.

Розвиток **G2B/B2G** має полегшити взаємодію між комерційними структурами й урядом за рахунок відкритого онлайн-доступу до законодавчої інформації (законодавчі акти, федеральні правила, інструкції) та забезпечити можливість надання звітності контролюючим держорганам через інтернет.

Основне призначення **G2G** – покращити взаємодію між федеральними, державними та місцевими органами влади, а **G2C/C2G** – надати громадянам зручний і швидкий онлайн-доступ до інформації та послуг.

Напрямок **G2E** надає пріоритет контактам між державою та державними службовцями. Іншими словами, електронний уряд відкриває доступ до законодавчої інформації, водночас дозволяючи громадянам і комерційним

структурам здійснювати різноманітні операції (від сплати комунальних рахунків до подання звітності до держорганів) через інтернет.

Сьогодні основною базою розвитку системи електронної демократії є **технологія Web 2.0**, яка уможлиблює взаємодію користувачів, організовану ними самими, обмін і подальшу переробку інформації (блоги, соціальні мережі, громадська журналістика тощо). У політичному житті інформаційних товариств блогосфера займає особливе становище, відіграючи роль провідного майданчика політичного дискурсу. Блогери висловлюються з найбільш актуальних суспільно-політичних проблем, і це відбувається безперервно в інтерактивному режимі. Блоги не піддаються цензурі (лише в деяких країнах висловлювання у блогах прирівняні до публічних і таким чином підпадають під кримінальну відповідальність).

Крім того, блогосфера безперервно розширюється, і стартові умови для її учасників рівні. У багатьох країнах блогосфера стала не тільки загальнодоступною платформою для прямого політичної участі громадян, а й значущим чинником у політичному житті. Найчастіше «серйозні» блогери виступають під реальними (а не віртуальними) іменами, стаючи помітними суспільно-політичними постатями.

Великою популярністю у політичному житті багатьох країн користуються також мікроблоги (особливо Twitter). Так, широко відома прихильність до цієї форми інформаційної взаємодії із суспільством з боку багатьох офіційних осіб і навіть глав держав. У деяких випадках «неофіційне» листування офіційних осіб у Twitter замінює усні перемовини. Нерідко така інформація швидко потрапляє до інтернету і тиражується там ще до того, як стане офіційною новиною.

Вищою формою електронної демократії визнається **електронна пряма демократія** (Electronic Direct Democracy, EDD), яка безпосередньо залучає громадян у виборчу діяльність з використанням інформаційно-комунікаційних засобів (наприклад, Сіті-холи у США зі створення системи

обліку думок виборців, досвід Флориди з регулювання діяльності громадських організацій ВНЗ; кантональні електронні системи у Швейцарії).

У дослідницьких роботах прийнято розподіляти **рівні електронної демократії**: міжнародний, національний, регіональний та місцевий. Найбільш складною у зарубіжній теорії та практиці вважається проблема правового обґрунтування реалізації електронної демократії. Як показало загальне дослідження цього питання, йдеться про побудову складних юридичних моделей на основі комплексів законодавства, покликаного врегулювати захист спільних демократичних прав і свобод громадян та нормативних актів, що регулюють відносини в сфері використання інформаційно-комунікаційних засобів.

У деяких країнах та регіонах світу вже створено дуже ефективну систему громадського контролю за діяльністю державної влади через інтернет (**електронна держава**). Однак моделі цієї системи мають яскраво виражену регіональну специфіку.

Європейська модель характеризується наявністю наддержавних інститутів – Європарламенту, Єврокомісії, Європейського суду, рішення яких є обов'язковими для виконання усіма країнами ЄС. Тому ця модель орієнтована насамперед на вирівнювання умов і координацію діяльності електронного уряду для країн – членів Європейського Союзу.

Вона втілює у реальність модель G2G.

