УДК 681.3+519.83

ЛАНДЕ Д.В., *доктор технічних наук, старший науковий співробітник.*
Інститут проблем реєстрації інформації НАН України

МЕРЕЖНА МОБІЛІЗАЦІЯ: ПИТАННЯ ДЕМОКРАТІЇ ТА БЕЗПЕКИ

Анотація. *Досліджуються питання усвідомлення ключових аспектів мереженої мобілізації у контексті забезпечення інформаційної та національної безпеки з одночасним додержанням конституційних прав і свобод людини.*

Ключові слова: *інформаційний вплив, соціальна мережа, мережна мобілізація, моделювання, інформаційна безпека, національна безпека.*

Аннотация. *Исследуются вопросы ключевых аспектов сетевой мобилизации в контексте обеспечения информационной и национальной безопасности при одновременном соблюдении конституционных прав и свобод человека.*

Ключевые слова: *информационное влияние, социальная сеть, сетевая мобилизация, моделирование, информационная безопасность, национальная безопасность.*

Summary. *The issues of key aspects of network mobilization in light of providing of informative and national security at the simultaneous observance of constitutional rights and freedoms of human are examined.*

Keywords: *informative influence, social network, network mobilization, modelling, informative security, national security.*

Постановка проблеми. Сьогодні при розгляді питань інформаційних впливів не можна обійти такий важливий напрям, як теорія соціальних мереж. Нині мережні інформаційні структури виступають, з одного боку, як джерела, а з іншого – як об’єкти інформаційного впливу.

Як відомо, соціальні мережі сприяють комунікаційним зв’язкам між людьми, реалізують їх соціальні потреби. Але вони також являють собою виклик безпеці суспільства, дозволяючи мобілізувати деструктивні сили, впливаючи на масову свідомість, іноді навіть маніпулюючи нею.

Соціальні мережі викликають все більшу зацікавленість у дослідників, зокрема тому, що у них виникають якісно нові властивості поведінки агентів, серед яких слід виділити спроможність до проведення ефективної мережної мобілізації.

Метою статті є дослідження ефектів та ризиків інформаційного впливу он-лайнових соціальних мереж на суспільне життя.

Виклад основних положень. Серед потенційних загроз в інформаційній сфері в Законі України “Про основи національної безпеки України” [1] (стаття 7) зазначаються й ризики інформаційних впливів: “намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації”. У Доктрині інформаційної безпеки України [2], яку увів у дію Президент України указом від 8 липня 2009 р. №514/2009, серед основних реальних і потенційних загроз інформаційній безпеці країни названі “зовнішні негативні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також мережу Інтернет”, “негативні інформаційні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності і недоторканності кордонів України”, “негативні інформаційні впливи, в тому числі із застосуванням спеціальних засобів, на індивідуальну та суспільну свідомість”, а також “поширення суб’єктами інформаційної

діяльності викривленої, недостовірної та упередженої інформації”, “поширення в засобах масової інформації невластивих українській культурній традиції цінностей і способу життя, культу насильства, жорстокості, порнографії, зневажливого ставлення до людської і національної гідності”, “поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України”.

Близьке до поняття мобілізації поняття впливу членів соціальної мережі (агентів) полягає у формуванні у суб’єктів керування такої інформованості, яка найбільш вигідна для того агента, що керує. Сьогодні все більшої популярності здобуває поняття репутації в соціальних мережах. Досліджуються репутаційні мережі, метрики репутації тощо [3]. Дійсно, можливість впливу в соціальній мережі залежить від репутації тих, хто здійснює вплив. Репутація розглядається як деяка вагова величина, яка зростає, якщо вибір агента співпадає з тим, що від нього очікують інші, або знижується при неефективному керуванні.

Он-лайнові мережі на даний час мають все більше значення не тільки для підтримки звичайних комунікаційних функцій, а все частіше засобами інформаційного керування і впливу з метою маніпулювання особою, соціальними групами або суспільством.

