

Оцінювання наслідків ураження складних мережевих систем

Дмитро Поліщук

Кандидат технічних наук, Інститут прикладних проблем механіки і математики ім. Я.С. Підстригача НАН України, 79060, Україна, Львів, вул. Наукова 3 «б», e-mail: do.polishchuk@gmail.com

В роботі аналізуються негативні впливи, які можуть пошкодити структуру та дестабілізувати процес функціонування складної мережевої системи (МС). Розглядаються три основні етапи потенційного впливу: аналіз загроз та забезпечення ефективного захисту системи; організація протидії поширенню впливу складною мережею та оцінювання наслідків ураження і відновлення МС. На підставі структурної та потокової моделей мережевої системи розроблені методи об'єктивного аналізу наслідків дії негативного впливу, спрямованих на розроблення дієвих стратегій її повернення до нормального функціонування. Ефективність пропонованого підходу ілюструється на прикладах транспортних систем України різних типів.

Ключові слова: складна мережа, мережева система, уразливість, відновлюваність, цілеспрямована атака, нецільове ураження, оцінювання наслідків.

Вступ. На кожную реальну складну систему можуть діяти негативні впливи різного походження [1]. Протягом останніх років ми стали свідками багатьох таких впливів: епідемії небезпечних інфекційних захворювань та військові конфлікти, терористичні та хакерські атаки, землетруси та цунамі, фінансові кризи та інвазія шкідливих біологічних видів, потужні урагани, посухи та лісові пожежі [2, 3] тощо. Більшість реальних систем є мережевими, тобто можуть бути зображені у вигляді сукупності взаємопов'язаних елементів, які спільно функціонують для досягнення певної цілі [4]. Тому теорія складних мереж (ТСМ) приділяє значну увагу дослідженню уразливості таких утворень та розробленню стратегій їхнього захисту від дії різномірних негативних впливів [5, 6]. Оскільки будь-яка велика складна система зазвичай не може захистити усі свої елементи, то основний акцент цих досліджень робиться на визначенні тих вузлів мережі, які потребують першочергового захисту [7, 8]. При цьому основна увага приділяється визначенню показників важливості вузла у структурі мережевої системи, а не у процесі її функціонування. Поза увагою також залишаються способи протидії поширенню негативного впливу та подолання наслідків його дії. Очевидно, що чим краще захищена система, тим простіше вирішувати ці проблеми. Однак, реальні події показують, що навіть системи, які вважаються добре захищеними, можуть бути захищені недостатньо (атомна електростанція у Фукусімі, будівлі та критична інфраструктура у сейсмічно активних регіонах Чилі, Японії, Каліфорнії, комп'ютерні мережі безпекових

відомств та великих фінансових установ і т. ін.). У цій статті на підставі побудованих на емпіричних даних структурної та потокової моделей МС розроблені методи об'єктивного оцінювання наслідків ураження реальних мережевих систем від дії різномірних негативних впливів. Пропоновані методи сприятимуть формуванню ефективних стратегій відновлення системи після ураження.

1. Основні етапи протидії негативному впливу

Протидія негативному впливу на систему насамперед залежить від його типу, масштабності та тривалості. Серед великого розмаїття таких впливів ми виділяємо внутрішні та зовнішні стосовно системи; локальні, групові та загальносистемні; централізовані та децентралізовані; цілеспрямовані атаки та нецільові ураження МС[9] тощо. Натепер основна увага приділяється розробленню стратегій захисту структури системи від послідовних локальних цілеспрямованих атак, які спрямовані на поступове ураження найважливіших за певними структурними ознаками (центральністю за ступенем, посередництвом, власним значенням тощо) вузлів складної мережі (СМ) [10, 11]. Особливо небезпечно, коли такі послідовні атаки переростають у групові, а потім – у загальносистемні [12, 13]. Формування стратегій захисту розпочинається з побудови сценаріїв цілеспрямованих атак, тобто опису послідовності дій, які відображають найбільш ймовірну реалізацію нападу на систему. Їх корисність полягає у можливості визначення тих елементів мережі, які потребують першочергового захисту. Цікаво, що у багатьох випадках сценарії цілеспрямованих атак успішно використовуються для протидії поширенню нецільових уражень системи, наприклад, поширенню епідемій небезпечних інфекційних захворювань [14].

