УДК 519.6

О.Д. ПОЛІЩУК

ПРО УРАЗЛИВІСТЬ СКЛАДНИХ МЕРЕЖЕВИХ СТРУКТУР ТА СИСТЕМ

Анотація. Розглянуто структурний та функціональний підходи до визначення уразливості складних мережевих структур та систем до негативних внутрішніх та зовнішніх впливів. Введено поняття параметрів впливу та посередництва елементів системи, які надають змогу визначати найважливіші з функціонального погляду вузли та ребра мережі та розробляти сценарії для ідентифікації складових системи, блокування яких може призвести до найбільших втрат у процесі її функціонування, а також кількісно оцінювати ці втрати. Проаналізовано чутливість системи до малих змін в об'ємах руху потоків, значення яких є близькими до критичної завантаженості її складових. Отримані результати можуть бути використані для удосконалення наявних та розроблення нових методів захисту реальних мережевих систем від природних та штучних уражень різних типів.

Ключові слова: складна мережа, мережева система, потік, стійкість, вплив, посередництво.

ВСТУП

Одним із напрямків системних досліджень, який почав бурхливо розвиватися протягом останніх десятиліть [1, 2], стало вивчення складних мережевих систем (СМС). Мережеві структури є у мікро- та макросвіті [3, 4], біологічних системах (нейронні, протеїнові, метаболічні, харчові, екологічні мережі тощо) та людському соціумі (економічні, соціальні, фінансові, політичні, релігійні, професійні, родинні та багато інших) [5–7]. Предметом дослідження теорії складних мереж (ТСМ) є створення універсальних моделей мережевих структур, визначення статистичних властивостей, які характеризують їхню поведінку, та прогнозування поведінки мереж у разі зміни їхніх структурних властивостей. Подібність багатьох природних та штучних мереж допомагає у розробленні універсальних методів дослідження таких структур, але не завжди процесів функціонування відповідних систем. Однією з визначальних особливостей реально функціонуючих СМС є рух потоків у них. В одних випадках забезпечення руху потоків є основною ціллю утворення та функціонування таких систем (транспортні мережі та системи постачання ресурсів, торговельні та соціальні мережі та ін.), в інших — процесом, який забезпечує їхню життєдіяльність (рух крові, лімфи, нейроімпульсів у тілі людини тощо). Зупинка руху потоків може призвести до припинення існування таких систем. Отже, рух потоків можна віднести до основної або однієї з основних функціональностей, яка реалізується СМС [8, 9].

Серед складних мереж (СМ) різних типів найбільший інтерес з прикладної точки зору викликають так звані безмасштабні мережі [10]. Визначальною особливістю цих мереж є степеневий розподіл ступенів вузлів, що призводить до наявності невеликої кількості вузлів, які мають високий ступінь, та величезної кількості вузлів з невисоким ступенем (кількість мегаполісів у кожній країні є невеликою порівняно із загальною кількістю населених пунктів, однак їхнє значення у житті країни важко переоцінити). Однією з основних проблем, яка досліджується у ТСМ, є уразливість мережі до випадкових або цілеспрямованих внутрішніх та зовнішніх впливів на її вузли [11–13]. Це пояснюється небезпечністю наслідків розгортання таких процесів, які можуть призвести до дестабілізації роботи транспортних систем та мережі Інтернет, фінансових криз та збоїв у роботі систем енергозабезпечення тощо. Виявляється, що безмасштабні

мережі є достатньо стійкими до випадкових уражень та дуже вразливими до цілеспрямованих атак [12]. У ТСМ розроблено низку структурних підходів до дослідження подібних явищ у мережі [13, 14]. Однак система може бути уразливою не лише до атак на її структуру, але й на процес функціонування. Наприклад, глобальна комп'ютеризація робить чутливою до кібератак практично всі сфери діяльності людини. Тільки протягом 2014–2018 рр. атаки хакерів та комп'ютерні віруси інфікували та дестабілізували роботу низки державних органів, служб безпеки, військових відомств, транспортних та енергетичних систем багатьох країн світу. Збитки від таких атак становили десятки мільярдів доларів [15]. В Україні за той самий час хакерські атаки неодноразово блокували роботу Держказначейства, Міністерства фінансів та пенсійного фонду, десятків великих банків, залізничної та авіаційної систем, систем енергопостачання окремих регіонів та ін. Очевидно, що надалі такі загрози будуть тільки посилюватися, а збитки від них — зростати. Тому визначення найбільш функціонально важливих, а отже і найбільш привабливих для атак елементів реальних СМС сприятиме удосконаленню наявних та побудові нових, значно ефективніших систем захисту.

Мета статті — визначення критеріїв функціональної важливості елементів складних мережевих систем та розроблення сценаріїв негативних впливів на них з метою запобігання або мінімізації наслідків потенційних уражень.

СТРУКТУРНІ ПІДХОДИ ДО ВИЗНАЧЕННЯ УРАЗЛИВОСТІ СКЛАДНИХ МЕРЕЖ

Структура мережі та низка характеристик її елементів повністю визначаються матрицею суміжності [1]. До таких характеристик належить ступінь вузла, значення якого для бінарних неорієнтованих мереж визначається кількістю його зв'язків із суміжними вузлами. Для безмасштабних мереж цього типу у ТСМ досліджуються такі сценарії цілеспрямованих атак [12, 13]:

1) готується перелік вузлів мережі у порядку зменшення значень їхніх ступенів, та вузли з початку цього переліку послідовно вилучаються зі структури до досягнення перколяційного порогу;

2) після вилучення чергового вузла сформований за першим сценарієм перелік вузлів переписується за тим самим принципом і атака здійснюється на перший вузол із модифікованого списку.

