НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК УКРАИНЫ
ИНСТИТУТ ПРОБЛЕМ РЕГИСТРАЦИИ ИНФОРМАЦИИ НАН УКРАИНЫ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И БЕЗОПАСНОСТЬ

МАТЕРИАЛЫ XIX МЕЖДУНАРОДНОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ

ВЫПУСК 19

Киев – 2019

Рекомендовано к печати Ученым советом
Института проблем регистрации информации НАН Украины
(протокол № 3 от 24 декабря 2019 г.)

Информационные технологии и безопасность. Материалы XIX Международной научно-практической конференции ИТБ-2019. – К.: ООО "Инжиниринг", 2019. – 236 с. ISBN 978-966-2344-72-1

В сборник вошли материалы докладов, представленных на XVI Международной научно-практической конференции «Информационные технологии и безопасность» (ИТБ-2019, 28 ноября 2019 года, г. Киев, Украина).

В сборнике представлены статьи, посвященные вопросам безопасности живучести критических инфраструктур, моделирования и противодействия информационным операциям, информационных технологий в управлении, методов и способов информационной поддержки принятия решений, комп'ютерного моделирования систем организационного управления, информационно-аналитических исследований на основе открытых источников информации, сценарного анализа при обеспечения информационной поддержки принятия решений, актуальным проблемам обеспечения информационной и кибернетической безопасности.

Для специалистов в области информационных технологий, информационной безопасности, информационного права а также для аспирантов и студентов старших курсов высшей школы соответствующих специальностей.

ISBN 978-966-2344-72-1

Рисунок 1 – Мережа джерел інформації за тематикою «Формула Штанмайера»

Література

1. Information Operations Recognition. From Nonlinear Analysis to Decision-Making / A. Dodonov, D. Lande, V. Tsyganok, O. Andriichuk, S. Kadenko, A. Graivoronskaya – LAP Lambert Academic Publishing, 2019. - 292 p.
2. Dmytro Lande, Ellina Shnurko-Tabakova. OSINT as a part of cyber defense system // Theoretical and Applied Cybersecurity, 2019. - N. 1. - pp. 103-108.
3. Ландэ Д.В., Снарский А.А. Применение графов горизонтальной видимости в информационной аналитике // CEUR Workshop Proceedings. Selected Papers of the XVII International Scientific and Practical Conference on Information Technologies and Security (ITS 2017) . – С. 86-91.

ПОКАЗНИК РЕЛАКСАЦІЇ В СКЛАДНИХ МЕРЕЖАХ

А.О. Снарський[1,2][0000-0002-4468-4542], Д.В. Ланде[1,2][0000-0003-3945-1178], О.О. Дмитренко [1][0000-0001-8501-5313]

[1]Інститут проблем реєстрації інформації НАН України, Київ, Україна
[2] Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна
dwlande@gmail.com asnarskii@gmail.com dmytrenko.o@gmail.com

Анотація. В роботі досліджуються нові характеристики вузлів мережевих структур – показник релаксації мережі та індивідуальний показник релаксації вузла. Для отримання показника релаксації застосовуються так звані уповільнені ітераційні алгоритми для HITS та PageRank. Встановлено, що на відновлення традиційних показників мережі, після збурення окремих вузлів, впливає її топологія. Як приклад, показник релаксації мережі та індивідуальний показник релаксації вузла були використані для дослідження структури мережі термінів, побудованої для предметної області “Кібербезпека”. Завдяки застосуванню показників релаксації вдалося визначити найбільш важливі змістовні компоненти мережі та ранжувати їх за введеними показниками. Отримане ранжування у порівнянні з ранжуванням за показникамиHITSта PageRank показує унікальністьзапропонованих показника релаксації мережі та індивідуального показника релаксації вузла.

Ключові слова:складна мережа, показник релаксації,індивідуальний показник релаксації,HITS, PageRank, предметна область, мережа термінів.

Вступ

Складні мережі широко поширені у природі. Більшість об'єктів у природі і суспільстві мають бінарні зв'язки, які можна представити у вигляді мережі. Топологічні властивості мереж, що розглядаються абстрактно від їх фізичної природи, але істотно визначають функціонування мереж, становлять предмет дослідження комплексних мереж. У багатьох прикладних галузях та сферах науки і техніки задачі аналізу топології мережі та дослідження особливостей її вузлівмають досить важливе значення.

