УДК 35:342.7

Л. М.НОВАК-КАЛЯЄВА

СУЧАСНІ АЛГОРИТМИ ВЗАЄМОДІЇ ДЕРЖАВИ ТА СУСПІЛЬСТВА У ВІРТУАЛЬНОМУ ПРОСТОРІ НА ЗАСАДАХ КОНЦЕПЦІЇ ПРАВ ЛЮДИНИ

Досліджено особливості взаємодії держави, суспільства й особи у віртуальному просторі на засадах концепції прав людини. Підкреслено потенціал свободи доступу до інформації – повної свободи, без фільтрів або цензури, а для органів влади запропоновано не стільки встановлювати бар'єри та заборони, скільки розвивати здатність особи до думки та критичного аналізу. Визначено навчання технологіям за допомогою технологій як актуальний шлях та одне з провідних завдань органів державного управління.

Ключові слова: державне управління, права людини, інформаційний простір, дотримання прав людини в інтернеті.

The features of co-operation of the state, society and person are investigational in virtual space on principles of conception of human rights. Potential of freedom of access is underline to information - complete freedom, without filters or censorship, and for the organs of power it is suggested not so much to set barriers and prohibitions, скільки develop the capacity of person for an idea and walkthrough. Studies to technologies by means of technologies are certain as an actual way and one of leading tasks of organs of state administration.

Key words: state administration, human rights, informative space, bservance of human rights in the internet.

Інформаційний простір у сучасному світі перетворився на істотний чинник функціонування всіх суспільних інституцій і вимагає чіткого окреслення їх позицій щодо алгоритмів взаємодії у віртуальному просторі. Мова йде як про політику влади, так і ставлення громадськості щодо її реалізації, зокрема в контексті забезпечення прав людини. Звичними заходами впливу для органів влади завжди були заборони та покарання, що вважалися дієвими засобами запобігання небезпекам і захисту користувачів від неякісної та негативної інформації. Натомість ці засоби не є ефективними щодо сучасних масштабів технологічних змін, отже, діяти необхідно способами, що не мають нічого спільного з насильством у будь-якому його вигляді. Значна частина учасників суспільної дискусії на цю тему схильна запропонувати в якості альтернативи заходи освіти та переконання, тобто фактично умотивувати користувачів до етичної поведінки в мережі. Скепсис з цього приводу – зрозуміла, але неоднозначна реакція. Дійсно, потрібно не стільки встановлювати бар'єри та заборони, скільки розвивати здатність особи до думки

та критичного аналізу. Навчання технологіям за допомогою технологій – актуальний шлях, це одне з провідних завдань органів державного управління.

Дослідженню проблем управління в умовах інформаційно-технологічних змін, дотримання прав людини у всесвітній мережі присвятили свої роботи зарубіжні вчені, зокрема В. Брітков, Ж. Бус, Х. Вегенер, Л. Вудс, Ж.-Г. Ганашиа, Дж. Девіс, М. Кастельс, Дж. Маркофф, А. Лехман, Х. Ніссенбаум, Х. Сенг-Хан, Є. Касперський та ін.

Серед українських науковців інформаційні системи в державному управлінні вивчали І. Клименко, О. Осауленко, А. Панчук, М. Сендзюк, В. Тронь. Проблемам розвитку державного управління в умовах інформатизації присвячено праці вітчизняних науковців О. Амоші, В. Бакуменка, М. Бутка, В. Гейця, О. Дація, М. Дітковської, М. Корецького, Я. Олійника, О. Суходолі, Л. Чернюк, М. Чумаченка. Вивченню ролі інформації в управлінні соціально-економічним розвитком України присвячено праці Л. Бакаєва, В. Ситника, М. Татарчука, Ю. Шарова. Однак у вітчизняній науці державного управління проблеми дотримання прав людини у віртуальному просторі висвітлено недостатньо, що обумовило актуальність теми.

Мета статті – окреслити основні аспекти взаємодії державних органів, суспільства та окремої особи в умовах інформаційного суспільства, що розвивається та вимагає від держави урегулювання відносин, що в ньому складаються.

