Ланде Д.В.
(НДЦПІ Академії правових наук України, dwl@visti.net)
Фурашев В.М.
(НЦЄАІ України, fur@nceai.gov.ua)

Дослідження терористичних зв'язків в рамках теорії складних мереж

На цей у світі є чітке усвідомлення, що головною загрозою його спокою є тероризм і це цілком обґрунтовано, зважаючи на його природу [1].

Як відомо, терор (від лат. terror – страх, жах) – це цілеспрямована застрашлива дія. Відповідно тероризм – це ідеологія насильства і практика впливу на суспільну свідомість, пов'язана із залякуванням населення та/або іншими формами протиправних насильницьких дій, тобто це один із варіантів політичної боротьби, пов'язаний із застосуванням ідеологічно мотивованого насильства. Тероризм можливий за умови співчуття справі терористів хоча б частини суспільства, тобто терористи потребують підтримки населення, саме з якого формуються так званні терористичні мережі.

Обов'язкова умова тероризму – резонанс терористичної акції в суспільстві. Тероризм принципово декларативний. Широке поширення інформації про теракт, перетворення його на найбільш обговорювану подію є ключовим елементом тактики тероризму. Теракт, який залишився непоміченим або засекречений, втрачає всякий сенс.

Це відрізняє терористичний акт від таких близьких явищ, як диверсія або політичне вбивство. Диверсія – силова акція підривного характеру, яка здійснюється спецслужбами держави. Диверсія коштовна безпосередніми втратами, якій несе противник, суспільний резонанс операції не цікавить диверсанта і є, навіть, небезпечним. В ідеалі диверсія імітує техногенну катастрофу, нещасний випадок або силову акцію, здійснену іншою силою. Такі диверсії, як політичні вбивства, здійснені спецслужбами, реальні виконавці вважають за краще звалювати на удаваних винних.

Суспільний резонанс на терористичний акт необхідний терористам для зміни суспільних настроїв. Теракти впливають на масову психологію. Терористичні організації демонструють свою силу і готовність йти до кінця, жертвуючи як власними життями, так і життями жертв. Терорист гучно заявляє, що в цьому суспільстві, на цьому світі є сила, яка ні за яких обставин не прийме існуючий порядок речей і буде боротися з ним до перемоги або до свого кінця.

В силу визначених причин, найбільше «вигідного» середовища поширення «необхідної» інформації про теракт, ніж глобальна мережа Інтернет і на наступний час, і на найближчу перспективу важко знайти.

Саме тому дослідження терористичних мереж на цей час є актуальними як ніколи. Так склалося, що до того ж бурхливий розвиток комп'ютерних засобів дозволяє не тільки аналізувати існуючі мережі, але й здійснювати моделювання, спираючись на принципи емерджентності [2]. Разом з тим, при моделюванні у цій галузі не можна діяти методом проб і помилок, тому необхідно розвивати методи, що дозволяють узагальнювати поточні та ретроспективні дані, і на їхній основі перевіряти адекватність моделей [3].

На цей час вже доведено, що терористичні мережі найчастіше мають властивості так званих безмасштабних мереж [4], які можна розглядати як базу для моделювання, аналізу та прогнозування сценаріїв можливих атак. Крім мережних властивостей терористичних мереж, їм притаманна властивість відродження після руйнувань структури, що є унікальною властивістю подібних мереж.

Для того, щоб пояснити поняття безмасштабності мереж, розглянемо таку їх характеристику, як розподіл ступенів вузлів $P(k)$, який визначається як ймовірність того, що вузол i має ступінь $k_i = k$ (ступінь вузла – це кількість ребер, зв'язаних з цим вузлом). Мережі, що характеризуються різними розподілами ступенів вузлів, демонструють досить різну поведінку. $P(k)$ у деяких випадках може бути, наприклад, розподілом Пуассона ($P(k) = e^{-m} m^k / k!$, де m - математичне очікування), експонентним ($P(k) = e^{-k/m}$), або показовим ($P(k) \sim 1/k^{\gamma}, \ k \neq 0, \ \gamma > 0$). Саме мережі з показовим розподілом ступенів вузлів називаються безмасштабними (scale-free), які, як з'ясувалося у останній час, найчастіше спостерігаються в реально існуючих великих мережах. Приклад візуалізації безмасштабної мережі наведено на рис. 1.