Другий сценарій цілеспрямованої атаки на безмасштабну СМ, який враховує можливу зміну після чергового вилучення структури зв'язків у мережі, виявився значно небезпечнішим за перший [12]. Зокрема, було встановлено, що у результаті застосування цього сценарію після вилучення зі складу Інтернету 4 % вузлів з найбільшим ступенем ця мережа поділяється на незв'язні складові.

Ступінь вузла є його локальною характеристикою у мережі. Однією з глобальних характеристик вузла є центральність посередництва, яка визначається кількістю усіх найкоротших шляхів мережі, що проходять через нього [16]. Центральність посередництва надає змогу формувати більш дієві сценарії атак на безмасштабні мережі, зокрема:

1) готується перелік вузлів мережі у порядку зменшення значень їхньої центральності посередництва, та вузли з початку цього переліку послідовно вилучаються зі структури до досягнення перколяційного порогу;

2) після вилучення чергового вузла сформований за попереднім сценарієм перелік вузлів переписується за тим самим принципом і атака здійснюється на перший вузол із модифікованого списку.

Останні два сценарії є небезпечнішими за попередні, тобто вузли з більшою центральністю посередництва є важливішими для мережі, ніж вузли з високим ступенем. Це було підтверджено, зокрема, на прикладі дослідження низки світових авіаційних мереж [14].

Вузол може мати високий ступінь або центральність посередництва у мережевій структурі, але це далеко не завжди визначає його реальну важливість у процесі функціонування системи. У багатьох країнах існують регіони, які після

періодів інтенсивного розвитку перейшли у стан депресії (вичерпання покладів корисних копалин, які видобувалися у регіоні; зменшення попиту на продукцію, на виробництві якої регіон спеціалізувався тощо). У таких регіонах зазвичай залишається розвинена інфраструктура, зокрема щільна транспортна мережа та мережа енергопостачання, але об'єми потоків до/з них суттєво скорочуються. Це означає, що незважаючи на високий ступінь вузлів, які знаходяться у відповідних частинах мережі, їхнє функціональне значення в системі може бути невеликим [8]. Ступінь таких міст, як Коростень, Куп'янськ, Тернопіль та Київ у залізничній мережі України дорівнює п'яти. Очевидно, що це не відповідає функціональній важливості цих міст у житті країни. До того ж, структурний підхід до аналізу вразливості СМС не дає чіткої відповіді принаймні на три питання:

1) атаки на процесс функціонування яких елементів системи можуть найбільше дестабілізувати її роботу навіть за неураженої структури;

2) на яку частину системи може розповсюдитися цей процесс дестабілізації;

3) які кількісні втрати очікують систему та окремі її складові унаслідок ураження.

ФУНКЦІОНАЛЬНІ ПІДХОДИ ДО ВИЗНАЧЕННЯ УРАЗЛИВОСТІ МЕРЕЖЕВИХ СИСТЕМ

Проблема стійкості системи є набагато глибшою та складнішою, ніж проблема стійкості її структури. Звичайно, ураження структури, наприклад її розбиття на незв'язні складові, неминуче призведе до дестабілізації роботи СМС, але збої в системі можуть виникати і при неураженій структурі. Окрім того, кількість елементів системи, цілеспрямовані атаки на роботу яких можуть призвести до збоїв СМС, зазвичай є значно більшою, ніж вузлів у структурі, вилучення яких призводить до перетину перколяційного порогу. Для підтвердження цього можна використати підхід М. Ньюмена [17], який зіставив зваженій мережі з цілочисельними вагами мультиграф з тією ж матрицею суміжності $\mathbf{V} = \{V_{ij}\}_{i,j=1}^{N}$, де V_{ij} — вага ребра, яке поєднує вузли n_i та n_j, $i, j = \overline{1, N}$, N — кількість вузлів мережі. Якщо прийняти як ваги зведені до цілочисельних значення об'ємів потоків, що проходять ребрами мережі за певний проміжок часу $[0, T]$, то за такого підходу на шляхах інтенсивного руху потоків навіть транзитні вузли мультиграфу можуть мати високі ступінь та центральність посередництва (рис. 1). Це означає, що атаки на них можуть призвести до серйозних збоїв у роботі системи.

Функціональну важливість вузла в СМС визначимо в такий спосіб. Нехай $v_k^{\text{out}}(n_i, n_j)$ — об'єм потоків, згенерованих у вузлі n_i та прийнятих у вузлі n_j, які пройшли шляхом $p_k(n_i, n_j)$ за період $[0, T]$, K_{ij} — кількість усіх можливих шляхів, які поєднують вузли n_i та n_j, $k = \overline{1, K_{ij}}$, $i, j = \overline{1, N}$. Позначимо

$$V^{\text{out}}(n_i, n_j) = \sum_{k=1}^{K_{ij}} v_k^{\text{out}}(n_i, n_j)$$

сумарний об'єм потоків, згенерованих у вузлі n_i та спрямованих для прийняття у вузол n_j всіма можливими шляхами за період $[0, T]$. Параметр $V^{\text{out}}(n_i, n_j)$ визначає реальну силу впливу вузла n_i на вузол n_j на підставі сумарних об'ємів потоків, які надійшли з нього у вузол n_j за період тривалістю T, $i, j = \overline{1, N}$. Чітка