Однак, поряд із організацією захисту МС від негативного впливу існує ще принаймні два важливі етапи, а саме протидія поширенню впливу системою та подолання наслідків дії цього впливу. Можливість протидії залежить від наявних засобів захисту та тривалості впливу. Так, через відсутність вакцин людство виявилось неготовим до боротьби з поширенням пандемії Covid-19; на початку російсько-української війни система ПРО могла збивати лише 10% крилатих та балістичних ракет; потужні землетруси практично неможливо передбачити та захиститися від них; каскадні явища в енергетиці неодноразово залишали без електропостачання десятки мільйонів споживачів [15] і т. ін. Тобто, відсутність або недостатність належних засобів захисту чи миттєвий перебіг впливу робить практично неможливою ефективну протидію йому. Тоді як довготривала дія негативного впливу дає змогу знаходити ефективні засоби протидії його поширенню: ліки від СНІДу та багатьох онкологічних захворювань, вакцини від Covid-19, натепер українська ПРО знешкоджує 85% ракет нападника тощо.

Не менш важливим є розроблення стратегій подолання наслідків ураження системи. Подібно тому, як вона не може рівноцінно захистити усі свої елементи, МС зазвичай також неспроможна одночасно відновити усі прямо чи

опосередковано постраждали вузли та зв'язки. Тому виникає проблема визначення послідовності їх відновлення, яка далеко не завжди співпадає із пріоритетністю захисту. Цю проблему можна вирішити, використовуючи побудовані на емпіричних даних структурну та потокову моделі реальної мережевої системи.

2. Моделі складних мереж та мережевих систем

Складна мережа зазвичай описується у вигляді графу $G=(V, E)$, у якому $V = \{v_n\}_{n=1}^N$ позначає множину вузлів, а $E = \{e_l\}_{l=1}^L$ – множину зв'язків (ребер), які поєднують вузли CM , N та L – кількості цих вузлів та ребер відповідно. Структура мережі повністю описується матрицею суміжності $A = \{a_{ij}\}_{i,j=1}^N$, елементи якої $a_{ij} = 1$, якщо існує зв'язок між вузлами v_i та v_j (такі вузли називаються суміжними), і $a_{ij} = 0$, $i, j = \overline{1, N}$, якщо такого зв'язку немає [16].

Складні мережі, на дослідженні яких загалом зосереджена ТСМ, описують структуру мережевої системи. Тому під динамікою CM зазвичай розуміють лише зміну складу її вузлів та зв'язків [17]. Процес функціонування мережевої системи зазвичай залишається поза увагою. Певні особливості цього процесу можна описати за допомогою так званих зважених мереж, у яких кожному ребру CM ставиться у відповідність певне число (вага), яке можна інтерпретувати як відображення процесу функціонування MC . Наприклад, кількість авіарейсів між двома аеропортами чи кількість пасажирів або вантажів, які були перевезені цими авіарейсами [18] тощо. Тому для опису процесу функціонування системи ми використовуємо потокову модель мережевої системи. Чому саме потоки обрані у якості основної функціональності MC ? Більшість із створених людиною систем призначені саме для забезпечення руху потоків певного типу (інформаційних, транспортних, фінансових, сировинних і т. ін.). У інших системах рух потоків забезпечує їхню життєдіяльність (рух крові, поживних речовин, нейроімпульсів у живих організмах тощо). Зупинка руху потоків у більшості із реальних складних систем ставить під ризик або й повністю припиняє їх існування.