Численні дослідження єдині в думці, що, наприклад, багато терористичних мереж мають властивості безмасштабності, тому їх можна розглядати з урахуванням цієї властивості для аналізу та прогнозування сценаріїв інформаційних операцій, інших атак. Висока ймовірність виникнення безмасштабних мереж, на противагу рівномірно розподіленим випадковим мережам, виникає завдяки тому, що швидкий ріст створює

переваги для перших членів мережі. Ніж довше діє вузол, тим вище кількість його зв'язків, тому важливість найбільших вузлів (з найбільшим ступенем) дуже велика.

Розглянемо деякі інші важливі для подальшого викладу параметри складних мереж [5]. Відстань між вузлами визначається як кількість кроків, які необхідно зробити, щоб по існуючих ребрах добратися від одного вузла до іншого. Природно, вузли можуть бути з'єднані прямо або опосередковано. Шляхом між вузлами l назвемо найкоротшу відстань між ними. Для всієї мережі можна ввести поняття середнього шляху, як середню по всіх парах вузлів найкоротшу відстань між ними:

$$l = \frac{2}{n(n+1)} \sum_{i \geq j} d_{ij},$$

де n - кількість вузлів, d_{ij} – найкоротша відстань між вузлами i й j.

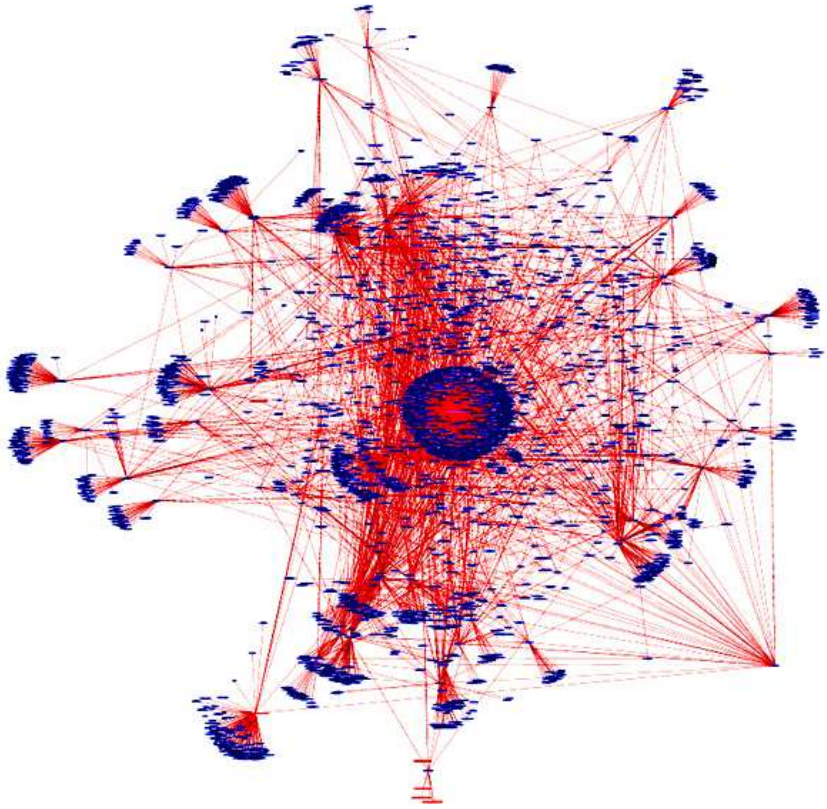


Рис. 1. Візуалізація безмасштабної мережі

Деякі мережі можуть виявитися незв'язними, тобто знайдуться вузли, відстань між якими виявиться нескінченною. Для урахування таких випадків уводиться поняття середнього інверсного шляху між вузлами, що розраховується за формулою:

$$il = \frac{2}{n(n-1)} \sum_{i>j} \frac{1}{d_{ij}}.$$

Мережі також характеризуються таким параметром як діаметр або максимальний найкоротший шлях, який дорівнює максимальному значенню з усіх d_{ij}.