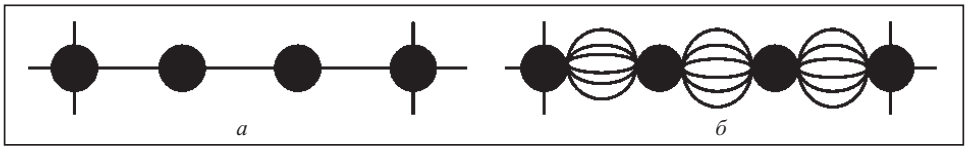

Рис. 1. Фрагмент цілочисельної зваженої мережі: значення ваг дорівнює шести (*а*); відповідний мультиграф (*б*)

визначеність шляхів та об'ємів руху потоків характерна для більшості промислових, фінансових, транспортних, торговельних мереж, систем постачання ресурсів, державного управління тощо. Наприклад, легко визначити, яка частина залізничних квитків продається з використанням мережі Інтернет, який відсоток комунальних платежів сплачується або пенсій виплачується через відділення Укрпошти, яка частка держзакупівель здійснюється з використанням системи «Прозорро» тощо. Ці дані дають можливість кількісно обчислити втрати, які можуть бути завдані відповідним системам, наприклад, у результаті кібератак на їхні комп'ютерні мережі.

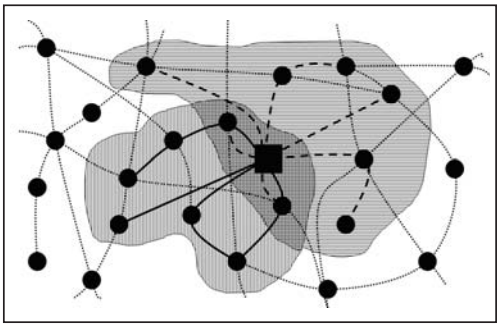

Рис. 2. Області вхідного (вертикальні смуги G_i^{in}) та вихідного (горизонтальні смуги R_i^{out}) впливу, відображеного квадратом вузла мережевої системи

Нехай $R_i^{\text{out}} = \{j_{i_1}, ..., j_{i_L}\}$ — множина номерів вузлів — кінцевих приймачів потоків, згенерованих у вузлі n_i, L — кількість елементів множини R_i^{out}. Параметр

$$\xi_i^{\text{out}} = \sum_{j \in R_i^{\text{out}}} V^{\text{out}}(n_i, n_j) / s(\mathbf{V}),\ \xi_i^{\text{out}} \in [0,1],$$

визначає силу впливу вузла n_i на СМС загалом, $i = \overline{1, N}$. Тут $s(\mathbf{V})$ — сума елементів матриці $\mathbf{V}$, яка дорівнює сумарному об'єму потоків у мережі за період $[0, T]$. Потужність впливу вузла n_i на систему визначимо за допомогою параметра $p_i^{\text{out}} = L / N$, $p_i^{\text{out}} \in [0,1]$, а множину R_i^{out}, $i = \overline{1, N}$, називатимемо областю впливу цього вузла на СМС (рис. 2).

Наприклад, область впливу органів місцевого управління або регіональних ЗМІ зазвичай обмежується відповідним регіоном країни, а загальнодержавних огранів управління та національних ЗМІ — всією державою. Параметри ξ_i^{out}, p_i^{out} та R_i^{out} називатимемо вихідною силою, потужністю та областю або вихідними параметрами впливу вузла n_i, $i = \overline{1, N}$, на СМС відповідно. У найпростішому випадку вихідна область впливу кожного вузла СМС обмежується суміжними вузлами, а у найскладнішому — утворює повний граф. Область R_i^{out} та параметр p_i^{out} дають можливість оцінити, на яку частину СМС розповсюдяться наслідки збоїв у процесі функціонування вузла n_i, а значення ξ_i^{out} — визначити, до яких втрат це призведе у сенсі недопостачання або затримки постачання відповідних об'ємів потоків.

Нехай $v_k^{\text{in}}(n_j, n_i)$ — об'єм потоків, згенерованих у вузлі n_j та прийнятих у вузлі n_i, які пройшли шляхом $p_k(n_j, n_i)$ за період $[0, T]$, K_{ji} — кількість усіх можливих шляхів, які поєднують вузли n_j та n_i, $k = \overline{1, K_{ji}}$, $i, j = \overline{1, N}$. Позначимо

$$V^{\text{in}}(n_j, n_i) = \sum_{k=1}^{K_{ij}} v_k^{\text{in}}(n_j, n_i)$$

сумарний об'єм потоків, згенерованих у вузлі n_j та спрямованих для прийняття у вузол n_i усіма можливими шляхами за період $[0, T]$. Параметр $V^{\text{in}}(n_j, n_i)$ визначає реальну силу впливу вузла n_j на вузол n_i відповідно до сумарних об'ємів потоків, які були прийняті у вузлі n_i за період тривалістю T, $i, j = \overline{1, N}$. Нехай

$G_i^{\text{in}} = \{j_{i_1}, \ldots, j_{i_M}\}$ — множина номерів вузлів, у яких генеруються потоки, що спрямовуються для прийняття у вузол n_i, M — кількість елементів множини G_i^{in}. Параметр

$$\xi_i^{\text{in}} = \sum_{j \in G_i^{\text{in}}} V^{\text{in}}(n_j, n_i) / s(\mathbf{V}),\ \xi_i^{\text{in}} \in [0,1],$$

визначає силу впливу СМС на вузол n_i, $i = \overline{1, N}$. Потужність впливу системи на вузол n_i визначимо за допомогою параметра $p_i^{\text{in}} = M / N$, $p_i^{\text{in}} \in [0,1]$, а множину G_i^{in} називатимемо областю впливу СМС на вузол n_i. Параметри ξ_i^{in}, p_i^{in} та G_i^{in} називатимемо вхідною силою, потужністю та областю або вхідними параметрами впливу СМС на вузол n_i відповідно. У найпростішому випадку вхідна область впливу кожного вузла СМС обмежується суміжними вузлами, а у найскладнішому — утворює повний граф.