Вивченням характеристик складних мереж займається область дискретної математики, що має назву теорія складних мереж (від англ. – ComplexNetworks) [1, 2], потужний математичний апарат якої дозволяє досліджувати, зокрема, поведінку окремих об’єктів такихмереж.

Наукові роботи вітчизняних та зарубіжних вчених В. М. Глушкова, В. М. Томашевського, П. Ердоша, А. Рені, М. Е. Дж. Ньюмана, Р. Альберт, А.-Л. Барабаші, Д. Дж. Ваттса, С. Г. Строґаца та інших дослідників внесли суттєвий вклад у розвиток теоретичних основ і практичних рішень для створення методів і засобів дослідження та проектування складних мереж. Пропонуються також нові методи до вирішення обчислювально складних задач, характерних для сучасних мережевих структур [1-3]. Незважаючи на наявність уже існуючих традиційних підходів, дослідження статистичних властивостей, які характеризують поведінку мереж; створення моделі мереж; прогнозування поведінки мереж при зміні структурних властивостей абопід час різних зовнішніх впливах – актуальні завдання теорії складних мереж.

У прикладних дослідженнях зазвичай застосовують типові для мережевого аналізу характеристики вузлів мережі, які описують її певну визначену властивість, найважливішими серед яких на цей час вважають степінь вузла та показники, що відповідають алгоритмам HITS та PageRank. Поруч із вже традиційними показниками мережі таких як HITS та PageRank в даній роботі були запропоновані та досліджені такі нові характеристики як: показник релаксації мережі та індивідуальний показник релаксації вузла.

Метою даної роботи є ввести нові характеристики вузлів складної мережі, визначити їх “фізичний зміст” і показати унікальність серед інших характеристик, а також навести приклади застосування, зокрема у комп’ютерній лінгвістиці.

1. Ітераційні алгоритми HITS та PageRank

1.1. HITS

Алгоритм ранжування *HITS* (HyperlinkInducedTopicSearch), що був запропонований та розроблений в 1998 році Дж. Клейнбергом (J. M. Kleinberg) [4] забезпечує вибір із інформаційного масиву кращих «авторів» (першоджерел, на які посилаються інші документи) та «посередників» (документів, які посилаються на ці першоджерела). Документ буде вважатися хорошим «автором», якщо на нього посилаються хороші «посередники». В свою чергу, хорошими «посередниками» вважаються ті, які містять посилання на цінні першоджерела.

Для кожного документа j обчислюється його важливість як «автора» $a(j)$ і як «посередника» $h(j)$ відповідно до формул:

$$a(j) = \sum_{i \to j} h(i)\,,\ h(j) = \sum_{j \to i} a(i) \qquad (1)$$

В ітераційному представлені наведений вище алгоритм можна записати наступним чином. Нехай **E**–множина всіх направлених ребер у графі, де e_{ij} –направлене ребро з вершини *i*у вершину *j*. Також задані початкові значення важливості документа як «автора» $a_i^{(0)}$ та «посередника» $h_i^{(0)}$. Далі ітераційно обчислюються значення:

$$a_i^{(k)} = \sum_{j:e_{ij} \in E} h_j^{(k-1)},\quad h_i^{(k)} = \sum_{j:e_{ij} \in E} a_j^{(k-1)},\quad k = 1,2,3,... \qquad (2)$$

В матричному вигляді ці рівняння можна записати за допомогою матриці суміжності *L* направленого графа.

$$\mathbf{L} = \begin{cases} 1, & \text{якщо існує ребро з вершини } i \text{ у вершину } j, \\ 0, & \text{в іншому випадку.} \end{cases} \qquad (3)$$

Отримуємо:

$$a^{(k)} = \mathbf{L}^T h^{(k-1)},\quad h^{(k)} = \mathbf{L}a^{(k)}, \qquad (4)$$

де $a^{(k)}$ та $h^{(k)}$–вектори значень важливості як «автора» та «посередника» на кожному ітераційному кроці.