Щодо мобілізації, то вона як правило застосовується зазвичай як засіб поєднання зусиль учасників соціальних груп, суспільства для вирішення деякої проблеми, наприклад, ліквідації катастрофи, відсічі агресії тощо. Мобілізація в мережевому середовищі, як правило вимагає, ієрархічної організації останньої або деякої близькості до неї.

Самомобілізація в мережі може базуватися на тому принципі, що поведінка сусідів кожного агента впливає на його власну поведінку. З іншого боку, соціальні зв’язки забезпечують агента інформацією щодо намірах і діях інших агентів в мережі і формують уявлення, на базі яких агент приймає свої рішення. Крім того, в соціальних мережах агенти можуть прикладати спільні зусилля, на що великий вплив має структура мережі. При цьому значення “впливу зверху” в ієрархії може бути зменшене.

Мережна мобілізація може розглядатися як початкова фаза “мережних війн”. Так відома “битва в Сіетлі” – велика демонстрація проти сесії СОТ у 1999 році була організована в мережі. У 2001 р. президент Філіппін Джозеф Естрада першим у світі втратив владу в Манілі через “мережну війну”. “Розповсюдження Інтернет-технологій полегшує реалізацію принципу вільного доступу до інформації, що позбавляє еліту монополії на контроль за нею”, – вважає І. Ейдман [4].

Соціальні системи можуть бути представлені у вигляді динамічних мереж [5]. Поточний стан інформаційної системи може бути представлено у вигляді графа $<M, L>$, де M – це множина компонент (наприклад, агентів) соціальної мережі, а L – множина ребер, наприклад, зв’язків, посилань тощо. Можливості мережної мобілізації напряму пов’язані з такими властивостями мереж, як зв’язність, кластеризація, середній коротший шлях між вершинами тощо.

Майже кожна соціальна процедура сьогодні є мережною, причому, на відміну від традиційних поглядів на мережні структури, у випадку мережної мобілізації при моделюванні необхідно враховувати ряд особливостей [6]:

- ребра мережного графа не обов’язково розглядаються як канали передачі інформації, вони можуть являти собою відбиття особливих соціальних відносин;
- ребра не є статичними в часі, вони можуть розвиватися на декількох рівнях, у тому числі прихованих, латентних;
- реальні мережі не є чітко ієрархічними, вони є еластичними комунікаційними системами;

- межі мереж визначаються за допомогою нечітких критеріїв;
- реальні мережі можуть роз’єднуватися, при цьому відділені підмережі можуть функціонувати як повнофункціональні.

При моделюванні мережної мобілізації унаслідок взаємного впливу агентів виникає необхідність урахування чинників, що мають місце у реальних соціальних мережах, які зумовлені як характеристиками і потребами агентів (надають вплив і піддаються впливу), характером їх взаємодії, так і основними властивостями самої соціальної мережі [7]:

- наявність власної думки агентів, яка може змінюватися під впливом інших членів соціальної мережі;
- цілеспрямована поведінка агентів;
- різна репутація агентів – різна значущість їх думок (від лідерів до аутсайдерів);
- різний ступінь схильності агентів до впливу (конформізму);
- різний поріг чутливості до зміни думки оточення;
- наявність “соціальної кореляції”;
- наявність зовнішнього впливу та зовнішніх агентів;
- вплив структурних властивостей соціальних мереж;
- асиметрична інформованість агентів;
- прийняття рішень агентами в умовах неповної інформованості тощо.

Соціальні мережі характеризуються наявністю так званої “структури співтовариства”, тобто існують групи вузлів-агентів, які мають високу щільність ребер між собою, при тому, що щільність ребер між окремими групами – низька. Традиційний метод для виявлення структури співтовариств – кластерний аналіз. Існують десятки прийнятних для цього методів, які базуються на різних мірах відстаней між вузлами. Зокрема, для великих соціальних мереж наявність структури співтовариств виявилося невід’ємною властивістю.