Параметри вхідного та вихідного впливу вузлів СМС дають можливість принаймні частково дати відповіді на сформульовані вище питання щодо найбільш функціонально важливих для дестабілізації роботи системи елементів. Однак існує й інший аспект проблеми захисту. Він полягає у своєчасному виявленні та блокуванні тих вузлів СМС, які містять потенційну або реальну загрозу та можуть дестабілізувати роботу системи — хакерських та терористичних групп, джерел розповсюдження небезпечних інфекційних захворювань тощо. У соціальних онлайн сервісах часто зустрічаються так звані бот-мережі [18], за допомогою яких одна особа може створити ілюзію спільної думки багатьох людей, масово розповсюджувати дезінформацію, організовувати DDoS-атаки тощо. Такі бот-мережі часто створюються під час передвиборчих кампаній та можуть спотворювати волевиявлення громадян. Вони є потужним інструментом недобросовісної конкурентної боротьби, реклами неякісної продукції або, навпаки, антиреклами нових товарів. Виявлення вузлів-генераторів таких бот-мереж та їхнє блокування надає змогу запобігати багатьом негативним соціальним та економічним явищам. Вхідні та вихідні параметри впливу вузлів СМС дають можливість достатньо точно ідентифікувати генератори бот-мереж. Зазвичай генератор бот-мережі, надсилаючи команди створеним ним ботам (інформацію про ціль та зміст атаки), зворотної відповіді не потребує та не отримує, тобто для таких утворень виконується нерівність

$$\frac{\xi_i^{\text{in}}}{\xi_i^{\text{out}}} << 1.$$

Із цих міркувань також випливає, що область та потужність вихідного впливу таких вузлів є достатньо великими (у мережі Twitter виявлені бот-мережі, які налічують більше 350 тис. вузлів [19]), а область та потужність вхідного впливу — малими, причому $R_i^{\text{out}} \cap G_i^{in} \approx 0$.

У реальних СМС практично не зустрічаються вузли, які є виключно генераторами або приймачами потоків. Дійсно, для виробництва певної продукції є необхідним постачання сировини та комплектування, видобування корисних копалин не може здійснюватися без відповідної гірничо-видобувної техніки тощо. Позначимо RG_i об'єднання областей вхідного та вихідного впливу вузла n_i, тобто $RG_i = R_i^{\text{out}} \cup G_i^{\text{in}}$.

Силу взаємодії вузла n_i з СМС визначимо за допомогою параметра $\xi_i = (\xi_i^{\text{in}} + \xi_i^{\text{out}})/2$, а потужність цієї взаємодії — за допомогою параметра p_i, який дорівнює кількості елементів множини RG_i.

Параметри взаємодії надають змогу визначити такі сценарії атак на СМС:

1) готується перелік вузлів мережі у порядку зменшення значень сил їхньої взаємодії з системою та вузли з початку цього переліку послідовно вилучаються зі структури до досягнення наперед визначеного рівня критичних втрат;

2) після вилучення чергового вузла сформований за попереднім сценарієм перелік вузлів переписується за тим самим принципом і атака здійснюється на перший вузол із модифікованого списку.

Другий сценарій враховує необхідність заміщення заблокованих вузлів-генераторів та вузлів-приймачів і відповідний перерозподіл руху потоків мережею. Залежно від способу протидії потенційним загрозам останні два сценарії можна формувати окремо для вузлів-генераторів (наприклад, пошуку ініціаторів DDoS-атак) та вузлів-приймачів потоків (пошуку найбільш ймовірних цілей DDoS-атак). Слід також враховувати, що у реальності поведінка параметрів впливу вузлів СМС може бути значно складнішою. Вузол, який спрямував потік у всі суміжні вузли, може знову стати приймачем, а суміжні з ним вузли із приймачів можуть перетворитися на генератори, які спрямовують цей потік далі. У такий спосіб відбувається розгортання епідемій інфекційних хвороб за так званим SIS-сценарієм [20]. Крім того, параметри впливу вузлів СМС загалом є динамічними характеристиками, значення яких може суттєво змінюватися з часом.

Як зазначено вище, однією з найбільш вживаних для визначення важливості вузлів мережі поряд із ступенем є центральність посередництва. Можливо, термін «посередництво» є найбільш вдалим для визначення участі елемента СМС у процесі спільного функціонування та взаємодії усіх вузлів мережі або певної її частини. Тому для визначення функціональної важливості вузла або ребра в системі вживатимемо саме термін «посередництво». Позначимо $P_{ij}^{K_{ij}} = \{p_{ij}^k\}_{k=1}^{K_{ij}}$ сукупність шляхів, які поєднують вузли-генератори та вузли-приймачі потоків СМС і містять, як елемент, ребро (n_i, n_j), $i, j = \overline{1, N}$. Нехай v_{ij}^k — об'єм потоків, які пройшли шляхом p_{ij}^k від вузла-генератора до вузла-приймача, а отже і ребром (n_i, n_j), за період $[0, T]$. Тоді величина

$$V_{ij}^{K_{ij}} = \sum_{k=1}^{K_{ij}} v_{ij}^k$$

визначає сумарний об'єм потоків, які пройшли сукупністю шляхів $P_{ij}^{K_{ij}}$, а отже і ребром (n_i, n_j), за цей самий проміжок часу. Параметр $\Phi_{ij} = V_{ij}^{K_{ij}} / s(\mathbf{V})$, який визначає питому вагу потоків, що проходять ребром (n_i, n_j) за період $[0, T]$, називатимемо мірою посередництва цього ребра у процесі функціонування СМС. Множину L_{ij} усіх вузлів мережі, які лежать на шляхах із сукупності $P_{ij}^{K_{ij}}$, називатимемо областю посередництва, а кількість η_{ij} цих вузлів — потужністю посередництва ребра (n_i, n_j), $i, j = \overline{1, N}$, (рис. 3).