Права людини ґрунтуються на принципах свободи, автономності особи та рівності. На таких саме принципах повинні ґрунтуватися й підходи до знання, в суспільстві, що усвідомлює потребу в знаннях глобально. Безпрецедентний масштаб інформаційних потоків в інформаційному суспільстві обумовлює формування попиту суспільства на знання. Різниця між інформацією і знанням укорінена, головним чином, в інтерпретації: інформація завжди нейтральна, її можна вимірювати, накопичувати та зберігати. Знання обумовлюють наявність суб'єкта, реального або потенційного, здатного до інтерпретації. Існування знання засноване на тому, що між людською свідомістю та навколишнім світом існує взаємодія, тобто не існує знання без свідомих суб'єктів, здатних до розуміння. Отже, засобами технології неможливо зберегти знання, тому що воно завжди залежить від дійсної або потенційної інтерпретації суб'єктом. Без носія інформація не може відбутися як знання.

Громадськість наполягає на необхідності свободи доступу, заборони будь-якого виду цензури, тобто слід не тільки заборонити обмеження доступу до знань, але й не допускати будь-якого відстежування, тобто інтернет як і бібліотека повинен залишатися місцем свободи та відвертості, що безпосередньо стосується позиції та політики влади в цьому питанні.

На практиці це означає виконання певних умов, зокрема, це стосується свободи доступу до інформації – повної свободи, без фільтрів або цензури. Питання щодо можливості допускати расизм, розпалювання ненависті, заклики до війни, прояви фанатизму – контраверсійні, а відповіді на них – неоднозначні.

Існують веб-сайты, на яких інформація присвячена, наприклад, технологіям терору або самогубства, або методиці наукового дослідження чи благодійності.

Мережа інтернет є глобальним об'єднанням комп'ютерних мереж і інформаційних ресурсів, що належать безлічі різних людей і організацій. Це об'єднання є децентралізованим, і єдиного загальнообов'язкового зведення правил (законів) користування інтернетом не встановлено. Існують, проте, загальноприйняті норми роботи в інтернеті, спрямовані на те, щоб діяльність кожного користувача мережі не заважала роботі інших користувачів. Фундаментальне положення цих норм таке: правила використання будь-яких ресурсів інтернету визначають власники цих ресурсів і лише вони. У цьому контексті під терміном "ресурс" розуміється будь-яка сукупність програмних і апаратних засобів, що становлять у тому або іншому значенні єдине ціле. Ресурсом інтернету можуть вважатися, наприклад, поштовий ящик, персональний комп'ютер, віртуальний або фізичний сервер, локальна обчислювальна мережа, канал зв'язку тощо.

Інтернет є чудовим засобом доступу до інформації, до знань і можливостей, що суттєво розширює можливості вибору, розкриває шляхи та засоби реалізації свідомого та вільного від самообмежень вибору. Тому обов'язково необхідно усунути цифрову нерівність, що постійно збільшується через невпинний прогрес технологій, між тими, хто може користуватися наявними знаннями і можливостями в мережі, і тими, хто недостатньо інтелектуально підготовлений для цього. Місце органів влади визначається там, де відбувається навчання, мається на увазі, як, власне, навчання функціонерів, так і обов'язок органів державного управління на державному рівні організувати та забезпечити таке навчання для широкого загалу, особливо для громадян старшого покоління.

Одним з найважливіших завдань органів державного управління щодо забезпечення рівного доступу громадян до інформації є сприяння щодо задоволення суспільних потреб матеріального характеру, зокрема наявності інфраструктури і доступності контента, а також свободи взаємодії користувачів і поширення контента.

Надмірно складний спосіб пошуку інформації вимагає спеціальної підготовки, що викликає труднощі у широкого загалу користувачів. Для вирішення цієї задачі створено такі технічні засоби, як пошукові служби або агрегатори інформаційних ресурсів, що діють на основі спеціально розроблених когнітивних стратегій звернення до інформації: мережний серфінг, перегляд, імітаційне моделювання, вибірка, перевірка рівнів достовірності інформації в мережі (reputation networks) тощо, хоча реально звільнити людину, що стикається з потоками і обігом інформації, подібні стратегії можуть лише в тому випадку, якщо користувач здатен критично сприймати весь представлений контент, тобто має певну підготовку та відповідний рівень освіти.

Згідно з принципом вільного доступу, кожна людина незалежно від рівня добробуту, раси або національності має право на доступ до всього контенту і право самому бути виробником контента. При цьому мережа переважно

використовується для роботи з електронною поштою, для пошуку інформації та здійснення електронної комерції. Існують також он-лайнові ігри або віртуальні світи, але вони цікавлять обмежену частину користувачів інтернету. Рівний доступ не зводиться лише до того, що кожному дано рівне право мати доступ до наявних інформаційних ресурсів, вільно виражати себе або передавати будь-які дані швидкісним каналом комунікації. Рівний доступ повинен також забезпечувати реальну і повну можливість для особи існувати в мережі згідно з власним вибором та власним прагненням.

