КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1354
УДК 004.056

Івкова Валерія Сергіївна
аспірант кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID: 0000-0002-2370-1497
valeriia.s.ivkova@lpnu.ua

Бортнік Леоніл Леонідович
к.т.н., доцент кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID: 0000-0002-6116-7491
leonid.l.bortnik@lpnu.ua

МОДЕЛЬ ОЦІНКИ ВРАЗЛИВОСТІ КОРПОРАТИВНОГО СЕРЕДОВИЩА ДО SOCMINT-АТАК НА ОСНОВІ АНАЛІЗУ ГРАФОВИХ МЕТРИК

Анотація. У статті розроблено та експериментально апробовано метод кількісної оцінки вразливості корпоративного середовища до SOCMINT-атак на основі апарату теорії складних мереж. Актуальність зумовлена стрімким зростанням обсягів відкритих даних соціальних платформ, які дедалі частіше використовуються зловмисниками для пасивної реконструкції внутрішньої організаційної структури підприємства та підготовки високотаргетованих атак соціальної інженерії. Показано, що традиційні підходи до аудиту інформаційної безпеки не забезпечують кількісної формалізації мережевої топології контактів персоналу, що унеможливлює спрямоване виявлення структурно вразливих співробітників. Для розв'язання цієї проблеми формалізовано дворівневу графову модель корпоративного середовища, яка поєднує зважений внутрішній комунікаційний граф службової взаємодії та вектор зовнішньої відкритої експозиції персоналу. Обґрунтовано застосування нормалізованої центральності за посередництвом (betweenness centrality) для виявлення вузлів, що виконують роль структурних «містків» між підрозділами незалежно від ієрархічного рангу. На цій основі розроблено інтегральний мультиплікативний індекс вразливості, який поєднує топологічну видимість вузла з коефіцієнтом функціональної критичності його ролі за аналогією до парадигми ризику «ймовірність × наслідки». Експеримент підтвердив здатність методу виявляти приховані критичні вузли витоку даних. Сформовано комплекс диференційованих рекомендацій Counter-SOCMINT щодо компартменталізації цифрового сліду персоналу, децентралізації внутрішніх потоків та переходу до безперервного моніторингу топологічних ризиків організації.

Ключові слова: OSINT, SOCMINT, кібербезпека, теорія графів, центральність посередництва, соціальна інженерія, Counter-SOCMINT, цифровий слід, компартменталізація

ВСТУП

Розвідка даних на основі відкритих джерел базується на даних, що розміщені в публічному просторі та доступ до яких не обмежено власником або розпорядником інформації. В умовах сьогодення OSINT являє собою стек технологій пошуку інформації з різних джерел, кожне з яких має свої особливості.

Згідно, щоквартального глобального звіту Digital 2026: April Global Statshot Report, який публікується дослідницькою агенцією DataReportal у партнерстві з Meltwater та We Are Social, кількість користувачів соціальних мереж у світі досягла 5,79 мільярда, що еквівалентно 69,9 % населення світу [1].

Згідно з аналітичними оцінками, щоденний обсяг генерації нового цифрового контенту на платформах соціальних медіа сягає 150–200 петабайтів. Така динаміка накопичення мультимодальних даних позиціонує сучасні соціальні мережі як масштабний структурований масив персональної, поведінкової та контекстної інформації про користувачів.

Таким чином, однією з найвагоміших підгазулей OSINT можна вважати SOCMINT. SOCMINT — це спеціалізований напрям інформаційної розвідки, що передбачає системний процес моніторингу, збору, агрегації та аналітичної обробки даних, отриманих із відкритих і закритих сегментів соціальних платформ

із застосуванням як ненав’язливих (пасивний моніторинг, аналіз публічного цифрового сліду та відкритих зв'язків), так і нав'язливих (активна соціальна інженерія, пряма цифрова взаємодія чи використання спеціалізованих інструментів доступу) методів дослідження [2, с. 168], що узгоджується з класичним визначенням SOCMINT, уведеним в академічний обіг Omand, Bartlett та Miller [3].

У контексті корпоративної кібербезпеки інструментарій SOCMINT становить критичну загрозу на етапі попередньої розвідки, згідно даних звіту техніки T1589 за матрицею MITRE ATT&CK [4].

Зловмисники використовують відкриті профілі співробітників, їхні професійні зв'язки, цифрові сліди та взаємні згадки для реконструкції внутрішньої організаційної структури підприємства. Це створює підґрунтя для реалізації високотаргетованих атак соціальної інженерії, зокрема цільового фішингу та компрометації ділового листування [5].

Актуальність цієї загрози підтверджується статистикою: за даними щорічного звіту Verizon, людський фактор (соціальна інженерія, фішинг, скомпрометовані облікові дані) фігурував у 62 % підтверджених витоків даних у світі [6].