З погляду можливості мобілізації в мережі застосовують ці поняття цінності мережі [8]. Загальноприйняте, що цінність мережі – це потенціальна доступність агентів, з якими будь-який може зв’язатися у випадку необхідності.

Засновник американської Національної радіомовної компанії NBC Д. Сарнов визначив свого часу, що цінність мереж суспільного мовлення зростає пропорційно кількості слухачів n (закон Сарнова).

Р. Меткалф визначив, що цінність соціальної мережі зростає як n (n – 1) (закон Меткалфа). Він міркував таким чином: кожний агент соціальної мережі може бути зв’язаний з n – 1 іншими агентами. Таким чином цінність всієї мережі пропорційна n (n – 1).

Д. Рід додав до виразу цінності соціальної мережі ще одну складову, пов’язану з поєднанням агентів мережі в групи (закон Ріда). Ця складова дорівнює $2n - n - 1$ і визначається як кількість підмножин множини із n агентів за виключенням одиничних елементів і пустої множини.

У деяких сучасних роботах пропонується оцінка цінності мережі як $n \ln(n)$. Основою цих міркувань є додаткове ранжирування цінності зв’язків, які відповідають закону Парето. Так, якщо для довільного агента соціальної мережі, яка складається з n членів, зв’язки з іншими агентами мають цінність від 1 до $1/(n\text{-}1)$, то внесок цього агента у загальну цінність мережі складає:

$$1+1/2+ \ldots +1/(n-1) \approx \ln(n).$$

Для цінності соціальної мережі пропонується опис, який відображує властивість адитивності: цінність об’єднання двох мереж має дорівнювати сумі цінностей цих

мереж. Так як кількість можливих конфігурацій при об’єднанні двох мереж дорівнює добутку кількості конфігурацій в кожній з мереж, то для функції цінності повинна виконуватись формула:

$f(m1m2) = f(m1) + f(m\ 2)$, де: m1 і m2 – кількості конфігурацій першої і другої мережі, відповідно.

Якщо існує тільки одна конфігурація зв’язків агентів, то будемо вважати, що цінність такої мережі дорівнює нулю, тобто $f(1) = 0$.

Відомо, що існує лише одна функція, яка задовольняє названим вимогам – це логарифм. Сенс цінності соціальної мережі у такій інтерпретації складається у тому, що вона показує, наскільки у мережі здійснюється потенційна доступність агентів.

Разом з тим, якщо кількість можливих конфігурацій для мережі з n вузлів оцінювати як $2n$, то $\ln(2n) = n$ і ми повертаємося до закону Сарнова.

Важливою характеристикою мережі є функція розподілу ступенів вузлів $P(k)$, яка визначається як ймовірність того, що вузол i має ступень $k_i = k$, тобто розподіл ступенів $P(k)$ відображує долю вершин із ступенем k.

Мережі з різними розподілами ступенів вузлів характеризуються досить різною поведінкою. $P(k)$ у деяких випадках може бути розподілом Пуасона ($P(k) = e^{-m}m^k / k!$, де m – математичне очікування, експоненційним ($P(k) = e^{-k/m}$) або ступеневим ($P(k) \sim 1/k^{\gamma}$, $k \neq 0,\ \gamma > 0$).

Мережі із ступеневим розподілом ступенів зв’язності вузлів називають безмасштабними (*scale-free*). Саме безмасштабний розподіл часто спостерігається у реально існуючих мережах. Зокрема, більшість соціальних мереж є безмасштабними.

Виявлено, що безмасштабні мережі досить толерантні до випадкових атак, руйнування випадкових вузлів. У випадковій мережі (мережі з рівномірним розподілом ступенів вузлів, які на цей час найбільше вивчені) у порівнянні з безмасштабними мережами менша кількість випадкових атак може зруйнувати мережу. Велика безмасштабна мережа може поглинати випадкові вилучення вузлів, що охоплюють до 80% її складу, і лише потім така мережа розпадається. Причина цього полягає у тому, що випадкові відмови більш ймовірні у відносно невеликих вузлах. Разом з тим, безмасштабні мережі дуже уразливі з погляду цілеспрямованих руйнувань їх концентраторів (вузлів з найбільшими значеннями посередництва). Атаки, які миттєво знищують лише 5 – 15 % концентраторів подібних мереж, можуть зруйнувати всю мережу.

