ва, без потреби звертатися безпосередньо до урядових структур [1]. Соціальний капітал в міру свого розвитку створює можливість для існування і функціонування сфери громадянської активності. Завдяки наявності соціального капіталу значна кількість суспільних процесів відбувається з залученням громадськості.

Можемо зробити висновок про те, що громадянське суспільство, як особливий етап розвитку соціуму формується значною мірою завдяки існуванню соціального капіталу. В контексті розбудови громадянського суспільства активність соціального капіталу набуває певної спрямованості. З іншого боку, громадянське суспільство, розвиваючись та ефективно функціонуючи, створює сприятливі умови для нагромадження та збільшення потенціалу соціального капіталу.

Список літератури: 1. Фукуяма Френсіс. Що таке соціальний капітал? Київська лекція // День. – 2006. – №177. 2. Социологический энциклопедический русско-английский словарь: Более 10 000 единиц/С.А. Кравченко. – М.: Издательство Астрель; Издательство АСТ; Транзиткнига, 2004. – 511 с. 3. Демків О. Соціальний капітал: теоретичні засади дослідження та операціональні параметри // Соціологія: теорія, методи, маркетинг. – 2004. – №4. – С. 99–111. 4. Карась А. Соціокультурний текст громадянського суспільства: конструктивність і деструктивність соціальності / Громадянське суспільство як здійснення свободи: центрально-східноєвропейський досвід / За ред. А. Карася. – Львів: Львівський національний університет імені Івана Франка, 1999. – 384 с. 5. Україна: проблеми самоорганізації: В 2 т. / В. Кремень, Д. Табачник, В. Ткаченко. К.: Промінь, 2003 – Т. 2. Десятиріччя суспільної трансформації. – 464 с. 6. Карась А. Філософія громадянського суспільства в класичних теоріях і некласичних інтерпретаціях: Монографія. – К.–Львів: Видавничий центр ЛНУ імені Івана Франка, 2003. – 520 с. 7. Білоконь І. Моральна складова громадянської спрямованості // Соціальна психологія. – 2007. – №6 (26). – www.politik.ogr.ua.

Надійшла до редколегії 23.10.08

О. І. Горошко

Проблема безпеки в соціальному просторі інтернет-комунікацій: веб-сайт як джерело інформаційної небезпеки

З кожним роком у світі відбувається постійне розширення інформаційно-комунікативного сектора, включаючи Інтернет: росте як чисельність аудиторії мережі, так й ареал її поширення. На сьогодні, за даними агентства *Інтернетворлдстат*, середньостатистична аудиторія становить 1, 407, 724, 920 чоловік [1]. Щодня обсяг інформаційних інтернет-ресурсів збільшується на 7 мільйонів сторінок [2]. У зв'язку з цим украй гостро постають проблеми інформаційної й суспільної безпеки, викликані бурхливим розвитком високих технологій, і комплекс проблем, пов'язаних із правовою базою функціонування й регулювання Інтернету як на національному, так і на міжнародному рівні [3; 4]. Способи підвищення рівня інформаційної безпеки мережі Інтернет є **метою цієї роботи**.

Інтернет є водночас як глобальним комунікативним каналом, так і простором комунікацій, поєднуючи безліч міжнародних і національних комп'ютерних мереж. При цьому практично кожний користувач мережі отримує неймовірні можливості як для здійснення комунікативних взаємодій у цьому просторі, так і для пошуку необхідної інформації. Однак, крім того, що Інтернет об'єднує людей з усього світу, всесвітня мережа чинить і негативний вплив на розвиток суспільства, загрожуючи його безпеці, що й обумовило **актуальність** досліджуваної проблематики [5].

Інтернет проектувався й створювалося як децентралізоване комунікаційне середовище, що діє на основі співробітництва й з'єднує один з одним найрізноманітніших користувачів. Найважливішою особливістю цієї глобальної мережі й донині є те, що вона нікому не належить. Не існує єдиної однієї організації, яка б володіла або управляла мережею чи контролювала її. Через відсутність централізованого керування Інтернетом в інформаційному просторі панує практично абсолютна свобода. З одного боку, саме відсутність будь-якої цензури матеріалів, розташовуваних в Інтернеті, залучає безліч користувачів до мережі, але з іншого боку, саме ця воля й становить основну причину проблеми інформаційної безпеки в мережі.