Водночас уразливість організації до таких загроз розподілена вкрай нерівномірно. Окремі посадові особи через характер своєї професійної діяльності або комунікаційні патерни виступають інформаційним сполученням між різними структурними підрозділами. Їхня висока публічна відкритість у поєднанні з доступом до конфіденційних ресурсів робить їх першочерговими цілями для зловмисників. Традиційні підходи до оцінки кіберзагроз переважно зосереджені на захисті апаратно-програмного периметра або якісному аналізі людського фактора, не забезпечуючи кількісної формалізації та топологічної оцінки каналів потенційного витоку даних.

Постановка проблеми. Автоматизація процесів збору відкритої розвідки суттєво розширює поверхню атак соціальної інженерії організації, уможливлюючи пасивну реконструкцію внутрішньої структури персоналу [7]. Проте, як зазначають Pastor-Galindo et al., наявні підходи до аналізу OSINT/SOCMINT-загроз переважно зосереджені на накопиченні первинних атрибутів і не забезпечують кількісної оцінки непрямих реляційних зв'язків між співробітниками [8]. Водночас традиційний аудит інформаційної безпеки не враховує мережеву топологію контактів: дослідження виявлення ключових акторів свідчать, що інформаційна експозиція визначається саме структурним положенням суб'єкта в системі комунікацій [9].

Відсутність формалізованих моделей для кількісної оцінки структурно вразливих вузлів унеможливлює здійснення спрямованого аудиту та впровадження превентивних механізмів захисту (Counter-SOCMINT). Розв'язання цієї науково-прикладної проблеми полягає в моделюванні відкритого комунікаційного простору компанії у вигляді зваженого графа, де інтеграція метрик центральності та функціональної критичності ролей дозволяє виявити приховані канали потенційного витоку даних.

Аналіз останніх досліджень і публікацій.

Питання формалізованої оцінки вразливості організацій до атак, що спираються на дані відкритих джерел, розглядається в науковій літературі за кількома взаємопов'язаними напрямами.

Перший напрям об'єднує роботи, присвячені прикладному застосуванню OSINT-інструментарію для аудиту безпеки підприємства. Так, Hayes та Capra на прикладі підприємства критичної інфраструктури електроенергетичного сектору США продемонстрували, що засоби OSINT дозволяють скласти детальний профіль апаратно-програмного забезпечення компанії та її ключового IT-персоналу, проте запропонована ними методика обмежується переліком виявлених вразливих артефактів і не передбачає кількісного ранжування персоналу за рівнем інформаційної експозиції [10]. Практичну здійсненність такої автоматизованої експлуатації відкритих даних соціальних мереж ще раніше продемонстрували Bilge et al., які показали можливість масового клонування профілів користувачів і розсилки запитів у контакти жертви для збору додаткової конфіденційної інформації [11]. Подібні висновки повторюються й у роботі Edwards et al. [7] та оглядовому дослідженні Pastor-Galindo et al. [8], де констатується розрив між масовим накопиченням первинних атрибутів (профілів, публікацій, метаданих) і відсутністю моделей, здатних формалізувати структурні взаємозв'язки між співробітниками.

Другий напрям формують дослідження в галузі теорії графів та аналізу соціальних мереж, орієнтовані на кількісне визначення значущості вузла в мережі. Класичну основу цього напряму заклав Freeman, який запропонував міру центральності за посередництвом (betweenness centrality) для виявлення вузлів, що контролюють потоки інформації між іншими учасниками мережі [12]. Розвиваючи цей підхід стосовно задач кібербезпеки, Fire, Goldschmidt та Elovici показали, що обчислювальні методи виявлення ключових акторів у соціальних мережах дозволяють ідентифікувати користувачів з аномально високою центральністю ще до того, як вони стануть об'єктом цілеспрямованої атаки [9]. Емпіричним підтвердженням значущості таких «місткових» вузлів є масштабне дослідження Ho et al., які на вибірці понад 113 мільйонів корпоративних листів показали, що зловмисники цілеспрямовано використовують скомпрометовані облікові записи співробітників з високим рівнем внутрішньої довіри для проведення

латерального фішингу всередині організації [13]. Водночас переважна більшість подібних досліджень зосереджена на топології мережі як такій, залишаючи поза увагою функціональну роль вузла та рівень його доступу до конфіденційних ресурсів організації.

Третій напрям — моделювання внутрішньоорганізаційних взаємодій для оцінки інсайдерських загроз. Зокрема, Sepehrzadeh запропонував підхід до моделювання взаємодій між співробітниками у вигляді орієнтованого графа, параметризованого індивідуальними показниками загрози, що дозволяє оцінити поширення впливу потенційно небезпечної поведінки одного співробітника на інших [14]. Цей підхід демонструє продуктивність графового моделювання для формалізації людського фактора, проте орієнтований на внутрішні, закриті канали корпоративної комунікації і не враховує зовнішню, публічно доступну складову комунікаційного профілю співробітника, яка є основним джерелом даних для SOCMINT-розвідки.