Параметри міри, області та потужності посередництва ребра (n_i, n_j), $i, j = \overline{1, N}$, є глобальними характеристиками його важливості у процесі функціонування СМС. Вони, зокрема, визначають, яким чином блокування цього ребра вплине на роботу області його посередництва, величину цієї області і, внаслідок цього, втрати всієї системи.

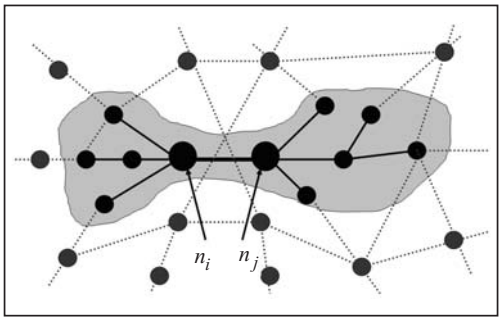

Рис. 3. Область посередництва ребра (n_i, n_j) у процесі функціонування СМС

Позначимо $P_i^{K_i} = \{p_i^k\}_{k=1}^{K_i}$ сукупність шляхів, які поєднують вузли-генератори та вузли-приймачі потоків СМС та проходять через вузол n_i, $i = \overline{1, N}$. Нехай v_i^k — об'єм потоків, які пройшли шляхом p_i^k від вузла-генератора до вузла-приймача, а отже і через вузол n_i, за період $[0, T]$. Тоді величина

$$V_i^{K_i} = \sum_{k=1}^{K_i} v_i^k$$

визначає сумарний об'єм потоків, які пройшли сукупністю шляхів $P_i^{K_i}$, а отже і через вузол n_i, за цей самий проміжок часу. Параметр $\Phi_i = V_i^{K_i} / s(\mathbf{V})$, який визначає питому вагу потоків, що проходять через вузол n_i за період $[0, T]$, називатимемо мірою посередництва цього вузла в процесі функціонування СМС. Множину M_i усіх вузлів СМС, які лежать на шляхах із сукупності $P_i^{K_i}$, називатимемо областю посередництва, а кількість η_i цих вузлів — потужністю посередництва вузла n_i. Параметри міри, області та потужності посередництва вузла n_i, $i = \overline{1, N}$, є глобальними характеристиками його важливості у процесі функціонування СМС. Вони, зокрема, визначають, яким чином блокування цього вузла вплине на роботу області його посередництва, величину цієї області і, внаслідок цього, втрати всієї системи.

Параметри посередництва надають змогу визначити такі сценарії атак на СМС:

1) готується перелік вузлів мережі у порядку зменшення значень міри їхнього посередництва в системі, та вузли з початку цього переліку послідовно вилучаються зі структури до досягнення наперед визначеного рівня критичних втрат;

2) після вилучення чергового вузла сформований за попереднім сценарієм перелік вузлів переписується за тим самим принципом і атака здійснюється на перший вузол із модифікованого списку.

Другий сценарій враховує необхідність заміщення заблокованих вузлів-генераторів та приймачів потоків і пошуку альтернативних шляхів руху транзитних потоків, які проходили через заблоковані вузли, тобто відповідний перерозподіл руху потоків мережею. Аналогічні сценарії атак формуються і для ребер, оскільки у багатьох випадках виведення з процессу функціонування СМС ребра мережі здійснити набагато простіше, ніж блокування одного з вузлів, які це ребро з'єднує. Параметри посередництва вузлів та ребер дають змогу оцінити, на яку частину СМС розповсюдяться наслідки збоїв відповідного елемента системи і до яких втрат це призведе у сенсі недопостачання певних об'ємів транзитних потоків.

Вище ми визначили параметри посередництва вузла, враховуючи лише транзитні потоки, які проходять через нього. Однак значення параметрів посередництва можна суттєво розширити, враховуючи, що вузол n_i може бути не лише транзитером, але й генератором та кінцевим приймачем потоків. Тоді множину $P_i^{K_i}$ можна доповнити шляхами руху потоків, які починаються (генеруються) або закінчуються (приймаються) у вузлі n_i. Позначимо таку доповнену множину $\widetilde{P}_i^{K_i}$, $i = \overline{1, N}$. Тоді величину

$$\widetilde{\Phi}_i = (\Phi_i + \xi_i^{\text{in}} + \xi_i^{\text{out}}) / 3$$

називатимемо узагальненою мірою посередництва вузла n_i у процесі функціонування СМС. Відповідно множину $\widetilde{M}_i$ усіх вузлів СМС, які лежать на шляхах із сукупності $\widetilde{P}_i^{K_i}$, називатимемо узагальненою областю посередництва, а кількість $\widetilde{\eta}_i$ цих вузлів — узагальненою потужністю посередництва вузла n_i, $i = \overline{1, N}$. Узагальнені параметри посередництва враховують взаємодію

між усіма прямо та опосередковано пов'язаними вузлами СМС (генераторами, приймачами та транзитерами) і надають змогу формувати найдієвіші сценарії атак на них. Принципи побудови таких сценаріїв описані вище.