Для опису процесу функціонування мережевої системи ми використовуємо потокову матрицю суміжності [9]

$$\mathbf{F}(t) = \{f_{ij}(t)\}_{i,j=1}^N, \quad f_{ij}(t) = \tilde{f}_{ij}(t) / \max_{l,m=1,N} \tilde{f}_{lm}(t), \quad f_{ij}(t) \in [0, 1], \quad i, j = \overline{1, N},$$

у якій значення $\tilde{f}_{ij}(t)$ дорівнюють обчисленим у відповідних одиницях реальним обсягам потоків певного типу, які пройшли ребром (n_i, n_j) мережі протягом часового інтервалу $[t-T, t]$ до поточного моменту t , $t \geq T \geq 0$, та $f_{ij}(t)$

дорівнюють їх нормалізованим (безрозмірним) значенням, $i, j = \overline{1, N}$. Ми використовуємо безрозмірні значення обсягів потоків, щоб уникнути їх «прив'язки» до конкретного типу потоку в системі. Очевидно, що структура матриці $\mathbf{F}(t)$ є ідентичною структурі матриці \mathbf{A} . Ми обираємо такий метод обчислення елементів матриці $\mathbf{F}(t)$ для згладжування функцій, які описують динаміку руху потоків у мережі, з метою фільтрації випадкових або нетипових для даної системи збурень у поведінці цих функцій. Під час кризових або екстремальних для системи ситуацій рекомендується зменшувати значення T (інколи до нуля), тоді як за умов стабільного функціонування це значення можна збільшувати. Якщо основними інтегральними структурними характеристиками МС є кількість вузлів та ребер мережі, її щільність та принцип розподілу ступенів вузлів, середня довжина найкоротшого шляху і т. ін., то основною інтегральною функціональною характеристикою мережевої системи є загальний обсяг потоків, що пройшли мережею за часовий інтервал тривалістю T , а саме значення $s(\mathbf{F}(t))$, яке обчислюється за формулою

$$s(\mathbf{F}(t)) = \sum_{i,j=1}^N f_{ij}(t), \quad t \geq T \geq 0. \quad (1)$$

Як структурна, так і потокова моделі реальної мережевої системи будуються на підставі емпіричних даних про її склад та процес функціонування. Наприклад, структура залізничної транспортної системи визначається на підставі карти залізничних шляхів і кожна залізнична компанія відстежує кількість пасажирів та вантажів, які пересуваються залізницею. Кожна енергопостачальна компанія обчислює кількість газу, нафтопродуктів чи електроенергії, які постачаються нею до споживачів. Засоби відеоспостереження дають змогу обчислювати кількість автотранспортних засобів, які проїхали ділянкою шляху, між двома перехрестями або між сусідніми населеними пунктами. Натепер можливо розраховувати обсяги атмосферних та океанічних течій, міграцію тварин, поширення епідемій і т. ін. Загалом, за допомогою сучасних засобів відбору та опрацювання інформації достатньо просто отримати дані про динаміку руху потоків у реальних складних системах як створених людиною, так і фізичних чи природних системах різного походження [19].

3. Оцінювання наслідків ураження системи

Знищення елементів структури безумовно впливає на процес функціонування МС. Однак, дестабілізувати її роботу можна і за неуразеної структури [20]. Наприклад, під час російсько-української війни ні пасажирські аеропорти, ні літаки практично не були ушкоджені. Однак, лише загроза їх збиття із пасажирами на борту практично зупинила процес функціонування авіаційної транспортної системи України. Подібна ситуація склалася із морською транспортною системою з моменту початку російської агресії до укладання так званої «зернової» угоди (березень – серпень 2022 р.). Певна частина вузлів та

зв'язків українських транспортних мереж були видалені з їх структур унаслідок окупації частини територій нашої країни. Це безпосередньо вплинуло на процес функціонування відповідних систем [21]. Тому для різнобічного об'єктивного оцінювання наслідків ураження ми використовуватимемо як структурну, так і потокову моделі мережевої системи.