Посередництво (betweenness) – це параметр вузла, що показує, скільки найкоротших шляхів проходить через вузол. Ця характеристика відображає роль даного вузла у встановленні зв'язків у мережі. Вузли з найбільшим посередництвом (комутатори) відіграють головну роль у встановленні зв'язків між іншими вузлами в мережі. Посередництво b_m вузла m визначається за формулою:

$$b_m = \sum_{i \neq j, i \neq m, j \neq m} \frac{B(i,m,j)}{B(i,j)},$$

де $B(i,j)$ - загальна кількість найкоротших шляхів між вузлами i та j, $B(i,m,j)$ - кількість найкоротших шляхів між вузлами i та j, що проходять через вузол m.

Складні терористичні мережі характеризуються наявністю так називаної "структури співтовариства", тобто коли існують групи вузлів, 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 терористичних мереж наявність структури співтовариств виявилося невід'ємною властивістю.

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 більше 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.

Безмасштабні мережі також досить прихильні до впливу епідемій (у випадках терористичних 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 [6], показують, що у безмасштабній мережі поріг для епідемії дорівнює нулю.

Ротенберг [7] відмітив, що ознаки безмасштабності реальних терористичних мереж вступає в протиріччя із вказівками для комунікаційної інфраструктури, установленої в навчальному посібнику Аль-Каїди [8]. 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.

Д. Уаттс і С. Строгатц виявили феномен, характерний для багатьох реальних мереж, названий ефектом малих світів (Small Worlds) [9]. Практикою доведено [7], що терористичні мережі найчастіше не тільки безмасштабні, але й демонструють властивості малих світів, тобто те, що наявність тісно зв'язаних кластерів (груп тісно зв’язаних вузлів) забезпечує локальний зв'язок навіть у випадках вдалих атак, коли концентратори (найбільші посередники) виходять з ладу.

При вивченні «малих світів» визначився цікавий підхід, логічно пов'язаний з поняттям перколяції (протікання) [10, 11]. Виявляється, що багато питань, що виникають при аналізі мережної безпеки в Інтернет, безпосередньо відносяться до цієї теорії. Найпростіше очищене від всіх фізичних і математичних нашарувань формулювання задачі теорії перколяції має такий вигляд: «Дана сітка зі зв'язків, випадкова частина якої проводить сигнал, а інша частина його не проводить. Основне питання - чому дорівнює мінімальна концентрація провідних зв'язків, при якій ще існує шлях через всю сітку?». До задач, які розв'язуються у рамках теорії перколяції та аналізу мереж відносяться такі, як визначення граничного рівня провідності, зміни довжини шляху та його траєкторії при наближенні до граничного рівня провідності, кількості вузлів, які необхідно вивести з ладу, щоб порушити зв’вязність мережі.

Терористичні організації часто характеризуються як клітинні - складені із майже незалежних кліток. Це нетрадиційна організаційна конфігурація, тому була створена спеціальна модель терористичних мереж [7, 12]. Формальне визначення клітинних мереж було дано в [13] у термінах мережних компонент і властивостей. Клітинні мережі мають таки властивості, як надлишковість, наявність тісно зв’язаних кліток (4-6 чоловік), відсутність управління вертикальним способом (нечіткі директиви), відсутність планування (формування за рахунок локальних обмежень), можливість еволюціонування у відповідь на антитерористичну діяльність [14].

Важливою характеристикою складних мереж є еластичність, що ставиться до розподілу відстаней між вузлами при вилученні окремих вузлів. Еластичність мережі залежить від її зв’язності, тобто існуванні шляхів між парами вузлів. Якщо вузол буде вилучений з мережі, типова довжина цих шляхів збільшиться. Якщо цей процес продовжувати досить довго, мережа перестане бути зв'язаною.

Для дослідження складних мереж з показовим авторами розподілом побудовано модель, яка охоплює 100 персон, що згадувалися у мережевих ЗМІ у 2000 статтях за тематикою, пов’язаною з тероризмом (ця модельна мережа виявилася безмасштабною, що дуже важливо для досліджень). Персони у цій моделі вважалися зв’язаними, якщо вони згадувалися у одних й тих же документах. Сила зв’язку (вага ребер мережі) відповідає кількості документів, де одночасно згадуються дві відповідні персони. Структуру саме цієї мережі у графічному вигляді наведено на рис. 1.