Дотримання принципів, закріплених у законодавстві Європейського Союзу, зокрема принципу ліберальності, як він сформульований у Директиві щодо електронної торгівлі та Директиві по телебаченню [1; 2], зводиться до дотримання принципу країни походження, хоча в зацікавлених колах активно обговорюється і припущення, що контент повинен також відповідати нормативно-правовому полю країни одержувача.

Питання про відповідальність за незаконний, заборонений, небезпечний або неетичний контент в інтернеті викликає бурхливу реакцію зацікавлених урядовців, дослідників і користувачів. Проблематика зводиться до ефективного здійснення регулювання і забезпечення виконання правових норм. Це важливе питання повинне розглядатися з точки зору не тільки, власне, ухвалення, а ще й можливостей застосування правових норм.

Сформувати електронне середовище, позбавлене небезпек, загроз, цинізму та обману – шляхетне завдання, до реалізації якого слід прагнути й постійно рухатися в цьому напрямку. Через моніторинг, контроль, блокування, видалення або покарання тих, хто не дотримується цих правил і норм, також можна впливати на зміст контенту, але неосяжність віртуального простору та досконалість засобів користування, що постійно урізноманітнюється, робить репресивні заходи переважно фрагментарними та приреченими ніколи не бути здійсненими в задуманому обсязі.

Рельєфною в цих умовах постає необхідність визнати моральні аспекти суспільного буття у віртуальному просторі, тобто потребу зміни парадигми й відходу від тільки ринкової демократії, що визнається значним колом юристів, управлінців і користувачів. Важливо визнати існування інших цінностей і благ, крім економічних: цінність відносин, досвіду, стабільного розвитку й етичної поведінки. Проблема контролю за дотриманням нормативних вимог у цьому контексті – це питання про те, яких саме цінностей повинне дотримуватися дане суспільство, стала предметом загальної дискусії, що ведеться в європейському суспільстві, однією зі складових якого є інтернет-співтовариство.

Права на інформацію не вимагають будь-якого документального підтвердження чи дозволу, тобто недоречно реалізацію прав людини ставити в залежність від документальних посвідчень або дозволів будь-яких третіх осіб або державних органів. Права людини, безумовно, поглинають свободу інформації як щодо свободи виразу, так і з точки зору права шукати і одержувати інформацію.

Отже, свобода виразу думок, як у мережі, так і поза нею, є таким самим основним і невід'ємним правом громадян, як виборче право, і ці фундаментальні права не можуть ставитися в залежність від того, чи пройшла людина "перевірку", або чи одержала "посвідчення".

Слід визнати, що між високими принципами, що відображені в конвенціях, договорах, національних законодавчих актах, правилах поведінки тощо, і реальністю інтернету, що живе за законами комерції, вигоди й волі виразу, існує глибокий розрив. Потрібні більш чіткі і точні правила та директиви, яких користувачі інтернету могли б дотримуватися й застосовувати на практиці. Водночас, існує потреба в ясному, точному, чіткому й докладному законодавстві та у відкритому й гнучкому інструменті, який міг би бути застосовуваним у різних контекстах у новаторській глобальній реальності інтернету.

У рамках європейської конвенції про захист прав людини постійно ведеться робота щодо вирішення цих завдань. Рішення європейського суду з прав людини показують, що навіть судді, що дотримуються загальних принципів європейської конвенції з прав людини і судової практики європейського суду, не завжди доходять узгоджених висновків з питань про те, чи порушує той чи інший публічний експонат, представлене на виставці полотно чи зображення в журналі права інших людей, право на недоторканність приватного життя, або, наприклад, право на людську гідність такою мірою, яка виправдовувала б втручання органів влади [3].

Усесвітня мережа має потенціал, що дозволяє вирішувати деякі практично безвихідні життєві ситуації, розкриває перед користувачами як індивідуальними, так і груповими, як приватними особами, так офіційними державними структурами незбагнене коло можливостей, перелік яких постійно буде збільшуватись. Отже, можливо, доцільно стримувати очікування відносно регулювання і контролю інтернету за допомогою досконалих правил і норм, натомість, зберігаючи певний чинник ризику, зосереджувати увагу на питаннях безпеки і реагувати на явні загрози та ситуації, що завдають серйозного збитку окремим людям, групам або народам в суспільстві. Забезпечення можливості свободи виразу думок, зокрема, можливість протестувати, реагувати, обговорювати і роз'яснювати, не погоджуватися з деякими діями і контентом в інтернеті, чи об'єднувати однодумців – це краще рішення, ніж будь-які заборони, хоча, звичайно, заборонити набагато простіше [6].