3.1. Ураження структури мережевої системи

Насамперед нагадаємо, що матриця суміжності A мережі будується на підставі емпіричних даних про її топологію, наприклад, карти залізниці або автошляхів, енергомережі, мережі водо- і газопостачання тощо. Під повним ураженням ребра мережі ми розумітимемо його видалення зі структури системи, тобто обнулення відповідного значення матриці суміжності A . Під повним ураженням вузла CM ми також розумітимемо його видалення зі структури системи, що супроводжується обнуленням елементів відповідного рядка та стовпця матриці суміжності A . Таке ураження може відбутися унаслідок знищення як самого вузла, наприклад, Трипільської ТЕЦ енергосистеми України, так і усіх його зв'язків, як це сталося на Запорізькій АЕС (сама електростанція залишилась практично неушкодженою). Під частковим ураженням вузла CM розумітимемо видалення зі структури системи лише частини його зв'язків, тобто обнулення не всіх елементів матриці суміжності A , які містяться у рядку та стовпці цієї матриці, що відповідають вузлу.

Опосередковано постраждалі елементи структури MC визначаються за допомогою центральностей вузла різних типів [22]. Так, за центральністю за ступенем, опосередковано постраждалими можна вважати усі суміжні з ураженим вузлом, а також ребра, які їх поєднують із цим вузлом (рис. 1а, чорним кольором позначено уражений вузол, сірим – опосередковано постраждалі, білим – неуразені вузли мережі). Такий підхід є цілком виправданим для асортативних мереж [23], у яких зв'язки існують між суміжними вузлами (біологічні, соціальні MC).

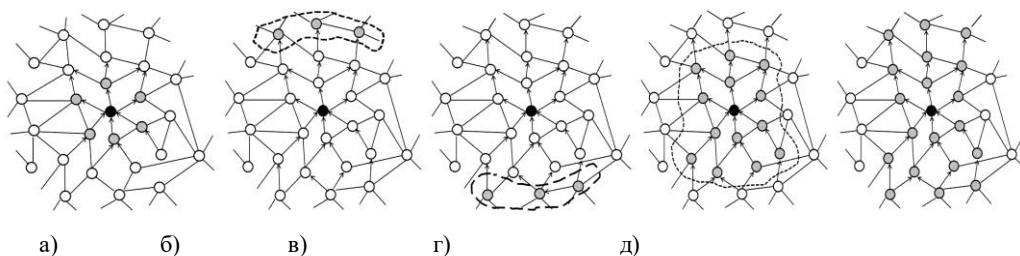


Рис. 1. Наслідки ураження вузла мережевої системи (а – сукупність суміжних до ураженого вузла елементів MC ; б – область вихідного впливу вузла; в – область вхідного впливу вузла; г – область посередництва вузла MC ; д – область взаємодії вузла з системою)

Однак, для дисасортативних мереж, у яких зв'язки між вузлами загалом реалізуються за допомогою шляхів (технологічні, фінансові МС), такий підхід застосовувати недоцільно, оскільки він може суттєво недооцінювати шкоду, заподіяну системі. У цьому випадку опосередковано постраждалими можна вважати вузли СМ, які лежать на найкоротших шляхах, що поєднують уражений вузол з усіма іншими вузлами мережі. Цей спосіб визначення опосередковано постраждалих елементів системи є достатньо складним з обчислювальної точки зору особливо для мереж, які налічують мільйони або мільярди елементів, а також може давати суттєву переоцінку кількості таких елементів СМ. Загальну кількість повністю уражених ребер та вузлів СМ можна визначити, порівнюючи кількість ненульових елементів та ранги матриці суміжності A до і після закінчення дії негативного впливу.