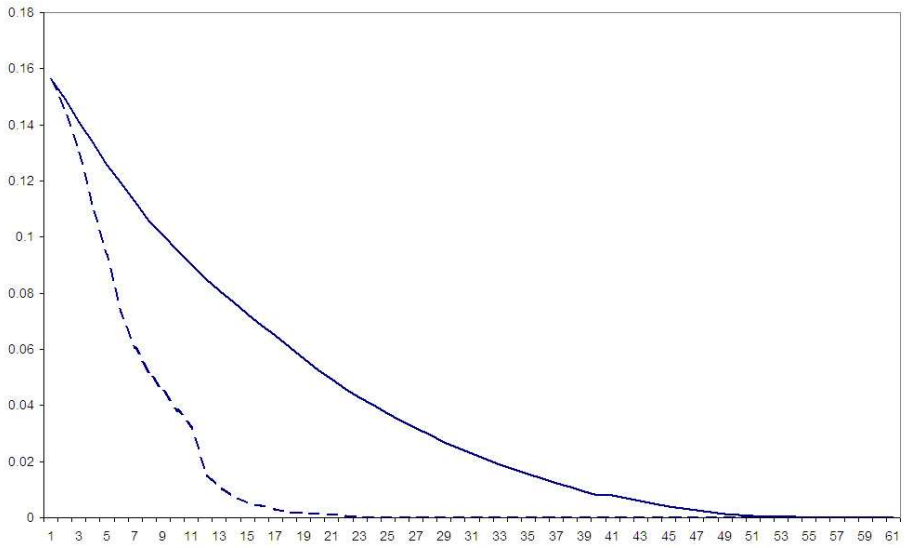


Рис. 2. Змінювання середнього інверсного шляху в мережі (вісь ординат) при зміні кількості вилучених вузлів з найбільшим показником посередництва (пунктирна лінія) та найбільшим ступенем (неперервна лінія)

Якщо з мережі вилучати вузли (нейтралізувати окремих терористів), то для збереження її структури вирішальне значення мають вузли з найбільшим ступенем та з найбільшим показником посередництва (так звані концентратори). Для вирішення питання, яки ж з двох наведених типів вузлів мають більше значення, було проведено експеримент. З мережі послідовно по одному вилучалися вузли (й відповідні їм ребра) з найбільшими значеннями відповідних показників, після чого розраховувалися показники середнього інверсного шляху. Виявилося, що вузли з великими значеннями

показника посередництва відіграють для зв’язності мережі найбільше значення. При послідовному вилученні таких вузлів зв’язність мережі втрачається вже на 7-му кроці, в той час, як при вилученні вузлів з максимальним ступенем (кількістю зв’язків), мережа втрачає зв’язність на 26 кроці. Результати цього моделювання наведено на рис. 2. З цього експерименту можна зробити висновок, що дослідження еластичності подібних складних мереж слід проводити шляхом вилучення вузлів з максимальними показниками посередництва.

На рис. 3 представлено зміни структури досліджуваної мережі при послідовному вилучені вказаної кількості вузлів з найбільшими показниками посередництва. Як можна бачити, в цій моделі вилучення лише 8 % таких вузлів приводить до повного руйнування її структури.

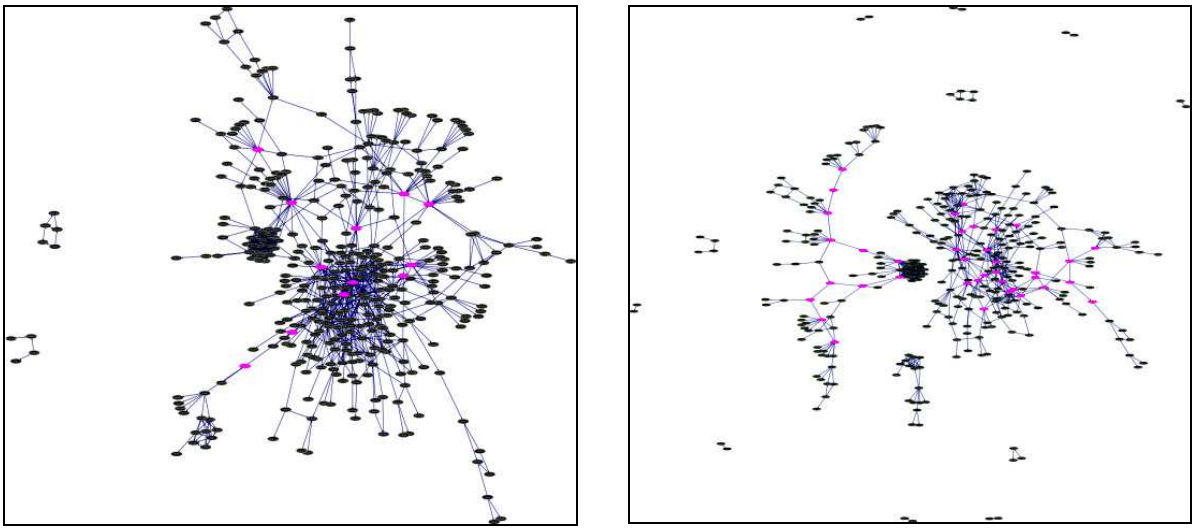
Виходячи з результатів наведеного моделювання здавалося б, що руйнування будь-якої терористичної мережі є відносно нескладним завданням – досить винищити ключові елементи – вузли й відповідні зв’язки. Разом з тим, у реальному житті здійснюються дещо інші процеси. Терористичні мережі мають властивість відновлення після атак, залучення невідомих раніше прихованих (латентних) зв’язків. На рис. 4 наведено схему відновлення зв’язків в мережі після вилучення вузла-концентратора [15].