Демократичне суспільство, що внаслідок активної акцептації та запровадження в повсякденне життя технологічних новацій перетворюється на інформаційне суспільство, має поширення свободи слова своєю основоположною характеристикою, тож напевне буде поступово позбуватися інтенцій щодо заборони, фільтрування або обмеження інформаційних потоків як недоцільних і безперспективних. Прозорість, дієві гарантії функціонування пошукових систем і використання інтелектуальної власності, доступу до інформації, а також відповідний рівень загальнодоступного контента демонструють тенденції до оздоровлення інтернет-простору, зокрема, щодо морально-етичних характеристик змісту.

Суть нових підходів полягає в тому, що саме свобода є засадничим принципом функціонування віртуального простору, хоча авторське право і може виправдовувати деякі обмеження щодо відтворення або передачі в загальне користування творів, ним захищених. У демократичному суспільстві будь-який випадок посилання на авторське право повинен мати обґрунтування, тобто свобода виразу думок має бути глобальною, а інформація, що охороняється авторським правом, повинна розташовуватися окремо й оберігатися обмеженим доступом, а не навпаки. Отже, доцільно ретельно погоджувати вимоги авторського права з інтересами інформаційного суспільства назагал, а не замикатися лише на економічних інтересах авторів та їх нащадків.

Європейська конвенція про захист прав людини відображає базові цінності, на яких будуються правові норми. На даний момент Конвенція вже гарантує права більше 800 мільйонів людей, що живуть в 47 країнах. Стаття 8, що розглядає право на недоторканність приватного життя, та стаття 10, що стосується свободи виразу думок та інформації, застосовувалися європейським судом з прав людини при розгляді справ, пов'язаних з інтернетом.

Існують "горизонтальні ефекти" закріплених у Конвенції прав і свобод, які означають, що права і свободи інших повинні поважатися не тільки державою, але також окремими громадянами і приватними компаніями. Держава покликана формувати відповідну політику і створювати таке середовище, яке на практиці гарантує всім громадянам права і свободи, закріплені в Конвенції. "Горизонтальні ефекти" і позитивні зобов'язання держави – це два поняття конституційного і міжнародного права, що забезпечують додаткові переваги для реалізації прав людини, включаючи свободу виразу думок. Концепції "горизонтального ефекту" і позитивних зобов'язань держави – важливі стимули для дій, спрямованих проти торгівлі людьми і жорстокого поводження з дітьми [5].

Основою для формування довірчих відносин, підвищення і розширення інформованості є залучення громадянського суспільства в процес регулювання та саморегулювання і спільного регулювання віртуального простору. Законодавство надмірно орієнтоване на покарання і санкції – це недостатньо ефективний підхід для вирішення вказаних проблем, який нерідко лише погіршує становище, особливо щодо молоді.

Органам державного управління спільно зі структурами громадянського суспільства необхідно створювати структури, які займалися б питаннями оцінки якості і відбору релевантної інформації. Насаджувати цінності під загрозою покарання в сучасних умовах також непродуктивно й безперспективно. Доцільно використовувати інші інструменти, які допоможуть успішніше вирішувати завдання інтерналізації норм і цінностей, тобто сприйняття користувачами різного віку, гендерної приналежності, професійного та соціального статусу норм, цінностей, поглядів, які пропонуються спільно дотичними державними та громадськими інституціями як обов'язкові чи бажані для функціонування мережі. Упровадження системи знаків якості, що дозволяє користувачам вибирати продукт

або послугу і відчувати себе упевнено в своєму електронному середовищі – завдання комплексне, що вимагає спільних позицій та дій.