3.2. Ураження процесу функціонування мережевої системи

Потокова матриця суміжності $F(t)$, $t \geq T \geq 0$, мережевої системи будується на підставі емпіричних даних про рух потоків мережею, наприклад, пасажирів та вантажів залізницею або автотранспортними засобами, електроенергії енергомережею, води та газу мережами водо- і газопостачання тощо. На підставі потокової моделі МС ми можемо визначити такі глобальні характеристики її вузлів, як вхідні та вихідні параметри їхнього впливу на систему, а також параметри посередництва та взаємодії вузла із МС [9]. А саме, вхідною (вихідною) силою впливу вузла – кінцевого приймача (генератора) потоків вважатимемо сумарні обсяги потоків, які були прийняті (згенеровані) у цьому вузлі за період $[t-T, t]$, $t \geq T \geq 0$; вхідною (вихідною) областю впливу вузла – кінцевого приймача (генератора) потоків вважатимемо сукупність вузлів МС, у яких були згенеровані (кінцево прийняті) спрямовані до (з) нього потоки за період $[t-T, t]$. На рис. 1б та 1в відображені області вихідного та вхідного впливу позначеного чорним кольором вузла мережевої системи. У випадку ураження цього вузла вважатимемо елементи цих областей одними із опосередковано постраждалих з функціонального погляду. Кількість таких вузлів визначається значеннями вхідної (вихідної) потужності впливу вузла – кінцевого приймача (генератора) потоків та дорівнює кількості елементів областей вхідного (вихідного) впливу цього вузла відповідно. Мірою посередництва вузла вважатимемо сумарні обсяги потоків, які пройшли через нього транзитом за проміжок часу $[t-T, t]$; областю посередництва вузла називатимемо сукупність вузлів МС, які спрямовували та в яких приймалися потоки, що проходили через даний транзитний вузол. На рис. 1г відображена область посередництва позначеного чорним кольором вузла мережевої системи. У випадку ураження цього вузла елементи цієї області також вважатимемо опосередковано постраждалими з функціонального погляду. Кількість таких вузлів визначається значеннями потужності посередництва вузла та дорівнює кількості елементів області посередництва цього вузла.

Ми навмисно поділяємо вузли МС на генератори, кінцеві приймачі та

транзитери потоків, оскільки їх ураження вимагає різних дій для подолання наслідків, наприклад, пошук нових підприємств-виробників, нових ринків збуту продукції або альтернативних шляхів руху потоків. Наприклад, ембарго на енергоносії означає блокування вузлів-генераторів (країн, що добувають та постачають такі носії), заборона на постачання високотехнологічної продукції (мікросхем, новітніх комп'ютерів чи обладнання) – блокування кінцевих приймачів потоків (країн чи компаній, які використовують таку продукцію), блокування вузлів-транзитерів (заборона міжнародних авіаперельотів над територією росії або перетину її військовими кораблями протоки Босфор) – переспрямування руху потоків іншими, зазвичай довшими та дорожчими, шляхами. Одним із недоліків сценаріїв цілеспрямованих атак, заснованих на структурних показниках важливості вузлів МС, є те, що до опосередковано постраждалих обгрунтовано можна віднести лише сукупність елементів системи, суміжних з ураженими. Перед проведенням атаки на вузли-генератори (кінцеві приймачі) або вузли-транзитери можна ідентифікувати їх області вхідного (вхідного) впливу або області посередництва. Ці області дають змогу ідентифікувати вузли, що можуть опосередковано постраждати унаслідок здійснення атаки, а також кількісно обчислити можливий рівень їхніх втрат. Такі дії є сенс проводити перед введенням санкцій проти країни-агресора. Кількісний вимір втрат сторони, яка вводить санкції, порівняно зі шкодою, завданою атакованій системі, дає змогу визначати доцільність проведення атаки. Однак, якщо поділ вузлів на типи не є суттєвим для оцінювання наслідків ураження вузла системи, можна використати параметр його взаємодії з МС [14], тобто усереднене значення вхідного, вихідного впливу та посередництва цього вузла. Можна вважати, що параметр взаємодії є поточковим аналогом ступеня вузла у складній мережі. Ступінь вузла є його локальною характеристикою у МС, оскільки описує взаємодію лише із суміжними вузлами мережі. Параметр взаємодії, незважаючи на подібний спосіб обчислення, є його глобальною характеристикою, оскільки загалом описує взаємодію із вузлами всієї мережевої системи. Область взаємодії вузла з системою визначається шляхом об'єднання областей його вхідного та вихідного впливу посередництва в системі (рис. 1д), а потужність взаємодії – кількістю вузлів, які входять до складу цієї області. Загалом, після ураження певного вузла МС параметри області та потужності взаємодії вузла з системою повністю визначають сукупність та кількість усіх опосередковано постраждалих унаслідок цього елементів системи. Поточковий підхід дає змогу значно простіше виявляти фіктивні та приховані елементи МС [9]. Ця проблема також стосується уразливості МС, адже поступове заміщення реальних елементів фіктивними також свідчить про ураження системи, наприклад, атрофія м'язів тіла або нейродегенеративні процеси у головному мозку людини. Поява та поширення прихованих елементів, наприклад, незареєстрованих підприємств, які не сплачують податків, або мережі наркодилерів, також свідчать про негаразди в економіці або соціальному житті