Після того, як терористична мережа розділяється на ізольовані осередки, вона продовжує використати свої латентні ресурси й швидко відновлює втрати.

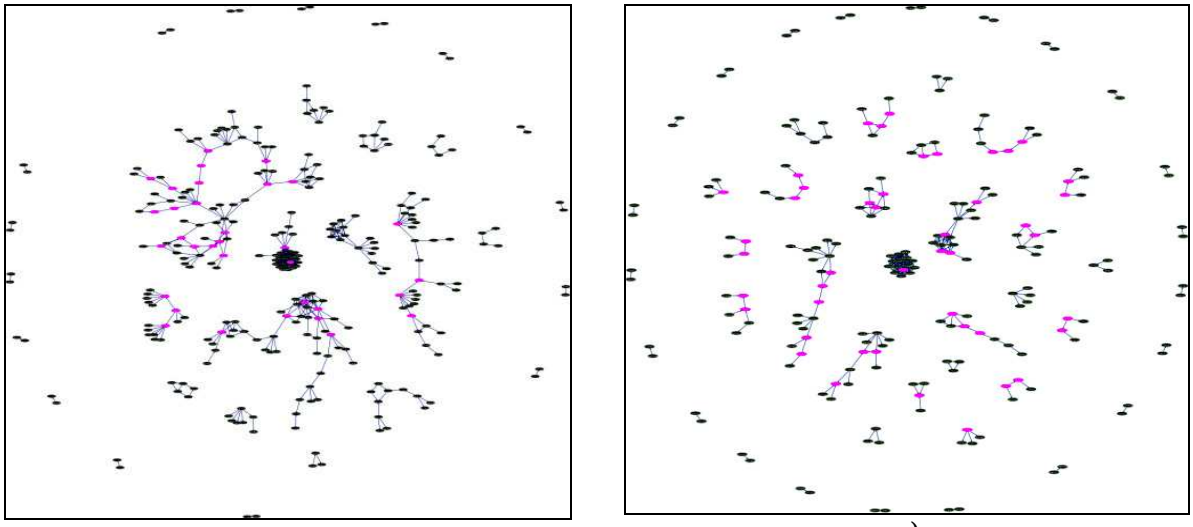
Процес відновлення заснований на використанні прихованих контактів з членами інших осередків без комутатора. Однак для успішності відновлення зв'язки повинні бути загальними - обидві сторони повинні містити взаємні приховані зв’язки.

Возз'єднання частин мережі не може відбутися, якщо жодна з пар агентів не може знайти взаємну реферативну інформацію друг про друга. У цьому випадку вплив роз'єднання на показники діяльності мережі залежить від того, чи зможуть знову роз'єднані частини мережі отримати взаємні зв’язки, недолік яких спостерігається у цій частині мережі. Якщо частина мережі була близькою до самодостатності, то вона продовжує функціонувати самостійно. У противному випадку, частина мережі припиняє дію доти, поки не сформується новий зв’язок.

Якщо одне з возз'єднань виявляється успішним, то ініціатор успішного з'єднання стає новим комутатором, що поєднує дві частини мережі.