Азіатська модель спирається на специфічний стиль управління, азіатський тип корпоративної культури та багатопланову систему державного управління, організованого за принципом ієрархічної піраміди. Така модель є практичним здійсненням G2E.

Північноамериканська модель електронного уряду отримала поширення у США та Канаді. Ця модель передбачає не просто доступ до сайтів урядових організацій, а багато в чому визначає її специфіку, стає

місцем вільного обміну ідеями, ініціативами, майданчиком для обговорення результатів тих чи інших робіт та укладання бізнес-угод. Вона розвивається у рамках теоретичних концепцій G2C і G2B та ставить за мету розвиток електронної демократії через побудову затребуваного електронного уряду. Американське бачення концепції електронного уряду орієнтоване задовільнення потреб громадян і спирається на ринкові механізми. Канадську модель можна назвати класичною, оскільки основне призначення електронного уряду в Канаді полягає у наданні громадянам через інтернет каналів доступу до державної інформації, а також у навчанні всіх фізичних та юридичних осіб з використанням нових систем – електронний уряд фокусується на надання громадянам послуг.

8.3. Географія інтернету. Безпека та стратегія в епоху інтернету

У географії глобальної мережі інтернет наприкінці XX – початок XXI ст. відбулися масштабні зрушення, пов'язані з суттєвим скороченням кількісних розривів між країнами світу та згладжуванням територіальних диспропорцій на рівні проникнення інтернету. Загострення глобальної проблеми інформаційної безпеки й управління Мережею у другому десятиріччі XXI ст. спричинило диверсифікацію трафік-потоків, розвиток незалежних регіональних мереж і внутрішньорегіональних телекомунікацій, а також значні геополітичні зрушення, що викликало суттєву децентралізацію та перебудову світової мережі «Інтернет».

Однак у сфері інформаційного наповнення та управління Мережею монополія розвинених країн зберігається. Інакше кажучи, цифровий розрив перемістився в іншу площину: не стільки питання доступу та технічної забезпеченості, скільки можливості з генерування інформації та управлінню інформаційними потоками визначають сьогодні розподіл сил у світовому господарстві. Світові тенденції розвитку телекомунікацій такі, що поступово всі традиційні інформаційно-комунікаційні послуги

мігрують до інтернету, як і значна частина державних послуг, торгових, культурно-освітніх та ін. У цьому зв'язку поширення та активне використання інтернету має сьогодні вирішальне значення для соціально-економічного розвитку та підвищення конкурентоспроможності будь-якої економіки, розширення можливостей її інтеграції у глобальне інформаційне суспільство та світове господарство.

У сьогоднішній економіці, з її вимогами безперервного функціонування та постійного зв'язку, компанії змушені посилювати стратегію кібербезпеки та демонструвати замовникам, що захист даних має для стратегії взаємодії вирішальне значення. У світовій економіці з цифровізацією операцій, ланцюжків поставок, бізнес-процесів, а також обслуговування співробітників і клієнтів кібератаки залишаються однією з основних загроз.

У звіті Всесвітнього економічного форуму про глобальні ризики за 2021 р. (Global Risk Report for 2021) проблеми кібербезпеки названі однією з найбільших загроз, з якими зіткнеться людство протягом найближчих десяти років. Нові загрози та вразливості виникають з неймовірною швидкістю; інструменти даркнету стають все більш розвиненими та доступними, а кібератаки – більш масштабними. Нові технології створюють можливості для інновацій, проте ми спостерігаємо серйозні втрати даних і зростання кількості атак програм-вимагачів, тому планування сталості бізнесу стає ключовим чинником його виживання. Згідно з недавнім дослідженням Gartner, програми-здирилки вважаються однією з найнебезпечніших загроз для організацій: до 2025 р. принаймні 75 % IT-організацій зіткнуться з однією або декількома атаками такого типу.