У цьому контексті органи державного управління повинні фінансувати послуги експертів та необхідні технічні служби для розробки відповідного програмного забезпечення щодо виявлення та знешкодження шкідливого контенту: відео- та фото- порнопродукції, вірусних загроз, погроз та закликів до насильства, пропозицій щодо нелегальної торгівлі зброєю, наркотиків, торгівлі людьми тощо. Сегрегація сайтів відносно їх контенту за віковими категоріями (до 18(?) років) щодо наявності тематичних тегів про алкоголь, "для дорослих" тощо вже проводиться у багатьох європейських країнах. Спеціальні державні служби, наприклад, ФБР у США, аналогічну роботу проводять щодо соціальних мереж, залишаючи за собою право розслідування та превентивних заходів у випадку терористичних загроз чи дій, небезпечних для особи, зокрема, наприклад, загрози замаху на самогубство.

Прикладом конструктивного походу до вирішення суспільних проблем, пов'язаних з інтернетом, може бути європейська практика дій, спрямованих проти жорстокого поводження з дітьми в інтернеті, як приклад галузі, де вже позначилися успіхи у справі захисту життя й психічного здоров'я дітей і молоді. Одним із важливих аспектів у цій проблематиці є законодавчі акти та правозастосовча практика відповідних служб та органів юстиції та державного управління.

Необхідність заборони на жорстоке поводження з дітьми визнана практично в усіх культурах, хоча й спостерігаються відмінності в розумінні того, якими методами слід боротися з насильством над дітьми, що не заважає глобальному підходу до превентивних дій, спрямованих на захист дітей, з акцентом на дії спеціальних служб і створення більш безпечного електронного середовища, комфортного для прав людини.

Інтернет надає кожному користувачеві, що виступає активним суб'єктом глобального інформаційного суспільства, можливість діяти безпосередньо, негайно і не зважаючи на державні кордони. Послуги і технології інтернету дозволяють користувачам різних переконань, різного походження та рівня освіти встановлювати контакт один з одним і об'єднуватися у співтовариства. За таких умов виникають проблеми ідентифікації й анонімності, що ставлять під сумнів здатність користувачів адекватно розуміти своє віртуальне життя, – як приватне, так і професійне, – усвідомлювати можливі наслідки та впливати на них у віртуальному середовищі, де виникають нові норми співіснування віртуальних учасників.

Виділяють два типи ідентичності: ipse-ідентичність: відчуття власної особи, й idem-ідентичність – як більш формальну ідентичність, залежну від віртуального контексту, оточення і ситуації. Захисники недоторканності приватного життя і прав людини підкреслюють загрозу для ipse-ідентичності в ситуації, коли комп'ютери накопичують знання, створюють профілі, здійснюючи вплив на idem-ідентичність користувача, який не підозрює про ці профілі і про те, як вони

впливають на його ipse-ідентичність. Наслідком такого алгоритму впливів мережі є вплив на позитивну свободу індивіда, який змушений взаємодіяти зі світом, який вибраний для нього, але не ним самим. Міркування на користь створення нового права, а саме права на захист ipse-ідентичності обумовлюють це право ідентичності як таке, що не повинне формулюватися як негативне.

Істотною проблемою віртуального суспільства є достовірність контента, в якому інформація повинна бути перевіреною, надійною та якісною. В інформаційному суспільстві, якщо людина невидима в інтернеті, з політичної точки зору вона не існує. З появою нових медіа в мережі, виникає "Мережа активної участі", яка протиставляється "Мережі споживання" і знаменує собою виникнення ряду нових механізмів участі і прояву власної зацікавленості користувачів. Нові цифрові медіа забезпечують право на участь і надають користувачу вибір, яку позицію займати: пасивного споживача або активного учасника. Суспільство стикається також і з появою змішаних варіантів. Наприклад, мережні соціальні сервіси Web 2.0 і соціальні мережі набувають особливої популярності в галузі освіти. У мережному доступі перебуває велика кількість різних матеріалів, які можуть бути використані як у навчальних, так і в професійних цілях. Сервіси соціального забезпечення спростили процес створення, редагування і публікації власних цифрових об'єктів, – текстів, фотографій, відеофрагментів, музичних записів тощо, – в інтернет-мережі. Тепер кожний користувач може не тільки отримати доступ до цифрових матеріалів, але й брати участь у їх формуванні. Web 2.0 дозволяють розширити межі взаємодії всіх учасників освітнього процесу, що виходять за рамки навчальних занять, зробити цю взаємодію більш продуктивною, зручною, результативною. Мережні сервіси спілкування надають користувачам можливість керувати своїм навчанням, публікувати власні думки і демонструвати розуміння матеріалу, а також забезпечують можливість індивідуалізації змісту навчання [4].