а) *б)*



в) *г)*

Рис. 3. Руйнування структури мережі при вилученні зазначеної кількості вузлів – найбільших посередників: а) – 0; б) – 30; в) - 60; г) – 90

Саме завдяки наведеним механізмам складним динамічним мережам притаманна самовилікованність. 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 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.

Аналізуючи зв'язки в мережі, можна довідатися щодо важливих її властивостей, наприклад, виявити наявність кластерів, визначити їх склад, розходження у зв'язності

усередині та між кластерами, ідентифікувати ключові елементи, що зв'язують кластери між собою тощо. Разом з тим серйозною перешкодою при аналізі є неповна інформація про зв'язки між окремими вузлами мережі. Нещодавно група дослідників з Інституту Санта Фе (Santa Fe Institute) представила алгоритм, за допомогою якого стає можливим автоматичне отримання інформації про ієрархічну структуру подібних мереж [16]. 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. Навіть не маючи повного опису системи, можна одержувати репрезентативну вибірку зв'язків і по ній намагатися добудовувати всю мережу. Аналіз графа, що вийшов, дозволяє виявити потенційно важливі зв'язки, які не вдалося виявити в реальній системі.

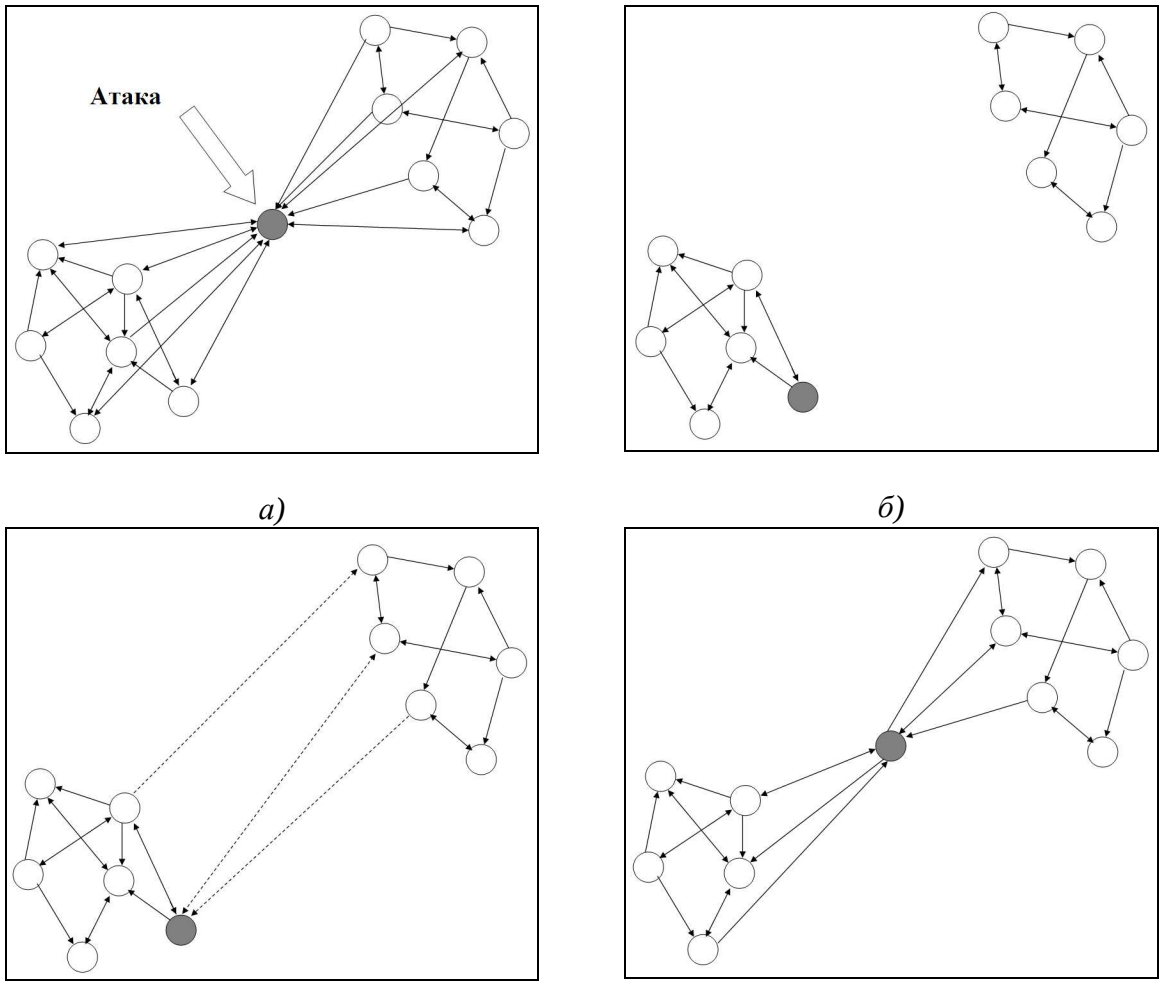


Рис. 4. Відновлення структури мережі шляхом вибору нового посередника: а) – атака на мережу; б) – незв'язна мережа з вилученим посередником; в) в – відродження прихованих (латентних) зв'язків; г) – зв'язність мережі відновлено

Маючи інформацію лише про половину контактів терористів між собою, можна з імовірністю 0,8 прогнозувати ті зв'язки, про які 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.

Дослідницька корпорація RAND опублікувала (Washington Profile від 5 лютого 2009 р.) доповідь про нові закономірності в діяльності терористів. Головний висновок: тероризм поступово стає ефективною стратегічною зброєю, що базується на розвиненій мережевій інфраструктурі. Тобто терористичні мережі являють собою найбільшій виклик суспільній безпеці. Тому вивчення, моделювання, прогнозування поведінки та їх руйнування – завдання як наукове, так і суто практичне. Сьогодні для моделювання та дослідження терористичних мереж застосовуються найперспективніші наукові напрямки – теорія складних мереж, індивідуум-орієнтоване моделювання (зокрема теорія клітинних автоматів), методи оптимізації, теорія ігор, методи соціології, психології тощо.