Для соціальних мереж виявлено ряд ефектів, які мають вирішальне значення при реалізації мережної мобілізації, зупинимось на деяких з них.

“Малі світи”. Ідею “шести рукостискань”, яка полягає у тому, що будь-які дві людини на Землі зв’язані між собою не більш ніж через п’ять посередників вперше висловив у 1929 році угорський письменник і журналіст Фрідеш Карінтія.

У 1967 р. психолог С. Мілгран в результаті масштабних експериментів обчислив, що існує ланцюжок знайомств, в середньому завдовжки шість, практично між двома будь-якими громадянами США [9].

Мережеві структури, відповідні властивостями малих світів мають наступні типові властивості: мала середня довжина шляху (що характерно також для випадкових мереж) і великий ступінь кластеризації (що властиво мережам з регулярною структурою).

До мереж соціальних зв’язків, які мають структуру малого світу застосовні мережеві технології “масової мобілізації”. Якщо в такі мережі “вкинути” яскраві, що мобілізують ідеї, то вони будуть поширюватися там, як епідемія. При точному виборі

відповідних образів виникає масова соціальна реакція. Відбувається мобілізація, причому мінімальними засобами і в мінімальний час. Таким чином, для успіху мережних технологій мобілізації вкрай важливі дві речі: наявність потужних соціальних мереж типу “малого світу” і система мобілізуючих ідей-образів.

У 2011 році дослідники з Міланського університету посилили гіпотезу шести рукостискань – виявилося, що у мережі Facebook більшість людей пов’язано між собою в середньому через чотирьох посередників (тобто п’ять рукостискань) [10].

У рамках роботи вчені проаналізували “соціальний граф” з понад 700 мільйонами вершин-користувачів соціальної мережі. Ребрами з’єднувалися ті вершини, між якими була встановлена дружба. Усього таких ребер в графі було більше 69 мільярдів. В результаті експериментів вдалося встановити, що середня мінімальна відстань між двома вершинами – 4,74 ребра (тобто п’ять рукостискань).

Вчені відзначають, що якщо обмежитися розглядом не всіх вершин, а тільки близьких до даної по деякому критерію, то ця відстань зменшується ще більше. Наприклад, для людей з Італії цей показник становить близько чотирьох ребер.

“Слабкі зв’язки”. Існує клас складних мереж, яким притаманні так звані **“**слабкі**”** зв’язки. Аналогом слабких соціальних зв’язків є, наприклад, відносини з далекими знайомими та колегами. У деяких випадках ці зв’язки виявляються більш ефективними, ніж зв’язки **“**сильні**”**. Так, нещодавно був отриманий концептуальний висновок в галузі мобільного зв’язку, який полягає у тому, що “слабкі” соціальні зв’язки виявляються найбільш важливими для існування соціальної мережі [11].

Якщо слабкі зв’язки проігнорувати, то мережа розпадеться на окремі фрагменти. Якщо ж не враховувати сильних зв’язків, то проблем із підключенням порушиться. Виявилося, що саме слабкі зв’язки є тим феноменом, який пов'язує мережу в єдине ціле.

“Клуб богатих”. У багатьох соціальних мережах спостерігається така тенденція, як хороша зв’язність між вузлами-концентраторами. Це явище, відоме під назвою елітарність (або феномен “клубу багатих” – rich-club phenomenon), може бути охарактеризоване коефіцієнтом елітарності [12]. Аналіз топології веб, зокрема, показав, що вузли з великим ступенем вихідних гіперпосилань мають більше зв’язків між собою, ніж з вузлами з малим ступенем, тоді як останні мають більше зв’язків з вузлами з великим ступенем, ніж між собою.