ЧУТЛИВІСТЬ МЕРЕЖЕВИХ СИСТЕМ ДО МАЛИХ ЗМІН

Одночасно з цілеспрямованими атаками існує й інший аспект стійкості системи, який полягає в її чутливості до малих змін в структурі або процесі функціонування. Такі зміни можуть бути зумовлені як внутрішніми, так і зовнішніми чинниками, та призводити до наслідків не менш негативних, ніж цілеспрямовані атаки. При цьому стійкість структури визначається чутливістю до малих змін її складу (сукупності вузлів та зв'язків між ними) [12]. Структура є нестійкою, якщо такі зміни можуть призвести до втрати певних властивостей мережі, наприклад зв'язності. Стійкість процесу функціонування СМС визначається його чутливістю до малих змін об'ємів руху потоків. Наприклад, система є уразливою в умовах критичної (близької до їхньої пропускної здатності) завантаженості частини її ребер або вузлів, а у СМС із повністю впорядкованим рухом потоків, наприклад залізничній транспортній системі, вона є чутливою до малих затримок у графіку руху поїздів. Очевидно, що стійкість процесу тією чи іншою мірою пов'язана зі стійкістю структури СМС. Якщо малі зміни (блокування кількох вузлів та ребер мережі) призводять до втрати її зв'язності, це безпосередньо впливає на процес функціонування системи. Якщо завантаженість певних елементів структури потоками є критичною, це також створює загрозу їхнього блокування.

Визначимо найбільш уразливі до умов критичної завантаженості функціонально важливі складові СМС. З цією метою введемо [21] потокову λ-серцевину СМС, як найбільшу підмережу вихідної мережі, для якої елементи матриці $\mathbf{V}$ є не меншими значення $\lambda \in [0,1]$. Матрицю суміжності λ-серцевини $\mathbf{V}^{\lambda} = \{V_{ij}^{\lambda}\}_{i,j=1}^{N}$ визначимо співвідношенням

$$V_{ij}^{\lambda} = \begin{cases} V_{ij}, & \text{якщо } V_{ij} \geq \lambda, \\ 0, & \text{якщо } V_{ij} < \lambda, \ i, j = \overline{1, N}. \end{cases}$$

Елементи матриці $\mathbf{V}^{\lambda}$ зі зростанням значення λ визначають функціональну пріоритетність відповідних підсистем СМС.

Визначимо також матрицю завантаженості СМС $\mathbf{U} = \{U_{ij}\}_{i,j=1}^{N}$, елементи якої $U_{ij} = V_{ij} / U_{ij}^{\max}$, де $U_{ij}^{\max}$ — пропускна здатність (максимально допустимий об'єм потоків) ребра (n_i, n_j), $i, j = \overline{1, N}$, та введемо β-серцевину завантаженості СМС, як найбільшу підмережу вихідної мережі, для якої елементи матриці $\mathbf{U}$ є не меншими, ніж значення $\beta \in [0,1]$.

Матрицю суміжності β-серцевини $\mathbf{U}^{\beta} = \{U_{ij}^{\beta}\}_{i,j=1}^{N}$ визначимо за співвідношенням

$$U_{ij}^{\beta} = \begin{cases} u_{ij}, & \text{якщо } U_{ij} \geq \beta, \\ 0, & \text{якщо } U_{ij} < \beta, \ i, j = \overline{1, N}. \end{cases}$$

Елементи матриці $\mathbf{U}^{\beta}$ зі зростанням значення β визначають найбільш завантажені складові системи. Тоді ненульові елементи матриці

$$\mathbf{W}^{\lambda \times \beta} = \{V_{ij}^{\lambda} \times U_{ij}^{\beta}\}_{i,j=1}^{N}$$

для значень λ та β, близьких до одиниці, визначають найбільш уразливі з функціонально найважливіших складових системи, які належать перетину λ- та β-серцевин СМС. Незначне збільшення об'ємів потоків у таких складових

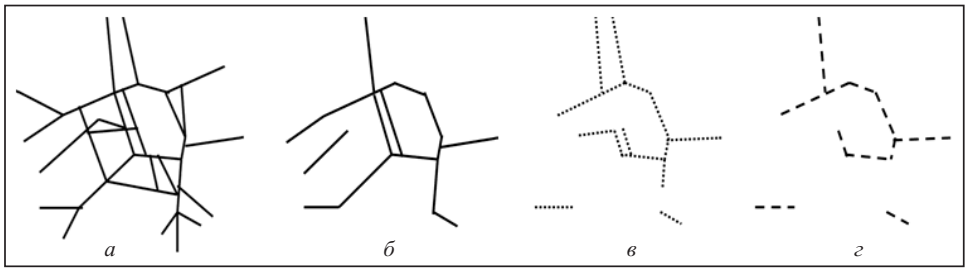

Рис. 4. Фрагменти: основних автошляхів середмістя великого міста (*а*); потокової серцевини середмістя (*б*); серцевини завантаженості середмістя (*в*); найбільш уразливої складової автошляхів середмістя (*г*)