2.2. PageRank

PageRank (Пейдж-ранк) – один з алгоритмів оцінки важливості та ранжирування веб-сторінок за гіперпосиланнями, був створений в Стенфордському університеті ЛарріПейджем і Сергієм Бріном в 1996 році в рамках науково-дослідного проекту про новий вид інформаційно-пошукової системи [5] й вперше використаний в Google.

Для складної мережі, що задається матрицею суміжності $\hat{\mathbf{H}}$, обчислюється $\hat{\mathbf{G}}$:

$$\hat{\mathbf{G}} = \alpha\hat{\mathbf{H}} + [\alpha\bar{\mathbf{a}} + (1-\alpha)\bar{\mathbf{e}}]\frac{1}{n}\bar{\mathbf{e}}^T, \qquad (4)$$

де $a_i = 1$якщо з *i*-го вузла не виходить жодна зв'язок,

та $a_i = 1$– в протилежному випадку;

n – кількість вузлів в мережі;

α – коефіцієнт загасання (зазвичай $\alpha = 0.85$).

Ліві власні значення $\hat{\mathbf{G}}$ і є PageRank мережі.

Незважаючи на відмінності HITS і PageRank, в цих алгоритмах спільним є те, що “авторитетність” (вага) вузла як «автора» залежить від ваги інших вузлів, а “авторитетність” «посередника» залежить від того, наскільки “авторитетними” є вузли, на які він посилається [6, 7].

3. Показник релаксації мережі

В даній роботі пропонуються новіхарактеристикивузлів складної мережі – показник релаксації мережі та індивідуальний показник релаксації вузла, які дозвлдятьранжувати відповідні вузли складної мережі.

Показник релаксації є аналогом часу релаксації Максвелла [8], яка відіграє важливу роль у фізиці твердого тіла.

Час релаксації τ – характерний час, за який "розсмоктується" електричний заряд у середовищі з питомою електричною провідністю σ та діелектричною проникністю ε. В однорідному нескінченному середовищі неоднорідність розподілу електричного заряду нестійка (систему можна вивести з рівноважного стану), з часом заряд "розсмоктується", розподіляється рівномірно в середовищі та уходить на скінченність. Час релаксації Максвелла – τ і є характерним часом переходу середовища в рівноважний стан, де зменшення щільності заряду ρ з часом t має вигляд $\rho(t) \sim e^{-t/\tau}$, де $\tau = \varepsilon/\sigma$.

По аналогії, введемо в складній мережі час релаксації k-го вузла – τ_k. Спочатку визначимо рівноважний стан складної мережі як набір значень вузлів s_k^0 (у векторному виді – $\vec{\mathbf{s}}^0$), які визначаються за певним правилом, наприклад за їх значенням HITS чи PageRank, чи будь-яким іншим [7].

Обчислення $\vec{\mathbf{s}}^0$ відповідно до вибраного правила (ітераційного алгоритму) завжди може бути записане в ітераційному виді:

$$\vec{\mathbf{s}}(n+1) = \vec{\mathbf{s}}(n) + \hat{\mathbf{L}}\vec{\mathbf{s}}(n), \quad n = 0,1,... \qquad (5)$$

де номери компонент вектора $\vec{\mathbf{s}}$ – номери вузлів, $\hat{\mathbf{L}}$ – оператор відповідного ітераційного алгоритму (в нашій роботі розглянуті ітераційні алгоритми, що відповідають HITSта PageRank), $\vec{\mathbf{s}}(0)$ – задані початкові значення вузлів.

$$\vec{\mathbf{s}}^0 = \lim_{n\to\infty} \vec{s}(n), \quad n = 0,1,... \qquad (6)$$

і, звичайно,

$$\hat{\mathbf{L}}\vec{\mathbf{s}}^0 = 0 \ . \qquad (7)$$

Візьмемо тепер величину початкових значень вузлів $\vec{\mathbf{s}}(0)$ у вигляді розв'язку – $\vec{\mathbf{s}}^0$ (будемо вважати ці значення рівноважними) й відхилимо значення, наприклад, m-го вузла:

$$\vec{\mathbf{s}}_i(0) = \vec{\mathbf{s}}_i^0 + \alpha\delta_{im}\vec{\mathbf{s}}_i^0, \qquad (8)$$

де α – величина відхилення (збурення) m-ї компоненти, δ_{ik} – символ Кронекера.