“Клітинні мережі”. Соціальні, зокрема, терористичні мережі часто характеризуються як клітинні – створені з майже незалежних клітин. Формальне визначення клітинних мереж було дане в [13] у термінах мережних компонентів і властивостей. Клітинні мережі мають такі властивості, як надмірність, наявність тісно зв’язаних клітин (4 – 6 чоловік), відсутність управління вертикальним способом (нечіткі директиви), відсутність планування (формування за рахунок локальних обмежень), можливість еволюціонування у відповідь на деструктивну діяльність [14].

Будь-яка соціальна мережа є динамічною системою, відновлення якої після вилучення кращих “посередніків” здійснюється за рахунок латентних зв’язків з іншими компонентами інформаційного простору. Після того як інформаційна система розділяється на ізольовані фрагменти, вона може “використовувати” ці зв’язки та швидко відновлювати зв’язність, тобто складним динамічним мережам притаманна самовиліковність. Як приклад можна вказати, що атаки на тренувальні табори терористів у Центральній Азії практично не зруйнували їх мережі яким-небудь значимим чином. Тому пріоритети в дослідженні задач дестабілізації терористичних мереж віддається пошуку ключових осіб, нейтралізація (усунення) яких розділить мережу на складові. Проте, експерименти показують, що після того, як терористична мережа розділяється на ізольовані осередки, вона продовжує

використати свої приховані ресурси та швидко відновлює втрати. Одночасність атак на концентратори в цьому випадку істотна.

Серйозною перешкодою при аналізі мереж є неповна інформація про зв’язки між окремими вузлами мережі. Група дослідників з Інституту Санта Фе представила алгоритм, за допомогою якого стає можливим автоматичне отримання інформації про ієрархічну структуру соціальних мереж [15]. Цей метод відновлення мереж може надійти на озброєння різних спецслужб. Так, знаючи, наприклад, лише про половину зв'язків між терористами, можна буде з високою ймовірністю відновити відсутні ланки всього ланцюжка. Маючи інформацію лише про половину контактів терористів між собою, можна з імовірністю 0,8 прогнозувати ті зв'язки, щодо яких спочатку нічого не було відомо. Очевидно, що даний метод може надати важливу допомогу в справі виявлення прихованих мережних організацій, і таким чином поставити справу забезпечення державної й міжнародної безпеки на якісно новий рівень.

Властивості складних мереж обумовлюють тактику їх руйнування, яка передбачає такі етапи як аналіз і планування, практично одночасна нейтралізація вузлів-концентраторів, послідовне знищення інших вузлів у порядку убування відповідних їм показників посередництва.

При дослідженні живучості мережевої структури основний інтерес представляє перехід від зв’язаної мережі до розрідженої в результаті деструктивних впливів, що виражаються у видаленні елементів мережі – ребер або агентів. При цьому функціональний відмова розглядається як видалення окремого елемента. У цьому випадку виникає досить точна аналогія з межею протікання (або перколяційним порогом), який зв’язується з фазовим переходом.

Безмасштабні мережі досить прихильні до впливу епідемій (у випадках соціальних мереж у якості “інфекції” можуть розглядатися ідеологічні впливи, технічні інновації тощо). У випадковій мережі епідемія повинна перебороти деякий критичний поріг (кількість заражених вузлів) і тільки тоді вона може поширюватися на всю систему. Нижче цього порогу епідемія зникає. Дані, наведені у роботі [16], показують, що у безмасштабній мережі поріг для епідемії практично дорівнює нулю. Ротенберг [17] відмітив, що ознаки безмасштабності реальних терористичних мереж вступає в протиріччя із вказівками для комунікаційної інфраструктури, установленої в навчальному посібнику Аль-Каїди [18]. Тому, якщо терористична мережа спостерігається як безмасштабна (у реальності найчастіше – саме так), можна стверджувати, що така природа не є предметом цілеспрямованого планування, а є результатом природного впорядкування.

