МАСШТАБНІСТЬ ТА КЛАСИФІКАЦІЯ УРАЖЕНЬ СКЛАДНИХ МЕРЕЖЕВИХ СИСТЕМ

Олександр Поліщук

Інститут прикладних проблем механіки і математики ім. Я. С. Підстригача НАН України, м. Львів,
od_polishchuk@ukr.net

Поняття захищеності реальної складної мережевої системи (МС) та класифікації типу цілеспрямованої атаки на неї тісно пов'язані із визначенням масштабності цієї атаки та її наслідків. Зокрема, доцільно розрізняти:

1) масштабність запланованої та здійсненої атаки, яка визначається кількістю цілей, що передбачається уразити, та кількістю задіяних для цього засобів, наприклад, 50 об'єктів енергетичної інфраструктури та 100 крилатих і балістичних ракет, спрямованих на них для знищення;

2) масштабність безпосереднього ураження, тобто кількість цілей, критично пошкоджених або повністю знищених унаслідок атаки, наприклад, із 100 запущених ракет 85 були збиті засобами протиракетної та протиповітряної оборони, а 15 ракет, що залишились, уразили 10 цілей; у цьому випадку масштабність безпосереднього ураження дорівнює відсотку знищених об'єктів із числа запланованих;

3) масштабність опосередковано постраждалих елементів системи, тобто кількість об'єктів, яким було заподіяно певної шкоди унаслідок здійсненої атаки окрім безпосередньо уражених, наприклад, введення графіків відключення світла, спричинених послідовно-одночасними атаками на енергетичну інфраструктуру України.

Масштабність безпосереднього ураження пов'язана із кількісним показником захищеності МС, який дорівнює відсотку знищених засобів ураження із усіх задіяних. Масштабність опосередкованого ураження, як і рівень захисту від нього, обчислити значно складніше, адже вона повинна враховувати порушення структури та дестабілізацію роботи усіх елементів МС і навіть морально-психологічну шкоду, заподіяну унаслідок атаки. Із масштабністю опосередкованого ураження можна пов'язати поняття чутливості системи до наслідків негативного впливу, як відношення кількості безпосередньо уражених до числа опосередковано постраждалих її елементів. Очевидно, що чим ближчим є значення цього показника до нуля, тим чутливішою до цілеспрямованих атак є система, оскільки невелика кількість безпосередньо уражених породжує велике число опосередковано постраждалих елементів МС.

Масштабність ураження можна кількісно визначати, як у статті [2], порівнюючи структурні і потокові моделі МС до, під час та після цілеспрямованої атаки. Питома вага «обнулених» елементів та рядків і стовпців відповідних матриць суміжності визначає кількість безпосередньо уражених зв'язків та вузлів системи. Опосередковано постраждалими у структурній моделі МС

можна вважати лише суміжні із безпосередньо ураженими вузли та поєднуючі їх зв'язки. Такий підхід достатньо адекватно відображає рівень втрат для асортативних, наприклад, біологічних чи соціальних мереж [1]. Однак, для дисасортативних мереж, до яких належать більшість створених людиною промислових, економічних, фінансових, транспортних, інформаційних та інших систем він є непридатним, оскільки у них багато вузлів пов'язані не прямими зв'язками, а шляхами, визначити які лише на підставі структурної моделі достатньо складно. У цьому випадку більш адекватною є потокова модель системи, а саме, області та потужності вхідного та вихідного впливу та посередництва сукупності безпосередньо уражених вузлів [2] достатньо однозначно визначають усі опосередковано постраждалі елементи МС. Це пояснюється тією обставиною, що вузли-приймачі та вузли-генератори потоків потрібно якимось чином замістити, а для транзитних вузлів – знайти альтернативні шляхи руху цих потоків. Все це має конкретний фінансовий вимір, який і можна використати для підрахунку рівня втрат, що зазнає система. Дійсно, унаслідок санкцій проти росії через її агресію в Україну свої ринки збуту (кінцеві приймачі потоків) втратили чимало провідних компаній світу. У багатьох із них принаймні тимчасово виникли серйозні проблеми із постачанням енергоресурсів та сировини, тобто постало завдання заміщення вузлів-генераторів потоків певного типу. Суттєво також обмежився рух транзитних потоків через територію росії, що потребувало знаходження альтернативних і, зазвичай, дорожчих та довших шляхів руху цих потоків. З подібними обставинами, але вже унаслідок бойових дій на своїй території, зіштовхнулася і Україна. Слід також враховувати, що навіть повітряні тривоги, які оголошуються унаслідок зльоту носіїв ракет, але не супроводжуються реальним ударом, також призводить до перебоїв у роботі навчальних і медичних установ, а також багатьох торгівельних, транспортних, державних та промислових підприємств, та породжують панічні настрої у населення тих регіонів, які постійно страждають від реальних нападів. Тому є сенс вважати, що характер атаки слід визначати не лише за кількістю безпосередньо уражених елементів МС, але й за масштабами опосередкованих втрат, заподіяних системі.

1. *Noldus R., Van Mieghem P.* Assortativity in complex networks // Journal of Complex Networks. – 2015. – **3**, № 4. – pp. 507-542.
2. *Polishchuk O., Yadzhak M.* On the Vulnerability and Protection Strategies of Complex Network Systems and Intersystem Interactions // CEUR-WS. – 2023. – **3538**. – pp. 267-281.

THE SCALE AND CLASSIFICATION OF COMPLEX NETWORK SYSTEM LESIONS

Means for determining the scale of real-world complex network systems lesions and methods for classifying the targeted attacks based on them are proposed. Indicators of the level of system protection against various negative influences and its sensitivity to the consequences of such influences are defined.