УДК 519.711.7:519.816

ПРО УРАЗЛИВІСТЬ СКЛАДНИХ МЕРЕЖЕВИХ СИСТЕМ ТА МІЖСИСТЕМНИХ ВЗАЄМОДІЙ

Олександр Поліщук

Інститут прикладних проблем механіки і математики ім. Я.С. Підстригача НАН України

od_polishchuk@ukr.net

Кожна природна або створена людиною система є уразливою до багатьох внутрішніх та зовнішніх негативних впливів. Серед основних видів таких впливів насамперед можна виділити цілеспрямовані атаки та нецільові ураження складних мережевих систем та міжсистемних взаємодій [1]. Відмінною рисою цілеспрямованих атак є їх умисність та штучний характер. Особливістю уражень цього типу є наявність цілі атаки, спрямованої на завдання якнайбільшої матеріальної та/або моральної шкоди атакованій системі, та зловмисника, який цю атаку здійснює. На відміну від цілеспрямованих атак, до нецільових уражень можна віднести різнорідні неумисні негативні впливи природного або штучного характеру, виникнення та наслідки яких людина не може своєчасно передбачити. У 2020–2022 роках людство зіштовхнулося з двома глобальними викликами, перший з яких (пандемія Covid-19) є яскравим прикладом загальносистемного нецільового ураження, а другий (напад рф на Україну) – цілеспрямованої атаки та викликаної нею загрози світової продовольчої, енергетичної, фінансової кризи і зворотних всеосяжних санкцій стосовно держави-агресора, негативні наслідки яких торкнулися практично усіх країн світу. Різнорідні негативні впливи можуть бути локальними, груповими або загальносистемними, умовно передбачуваними або неочікуваними, централізованими або децентралізованими, поширюватися із різною швидкістю та бути спрямованими на ураження структури та/або процесу функціонування системи чи міжсистемних взаємодій. Особливістю сучасних досліджень стійкості мережевих систем (МС) до різнорідних негативних впливів є розроблення сценаріїв послідовного ураження групи найважливіших зі структурного погляду вузлів мережі, хоча очевидно, що одночасна атака на таку групу або загальносистемна атака, яка у тій або іншій мірі вражає усі елементи МС, є значно небезпечнішою для будь-якої реальної мережевої системи [3]. Корисність таких сценаріїв полягає у тому, що вони, даючи картину можливого розвитку атаки, дозволяють розробляти ефективні засоби захисту від неї. Що не менш важливо, сценарії цілеспрямованих атак часто задають ефективні алгоритми протидії поширенню нецільових уражень (методи захисту від поширення комп'ютерних вірусів є подібними

http://iapmm.lviv.ua/mpmm2023/materials/mm11_03.pdf

до заходів протидії розгортанню епідемій небезпечних інфекційних захворювань і т.ін.), а способи боротьби з нецільовими ураженнями можуть підказувати дієві сценарії реалізації цілеспрямованих атак. Аналізуючи загрози, які можуть порушити структуру або дестабілізувати процес функціонування реальних МС, та розробляючи відповідні засоби їх захисту, дослідники часто абстрагуються від джерел цілеспрямованих атак та нецільових уражень, які можуть бути і внутрішніми, і зовнішніми по відношенню до системи. Водночас, блокування таких джерел є одним із дієвих засобів захисту як окремої МС, так і процесу міжсистемних взаємодій загалом, адже своєчасна нейтралізація терористичної або хакерської групи чи розроблення вакцин та ліків від небезпечних інфекційних захворювань може запобігти тій шкоді, яку вони можуть заподіяти.

У доповіді на підставі структурної моделі багатошарової мережевої системи (БШМС), яка описує процеси міжсистемних взаємодій, побудована модель її агрегат-мережі та введені поняття серцевин різних типів. Виділення таких складових дає змогу визначати найважливіші за тими або іншими ознаками компоненти багатошарової мережі, які потребують першочергового захисту. Побудовані ефективні сценарії послідовних та одночасних групових, а також загальносистемних атак на структуру БШМС. Однак, структурні показники далеко не завжди адекватно відображають функціональну важливість окремих складових БШМС, а отже структурні сценарії, які базуються на таких показниках, можуть виявитися не найефективнішими. До того ж, на рівні структурного підходу достатньо важко кількісно проаналізувати наслідки уражень, заподіяних цілеспрямованою атакою, та розробити стратегії відновлення процесу функціонування уражених елементів, підсистем або багатошарової системи загалом. Для подолання цього недоліку в роботі розроблена потокова модель міжсистемних взаємодій [2], на підставі якої сформована модель агрегат-мережі БШМС та введені поняття потокових серцевин різних типів. Виділення таких складових дають змогу визначати найважливіші з функціонального погляду компоненти багатошарової мережі, які потребують першочергового захисту. Побудовані значно ефективніші порівняно зі структурними сценарії послідовних та одночасних групових, а також загальносистемних атак на процес функціонування багатошарових мережевих систем.

1. *Polishchuk O.* "About group and system-wide lesions of complex network systems and intersystem interactions", arXiv: 2211.11207 [physics.soc-ph], 2022.
2. *Polishchuk O.* "Flow model of intersystem interactions and influence of components of multilayer network systems", arXiv: 2302.02134 [physics.soc-ph], 2023.
3. *Polishchuk O.* "Strategies for protecting of multilayer networks from group and system-wide targeted attacks", arXiv: 2211.15090 [physics.soc-ph], 2022.

ABOUT VULNERABILITY OF COMPLEX NETWORK SYSTEMS AND INTERSYSTEM INTERACTIONS

The main types of lesions of complex network systems and intersystem interactions are analyzed. Effective scenarios of group and system-wide attacks on the structure and operation process of multilayer network systems have been developed.