Отже, проведений аналіз свідчить, що: OSINT/SOCMINT-орієнтовані роботи здебільшого обмежуються якісним описом загроз без кількісної формалізації [8], [9], 12]; графові методи аналізу центральності добре розроблені на рівні загальної теорії мереж [9], [12], проте не адаптовані до специфіки корпоративного середовища, а моделі оцінки інсайдерських загроз [14] враховують внутрішню організаційну структуру, але ігнорують зовнішню, відкриту експозицію співробітників. Це підтверджує наявність наукової прогалини на перетині зазначених напрямів і обумовлює необхідність розробки інтегрального підходу, що поєднує топологічні метрики центральності з функціональною критичністю ролі співробітника для формалізованої оцінки вразливості корпоративного середовища до SOCMINT-атак.

Метою статті є розробка та експериментальна апробація методу оцінки вразливості корпоративного середовища до SOCMINT-атак на основі аналізу топологічних графових метрик центральності та функціональної критичності співробітників для формування превентивних механізмів захисту.

Завдання дослідження:

1. Формалізувати модель корпоративного середовища у вигляді зваженого графа відкритих взаємодій та інформаційних зв'язків;
2. Обґрунтувати вибір графових метрик центральності для кількісної оцінки зовнішньої експозиції та внутрішнього комунікаційного посередництва вузлів;
3. Розробити інтегральний індекс вразливості до SOCMINT-атак, що враховує топологічне положення співробітника та коефіцієнт функціональної критичності його ролі;
4. Провести програмний експеримент на модельному корпоративному графі для верифікації методу та виявлення прихованих критичних вузлів витоку даних;
5. Сформулювати комплекс техніко-організаційних рекомендацій щодо зниження ідентифікованості та розриву критичних зв'язків у відкритих джерелах.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Формалізація графової моделі корпоративного середовища.

Корпоративне середовище формалізовано у вигляді дворівневої графової моделі, що складається з внутрішнього та зовнішнього периметру.

Внутрішній рівень представлено зваженим неорієнтованим графом:

$$G_{int} = (V, E, w) \tag{1}$$

де $V = \{v_1, v_2, \dots, v_n\}$ — множина вершин ($|V| = n$), що відповідає співробітникам організації; $E \subseteq V \times V$ множина неорієнтованих ребер $e_{ij} = (v_i, v_j)$, які відображають верифіковані канали службової комунікації (адміністративне підпорядкування, спільна проєктна діяльність, регулярний документообіг), тощо; $w: E \to \mathbb{R}^+$ — вагова функція, що визначає інтенсивність (частоту) службової взаємодії між суб'єктами.

Зовнішній рівень моделюється вектором експозиції відкритої присутності:

$$\mathrm{E}_{ext} = [\mathrm{E}_{ext}(v_1), \mathrm{E}_{ext}(v_2), \dots, \mathrm{E}_{ext}(v_n)]^T, \quad \mathrm{E}_{ext}(v_i) \in \mathbb{R}^+ \cup \{0\} \tag{2}$$

де кожна компонента $\mathrm{E}_{ext}(v)$ є кількісною агрегованою оцінкою цифрового сліду співробітника у відкритих джерелах (кількість публічних зв'язків у соціальних мережах, цитування та згадки в інтернет-ресурсах, виступи на конференціях тощо), зібраних засобами пасивного моніторингу.

Для кількісної оцінки функціональної критичності ролей кожному вузлу $v \in V$ поставлено у відповідність коефіцієнт $\kappa(v) \in [0,1]$, що визначається на основі корпоративної матриці розмежування доступу та посадових інструкцій і відображає рівень доступу співробітника до конфіденційних та критичних інформаційних активів, таких як фінансові, технічні, кадрові чи юридичні дані.

Обгрунтування вибору графових метрик центральності.

Для приведення різнорідних параметрів до порівнянного безрозмірного вигляду здійснюється їхня нормалізація на множині V

Показник нормалізованої зовнішньої експозиції співробітника визначається як:

$$\hat{C}_{ext}(v) = \frac{E_{ext}(v)}{max_{u \in V} E_{ext}(u)} \quad \hat{C}_{ext}(v) \in [0,1] \tag{3}$$

що відображає відносну видимість цифрового сліду вузла для зловмисника на етапі пасивної розвідки.