може призвести до їхнього блокування в системі, заподіявши їй найбільшу шкоду. На рис. 4, *а* відображено основні автомагістралі центральної частини м. Львова, структура яких сформувалася задовго до появи автомобільного та електротранспорту. Це є основною причиною тривалих заторів (блокування важливих складових автотранспортної мережі), які постійно виникають у середмісті Львова. Рис. 4, *б* та 4, *в* містять фрагменти потокової 0,8-серцевини та 0,9-серцевини завантаженості цієї автотранспортної системи (АТС) відповідно. На рис. 4, *г* зображено найбільш уразливі до виникнення заторів ділянки автотранспортної мережі (ненульові елементи матриці $\mathbf{W}^{\lambda\times\beta}$), які неодноразово призводили до тимчасового колапсу АТС середмістя Львова. Загалом для довільної мережевої системи елементи її матриці $\mathbf{W}^{\lambda\times\beta}$ визначають найбільш уразливі, тобто привабливі з погляду успішної реалізації складові для цілеспрямованих атак на неї. Очевидно, що блокування цих складових породжує труднощі для руху потоків на усіх прилеглих шляхах.

На відміну від цілеспрямованих уражень збоям, які виникають у результаті малих змін об'ємів руху потоків, часто можна запобігти. Так, аналіз ризиків, пов'язаних із критичним завантаженням, надає змогу завчасно збільшувати пропускну здатність елементів СМС, обирати альтернативні або формувати нові шляхи руху потоків. Недоліки, пов'язані з чутливим до малих затримок графіком руху потоків, можна подолати шляхом оптимізації цього графіка і т.ін. Оскільки збої окремого елемента негативно впливають на роботу усіх прямо чи опосередковано пов'язаних із ним елементів СМС, тобто на певну її підсистему, а недоліки у функціонуванні окремих підсистем — на СМС загалом, то для оперативного аналізу та прогнозування наслідків, спричинених цими збоями ушкоджень, доцільно використовувати методи неперервного моніторингу та комплексного оцінювання процесу функціонування складних систем, детально описані у [22, 23].

Зазвичай після блокування системи, структура якої визначається матрицею $\mathbf{W}^{\lambda\times\beta}$, СМС намагається переспрямувати потоки іншими шляхами. Як результат у мережі утворюються інші потокові серцевини та серцевини завантаженості, перетин яких створює нові загрози для блокування складових системи. Цей процес може розповсюджуватися значними областями СМС і потребує оперативного аналізу та прийняття відповідних рішень для запобігання широкомасштабному поширенню таких процесів. У разі великої швидкості розповсюдження вони можуть перерости у так звані каскадні явища у мережі. Найбільш надійним та ефективним способом протидії таким процесам є резерв альтернативних шляхів руху потоків, іншими словами, ущільнення мережі.

ВИСНОВКИ

Визначення найважливіших з функціонального погляду елементів реальних СМС з безмасштабною структурою є актуальним для удосконалення засобів захисту цих систем від цілеспрямованих атак та інших негативних внутрішніх та зовнішніх впливів. Уведені в роботі поняття параметрів впливу та посеред-

ництва елементів СМС дали можливість розробити сценарії для ідентифікації тих складових системи, блокування яких може призвести до найбільших втрат у процесі її функціонування, а також кількісно оцінювати ці втрати. Проаналізовано чутливість системи до малих змін в об'ємах руху потоків, значення яких є близькими до критичної завантаженості складових СМС. Показано, що критична завантаженість елементів системи може призвести до тих самих наслідків, що й навмисне вилучення їх зі структури мережі або цілеспрямоване блокування процесу функціонування. Отримані результати можуть бути використані для удосконалення наявних та розроблення нових методів захисту реальних мережевих систем від природних та штучних уражень різних типів.

СПИСОК ЛІТЕРАТУРИ

1. Boccaletti S., Latora V., Moreno Y., Chavez M., Hwang D.U. Complex networks: Structure and dynamics. *Physics Reports.* 2006. Vol. 424, N 4. P. 175–308. https://doi.org/10.1016/j.physrep.2005.10.009.
2. Barabási A.-L., Frangos J. Linked: The new science of networks. New York: Basic Books, 2002. 280 p.
3. Bianconi G., Barabási A.-L. Bose-Einstein condensation in complex networks. *Physical Review Letters*. 2001. Vol. 86, N 24. P. 5632–5635. https://doi.org/10.1103/PhysRevLett.86.5632.
4. de Regt R., Apunevych S., von Ferber C., Holovatch Yu., Novosyadlyj B. Network analysis of the COSMOS galaxy field. *Monthly Notices of the Royal Astronomical Society.* 2018. Vol. 477, Iss. 4. P. 4738–4748. https://doi.org/10.1093/mnras/sty801.
5. Dorogovtsev S.N., Mendes J.F.F. Evolution of networks: From biological nets to the Internet and WWW. Oxford: Oxford University Press, 2013. 280 p.
6. Bornholdt S., Schuster H.G. Handbook of graphs and networks: From the genome to the Internet. New York: Jon Wiley & Sons, 2006. 396 p.
7. Caldarelli G., Vespignani A. Large scale structure and dynamics of complex networks: From information technology to finance and natural science. New York: World Scientific, 2007. 251 p.
8. Поліщук О.Д., Яджак М.С. Мережеві структури та системи: I. Потокові характеристики складних мереж. *Системні дослідження та інформаційні технології.* 2018. № 2. С. 42–54. https://doi.org/10.20535/SRIT.2308-8893.2018.2.05.
9. Поліщук Д.О., Поліщук О.Д. Моніторинг потоку транспортних мереж із частково впорядкованим рухом. *Зб. наук. праць XXIII наук.-техн. конф. молодих науковців Фізико-механічного інституту ім. Г. В. Карпенка НАНУ* (23–25 жовтня 2013, Львів). Львів, 2013. С. 326–329.
10. Albert R., Barabási A.-L. Statistical mechanics of complex networks. *Review of Modern Physics*. 2002. Vol. 74, N 1. P. 47–97. https://doi.org/10.1103/RevModPhys.74.47.
11. Головач Ю., Олємской О., фон Фербер К., Головач Т., Мриглод О., Пальчиков В. Складні мережі. *Журнал фізичних досліджень*. 2006. Т. 10, № 4. С. 247–289.
12. Albert R., Jeong H., Barabási A.-L. Error and attack tolerance of complex networks. *Nature*. 2000. Vol. 406. P. 378–482. https://doi.org/10.1038/35019019.
13. Holme P., Kim B.J., Yoon C.N., Han S.K. Attack vulnerability of complex networks. *Physical Review E*. 2002. Vol. 65, Iss. 5. P. 056109-1–056109-14. https://doi.org/10.1103/PhysRevE.65.056109.
14. Guimera R., Mossa S., Tutschi A., Amaral A.N. The worldwide air transportation network: Anomalous centrality, community structure, and cities' global roles. *Proc. Nathional Academy of Sciences of USA*. 2005. Vol. 102, N 22. P. 7794–7799. https://doi.org/10.1073/pnas.0407994102.
15. Збитки від атаки вірусу Petya.A у світі сягають 8 мільярдів доларів. URL: https://www.unian.ua/science/2003241-zbitki-vid-ataki-virusu-petyaa-syagayut-8-milyardiv-dolariv-ekspert.html
16. Freeman L.C. A set of measures of centrality based upon betweenness. *Sociometry*. 1977. Vol. 40, N 1. P. 35–41. https://doi.org/10.2307/3033543.
17. Newman M.E.J. Analysis of weighted networks. *Physical Review* E. 2004. Vol. 70, N 5. P. 056131-1–056131-9. https://doi.org/10.1103/PhysRevE.70.05613.