Контент, що створюється користувачами, – "user-generated content" (UGC), – може бути продуктом не тільки індивідуального користувача, а й різних форм мережних об'єднань. Контент, створюваний користувачами, охоплює широкий спектр медіа-контенту, доступного в діапазоні сучасних технологій зв'язку. Він може бути використаний для широкого спектру додатків, включаючи завдання дослідження й обробки новин, та відображає розширення виробництва засобів масової інформації за допомогою нових технологій, які є доступними для широкої громадськості.

Усі цифрові медіа-технології, як правило, мають, наприклад, бази даних "питання-відповідь", цифрове відео, блоги, підкастинг, форум, огляд-сайти, соціальні мережі, соціальні медіа. На додаток до цих технологій, створюваний користувачами контент може використовувати безкоштовне програмне забезпечення, а також гнучке ліцензування або пов'язані з ним угоди щодо подальшого скорочення бар'єрів на шляху співпраці користувачів, набуття ними певних навичок і умінь. Іноді UGC може становити лише частину веб-сайту.

Наприклад, є сайти, де більшість змісту складають матеріали, підготовлені адміністраторами, а численні відгуки від регулярних користувачів сайту стають його істотною динамічною складовою. UGC частково або повністю контролюється адміністраторами сайту, щоб уникнути образливого змісту або нецензурної лексики, дотримуватись вимог щодо авторського права, або просто, щоб визначити, чи має розміщений UGC відношення до загальної теми сайту.

Нові медіа-засоби, таким чином, кардинально змінили роль пасивної аудиторії, що, отримавши інтерактивні можливості створення в інтернеті незалежного контенту, постійно збільшується та набуває автономного статусу у віртуальному світі. Інформаційна мережа сповнена масових експериментів, що генеруються в інновації в різних галузях знань, як технічній, так і гуманітарній, що в асоціації з аудиторіями користувачів набувають значної популярності й близькі до конкуренції з традиційними інституалізованими суспільними інституціями, адже утримують власне експертне середовище й популяризуються в засобах масової інформації значних масштабів охоплення.

Така ситуація істотно змінює саму аудиторію користувачів, алертність яких має величезний потенціал, у тому числі й політичний, що є важливим чинником суспільного життя, отже повинен бути акцептований органами влади.

Глобальною проблемою для інформаційного простору є проблема боротьби із кіберзлочинністю. Визнаючи зростаючий ризик кібератаки, які можуть виникати в будь-якому місці й торкнутися кожної країни, Міжнародний союз електрозв'язку (МСЕ) запропонував п'ять керівних принципів для встановлення і захисту миру в кіберпросторі. Міжнародний Регламент електрозв'язку (РМЕ) МСЕ є одним з прикладів сприяння гармонійному розвитку, ефективній роботі та універсальному доступу до міжнародного електрозв'язку і технології. РМЕ був створений як нова концепція нормативно-правової бази вирішення питань і проблем, які супроводжують нові умови у сфері електрозв'язку, що проявилися в кінці 1980-х рр., з метою підвищення ефективності та прискорення розвитку в рамках співробітництва, взаємодії та рівного доступу. Він відображає позицію Союзу щодо проблеми захисту права на спілкування за умови не нанесення шкоди об'єктам зв'язку [7].

П'ять принципів визначають необхідність конкретних дій і зобов'язань щодо забезпечення миру і стабільності в кіберпросторі: уряд кожної країни повинен взяти на себе зобов'язання надати своєму народові доступ до засобів зв'язку; уряд повинен взяти на себе зобов'язання захищати населення своєї країни в кіберпросторі; кожна країна візьме на себе зобов'язання не приховувати терористів/злочинців на своїх територіях; кожна країна повинна взяти на себе зобов'язання не застосовувати перші кібератаки по відношенню до інших країн; кожна країна повинна взяти на себе зобов'язання взаємодіяти з іншими країнами в рамках міжнародного співробітництва з метою забезпечення миру в кіберпросторі. Отже, масштаби і характер завдань кібербезпеки вимагають скоординованих багатосторонніх дій, зокрема, заходів у галузі стандартизації та

технічної допомоги країнам, що розвиваються, з урахуванням їх специфічних потреб.