У векторному вигляді – ми відхиляємо від рівноважного стану одну із компонент (проекцій) вектора $\vec{\mathbf{s}}^0$.

Відхилення вектора $\vec{\mathbf{s}}^0$, за рахунок зсуву компоненти, виводить систему з рівноваги.

Тепер (1) для n=0 має вигляд:

$$s_i = s_i(0) + \sum_k L_{ik} s_i(0), \qquad (9)$$

що з урахуванням (4) дає:

$$s_i(1) = s_i(0) + \sum_k L_{ik} s_i^{\,0} + \alpha \sum_k L_{ik}\delta_{km} s_k^0 = s_i^{\,0} + \alpha q_i^{(m)}, \qquad (10)$$

де вектор $q_i^{(m)} = \sum_k L_{ik}\delta_{km} s_k^0$, для кращого наочного сприйняття, запишемо у вигляді

$$q_i^{(m)} = \begin{pmatrix} L_{11} & L_{12} & \dots & L_{1m} & \dots & L_{1N} \\ L_{21} & \dots & \dots & L_{2m} & \dots & L_{2N} \\ \vdots & & & \vdots & & \\ L_{m1} & & & \vdots & & \\ \vdots & & & \vdots & & \\ L_{N1} & & & L_{Nm} & & L_{NN} \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ \vdots \\ s_m^0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} L_{1m} \\ L_{2m} \\ \vdots \\ \vdots \\ \vdots \\ L_{1m} \end{pmatrix} s_m^0. \qquad (11)$$

Для початкової умови $s_i(1)$ (6) $s_i(n)$ при збільшенні nвідповідно до (2) збігається до рівноважного розв'язку $\vec{\mathbf{s}}^0$.

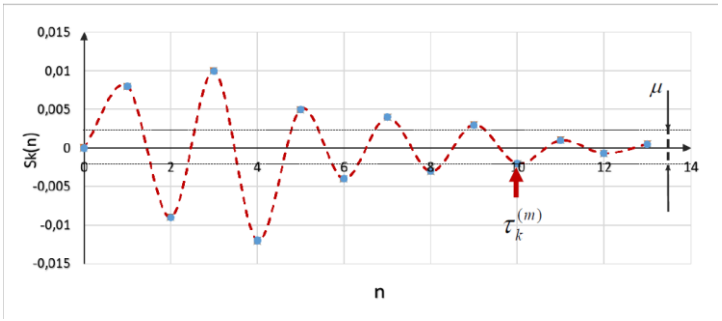

Рис. 1. Схематичне зображення збіжності *k*-го вузла

Вибравши випадок $k \neq m$, початкові значення $s_k(0) = s_k^0$. Починаючи з деякого $n \geq 10$ значення $s_k(n \geq 10)$ стає меншим μ – наперед заданого значення, яке визначає точність збіжності (рис. 1).
Те значення $\tau_k^{(m)}$, при якому для *k*-го вузла виконується умова (при заданому значенні μ)

$$\left| s_k(n \geq \tau_k^{(m)}) \right| \leq \mu, \tag{10}$$

і є показником релаксації *k*-го вузла у випадку збурення *m*-го вузла.
Загалом нас буде цікавити показник релаксації мережі [9] для *m*-го вузла $\max_k(\tau_k^{(m)})$ – найбільше значення $\tau_k^{(m)}$ серед $\forall_k$ при збуренні *m*-го вузла.

Також у роботі паралельно досліджується індивідуальний показник релаксації $\tau_m^{(m)}$, тобто показник релаксації вузла, який і був виведений зі стану рівноваги. В цьому випадку далі будемо користуватись записом τ_m, опустивши верхній символ у $\tau_m^{(m)}$.

4. Дослідження показника релаксації для мережі термінів

Як приклад, показник релаксації мережі та індивідуальний показник релаксації вузла були використані для дослідження структури мережі термінів, побудованої для предметної області "Кібербезпека" (рис. 2).