Мережна мобілізація безпосередньо пов’язується із структурою “малих світів”. Зокрема, швидкість поширення інформації завдяки ефекту “малих світів” у реальних мережах зростає на порядки порівняно з випадковими мережами, адже більшість пар вузлів реальних соціальних мереж з’єднані короткими шляхами.

Досліджуючи когнітивні процеси в соціумі, соціологи з Центру академічних соціально-когнітивних досліджень при Політехнічному інституті Ренсселира (США) побудували модель формування громадської думки, в якій члени колективу також вільно обмінюються думками [19]. Кожен учасник мережної моделі міг обмінюватися думкою з іншими за певними правилами. Якщо думка “слухача” співпадала з думкою “співрозмовника”, точка зору “слухача” отримувала додаткові очки. Якщо вона не співпадало з чужою думкою, слухач приймав цю думку до відома і перемикався на іншого “спікера”. Якщо і цього разу співрозмовник транслював ті ж “нові погляди”, слухач приймав нову точку зору. Таким чином модель імітувала конкуренцію особистих поглядів з різними ваговими коефіцієнтами.

Побудувавши консенсно-орієнтовану мережу соціологи почали додавати до неї “принципових” агентів, не схильних міняти свою точку зору. Поки доля таких агентів не перевищувала 10 відсотків, не спостерігалося видимого прогресу в поширенні їх ідей. Але як тільки десятипроцентна планка долалася, ідея поширювалася по мережі як пожежа. Як приклад подібного фазового переходу автори навели події 2011 р. в Тунісі і Єгипті, де суспільний консенсус, в якому довгий час не спостерігалися ніяких істотних переміщень, трансформувався буквально за тиждень.

Показово також, що розмір долі “принципових”, критичний для запуску перехідних процесів, ніяк не залежав від типу використовуваної мережевої моделі. Іншими словами, не важливо з яких саме мережевих позицій починала поширюватися нова ідея, виявляється, що для успішного впливу на соціум досить, щоб “принциповим” був кожен десятий незалежно від його громадського положення.

У 2009 році американське агентство оборонних розробок DARPA оголосило конкурс “Мережний виклик”, учасники якого повинні були розробити найкращий метод для мобілізації та координації громадських дій по всій території США. Організатори конкурсу заховали на континентальній території США десять червоних метеорологічних куль-зондів, запуск яких повинні були зафіксувати учасники “виклику”.

Випускники Масачусентського технологічного інституту (MIT) під керівництвом Алекса Пентланда створили універсальний алгоритм мобілізації та координації дій великих груп людей через Твіттер, інші блоги та соціальні мережі. Обрана авторами стратегія дозволила їм зібрати 845 пірамід з добровільних послідовників, загальна чисельність яких склала 4,5 тисячі користувачів. Найширша мережа містила 602 користувача, а сама “висока” складалася з 14 рівнів “піраміди”. Були виміряні відстані між користувачами за допомогою LiveJournal і було виявлено, що люди прикладали найбільші зусилля і досягали більшого успіху в тому випадку, якщо вони намагалися залучити своїх друзів з віддалених від них міст (слабкі зв'язки).

Типовий сценарій мережевий мобілізації спирається на, умовно кажучи, дешеву мережу (скелет цієї мобілізаційної структури, первинну мережу людей-хабів, які мають велику кількість особистих зв’язків і можуть організувати розповсюдження потрібних образів), надбудовані над уже існуючою структурою малих світів.

Терористичні мережі являють собою найбільшій виклик суспільній безпеці. Тому вивчення, моделювання, прогнозування поведінки та їх руйнування – завдання як наукове, так і суто практичне.