Глобальні інституції працюють над формуванням стратегії розробки типового законодавства у сфері кіберзлочинності, яке було б придатним для глобального застосування і повністю сумісним з існуючими національними та регіональними законодавчими заходами. Відбувається розробка глобальних стратегій для створення відповідних національних і регіональних організаційних структур і політики в галузі кіберзлочинності. Розробляються стратегії створення визнаних на глобальному рівні мінімальних критеріїв безпеки та схем акредитації для апаратних і програмних додатків і систем, а також стратегії для створення глобальної рамкової основи щодо відстеження, попередження та реагування на інциденти з метою забезпечення транскордонної координації між новими та ініціативами, що вже існують.

Опрацювання глобальних стратегій для створення та затвердження загальної та універсальної цифрової системи ідентифікації та необхідної організаційної структури щодо забезпечення визнання цифрових облікових даних у різних географічних межах та розробка глобальної стратегії для полегшення створення людського та організаційного потенціалу з метою підвищення обізнаності та поширення "ноу-хау" в різних секторах і в усіх означених галузях обумовили появу пропозиції щодо створення основи глобальної багатосторонньої стратегії міжнародного співробітництва, діалогу та координації в усіх означених галузях. Основа базується на окремих видах заходів, що створюють дієвий на результативний комплекс, запровадження якого істотно підвищить шанси урядів щодо наувональнох кібербезпеки.

Існують також приватні проблеми глобального охоплення, пов'язані з порушенням прав людини на приватність. Потенційні варіанти використання будь-якої частини особистої інформації та поводження з ними – безмежні. Наявність в інтернеті чітко структурованого та більшою чи меншою мірою повного набору даних конкретної людини, що певним чином характеризують її он-лайн-поведінку – це також істотна проблема безпеки і привід для хвилювання, адже урядові та неурядові структури здатні отримати до них доступ. Цілі та методи використання цих даних можуть бути далеко неоднозначними та далеко не завжди співпадають із задекларованими. Без накладання обмеження на способи використання інформації і без їх урахування складно оцінити потенційні небезпеки від знаходження особистих даних під контролем владних органів.

Люди свідомо поступаються приватністю на користь безпеки, погоджуючись перебувати під об'єктивами камер спостереження на вулицях та службових приміщеннях, але межа, за якою людина готова поступатися своєю приватністю в обмін на зручність і персоналізацію інтернету, – є неоднозначною, індивідуальною, такою, що залежить від надто великої кількості показників, для того щоб її визначити. Критерії визначення цієї межі є надто широкими і досі не зрозуміло, на кого з учасників процесу доцільно покласти обов'язок їх визначення.

Права щодо захисту недоторканності приватного життя мають, на думку експертів, мінімальну вагу, порівняно з правами забезпечення безпеки у справі запобігання терористичних актів, що трактуються як набагато важливіші, що стосується екстремальних ситуацій, хоча знецінення права на приватне життя і усвідомлення та акцептування його цінності виключають одне одного.

У межах концепції прав людини право недоторканості приватного життя обумовлене необхідністю дефінувати значну кількість характеристик, провести пошук спільних, які об'єднують різні об'єкти, класифікуються й розкривають суть поняття "недоторканність приватного життя". Водночас поняття недоторканності приватного життя є настільки багатогранним, що його неможливо привести до одного знаменника, з огляду на множинність різних об'єктів, які, хоч і не мають загальних елементів, але перебувають у колі означників його суті. Серед форм вторгнення в приватне життя, наприклад, розголошування особистих таємниць, підглядання, шантаж або неналежне використання персональних даних або акумулювання персональних відомостей урядовими органами в досьє.

Суди, члени законодавчих органів та інші посадовці переважно не визнають факт порушення ними недоторканності приватного життя. Велика частина даних, зібраних у базах даних комп'ютерів, зокрема дата народження, раса, стать, адреса, сімейний стан, не є інформацією для обмеженого коло осіб і доступність цих даних переважно не викликає занепокоєння. Натомість проблема виникає у випадку взаємовідносин між людьми й інституціями сучасної держави, що приймають рішення, здатність яких суттєво або навіть кардинально впливати на життя кожної конкретної особи, таке занепокоєння пробуджує, адже міра добросовісності використання цих даних має істотну залежність від особи державного службовця, що виконує маніпуляції з цими даними та трактує їх на основі особистого досвіду чи отриманого завдання. Байдужістю, допущенням помилок, зловживанням, відсутністю прозорості і підзвітності чиновників наноситься шкода й порушуються права людини навіть за умов, коли особисті дані або секретна інформація не розголошуються.