Зазначимо також, що концептуальні й науково-методологічні основи інформаційної безпеки ще тільки починають розроблятися. Тому на сьогодні відбувається формування категоріального й понятійного апарату даного наукового напрямку, структуризація його проблемного поля, виробляються основи класифікації життєво важливих інтересів у сфері інформаційної безпеки й джерел інформаційних погроз; визначаються показники, критерії й нормативи рівнів інформаційної безпеки [6]. Провідні спеціалісти в цій галузі вказують, що першочерговим завданням при створенні теорії інформаційної безпеки варто вважати формування понятійного апарату у вигляді системи понять, серед яких базовими є інформаційна небезпека, інформаційна погроза й інформаційна безпека [6, с. 342]. На жаль, на сьогодні не існує єдиної думки з приводу ключового поняття цього напрямку – інформаційна безпека. Одне із загальновизнаних визначень наводиться Р. М. Юсуповим і В. П. Заболотським: інформаційна безпека – це захищеність інформаційного середовища особистості, суспільства й держави від навмисних і ненавмисних погроз і впливів. Це певний стан об'єкта, коли шляхом впливу на його інформаційну сферу не можна завдати істотного збитку або шкодип. Також це певна властивість об'єкта, що характеризує його здатність не завдати істотного збитку якому-небудь об'єкту шляхом впливу на його інформаційну сферу [6]. На відміну від інформаційної безпеки, інформаційною небезпекою вважається той стан навколишнього середовища

або об'єкта, коли існує можливість завдати об'єкту істотних збитків або шкоди шляхом впливу на його інформаційну сферу [6].

У цій же теоретичній парадигмі вибудовується й визначення інформаційної погрози, під якою мається на увазі намір завдати об'єкту істотних збитків шляхом впливу на його інформаційну сферу або деяка інформаційна небезпеку, реалізація якої стає досить імовірною, або фактор чи сукупність факторів, що створюють інформаційну небезпеку для об'єкта. До цих факторів належать певні дії, поводження об'єктів, природні явища тобто.

Серед питань інформаційної безпеки стає актуальним і визначення поняття *інформаційної безпеки особистості,* що розглядається як стан людини, в якому особистості не може бути завдано істотних збитків шляхом впливу на людину інформаційного простору. У процесі інформатизації індивід стає інформаційно «прозорим». За наявності бажання й засобів будь-яка інформація про конкретну людину може стати доступною й бути використаною з певною метою іншою людиною, групою осіб, суспільною групою й державою. Тільки невеликий відсоток населення може відмежувати себе від небажаного доступу до інформації про себе, проте більшість населення залишається беззахисною перед можливостями інформаційних технологій – як засобів маніпуляції й впливу на психіку людини.

Слід підкреслити, що проблема інформаційної безпеки в сучасному світі розглядається на трьох рівнях: *особистісному*, *груповому* й *соціальному*. На рівні суспільства інформаційну безпеку визначають як стан суспільства, в якому суспільству не можуть бути завдані істотні збитки шляхом впливу на його інформаційну сферу. Основу інформаційної безпеки цього рівня становить безпека індивідуальної, групової й масової свідомості громадян за наявності інформаційних погроз, до яких, варто віднести у першу чергу, інформаційно-психологічні впливи. Дія цих погроз може викликати психоемоційну й соціально-психологічну напруженість, перекручування моральних та етичних критеріїв і норм, морально-політичну дезорієнтацію і, як наслідок, неадекватне поводження окремих осіб, груп і мас людей. У результаті таких впливів можливі глибокі трансформації індивідуальної, групової й масової свідомості, негативні зміни морально-політичного й соціально-психологічного суспільного клімату тощо [7; 8].

У зв'язку з цим вкрай актуальним стає й визначення інформаційної безпеки держави –стан, у якому державі не можуть бути завдані істотні збитки шляхом впливу на його інформаційну сферу. Природно, забезпечення інформаційної безпеки держави невідривно пов'язане із забезпеченням національної безпеки.