Події кінця 2010 року на Манежній площі в Москві показали, що со общество російських футбольних фанатів представляє серйозну силу, здатну мобілізувати декілька тисячі чоловік в достатньо короткі терміни. Акція пам’яті загиблого Е. Свірідова (члена фанатського угрупування “Юніон”, який був убитий в результаті зіткнення з групою з восьми кавказців) переросла в масові виступи, що закінчилися нападами на представників Північного Кавказу і Центральної Азії і одним вбивством. Всі вони носили ксенофобний характер і виражали незадоволеність на адресу системи правосуддя, що відпустила співучасників Аслана Черкесова (вбивці Свірідова) нібито під тиском кавказької діаспори.

Аналіз відкритої статистики основних сайтів московських фанатів, таких як fratria.ru, fanat1k.ru і spartak.msk.ru, показує, що на всіх фанатських сайтах виросла активність, проте основне зростання мережної активності спостерігається на сайті fanat1k.ru, пов’язаний з хуліганами “Спартака”. Зараз, як ми могли бачити, етно-націоналісти знайшли спосіб підсилити своє он-лайн-присутність, при цьому не тільки активно діючи офф-лайн і он-лайн, але і інтегруючи свої ідеї в співтовариства фанатів.

Субкультура, де масові бійки – форма розваги, а “кавказець” – синонім ворога, заявила про себе на центральній московській площі.

Народні хвилювання в Тунісі (вони вже отримали назву “жасминової революції”) стали своєрідним детонатором, спробою підірвати ситуацію в, здавалося б, спокійних сусідніх країнах. Найбільшу увагу прикував до себе Єгипет – найбільша арабська держава. Аналітики вже давно називали його “колосом на глиняних ногах”. Аналітики багато в чому пов’язують радикалізацію молоді з впливом такого фактора сучасної цивілізації, як розвиток інформаційних технологій. Соціальні мережі Інтернету дозволили згуртуватися молодим представникам інтелігенції і сформулювати свої вимоги.

На це звернув увагу російський сходознавець Георгій Мирський: “Варто відзначити стійкість і непохитність людей, в авангарді яких йшла молода інтелігенція. Побачивши, що сталося в Тунісі, вони за допомогою Інтернету мобілізували народні маси. Без Інтернету взагалі нічого не було б”.

Єгипетську революцію 2011 р. в засобах масової інформації іноді називають “Революцією 2.0” і “першою твіттерною революцією”, оскільки в ході революції активно використовувався Твіттер для інформування широкої громадськості щодо подій та масової мобілізації протестувальників.

Після “Арабської весни” технології мережної мобілізації продовжили витати над Нью-Йорком. Під впливом мережної мобілізації була проведена серія мітингів критиків економічної політики США, фінансистів і великих корпорацій. На їхню думку, майнова нерівність підриває основи державного устрою і ведуть країну в прірву. Всього було затримано та оштрафовано близько 700 осіб. Ядром мітингувальників є організація Occupy Wall Street, представники якої не заперечують факт того, що їх натхненницею стала так звана “Арабська весна”. Occupy Wall Street хоче ненасильницькими методами відновити демократію в країні. При цьому організатори акції зізнаються, що трохи переоцінили потенціал “мережний мобілізації”. Насправді якщо вірити даним організаторів, загальна кількість учасників американського “дня гніву” було близько 5 000 розкиданих по різних парках і скверах

Висновки.

Соціальні мережі на цей час все більше розглядаються як свій частковий випадок, а саме як он-лайнові соціальні мережі в Інтернеті, такі як Twitter, Facebook, “Одноклассники” тощо. Чому така велика увага при викладенні приділяється Інтернету? Очевидно, більшість людства не має до нього постійного не цензурованого доступу. Ситуація може змінитися в корні. Колись телебачення вважалось елітарною розвагою – сьогодні це буденність. Так само буде і з Інтернетом, тільки швидше. Або вже не з Інтернетом, а тим, що прийде за ним. Відомо, що нововведення впроваджуються з усе більшим прискоренням.