Для оцінки внутрішнього комунікаційного посередництва обрано міру центральності за посередництвом (betweenness centrality):

$$C_{bet}(v) = \sum_{s \neq v \neq t \in V} \frac{\sigma_{st}(v)}{\sigma_{st}} \tag{4}$$

де σ_{st} - загальна кількість найкоротших шляхів між вершинами s та t у зваженому графі G_{int} розрахованих з урахуванням комунікаційної відстані $d(u,v) = \frac{1}{w(u,v)}$; $\sigma_{st}(v)$ — кількість найкоротших шляхів між s і t, які проходять через проміжну вершину v.

Вибір саме цієї метрики (а не міри ступеня, близькості чи власного вектора) обумовлений її здатністю виявляти вузли, що виконують роль «містків» між структурно відокремленими підрозділами, незалежно від їхнього ієрархічного рангу [10].

Саме такі вузли становлять цінність для зловмисника, оскільки їх компрометація забезпечує латеральний рух інформації між відділами та підвищує правдоподібність соціоінженерних претекстів. Міра ступеня, на відміну від посередництва, відображає лише локальну кількість зв'язків і не враховує структурного положення вузла в мережі загалом; міра близькості передбачає високу зв'язність графа і менш придатна для типово сегментованих (силосних) організаційних структур; центральність за власним вектором схильна надавати перевагу вузлам, пов'язаним із вже центральними вузлами, що дублює ефект ієрархічної належності. Тому для внутрішнього рівня моделі використано нормалізовану центральність за посередництвом, яка обчислюється як:

$$\hat{C}_{bet}(v) = \frac{C_{bet}(v)}{max_{u \in V} C_{bet}(u)} \quad \hat{C}_{bet}(v) \in [0,1] \tag{5}$$

Інтегральний індекс вразливості до SOCMINT-атак.

На основі нормалізованих метрик сформовано узагальнений показник топологічної видимості вузла $T(v)$:

$$T(v) = \alpha \cdot \hat{C}_{ext}(v) + \beta \cdot \hat{C}_{bet}(v),\ \alpha, \beta \geq 0,\ \alpha + \beta = 1 \tag{6}$$

де вагові коефіцієнти α і β визначають відносний пріоритет зовнішньої експозиції та внутрішнього комунікаційного посередництва відповідно до політики безпеки та моделі загроз організації. У базовій конфігурації моделі прийнято $\alpha = \beta = 0{,}5$ (рівнозначний внесок), проте значення можуть уточнюватися методом попарних порівнянь (AHP) для конкретного підприємства.

Підсумковий інтегральний індекс вразливості суб'єкта до SOCMINT-атак $IV(v)$ формалізовано на основі мультиплікативної парадигми ризику («ймовірність вибору цілі × потенційні збитки») що узгоджується із загальновизнаною методологією оцінки ризиків інформаційної безпеки [15]:

$$IV(v) = T(v) \times \kappa(v), \qquad IV(v) \in [0,1] \tag{7}$$

де $T(v)$ виступає мірою ймовірності ідентифікації та таргетингу співробітника під час SOCMINT-розвідки, (топологічну «видимість» вузла), а $\kappa(v)$ — вагою критичності несанкціонованого доступу до його активів, зумовлену функціональною критичністю ролі.

Мультиплікативна структура забезпечує коректну поведінку моделі на межових значеннях: вузол із високою експозицією, але нульовим доступом до критичних ресурсів (наприклад, суто представницька роль), отримує низький індекс вразливості, і навпаки — вузол із високим рівнем доступу, але практично відсутньою публічною видимістю, залишається малопомітним для типової SOCMINT-розвідки, що й підтверджено результатами програмного експерименту.

Програмна верифікація моделі на модельному корпоративному графі.

Для верифікації розробленого методу здійснено програмну імплементацію середовища аналізу (Python, бібліотека NetworkX) та побудовано модельний корпоративний граф, що охоплює 15 співробітників у межах 7 функціональних підрозділів (виконавче керівництво, бухгалтерія, кадри, служба IT-безпеки, комерційний відділ, юридичний відділ, маркетинг/PR). Внутрішні зв'язки графа відображають типову організаційну взаємодію, а показники зовнішньої експозиції — узагальнені (симульовані на основі емпіричних спостережень) значення публічної присутності відповідних посад у відкритих джерелах.Службові взаємодії G_{int} та показники публічного сліду E_{ext} параметризовано згідно з типовими профілями організаційної активності.