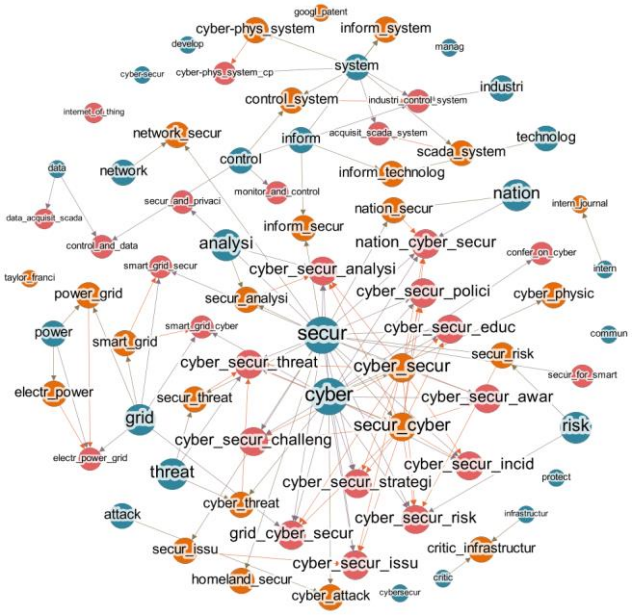

Рис. 2. Мережа термінів, що представляє предметну область "Кібербезпека"

У таблицях 1, 2 представлені топ-20 значень показника релаксаціїмережі та індивідуального показника релаксаціїдля вузлів мережі, отриманих для уповільненого алгоритму HITS та PageRank (коефіцієнт уповільнення рівний 0.9) відповідно (див. Додаток А). Терміни у таблицях відсортовані за спаданням значень показника релаксації мережі. Значення μ було підібрано таким чином, щоб значення показника релаксації мережі для кожного вузла відрізнялись одне від одного якомога

більше: для уповільненого алгоритму HITS було обрано значення 0.001, а для уповільненого алгоритму PageRank – 0.00001.

Таблиця 1.Топ-31 вузол мережі та їх показник релаксації для уповільненого та звичайного алгоритму HITS

Термін	Показник релаксації мережі для звичайного HITS	Показник релаксації мережі для уповільненого HITS	Індивідуальний показник релаксації вузла	HITS
secur	8	107	107	0.0869
cyber	8	104	102	0.0765
cyber_secur	7	99	94	0.0725
secur_cyber	7	99	94	0.0725
grid_cyber_secur	7	94	77	0.0373
cyber_secur_analysi	7	93	76	0.039
cyber_secur_awar	7	93	75	0.039
cyber_secur_challeng	7	93	75	0.039
cyber_secur_educ	7	93	75	0.036
cyber_secur_incid	7	93	75	0.036
cyber_secur_polici	7	93	75	0.036
cyber_secur_risk	7	93	76	0.036
cyber_secur_strategi	7	93	75	0.036
nation_cyber_secur	7	93	76	0.041
cyber_secur_issu	7	92	75	0.036
cyber_secur_threat	7	92	76	0.038
smart_grid_secur	6	78	71	0.0115
inform_secur	6	75	69	0.01042
network_secur	6	75	69	0.01041
smart_grid_cyber	6	75	70	0.0103
grid	6	74	74	0.0076
homeland_secur	6	74	68	0.0102
secur_and_privaci	6	74	68	0.0102
secur_for_smart	6	74	68	0.0102
system	4	74	74	0.0001
confer_on_cyber	6	71	68	0.009
control	4	71	71	0.0001
cyber_attack	6	71	69	0.0091
cyber_physic	6	71	68	0.009
electr_power_grid	3	71	71	0.001
industri_control_system	3	71	71	0.0001

Таблиця 2.Топ-32 вузлів мережі та їх показник релаксації для уповільненого та звичайного алгоритму PageRank

Термін	Показник релаксації мережі для звичайного PageRank	Показник релаксації мережі для уповільненого PageRank	Індивідуальний показник релаксації вузла	PageRank
power	4	75	48	0.0094
threat	4	75	48	0.0094
analysi	4	72	48	0.0094
nation	4	72	48	0.0094
risk	4	72	48	0.0094

control_system	3	66	49	0.01256
cyber_threat	3	66	49	0.01251
electr_power	3	66	49	0.012
industri	3	66	49	0.0094
power_grid	3	66	49	0.0134
secur_threat	3	66	49	0.0124
attack	3	65	49	0.0094
critic	3	65	49	0.0094
cyber-phys_system	3	65	49	0.0105
infrastructur	3	65	49	0.0094
intern	3	65	49	0.0094
nation_secur	3	65	49	0.0137
network	3	65	49	0.0094
scada_system	3	65	49	0.0105
secur_analysi	3	65	49	0.0137
secur_issu	3	65	49	0.0097
secur_risk	3	65	49	0.0137
technolog	3	65	49	0.0094
control	4	63	48	0
grid	4	57	48	0
data	3	56	49	0
smart_grid	3	56	49	0.0512
system	4	54	48	0
cyber_secur_threat	2	51	51	1
electr_power_grid	2	51	51	0.9868
industri_control_system	2	51	51	0.8387