суспільства. Поєднуючи області вхідного та вихідного впливу безпосередньо уражених вузлів мережі, а також області їх посередництва або взаємодії, ми можемо визначити усі опосередковано постраждали унаслідок послідовних поелементних або одночасних групових атак елементи МС. Очевидно, що отримана на підставі структурної моделі мережевої системи оцінка сукупності постраждалих від ураження елементів системи є значно менш точною. Загальні втрати, заподіяні МС унаслідок дії негативного впливу, обчислюються за формулою (1). Саме на підставі результатів оцінювання наслідків ураження структури та процесу функціонування мережевої системи доцільно формувати стратегії відновлення реальної МС.

Для глибшого багатокритеріального об'єктивного аналізу захищеності та відновлюваності елементів МС [9]

- на етапі дослідження ризиків та загроз доцільно використовувати методи регулярного локального, прогностичного та агрегованого оцінювання захищеності найважливіших об'єктів системи;
- на етапі протидії поширенню негативного впливу слід застосовувати методи інтерактивного локального, прогностичного та агрегованого оцінювання уражених на поточний момент об'єктів системи для мінімізації наслідків його дії;
- на етапі відновлення мережевої системи також доцільно використовувати методи регулярного локального, прогностичного та агрегованого оцінювання її елементів для розроблення ефективних стратегій повернення МС до нормального функціонування.

Окрім того, на етапі відновлення та після його завершення доцільно застосовувати методи регресивного локального, прогностичного та агрегованого оцінювання поведінки об'єктів системи для відстеження віддалених наслідків дії негативного впливу (постковідний синдром, наслідки вакцинації чи ускладнення, спричинені інфекцією, ПТСР, підтримка ветеранів та інвалідів війни, їх сімей і т. ін.).

4. Відновлення структури та процесу функціонування мережевих систем

Зі структурного погляду відновлення мережевої системи означає повернення до її складу видалених унаслідок дії негативного впливу вузлів та ребер, а з функціонального – забезпечення їх діяльності. Для повноцінного відновлення процесу функціонування опосередковано постраждалих елементів МС зазвичай достатньо відновити вузли мережі, які були генераторами потоків, що спрямовувались у ці елементи для кінцевого прийняття; кінцевими приймачами потоків, до яких спрямовувались згенеровані уражених вузлах МС потоки для їх споживання; транзитерами потоків, які забезпечували їхній рух мережею. Такий підхід суттєво зменшує кількість елементів системи, які необхідно реально відбудовувати.