Службові взаємодії G_{int}та розподіл інтегрального індексу вразливості $IV(v)$ для модельованої структури підприємства представлено на рис. 1

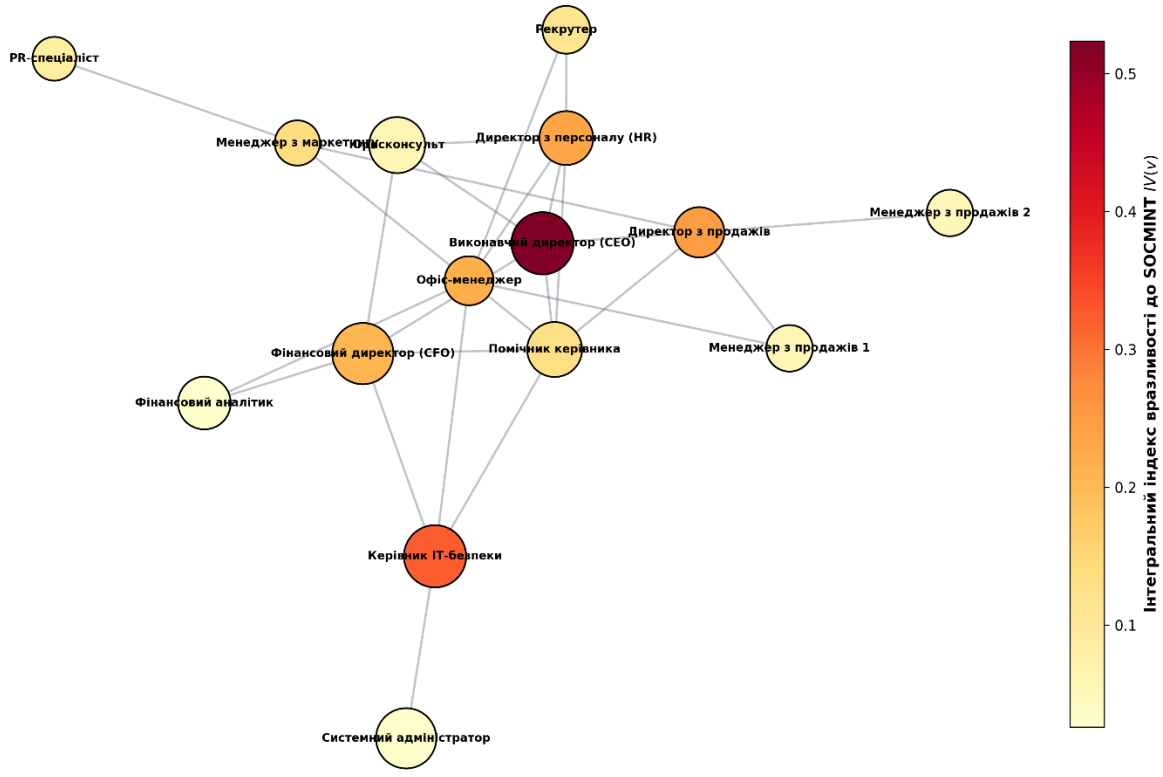

Рис. 1, Топологія графа з тепловою картою вразливості $IV(v)$

Результати обчислення метрик та інтегрального індексу вразливості (за $\alpha = \beta = 0{,}5$) наведено в таблиці 1.

Таблиця 1

Результати обчислення графових метрик та інтегрального індексу вразливості для модельного корпоративного графа (рейтинг за спаданням IV(v))

Посада	$\hat{C}_{ext}(v)$	$\hat{C}_{bet}(v)$	$T(v)$	$\kappa(v)$	$IV(v)$
Виконавчий директор (CEO)	1,000	0,047	0,524	1,00	0,524
Керівник IT-безпеки	0,158	0,488	0,323	1,00	0,323
Директор з продажів	0,737	0,370	0,553	0,45	0,249
Директор з персоналу (HR)	0,526	0,260	0,393	0,60	0,236
Офіс-менеджер	0,074	1,000	0,537	0,40	0,215
Фінансовий директор (CFO)	0,337	0,094	0,216	0,95	0,205
Менеджер з маркетингу	0,642	0,449	0,545	0,25	0,136
Помічник керівника	0,189	0,213	0,201	0,65	0,131
Рекрутер	0,653	0,000	0,326	0,35	0,114
PR-спеціаліст	0,874	0,000	0,437	0,20	0,087
Менеджер з продажів 1	0,400	0,000	0,200	0,30	0,060
Юрисконсульт	0,147	0,024	0,085	0,70	0,060
Менеджер з продажів 2	0,358	0,000	0,179	0,30	0,054
Системний адміністратор	0,063	0,000	0,032	0,90	0,028
Фінансовий аналітик	0,095	0,000	0,047	0,55	0,026

Отримані результати підтверджують працездатність запропонованого підходу. Найвищий індекс вразливості (IV = 0,524) закономірно демонструє виконавчий директор, що поєднує максимальну зовнішню експозицію з граничним значенням функціональної критичності (κ = 1,00) — цей результат слугує перевіркою адекватності моделі на очікуваному (базовому) випадку.