З таблиці 1 та таблиці 2 видно, що по-перше, ранжування вузлів за показником релаксації мережі, яке отримане для звичайних алгоритмів та уповільнених алгоритмів HITS та PageRank,відрізняється:на думку експертів, застосування уповільнених алгоритму HITS та PageRankдає краще ранжування вузлів за показником релаксації мережі. По-друге, ранжування вузлів за показником релаксації мережі в порівнянні з ранжуванням за показником, відповідно,HITS та PageRankзначно відрізняється. А отже, запропонований показник релаксації мережі є унікальною числовою характеристикою вузлів мережі. По-третє, розглянувши числові значення індивідуального показника релаксації вузлів, можна зробити висновок, що він є окремою характеристикою вузлів, яка не подібна до показника релаксації мережі.Відповідно до таблиць 1 та 2 на рис. 2 та рис. 3 зображені порівняльні стовбчасті діаграми, де представленінормовані значення показника релаксації, отриманого для уповільнених алгоритмів HITS та PageRank, та відповідні нормовані показники HITS та PageRank для кожного вузла мережі (вузли відсортовані у порядку зростання їх показника релаксації).

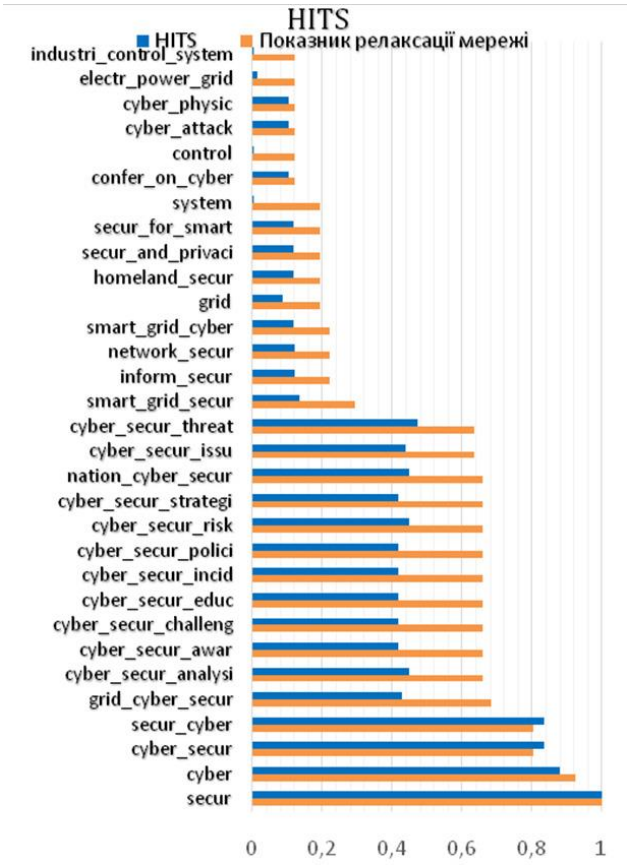

Рис. 2. Стовбчаста діаграманормованогопоказника релаксації, отриманого для уповільненого алгоритму HITS