Он-лайнові соціальні мережі, як і будь-яке інше масштабне соціальне явище, породжують ряд проблем: відрив користувача від реальності; брак живого спілкування; користувач починає витрачати надто багато часу на спілкування, у тому числі з незнайомими йому людьми, що може негативно позначитися на його навчанні, роботі та особистому житті і т. д.

Підкреслимо, що якщо соціальні мережі дозволяють здійснювати інформаційне управління (маніпулювання, приховане управління), то неминуче виникає і «подвійне» завдання – аналіз та забезпечення інформаційної безпеки соціальних мереж. Наприклад, загрозою правам і свободам громадянина у сфері духовного життя та інформаційної діяльності може бути витіснення вітчизняних інформаційних агентств, засобів масової

інформації з інформаційного ринку і посилення залежності всіх сфер суспільного життя від зарубіжних інформаційних структур.

Використана література

1. Про основи національної безпеки України : Закон України // Відомості Верховної Ради України. – 2003. – № 39. – С. 351.

2. Доктрина інформаційної безпеки України : Указ Президента України від 08.07.09 р. № 514/2009 // Офіційний вісник України. – 2009. – № 52. – С. 1783.

3. Губанов Д.А., Новиков Д.А., Чхартишвили А.Г. Модели репутации и информационного управления в социальных сетях // Управление большими системами. – [Вып. 26.1]. – М.: ИПУ РАН, 2009. – С. 209 – 234.

4. Давыдова С.И., Усачева О.А. Сетевая организация экологических движений России и Европы // Социологические исследования. – 2009. – № 11. – С. 56 – 64.

5. Newman M., Barabási A.-L., Watts D.J. The Structure and Dynamics of Networks // Princeton and Oxford: Princeton University Press, 2006. – 624 p.

6. Stohl C., Stohl M. Networks of Terror : Theoretical Assumptions and Pragmatic Consequences // Communication Theory. – 17 (2007). – P. 93 – 124.

7. Губанов Д.А., Новиков Д.А., Чхартишвили А.Г. Модели информационного влияния и информационного управления в социальных сетях // Проблемы управления. – 2009. – № 5. – С. 28 – 35.

8. Бреер В.В. Стохастические модели социальных сетей // Управление большими системами. – 2009. – № 27. – С. 169 – 204.

9. Milgram S. The small world problem, Psychology Today, 1967. – Vol. 2. – P. 60 – 67.

10. Backstrom L., Boldi P., Rosa M., Ugander J, Vigna S. Four Degrees of Separation // ePreprint arXiv : 1111.4570.

11. Boyle A. Net not as interconnected as you think. – Режим доступу : //www.news.zdnet.com/2100-9595_22-502388.html

12. Zhou Sh., Mondragon R.J. The rich-club phenomenon in the Internet topology // Communications Letters, IEEE, March 2004. – Vol. 8 Issue 3. – P. 180 – 182.

13. Frantz T., Carley K.M. A formal characterization of cellular networks // Carnegie Mellon University School of Computer Science Institute for Software Research International, Tech. Rep. CMU-ISRI-05-109, 2005.

14. Sageman M. Understanding Terror Networks. – University of Pennsylvania Press, 2004.

15. Clauset A., Moore C., Newman M.E.J. Hierarchical structure and the prediction of missing links in networks // Nature 453, 98-101 (1 May 2008).

16. Pastor-Satorras R., Vespignani A. Epidemic spreading in scale-free networks // Physics Review Letters, vol. 86, no. 14, april 2001.

17. Rothenberg R. From whole cloth: Making up the terrorist network // Connections, vol. 24, no. 3, pp. 36 – 42, 2002.

18. Al quaeda training manual: Declaration of jihad against unholy tyrants // Al-Quaeda, 2001. – Режим доступу : //www.usdoj.gov/ag/trainingmanual.htm

19. Asztalos A., Sreenivasan S., Szymanski B.K., Korniss G. Distributed flow optimization and cascading effects in weighted complex networks // ePreprint arXiv: 1110.3832.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~