Водночас показовим є те, що другу позицію посідає керівник IT-безпеки (IV = 0,323): попри відносно низьку зовнішню експозицію ($\hat{C}_{ext}$ = 0,158), його граничний рівень доступу до критичних систем (к = 1,00) у поєднанні з істотним внутрішнім посередництвом ($\hat{C}_{bet}$= 0,488) виводить цей вузол у число пріоритетних об'єктів захисту — статус, який традиційний аудит, орієнтований на публічну видимість, істотно недооцінив би.

Найбільш промовистим результатом експерименту є позиція офіс-менеджера: маючи мінімальну зовнішню експозицію ($\hat{C}_{ext}$ = 0,074, передостаннє місце в організації) та середній рівень функціональної критичності (к = 0,40), цей вузол демонструє максимальне в усьому графі значення центральності за посередництвом ($\hat{C}_{bet}$ = 1,000), оскільки де-факто координує інформаційні потоки між шістьма з семи підрозділів. У результаті інтегральний індекс виводить офіс-менеджера на 5-ту позицію рейтингу вразливості — вузол, який жодна методика оцінки на основі самої лише публічної видимості (традиційний SOCMINT-аудит) не змогла б виявити як пріоритетний.

Обернену картину демонструє PR-спеціаліст: маючи одну з найвищих зовнішніх експозицій у вибірці ($\hat{C}_{ext}$ = 0,874), унаслідок мінімальної функціональної критичності (κ = 0,20) він отримує один із найнижчих інтегральних індексів (IV = 0,087, 10-та позиція). Цей випадок ілюструє систематичну похибку методів, що ототожнюють публічну видимість співробітника з реальним рівнем вразливості організації.

Таким чином, експериментальна верифікація підтверджує сформульовану в постановці проблеми гіпотезу: інтеграція топологічного положення вузла з коефіцієнтом функціональної критичності дозволяє виявляти приховані канали потенційного витоку даних, що залишаються поза увагою підходів, орієнтованих виключно на аналіз відкритої публічної присутності персоналу.

Техніко-організаційні рекомендації щодо зниження ідентифікованості критичних вузлів (Counter-SOCMINT).

На основі отриманого рейтингу вразливості сформульовано комплекс техніко-організаційних заходів, диференційованих за рівнем інтегрального індексу вразливості суб'єкта($IV(v)$):

– для співробітників із високим інтегральним індексом вразливості обмежити деталізацію посадової інформації та схем підпорядкування, що публікуються в загальнодоступних профілях і на сайті компанії;

– перерозподілити функції міжвідділового посередництва (типові для помічників керівника та офіс-менеджерів) між кількома співробітниками почергово, що знижує централізацію інформаційних потоків навколо єдиного вузла та зменшує його показник нормалізованої центральності за посередництвом ($\hat{C}_{bet}(v)$);

– запровадити цільове навчання з кібергігієни та розпізнавання соціоінженерних атак саме для співробітників із верхніх позицій рейтингу інтегрального індексу вразливості суб'єкта ($IV(v)$), оскільки поєднання доступності та критичності робить їх пріоритетною ціллю;

– обмежити публічне розкриття технологічного стеку та інструментів захисту, використовуючи узагальнені формулювання посад у відкритих джерелах;

– запровадити періодичний (не рідше ніж раз на квартал) перерахунок індексу вразливості з урахуванням кадрових змін та оновленої мережі комунікацій, перетворюючи одноразовий аудит на безперервний процес управління вразливістю (continuous Counter-SOCMINT monitoring);

– для вузлів із найвищим коефіцієнт функціональної критичності ролі ($\kappa(v)$) розглянути впровадження honeytoken-профілів і моніторингу згадувань у відкритих джерелах як засобу раннього виявлення цілеспрямованої розвідувальної активності;

- реалізувати концепцію компартменталізації інформаційного сліду співробітників, яка передбачає розрив публічних зв'язків між критичними функціональними підрозділами та відкритими представницькими контурами організації [16].

Викладені результати в комплексі забезпечують досягнення сформульованої мети дослідження — створення методу оцінки вразливості корпоративного середовища до SOCMINT-атак, придатного для практичного впровадження в межах превентивних механізмів захисту (Counter-SOCMINT).

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У ході проведеного дослідження повністю виконано поставлені науково-практичні завдання та досягнуто визначену мету щодо побудови й апробації методу оцінки вразливості корпоративного середовища до SOCMINT-атак.

Формалізація корпоративного комунікаційного середовища у вигляді дворівневої графової моделі уможливила інтеграцію структури внутрішньої службової взаємодії та кількісних параметрів зовнішньої відкритої експозиції співробітників у публічному просторі. Теоретично обґрунтовано доцільність застосування метрики центральності за посередництвом, яка довела свою ефективність для кількісної ідентифікації прихованих структурних «містків» між сегментованими підрозділами, що становлять пріоритетний інтерес для зловмисників під час підготовки цільових соціоінженерних атак.