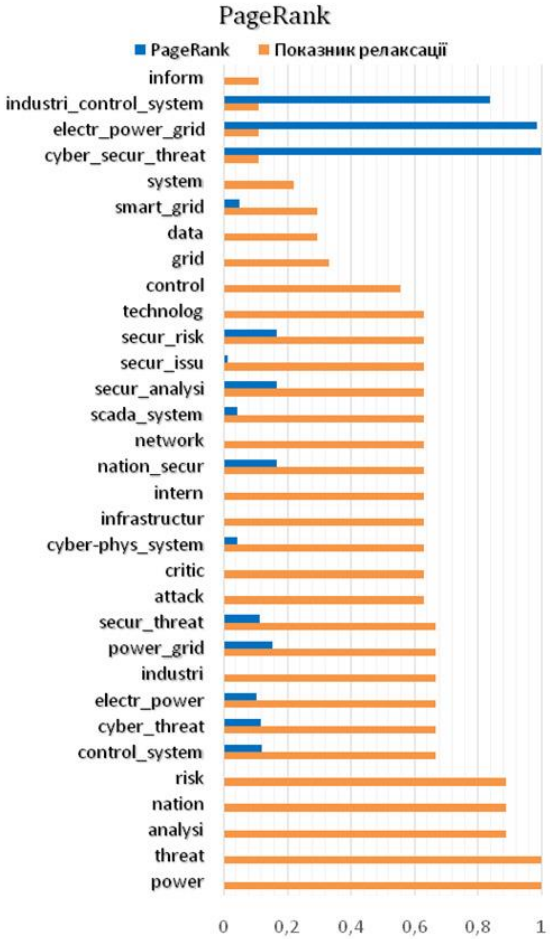

Рис. 3. Стовбчаста діаграма нормованогопоказника релаксації, отриманого для уповільненого алгоритму PageRank

Висновки

В роботі було досліджено нові характеристики вузлів мережевих структур – показник релаксації мережі та індивідуальний показник релаксації вузла.

Було показано, що процес уповільнення алгоритмів впливає на результат обчислення показника релаксації. При цьому ранжування вузлів за показником релаксації у випадку застосування уповільнених алгоритмів HITS та PageRank, на думку експертів, є кращим. Також важливе значення має порогове значення, яке є головною умовою зупинки алгоритму, та від якого залежить показник релаксації. Порогове значення вибиралося таким чином, щоб значення показника релаксації мережі для кожного вузла відрізнялись одне від одного якомога більше, й щоб надалі можна було ранжувативузли за цим показником.

Також було встановлено, що релаксація числових значень деяких вузлів відбувається швидше, ніж релаксація всієї мережі у результаті застосування одного із уповільнених ітераційних алгоритмів (HITS або PageRank). В результаті цього було досліджено так званий індивідуальний показник релаксації вузла.

Показник релаксації мережі та індивідуальний показник релаксації вузла були використані для дослідження структури мережі термінів, побудованої для предметної області “Кібербезпека”. Застосування показників релаксації дало змогуранжувати та визначити найбільш важливі змістовні компоненти мережі.

Отже, запропоновані числові характеристики вузлів мережі можуть бути використані під час дослідження та аналізу структури мережі, даючи змогу виявити найбільш важливі змістовні елементи.

Список використаних джерел

1. Newman, M. E. J.: The structure and function of complex networks. SIAM Review, vol. 45. pp. 167–256. (2003).
2. doi:10.1137/S003614450342480
3. Snarskii, A.,Lande, D.: Modeling of complex networks: tutorial. K.: Engineering, (2015).
4. Dorogovtsev,S.N., Mendes, J.F.: Evolution of networks: from biological networks to the Internet and WWW. Oxford University Press, Oxford (2013).
5. Kleinberg, J. M.: Authoritative sources in a hyperlinked environment. In Processing of ACM-SIAM Symposium on Discrete Algorithms, 46(5), pp. 604–632 (1998).
6. Brin, S., & Page, L.: The anatomy of a large-scale hypertextual web search engine. Computer networks and ISDN systems, 30(1-7), 107-117 (1998).
7. doi:10.1016/S0169-7552(98)00110-X
8. Rajaraman, A., Ullman, J. D.: Mining of massive datasets. Cambridge University Press, Cambridge(2011).
9. doi:10.1017/cbo9781139058452
10. Langville, A. N., Meyer, C. D.: Google's PageRank and beyond: The science of search engine rankings. Princeton University Press, Princeton(2011).
11. Christensen, R.: Theory of viscoelasticity: an introduction. Elsevier(2012).
12. Lande, D.V., Dmytrenko, O.O., Snarskii, A.A.: Research of network relaxation time as characteristics of network nodes. Data Registering, Storing and Processing 21(1), 83-94 (2019) (in Ukrainian).