Через відсутність централізованого контролю над мережею Інтернет у ній створюється вкрай сприятливе середовище для роз-

міщення сайтів із матеріалами чіткої асоціальної, антигромадської спрямованості. У мережі міститься не тільки порнографічна або псевдонаукова інформація, але й інформація, що сприяє розпаленню національної й релігійної ворожнечі пов'язана з тероризмом, екстремізмом, антигромадськими й антидержавними діями, а проблема тероризму, що загострилась останнім часом через те, що терористи отримали доступ до Інтернету, перетворилася дійсно на глобальну. Як і для всіх інших користувачів Інтернету, для учасників терористичних груп уже не існує проблеми простору й часу, які раніше істотно обмежували спілкування й відігравали роль своєрідних комунікаційних фільтрів, а будь-який комунікативний сервіс мережі (*персональний сайт*, *блог* або *електронна пошта*) дозволяє миттєво встановлювати контакти, визначати місце збору й чітко координувати дії, у чому світове співтовариство мало можливість уже не раз переконатися.

Існує кілька способів, за допомогою яких можна використовувати Інтернет з метою сприяння терористичним групам. Експерт із боротьби з тероризмом Тімоті Чи Томас уважає, що міжнародні терористи за допомогою Інтернету можуть:

1) здійснювати збір докладної інформації про передбачувані цілі, включаючи зображення місцезнаходження цілей і їхньої характеристики. Інтернет-технології надають неймовірні раніше можливості візуального передання інформації;

2) здійснювати фінансову підтримку своєї діяльності;

3) консолідувати розрізнені групи людей для здійснення заздалегідь спланованих акцій (на зразок *флешмобів*). За допомогою сайту або блога в мережі можна давати вказівки про час і місце проведення зустрічі, форми протесту або певні питання, пов'язані з проведенням тієї або іншої акції. Таким чином, Інтернет стає прекрасним засобом консолідації таких груп і керування ними;

4) організовувати «крапкові» акції, спрямовані на підрив фінансових, політичних і соціальних інститутів як на регіональному, так і на міжнародному рівні, що останнім часом одержало назву *кібершантажу*;

5) Інтернет має величезні можливості для реклами і часто використовується з цією метою. За допомогою Інтернету можна миттєво звернутися як до масової аудиторії в усьому світі, так і до окремих осіб. Для досягнення своїх цілей терористичні групи ставлять доступ до засобів масової інформації на перше місце серед своїх стратегічних пріоритетів;

6) терористи можуть залишати повідомлення про орієнтовні або вже сплановані дії на сторінках сайтів в Інтернеті або розсилати їх електронною поштою, а також можуть широко розголошувати свою відповідальність за здійснення того або іншого терористично-

го акту. В інформаційну епоху комунікаційні можливості еквівалентні володінню силою, а суспільна думка стала пріоритетною;

7) Інтернет може бути ініціатором психологічного тероризму. Часто психологічним аспектам можливостей Інтернету не приділяють належної уваги. Завдяки надійності й високій репутації, які нібито має Інтернет, його можна використовувати для того, щоб зчиняти паніку, увести кого-небудь в оману або спричинити до руйнування чого-небудь. Інтернет також став благодатним ґрунтом для поширення чуток;

8) Інтернет істотно змінив комунікаційну мережу терористів. Якщо раніше такі мережі мали центральний командний пункт, то тепер вони не мають чітких командних пунктів завдяки ще більшому розгалуженню цих структур. Нічого не підозрюючи, співучасники, наприклад, хакери, можуть бути використані «в темну» – як підставні особи, що можуть ніколи не довідатися, до чого призвели їхні дії;

9) Інтернет може бути використаний і для відправлення таємних повідомлень, що схоже на те, як раніше використовувалися симптатичне чорнило. Наприклад, повідомлялося, що єгипетські комп'ютерні фахівці «афганського походження» створили комунікаційну мережу, що надавала екстремістам можливість обмінюватися інформацією через Всесвітню мережу шляхом відправлення повідомлень електронною поштою й на електронні дошки оголошень без усякого побоювання бути пійманими. Саме цю сферу діяльності посилено досліджують фахівці зі стенографування й шифрування повідомлень, що надсилаються через Інтернет, наприклад, терористичною групою Усами бен Ладена «Аль-Кайда» [9].