Розроблений мультиплікативний інтегральний індекс вразливості забезпечив збалансоване поєднання показника топологічної видимості вузла з коефіцієнтом функціональної критичності його ролі, усунувши методологічну похибку традиційних аудитів безпеки. Програмний експеримент на модельному корпоративному графі підтвердив високу селективність методу та виявив критичні вузли з низькою публічністю, але максимальним комунікаційним посередництвом.

На основі отриманих результатів сформовано комплекс диференційованих техніко-організаційних рекомендацій Counter-SOCMINT, спрямованих на децентралізацію внутрішніх інформаційних потоків, компартменталізацію цифрового сліду персоналу та перехід до безперервного моніторингу топологічних ризиків організації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kemp, S. (2026). Global social media statistics. DataReportal. https://datareportal.com/social-media-users
2. Івкова, В., & Опірський, І. (2025). OSINT-ТЕХНОЛОГІЇ ЯК ЗАГРОЗА КІБЕРБЕЗПЕЦІ ДЕРЖАВИ. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *3*(27), 165–179. https://doi.org/10.28925/2663-4023.2025.27.749

3. Omand, D., Bartlett, J., & Miller, C. (2012). Introducing Social Media Intelligence (SOCMINT). *Intelligence and National Security*, 27(6), 801–823. https://doi.org/10.1080/02684527.2012.716965
4. MITRE ATT&CK. (2020). *Gather victim identity information (Technique T1589)*. MITRE Corporation. https://attack.mitre.org/techniques/T1589/
5. Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, 22, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005
6. Verizon Business. (2026). *2026 Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/dbir/
7. Edwards, M., Larson, R., Green, B., Rashid, A., & Baron, A. (2017). Panning for gold: Automatically analysing online social engineering attack surfaces. *Computers & Security*, 69, 18–34. https://doi.org/10.1016/j.cose.2016.12.013
8. Pastor-Galindo, J., Nespoli, P., Gomez Marmol, F., & Martinez Perez, G. (2020). The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends. *IEEE Access*, 8, 10282–10304. https://doi.org/10.1109/access.2020.2965257
9. Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Computationally identifying key actors in online social networks. *Computers in Human Behavior*, 40, 1–13. https://doi.org/10.1016/j.chb.2014.07.039
10. Hayes, D. R., & Cappa, F. (2018). Open-source intelligence for risk assessment. *Business Horizons*, 61(5), 689–697. https://doi.org/10.1016/j.bushor.2018.02.001
11. Bilge, L., Strufe, T., Balzarotti, D., & Kirda, E. (2009). All your contacts are belong to us: Automated identity theft attacks on social networks. In *Proceedings of the 18th International Conference on World Wide Web (WWW '09)* (pp. 551–560). ACM. https://doi.org/10.1145/1526709.1526784
12. Freeman, L. C. (1977). A set of measures of centrality based on betweenness. *Sociometry*, 40(1), 35–41. https://doi.org/10.2307/3033543
13. Ho, G., Cidon, A., Gavish, L., Schweighauser, M., Paxson, V., Savage, S., Voelker, G. M., & Wagner, D. (2019). Detecting and characterizing lateral phishing at scale. In *Proceedings of the 28th USENIX Security Symposium* (pp. 1273–1290). USENIX Association. https://www.usenix.org/system/files/sec19-ho.pdf
14. Sepehrzadeh, H. (2023). A method for insider threat assessment by modeling the internal employee interactions. *International Journal of Information Security*, 22(5), 1385–1393. https://doi.org/10.1007/s10207-023-00697-9
15. Joint Task Force Transformation Initiative. (2012). *Guide for Conducting Risk Assessments* (NIST Special Publication 800-30, Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30r1
16. Івкова В.С. & Опірський, І. (2025). Дослідження можливості інтеграції методу компартменталізації у захист інформації у відкритих джерелах. *Computer Systems and Networks*, 7(2), 71–83 https://doi.org/10.23939/csn2025.02.071

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023

Valeriia Ivkova
Postgraduate Student, Department of Information Protection
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0000-0002-2370-1497
valeriia.s.ivkova@lpnu.ua

Leonid Bortnik
Candidate of Technical Sciences, Associate Professor, Department of Information Protection
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0000-0002-6116-7491
leonid.l.bortnik@lpnu.ua