Пересічна особа, як правило, не має інформації про те, яким чином дані про неї використовуються, не має доступу до даної інформації та її корекції. Заходи щодо забезпечення національної безпеки припускають ведення величезних баз даних, до яких громадяни не мають доступу, а існування таких програм тримається в секреті, адже вони кваліфікуються як питання національної безпеки. Це проблема належних правових процедур, структурна проблема, що охоплює питання диспропорції сил між громадянами і державою. Ступінь влади державних службовців над громадянами вирішується індивідуально в кожному конкретному випадку та багато в чому залежить від формалізації дій чиновника та його мотивації. Отже, питання не в тому, яку інформацію люди бажають приховати, а в об'ємі влади органів державного управління.

Отже, інформаційна та мережева безпека, аутентифікація, конфіденційність і захист прав споживачів є передумовою для розвитку інформаційного суспільства та зростання довіри з боку користувачів. Для досягнення поставлених цілей

необхідно у співпраці з усіма зацікавленими сторонами і міжнародними експертними органами активно формувати, розвивати і впроваджувати глобальну культуру кібербезпеки. Загрози, що супроводжують розвиток інформаційного простору та посилення залежності від технологій, є суттєвими та неоднозначними ризиками, що прийшли в наше життя. Водночас потенційні вигоди є більш переконливими, а можливості для майбутніх вигод є нескінченними. Існування в умовах кіберзалежності, що постійно зростає, вимагає розвитку та інтеграції, захисту ресурсів, створення стабільних умов подальшого розквіту інфраструктури і нових технологій та забезпечення міцного миру в мережі.

Етичні проблеми, що стосуються захисту прав і свобод користувачів інтернету, у зв'язку з їх діями та обов'язками, стикаються з переконанням, що кожному окремому користувачеві повинен бути наданий і забезпечений однаковий рівень захисту прав і свобод в інтернеті, включаючи право на приватне життя і безпеку. Однак такий захист від кіберзлочинів і неналежного використання інтернету підлягає перегляду, коли мова йде про нерозумне застосування технологій і послуг, яке має згубні наслідки для права на недоторканність приватного життя і таємницю обміну інформацією. Таким чином, необхідно знайти оптимальне співвідношення між захистом прав і дій користувача інтернету та їх відповідальністю; причому сумнівно, щоб держава одна змогла забезпечити ефективний захист прав кібергромадян усього світу. Модель спільної відповідальності за визначення та забезпечення балансу між захистом прав і відповідальністю користувачів у віртуальному світі залишається дискусійною.

Література:

1. Директива 2000/31/ЄС Європейського парламенту та Ради "Про деякі правові аспекти інформаційних послуг, зокрема, електронної комерції, на внутрішньому ринку" від 08.06.2000 р. [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/94_224.

2. Директива Совета Европейского Союза 89/552/ЕЕС о координации определенных положений, установленных законодательно, регулятивно либо административно странами-участниками (Европейской Конвенции о трансграничном телевещании) в области осуществления телевизионного вещания (в редакции 19.06.1997 г.) [Електронний ресурс]. – Режим доступа : http://zakon4.rada.gov.ua/laws/show/994_446.

3. Декларация о европейской политике в области новых информационных технологий // Дипломатический вестник. – 1999. – № 6. – С. 37–39.

4. Управління Інтернетом. Стратегія Ради Європи на період 2012 – 2015 рр. від 15.03.2012 р. // Internet Governance - Council of Europe Strategy 2012-2015 [Електронний ресурс]. – Режим доступу : http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/pdf.

5. *Шевчук С.* Судова правотворчість: сучасний досвід і перспективи в Україні / С. Шевчук. – К. : Реферат, 2007. – С. 51–74.

6. *Сергієнко Н. В.* Можливості використання сервісів WEB 2.0 в освіті / Н. В. Сергієнко // Сучасна наука в мережі Internet : матеріали Міжнар. наук.-практ. інтернет-конф. (25–27 лютого 2013 р.) [Електронний ресурс]. – Режим доступу : http://intkonf.org/sergienko-n-v-mozhlivosti-vikoristannya-servisiv-web-20-v-osviti.

7. *Nissenbaum H.* Securing Trust Online: Wisdom or Oxymoron? / H. Nissenbaum // Boston University Law Review, 2001. – Vol. 81. – № 3. – June. – P. 635–664 [Електронний ресурс]. – Режим доступу : http://www.nyu.edu/projects/nissenbaum/main_cv.html.

Надійшла до редколегії 15.04.2013 р.