Ці проблеми є лише частиною того айсберга, з яким зіштовхується суспільство при використанні Інтернету в епоху глобалізації та повсюдної інтернетизації й інформатизації.

Ще одна проблема полягає в тому, що розміщення на сайтах порнографічних картинок, безсумнівно, порушує сформовані в суспільстві стандарти моралі. Треба визнати, що сервери з такою інформацією відвідуються часто, в тому числі дітьми й підлітками. Інтернет гарантує набагато вищий рівень конфіденційності й анонімності, ніж відвідування реальних кінотеатрів або магазинів, де відкрито або підпільно продають порнографічні матеріали. Дані також свідчать, які зламати або обійти обмеження, що накладаються програмними фільтрами, не становить великих труднощів [2], а фірми-провайдери, що забезпечують доступ до мережі, не завжди виконують навіть ті вимоги нечисленних законодавчих актів, які регулюють розміщення матеріалів асоціального характеру.

Проблеми обмеження доступу користувачів мережі до несанкціонованої інформації виникають у багатьох країнах. Законодавства різних країн пропонують різні способи розв'язання проблеми відповідальності провайдерів: у Китаї й на Близькому Сході про-

вайдери відповідають за всі дії користувачів незалежно від того, знають вони про ці дії чи ні; в Німеччині принцип свободи слова не є вищим пріоритетом: нещодавно прийнятий закон про мультимедіа забороняє поширення в Інтернеті даних на підставі всього корпусу законів. Більше того, закон пропонує провайдерам інтернет-послуг (відповідно до нового закону, вони поділяють відповідальність за зміст інформації, доступ до якої вони забезпечують) аналізувати призначену для неповнолітніх інформацію й блокувати поширення заборонених наявними законами відомостей. Однак у більшості випадків провайдери все-таки не несуть відповідальності за дії своїх користувачів, зокрема, якщо не були інформовані про їхню незаконну діяльність і після одержання інформації припинили розміщення або доступ до інформації [2, с. 80–110].

Це вимагає пріоритетної уваги до розробки універсальних міжнародних угод. Передбачається, що з метою створення режиму колективної інформаційної безпеки угода, що регулює правові основи функціонування Інтернету в країні, повинна містити умови для рівноправного й безпечного міжнародного інформаційного обміну на основі загальновизнаних норм і принципів міжнародного права. Вона повинна включати й запобіжні засоби використання ІКТ і Інтернету зі злочинною метою, розробку процедури взаємного повідомлення й запобігання трансграничному несанкціонованому інформаційному впливу, а також положення про розвиток системи міжнародної взаємодії правоохоронних органів із запобігання й припинення правопорушень у світовому інформаційному просторі [2]. Якщо взяти до уваги, що Інтернет є надскладною саморегулюючою соціальною системою, що створювалася із заздалегідь поставленою метою – вціліти після ядерного вибуху, то вирішити питання фільтрації, технологічного відключення певних серверів тощо досить складно, хоча такі методи й використовуються у країнах із тоталітарними режимами (Китай, Північна Корея, В'єтнам, Саудівська Аравія, Білорусія, Куба, Узбекистан). Однак у демократично орієнтованих країнах, де діє закон про свободу слова й волевиявлення, питання правового регулювання інтернет-мережі є дуже актіальними. Власне, й проблема інформаційної безпеки є багатобічною й досить складною. Цікаво, що вже при створенні мережі, деякі інтернет-аналітики вказували, що питання інформаційної безпеки мережі, варто вирішувати насамперед, через регулювання доступу до неї. Однак проблема інтернет-контенту (змістової частини інформації), а також використання веб-сайта як засобу комунікативного впливу й керування в ті часи навіть не прогнозувалися. Із розвитком мережі набув актуальності юридичний аспект її функціонування. Як правило, виділяють такі види інформаційних погроз: несанкціонований доступ до інформації; логічні й тимчасові бомби, розробка й поширення

комп'ютерних вірусів; підроблення або розкрадання комп'ютерної інформації, злочинна недбалість у розробці, виготовленні й експлуатації програмно-обчислювальних комплексів; поширення «закритих» матеріалів (урядового сервера) і надання відкритого доступудо них; створення й поширення сайтів, що містять інформацію «асоціальної спрямованості» (поширення й продаж наркотиків, тероризм, екстремізм, порнографія) і її рекламування; створення сайтів-клонів і розміщення свідомо неправдивої інформації в мережі; використання мережі Інтернет як інструменту для реалізації будь-яких протиправних дій (терористичних актів, спін- і маніпулятивних технологій тощо) [2, с. 82].