MODEL FOR ASSESSING CORPORATE ENVIRONMENT VULNERABILITY TO SOCMINT ATTACKS BASED ON GRAPH METRICS ANALYSIS

Abstract. The article develops and experimentally validates a method for the quantitative assessment of corporate environment vulnerability to SOCMINT attacks based on the apparatus of complex network theory. The relevance of the study is driven by the rapid growth in the volume of open data on social platforms, which is increasingly exploited by attackers to passively reconstruct an enterprise's internal organizational structure and prepare highly targeted social engineering attacks. It is shown that traditional information security audit approaches fail to provide a quantitative formalization of the personnel contact network topology, which precludes the targeted identification of structurally vulnerable employees. To address this problem, a two-level graph model of the corporate environment is formalized, combining a weighted internal communication graph of official interactions with a vector of employees' external open exposure. The use of normalized betweenness centrality is justified for identifying nodes that act as structural "bridges" between departments regardless of their hierarchical rank. On this basis, an integral multiplicative vulnerability index is developed, combining the topological visibility of a node with a coefficient of the functional criticality of its role, by analogy with the classical risk paradigm "probability × consequences". The experiment confirmed the method's ability to reveal hidden critical data-leakage nodes. A set of differentiated Counter-SOCMINT recommendations has been formulated regarding the compartmentalization of personnel digital footprints, the decentralization of internal information flows, and the transition to continuous monitoring of the organization's topological risks.

Keywords: OSINT, SOCMINT, cybersecurity, graph theory, betweenness centrality, social engineering, Counter-SOCMINT, digital footprint, compartmentalization

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Kemp, S. (2026). Global social media statistics. DataReportal. https://datareportal.com/social-media-users
2. Ivkova, V., & Opirsky, I. (2025). OSINT TECHNOLOGIES AS A THREAT TO STATE CYBERSECURITY. *Electronic professional scientific publication "Cybersecurity: Education, Science, Technology"*, 3(27), 165–179.. https://doi.org/10.28925/2663-4023.2025.27.749
3. Omand, D., Bartlett, J., & Miller, C. (2012). Introducing Social Media Intelligence (SOCMINT). *Intelligence and National Security*, 27(6), 801–823. https://doi.org/10.1080/02684527.2012.716965
4. MITRE ATT&CK. (2020). *Gather victim identity information (Technique T1589)*. MITRE Corporation. https://attack.mitre.org/techniques/T1589/
5. Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, 22, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005
6. Verizon Business. (2026). *2026 Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/dbir/
7. Edwards, M., Larson, R., Green, B., Rashid, A., & Baron, A. (2017). Panning for gold: Automatically analysing online social engineering attack surfaces. *Computers & Security*, 69, 18–34. https://doi.org/10.1016/j.cose.2016.12.013
8. Pastor-Galindo, J., Nespoli, P., Gomez Marmol, F., & Martinez Perez, G. (2020). The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends. *IEEE Access*, 8, 10282–10304. https://doi.org/10.1109/access.2020.2965257

9. Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Computationally identifying key actors in online social networks. *Computers in Human Behavior*, 40, 1–13. https://doi.org/10.1016/j.chb.2014.07.039
10. Hayes, D. R., & Cappa, F. (2018). Open-source intelligence for risk assessment. *Business Horizons*, 61(5), 689–697. https://doi.org/10.1016/j.bushor.2018.02.001
11. Bilge, L., Strufe, T., Balzarotti, D., & Kirda, E. (2009). All your contacts are belong to us: Automated identity theft attacks on social networks. In *Proceedings of the 18th International Conference on World Wide Web (WWW '09)* (pp. 551–560). ACM. https://doi.org/10.1145/1526709.1526784
12. Freeman, L. C. (1977). A set of measures of centrality based on betweenness. *Sociometry*, 40(1), 35–41. https://doi.org/10.2307/3033543
13. Ho, G., Cidon, A., Gavish, L., Schweighauser, M., Paxson, V., Savage, S., Voelker, G. M., & Wagner, D. (2019). Detecting and characterizing lateral phishing at scale. In *Proceedings of the 28th USENIX Security Symposium* (pp. 1273–1290). USENIX Association. https://www.usenix.org/system/files/sec19-ho.pdf
14. Sepehrzadeh, H. (2023). A method for insider threat assessment by modeling the internal employee interactions. *International Journal of Information Security*, 22(5), 1385–1393. https://doi.org/10.1007/s10207-023-00697-9
15. Joint Task Force Transformation Initiative. (2012). *Guide for Conducting Risk Assessments* (NIST Special Publication 800-30, Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30r1
16. Ivkova, V., & Opirsky, I. (2025). Investigation of the possibility of integrating the compartmentalization method into the protection of information in open sources. *Computer systems and network*. 2025. Vol. 7, No. 2. P. 71–83. URL: https://doi.org/10.23939/csn2025.02.071

Отримано редакцією журналу / Received: 12.02.26
Прорецензовано / Revised: 26.02.26
Схвалено до друку / Accepted: 24.09.26