Наведені в цій роботі 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.

Література

[1] Фурашев В.М., Джердж С.Ф. Національна безпека України: шляхи забезпечення, роль і місце суспільства. Євроатлантичний курс. – К.: «Синопсис», 2009. – 176 с.

[2] The Re-Emergence of Emergence: The Emergentist Hypothesis from Science to Religion. Edited by Philip Clayton and Paul Davies. Oxford University Press. NY. 2006. - 346 pp.

[3] Ланде Д.В. Новітні підходи й технології інформаційно-аналітичної підтримки прийняття рішень // Національна безпека: український вимір: щокв. наук. зб. / Рада нац. безпеки і оборони України, Ін-т пробл. нац. безпеки; - К., 2008. - Вип. 1-2 (20-21). - С. 87-105.

[4] Robb J. Scale-free terrorist networks // 2004, jef Allbrights Web Files; URL:www.jefallbright.net/node/view/2632.

[5] Newman M.E.J. The structure and function of complex networks // SIAM Review. - 2003. - Vol. 45. - pp. 167–256.

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

[7] Rothenberg R. From whole cloth: Making up the terrorist network // Connections, vol. 24, no. 3, pp. 36-42, 2002.

[8] Al quaeda training manual: Declaration of jihad against unholy tyrants // Al-Quaeda, 2001, URL: http://www.usdoj.gov/ag/trainingmanual.htm

[9] Watts D.J., Strogatz S.H. Collective dynamics of ″small-world″ networks // Nature. - 1998. - Vol. 393. - pp. 440–442.

[10] Broadbent S.R., Hammersley J.M. Percolation processes // I. Crystals and mazes, Proc Cambridge Philos. Soc. – pp. 629-641. – 1957.

[11] Снарский А.А., Безсуднов И.В., Севрюков В.А. Процессы переноса в макроскопических неупорядоченных средах: От теории среднего поля до перколяции. – М.: УРСС, Изд-во ЛКИ, 2007. - 304 с.

[12] Carley K., Lee J., Krackhardt D. Destabilizing networks // Connections, vol. 24, no. 3, pp. 79-92, 2002.

[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] Цветоват М. Симуляция человеческих обществ с искусственным интеллектом. Случай террористических сетей // Ежеквартальный Интернет – журнал «Искусственные общества», II квартал 2007. – Т. 2. - № 2. - С. 5-29.

[16] 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).