Додаток А (Уповільнення ітераційних алгоритмів)

Розглянутий вище процес пошуку показника релаксації мережі може бути успішно застосований для розріджених матриць. Проте у випадку, коли вузли мережі мають велику кількість взаємозв’язків, ітераційний процес перерахунку значень вузлів після їх збурення буде швидким. Достатньо велика кількість вхідних та вихідних посилань на вузли спричиняє швидку релаксацію числових значень вузлів мережі. Як наслідок, при дослідженні показника релаксації мережі достатньо лише декілька ітераційних кроків, аби числові значення вузлів повернулись до рівноважного стану після збурення. Для того, щоб уповільнити процес збіжності до рівноважного розв’язку числових значень вузлів після їх збурення, у даній роботі пропонується здійснити уповільнення алгоритмів. Після надання збурення

одному із вузлів мережі, як і у випадку описаному вище, застосовується відповідний ітераційний алгоритм HITS або PageRank з уповільненням:

$$h_0(i) \to h_1(i) \to h_2(i) \to .... \to h_{рівноважне}(i)\ \hat{\mathbf{A}}h_1(i) = h_2(i)$$
$$\hat{\mathbf{A}}h_n(i) = h_{n+1}(i)$$
$$h_{n+1}(i) \longleftarrow\!\!\!\!- \beta h_{n+1}(i)\,,$$

де $0 < \beta < 1-$ коефіцієнт уповільнення.

Таким чином, зменшуючи або збільшуючи числове значення показника “авторитетності” або PageRank вузлів на відповідному ітераційному кроці (уповільнюючи алгоритм), вдається досягти уповільнення релаксаційчислових значень вузлів мережі.

METHODOLOGY OF RATIONAL CHOICE OF SECURITY INCIDENT MANAGEMENT SYSTEM FOR BUILDING OPERATIONAL SECURITY CENTER

Igor Y. Subach, Volodymyr O. Kubrak, Artem V. Mykytiuk

Institute of Special Communications and Information Protection of the National Technical University of Ukraine "Igor Sikorsky Kiev Polytechnic Institute", Ukraine

igor_subach@ukr.net

Abstract. This article discusses the purpose, tasks and composition of the Operational Security Center (SOC). The basic technological tools which should include modern effective SOC are indicated. The focus is on the key role of the Information Security Incident Management System (SIEM) in the SOC. The purpose of SIEM and the main tasks that it should solve are reviewed. The peculiarities of solving the problem of choosing of information security incident management system (SIEM) are analyzed. The groups of indicators that characterize the degree of fulfillment of the requirements to SIEM are highlighted. The application of fuzzy set theory for processing expert information on qualitative indicators characterizing SIEM is proposed. The formulation of the SIEM selection problem is done and the main stages of its solution are proposed: preparation of initial data; choosing the method of solving the multicriteria problem; algorithm development. The method of normalization of SIEM quantitative indicators and the method of paired comparison based on the rank estimates for processing of SIEM qualitative indicators are proposed. It is proposed to use the 9-point Saaty scale to derive functions of SIEM qualitative values based on the processing of expert assessments. The algorithm of the considered method is implemented. Methods for solving multicriteria problems are analyzed and the use of a lexographic method is proposed for solving the SIEM solution for the Security Center (SOC). An algorithm for its implementation has been developed. To illustrate the operation of the proposed algorithm, we give an example of how to apply it to choose a rational SIEM option. Recommendations for application of the results obtained are offered.

Key words: cybersecurity, SIEM, SOC, lexographic method, fuzzy sets theory.

1. Introduction

It is impossible to counteract the modern cyber threats without the use of modern cybersecurity technologies that enable monitoring, collection, collation and processing of information in order to identify existing and predict future threats. Important role is given to the special units that deal with information and cyber security issues at the organizational and technical level – the Security Operation Centers (SOC).

Modern SOC solves the following tasks [1]:

taking immediate actions to protect against cyberattacks and minimize their damage;

identification of system security vulnerabilities and taking actions to eliminate them;

centralized security management of various devices in the system;

continuous monitoring of system threats status;

technical support for cyber security of the system and others.

Structurally, the SOC has three main components: personnel – skilled professionals using modern cybersecurity technologies with teamwork and management competencies; processes – business processes,

СОДЕРЖАНИЕ