18. Cao Q., Sirivianos M., Yang X., Pregueiro T. Aiding the detection of fake accounts in large scale social online services. *Proc. 9th USENIX Symposium on Networked Systems Design and Implementation* (April 25–27, 2012, San Jose, CA, USA). San Jose, 2012. P. 197–210.

19. Abokhodair N., Yoo D., McDonald D.W. Dissecting a Social Botnet: Growth, Content and Influence in Twitter. *Proc. 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (March 14–18, 2015, Vancouver, BC, Canada). Vancouver, 2015. P. 839–851.

20. Pastor-Satorras R., Vespignani A. Epidemic spreading in scale-free networks. *Physical Review Letters.* 2001. Vol. 86, N 14. P. 3200–3202. https://doi.org/10.1103/PhysRevLett.86.3200.

21. Поліщук О.Д., Яджак М.С. Мережеві структури та системи: II. Серцевини мереж та мультиплексів. *Системні дослідження та інформаційні технології*. 2018. № 3. С. 38–51. https://doi.org/10.20535/SRIT.2308-8893.2018.3.04.

22. Поліщук Д.О., Поліщук О.Д., Яджак М.С. Комплексне детерміноване оцінювання складних ієрархічно-мережевих систем: I. Опис методики. *Системні дослідження та інформаційні технології*. 2015. № 1. С. 21–31.

23. Поліщук О.Д., Тютюнник М.С., Яджак М.С. Оцінювання якості функціонування складних систем на основі паралельної організації обчислень. *Відбір і обробка інформації*. 2007. Вип. 26 (102). С. 121–126.

Надійшла до редакції 26.03.2019

А.Д. Полищук
ОБ УЯЗВИМОСТИ СЛОЖНЫХ СЕТЕВЫХ СТРУКТУР И СИСТЕМ

Аннотация. Рассмотрены структурный и функциональный подходы к определению уязвимости сложных сетевых структур и систем к негативным внутренним и внешним воздействиям. Введены понятия параметров воздействия и посредничества элементов системы, позволяющие определять важнейшие с функциональной точки зрения узлы и ребра сети и разрабатывать сценарии для идентификации составляющих системы, блокирование которых может привести к наибольшим потерям в процессе ее функционирования, а также количественно оценивать эти потери. Проанализирована чувствительность системы к малым изменениям в объемах движения потоков, значения которых близки к критической загруженности ее составляющих. Полученные результаты могут быть использованы для усовершенствования существующих и разработки новых методов защиты реальных сетевых систем от естественных и штучных воздействий различных типов.

Ключевые слова: сложная сеть, сетевая система, поток, устойчивость, влияние, посредничество.

O.D. Polishchuk
VULNERABILITY OF COMPLEX NETWORK STRUCTURES AND SYSTEMS

Abstract. Structural and functional approaches to the determination of vulnerability of complex network structures and systems to negative internal and external influences are considered. The concept of parameters of influence and betweenness of system elements is introduced, which allows us to identify the most important from the functional point of view nodes and edges of the network and develop scenarios for identifying those components of the system whose blocking can cause greatest losses in the process of its functioning, and also quantify these losses. The sensitivity of the system to small variations in the volume of flow movement, which are close to the critical loading of its components, is analyzed. The obtained results can be used to improve the available methods and develop new ones to protect real network systems from various natural and artificial damages.

Keywords: complex network, network system, flow, stability, influence, betweenness.

Поліщук Олександр Дмитрович,
кандидат фіз.-мат.наук, старший науковий співробітник Інституту прикладних проблем механіки і математики ім. Я.С. Підстригача НАН України, Львів, e-mail: od_polishchuk@ukr.net.