У цілому сукупність проблемних питань можна звести до двох тем: це – питання, пов'язані із захистом інформації, і питання, пов'язані із захистом від інформації (з її фільтрацією).

Пропонований автором підхід до фільтрування інформації ґрунтується на введенні й використанні в правовому полі інтернет-комунікацій ряду понять, які згодом можуть бути взяті за основу формування нової інформаційної політики регулювання Мережі й використовуватися для забезпечення або інформування про певний рівень інформаційної безпеки сайта або портала, розміщених у глобальній павутині. Ми пропонуємо ідею використання *індексу інформаційної безпеки сайта* з його автоматичним відображенням у пошукових системах Інтернету. Цей індекс вираховується на основі аналізу вербального контента сайта, що може проводитися автоматично з підрахунком частоти використання того або іншого слова на веб-сторінці. Наприклад, якщо слово *джихад* зустрічається на сайті з обсягом текстового матеріалу близько 1000 слів п'ять разів, а слово *невірні* три рази, то може виникнути підозра, що даний сайт містить інформацію екстремістської або терористичної спрямованості. Якщо створити деякий лематизатор, що містить список специфічної лексики з певної тематики, пов'язаної з асоціальною діяльністю (тероризм, екстремізм, тощо), то за частотою слів із цього списку та їхньою комбінацією, можна розрахувати такий індекс, який автоматично буде обчислений пошуковими машинами Інтернету, а користувачі будуть попереджені, що цей матеріал несе певну інформаційну загрозу його читачам.

Відомо також, що будь-яка пошукова машина знаходить запитуваний матеріал за певним набором дескрипторів, які творці сайту закладають у його інформаційний код. Якщо ці дескриптори належать до інформаційно *небезпечних*, то це теж може відбиватися в значенні цього індексу, що автоматично відображається на пошуковій сторінці. Прогнозується, що одним зі шляхів підвищення рівня інформаційної безпеки може стати своєчасне й усебічне інформування користувачів мережі та населення взагалі про небезпеку в мережі Інтернет.

Список літератури: 1. Internet World Stats: Usages and Population Statistics, 2008. [Режим доступу: http://www.internetworldstats.com/stats.htm] станом 12.08.2008. 2. Смолян Г. Л., Цыгичко В. Н., Хан-Магомедов Д. Д. Интернет в России. Перспективы развития. – М.: Эдиториал УРСС, 2004. – 200 с. 3. Монахов В. Н. СМИ и Интернет: проблемы правового регулирования. – М.: Экспринт, 2003. – 320 с. 4. Наумов В. Б. Право и Интернет: Очерки теории и практики. – М.: Книжный дом «Университет», 2002. – 432 с. 5. Горошко Е. И. Проблема правового регулирования Интернета // Зб. наук.-практ. матеріалів конф. «Теорія та практика судової експертизи і криміналістики». – Х.: Право, 2007. – Вип. 7. – С. 508–518. 6. Юсупов Р. М., Заболотский В. П. Научно-методологические основы информатизации. – СПб.: Наука, 2000. – 455с. 7. Интернет-преступность наступает // Crime.ru, 2006. [Режим доступу: http://www.crime-research.ru/news/25.02.2004/2004-02-2503] станом на 12.09.2008. 8. Старостина Е. Терроризм и кибертерроризм – новая угроза международной безопасности // Ваш личный Интернет, 2006. [Режим доступу: http://contentfiltering.ru/doc.asp?ob_no=1374] станом на 22.08.2008. 9. Томас Т. Л. Терроризм и Интернет: проблемы взаимодействия // Право и безопасность. – 2001. – №1. [Режим доступу: http://www.dpr.ru/pravo/pravo_1_9.htm] станом на 01.09.2008.

Надійшла до редколегії 17.10.08