Перевагою потокового підходу порівняно зі структурним є можливість визначення пріоритетності відновлення уражених, але не повністю знищених

елементів системи. Це пояснюється тим, що найважливіші елементи системи зазвичай є найбільш захищеними, тобто можуть незначно постраждати унаслідок ураження порівняно із менш важливими та захищеними. Тому перелік пріоритетності відновлення загалом може не співпадати зі списком найважливіших за певною центральністю вузлів МС. Важливість відновлення об'єкта визначатимемо за формулою

$$\gamma = \frac{\alpha}{\alpha_{\max}} \left(1 - \frac{\beta_{\text{after}}}{\beta_{\text{before}}} \right),$$

у якій α – значення обраної центральності для ураженого вузла, α_{\max} – максимальне значення цієї центральності для усіх вузлів системи, β_{after} – середній обсяг потоків у вузлі після ураження, β_{before} – середній обсяг потоків у вузлі до ураження. Згідно цієї формули більш уражений вузол серед менш важливих може потребувати першочергового відновлення. Загалом, порядок відновлення на кожному кроці повинен забезпечувати максимальне повернення руху потоків мережею до його обсягів перед ураженням. При цьому виникає питання: чи можливо відновити усі уражені елементи системи або чи доцільно їх відновлювати у тому вигляді, у якому вони були до початку дії негативного впливу? Відповідь на нього є предметом наших подальших досліджень.

Висновки. У роботі описані найбільш поширені види негативних впливів на складні мережеві системи та виділені основні етапи боротьби із ними: оцінка реальних та потенційних загроз та забезпечення захисту МС; організація протидії поширенню негативного впливу мережею з метою мінімізації його наслідків для системи; розроблення стратегій відновлення МС для її якнайшвидшого повернення до нормальної життєдіяльності. На підставі структурної та потокової моделей мережевої системи визначені структурні та функціональні показники важливості її елементів, які визначають перелік їх першочергового захисту. Ці ж показники використовуються для об'єктивного оцінювання наслідків ураження МС. Показано, що потоковий підхід дає змогу отримувати значно точніші оцінки безпосередньо уражених та опосередковано постраждалих елементів системи. На підставі цих оцінок сформована послідовність відновлення вузлів МС, застосування якої сприятиме якнайшвидшому поверненню системи до нормального функціонування.

Література

- [1] Sawada Y., Bhattacharyay M., Kotera T., Aggregate impacts of natural and man-made disasters: A quantitative comparison. *International Journal of Development and Conflict*, Vol. 9(1), 2019, 43-73.