Сьогодні кіберзлочинність безпосередньо пов'язана із вартістю даних. Дані – це нове золото, і захистити величезний портфель активів непросто, особливо з урахуванням його зростання. Глобальний індекс захисту даних Dell Technologies (2021 Global Data Protection Index) показав, що особи, які ухвалюють рішення у сфері IT, розуміють потенційну цінність даних, але,

незважаючи на ризики, не дуже впевнені у своїх рішеннях щодо захисту даних. Понад 2/3 респондентів заявили, що їх поточні рішення стосовно захисту даних не дозволяють вирішувати майбутні бізнес-завдання.

Для організації безпечного віддаленого доступу до захищених мереж важливо використовувати засоби криптографічного захисту. Для предиктивного захисту можна застосовувати системи аналізу трафіку NTA (Network Traffic Analysis), розгортати системи виявлення (IDS) та запобігання (IPS) вторгненням, які фіксують і блокують несанкціонований доступ до комп'ютерних систем.

Швидке зростання кількості атак програм-вимагачів останніми роками турбує багатьох. Якщо дані стали жертвою атаки програми-здирика, і їх неможливо розшифрувати, то сплата викупу, на жаль, не дає результату. За даними щорічного звіту Sophos щодо вірусів-вимагачів, із 32 % організацій, які заплатили викуп за останній рік, лише 8 % вдалося розшифрувати й отримати всі свої дані, з них 29 % змогли відновити не більше половини своїх даних.

Рішення для захисту та відновлення даних можуть стати важливою частиною безпекової стратегії. Такі рішення мають кілька рівнів безпеки, захищаючи й ізолюючи дані, забезпечуючи проактивний моніторинг та оповіщення, а також швидке відновлення у разі успішної атаки програми-вимагача. Передові технології, засновані на штучному інтелекті та машинному навчанні, дозволяють одразу виявляти потенційні атаки та попереджати про них.

Захист бізнесу від найгіршого сценарію – втрати критично важливих даних – потребує досвіду в галузі кібербезпеки та цілісного підходу до забезпечення стійкості. Синергія технології та бізнес-процесів – ось за рахунок чого досягається справжня стійкість. Кожен підрозділ бізнесу має розуміти, де знаходяться їх найцінніші конфіденційні дані та сервіси, який у них рівень ризику.

З цієї причини регулярне сканування та аналіз внутрішнього ІТ-ландшафту необхідні для розуміння змін та стороннього впливу на них.

Крім забезпечення опору потенційним перешкодам для бізнесу, компанії викривають «сліпі зони» та вразливості, які можуть призвести до серйозних фінансових втрат та репутаційних ризиків.

Щоб подолати проблеми та залучити до процесів забезпечення безпеки своїх співробітників, організації мають використовувати багатосторонній підхід, який включає:

навчання співробітників у сфері безпеки: дуже важливо, щоб усі співробітники розуміли, чому безпека даних важлива на кожному рівні, що вони є важливою частиною забезпечення безпеки, знали свою роль;

управління ризиками: враховуючи продовження експоненційного зростання обсягів даних, важливо використовувати різні стратегії захисту для забезпечення безперервної доступності, реплікації, резервного копіювання та архівування даних, створюючи ефективне та масштабоване рішення для захисту даних;

створення цифрового сховища: переконайтеся, що є чиста копія критично важливих для бізнесу даних, яка зберігається в ізольованому середовищі та придатна для відновлення у разі будь-якої кібератаки;

узгоджену систему безпеки: щоб компанії могли випереджати конкурентів, вони мають зробити інвестиції в заходи та засоби безпеки своїм головним пріоритетом і проактивно вирішувати питання забезпечення конфіденційності даних, упереджуючи та нівелюючи загрозу атаки.

Це означає, зокрема, впровадження ІТ-рішень (наприклад, ноутбуків, серверів, сховищ), в основу яких безпека вже закладена.

Отже, описані заходи в рамках багатостороннього підходу дозволяють здійснювати антиризиковий механізм управління безпекою співробітників організації в епоху інтернету.