- [2] *Polishchuk O.*, Structural and flow-based approaches to vulnerability analysis of complex network systems. In: *Complex Networks and their Applications XIII*, Vol. 3, Springer, Cham, 2024, pp. 353-365. doi: 10.1007/978-3-031-82435-7_29.
- [3] *Wandel S.*, A comparative analysis of approaches to network-dismantling. *Scientific Reports*, Vol. 8(1), 2018, 13513. doi: 10.1038/s41598-018-31902-8.
- [4] *Barabási A.-L.*, *Network Science*. Cambridge: Cambridge University Press, 2016. doi: 10.1063/PT.3.3526.
- [5] *Bellingerio M., Cassi D., Vincenzi S.*, Efficiency of attack strategies on complex model and real-world networks. *Physica A: Statistical Mechanics and its Applications*, Vol. 414, 2014, 174-180. doi: 10.1016/j.physa.2014.06.079.
- [6] *Nguyen Q. et al.*, Conditional attack strategy for real-world complex networks. *Physica A: Statistical Mechanics and its Applications*, Vol. 530, 2019, 12156. doi: 10.1016/j.physa.2019.121561.
- [7] *Glenn L.*, Understanding the influence of all nodes in a network. *Scientific Reports*, Vol. 5, 2015, 8665. doi: 10.1038/srep08665.
- [8] *Mariyam J., Lekha D.S.*, Need for a realistic measure of attack severity in centrality based node attack strategies. In: *Complex Networks and Their Applications XI*, Springer, Cham, 2022, pp. 857-866.
- [9] *Поліщук О., Яджак М.*, Моделі та методи комплексного дослідження складних мережевих систем та міжсистемних взаємодій. Львів: Інститут прикладних проблем механіки і математики ім. Я.С. Підстригача НАН України, 2023.
- [10] *Sun W. et al.*, Identification of important nodes in complex networks based on node and edge information. *Communications in Nonlinear Science and Numerical Simulation*, Vol. 152(A), 2025, 109116. doi: 10.1016/j.cnsns.2025.109116.
- [11] *Wan Z. et al.*, A survey on centrality metrics and their network resilience analysis. *IEEE Access*, Vol. 9, 2021, 104773-104819. doi: 10.1109/ACCESS.2021.3094196.
- [12] *Polishchuk O., Polishchuk D.*, Protection of multilayer network systems from targeted group attacks. arXiv:2503.20269, 2025. doi: 10.48550/arXiv.2503.20269.
- [13] *Polishchuk O., Polishchuk D.*, Vulnerability of multilayer network systems to system-wide lesions. arXiv:2503.21161, 2025. doi: 10.48550/arXiv.2503.21161.
- [14] *Polishchuk O.*, Protection of multilayer network systems from successive attack on the process of inter system reactions. *CEUR-WS*, Vol. 3790, 2024, 545-557.
- [15] *Yang Y., Nishikawa T., Motter A.E.*, Small vulnerable sets determine large network cascades in power grids. *Science*, Vol. 358(6365), 2017, eaan3184. doi: 10.1126/science.aan3184.
- [16] *Boccaletti S. et al.*, *Complex networks: Structure and dynamics*. *Physics reports*, Vol. 424(4), 2006, 175-308. doi: 10.1016/j.physrep.2005.10.009.
- [17] *Mimar S.*, *Learning Dynamical Processes from Structure in Complex Networks*. Rochester: University of Rochester, 2022.
- [18] *Barrat A. et al.*, The architecture of complex weighted networks. *PNAS*, Vol. 101(11), 2004, 3747-3752. doi: 10.1073/pnas.040008710.
- [19] *Barabasi A.-L.*, The architecture of complexity. *IEEE Control Systems Magazine*, Vol. 27(4), 2007, 33-42. doi: 10.1109/MCS.2007.384127.
- [20] *Polishchuk O.*, Vulnerability of Complex Network Structures and Systems. *Cybernetics and Systems Analysis*, Vol. 56(2), 2020, 312 – 321. doi: 10.1007/s10559-020-00247-4.
- [21] Транспорт України. Державна служба статистики України, 2024. Режим доступу: https://www.ukrstat.gov.ua/druk/publicat/kat_u/2024/zb/10/zb_Trans_23.pdf
- [22] *Ugurlu O.*, Comparative analysis of centrality measures for identifying critical nodes in complex networks. *Journal of Computational Science*, Vol. 62, 2022, 101738. doi: 10.1016/j.jocs.2022.101738.
- [23] *Noldus R., Van Mieghem P.*, Assortativity in complex networks. *Journal of Complex Networks*, Vol. 3(4), 2015, 507-542. doi: 10.1093/comnet/cnv005.

Assessing the consequences of a disruption to complex network systems

Dmytro Polishchuk

This paper analyzes the negative impacts that can damage the structure and destabilize the functioning of a complex network system (CNS). It examines three main stages of potential impact: threat analysis and ensuring effective system protection; organizing countermeasures against the spread of the impact through the complex network; and assessing the consequences of damage and the restoration of the CNS. Based on structural and flow models of the network system, methods have been developed for the objective analysis of the consequences of negative impacts, aimed at developing effective strategies for restoring the system to normal operation. The effectiveness of the proposed approach is illustrated using examples of various types of transportation systems in Ukraine.

Отримано 15 січня 2026 р.