**Лекція 14. Використання теорії графів при моделюванні групи супротивника системи інформаційної безпеки**

**План**

1. **Використання зваженого графа при моделюванні групи супротивника, атаки на систему захисту інформації.**
2. **Використання операцій над графами для моделювання процесу руйнування групи супротивника**

**1. Використання зваженого графа при моделюванні групи супротивника, атаки на систему захисту інформації**

Традиційним шляхом для представлення групи людей із вказівкою взаємних відносин між ними є використання теорії графів. Це обумовлене багатьма факторами, серед яких наочність одержуваної моделі, можливість адекватного відображення за допомогою стандартних операцій на графах реальних дій над групами й подій у групах, існуванням розробленого математичного апарата для роботи із графами, включаючи велику кількість евристичних методів їх обробки, що добре зарекомендували себе на практиці.

У даний момент у науковому світі надзвичайно активізувалася робота з математичного моделювання терористичних організацій і інших типів кримінальних груп, метою яких є, зокрема, несанкціонований доступ до інформації, її підміна й інші неавторизовані дії.

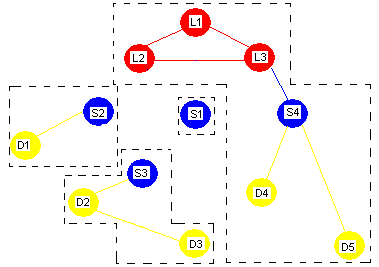
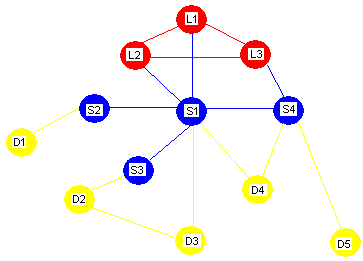
Розглянемо задачі, пов'язані з організацією протидії групам супротивника, розв'язок яких здійснюється з використанням графових математичних моделей супротивника. Окремі індивідууми представляються в такій моделі у вигляді вузлів (вершин), пари яких з'єднуються ребром при існуванні певного взаємозв'язку між відповідними членами розглянутої групи.

Нехай група супротивника у своїй ієрархії має 3 основних рівня: лідера (керівника) або декількох лідерів, представників з’єднуючої ланки (керівництво на місцях) і безпосередніх виконавців. При побудові найпростішої графової моделі (неорієнтований незважений граф) кожному члену організації супротивника відповідає вершина, ребра графа з'єднують вершини в тому випадку, якщо між відповідними їм членами існує безпосередній зв'язок. Приклад такої моделі представлений на рис.1(а), де вузли, відповідні до лідерів організації, середній ланці й виконавцям, для наочності мають відповідно червоний, синій і жовтий колір. Граф очевидно є зв'язним. Як правило, безпосереднього зв'язку між лідерами й виконавцями не існує, хоча така можливість і не виключається.

Традиційно графові моделі супротивника використовуються для розв'язку наступних задач:

1. Визначення членів групи супротивника, блокування (видалення) яких *реально можливо здійснити*, при цьому блокування приведе до *розпаду* організації супротивника на декілька незв'язаних між собою частин. Результатом такого розпаду може виявитися як повне знищення групи, так і зниження ефективності її діяльності.

Мовою графів дане завдання буде формулюватися наступним чином: необхідно визначити точку зчленування або множину вузлів (множину, що містить мінімальну кількість вузлів), видалення яких приведе до розпаду зв'язного графа на декілька компонент. У прикладі, наведеному на рис.1(а), точкою зчленування є *S1*. Блокування цього єдиного члена організації супротивника приводить до її розпаду на чотири частини, причому три з них стають «обезголовленими», а тому недієздатними (рис.1(б)). Відмітимо, що таке можливо не завжди.



а б

Рис.1. Приклад графової моделі групи супротивника: (а - первісний вид; б - вид після видалення точки зчленування графа

1. Виділення в організації супротивника таких зв'язків між його членами, видалення яких приводить до розпаду групи на окремі частини, незв'язані між собою, що очевидно значно обмежить можливості діяльності розглянутої структури.

Мовою графів завдання формулюється наступним чином: визначити множину ребер (мінімальну множину ребер) у графові, видалення яких приведе до його розпаду на декілька компонент.

Для отримання задовільного результату при розв'язку поставлених задач графова модель супротивника повинна мати максимально можливу інформативність, враховувати ієрархію розглянутої групи супротивника. Для цього будемо використовувати в якості моделі супротивника неорієнтований ***зважений*** граф: кожній вершині й кожному ребру такого графа ставиться у відповідність деяке число - вага.

***Вага вершини*** формується, виходячи з апріорних даних про відповідного члена групи супротивника, з врахуванням

а) його поінформованості про об'єкт, на який спрямована увага;

б) матеріальних і часових можливостей для здійснення відведеної даному члену групи ролі (в операції здійснення несанкціонованого доступу до інформації);

в) значимості розглянутого члена в групі.

Врахування усіх перерахованих вище складових частин вагових коефіцієнтів автоматично виділить лідерів (вершини з найбільшими значеннями ваг) і інших менш значимих членів групи.

***Вага ребра*** визначається залежно від

а) реальної цінності інформації, що передається за допомогою даної лінії зв'язку (наприклад, інформація, передана від керівників групи підлеглим, є більш значимою, чим інформація, що циркулює між безпосередніми виконавцями);

б) надійності розглянутої лінії зв'язку (наприклад, зв'язок при безпосередньому контакті є більш надійним, чим при використанні телефонної лінії).

Приклад зваженого графа-моделі наведений на рис.2 (порядок нумерації відповідає ієрархії членів організації, у середині вузла - його номер, поруч із вузлом - його вага, поруч із ребром у дужках - вага ребра).

**2.Використання операцій над графами для моделювання процесу руйнування групи супротивника**

Задачі 1,2 були сформульовані в загальному виді. Результат видалення деяких членів групи або блокування якихось зв'язків, що приводить до її розпаду на окремі підгрупи, у реальності може виявитися зовсім незначним з погляду зниження дієздатності супротивника. Наприклад, якщо зруйнувати зв'язок між членами S4 і D5 (міст у графовій моделі супротивника (рис.1(а))), це чи навряд нанесе відчутний удар по всій групі, тому що частина, що залишилася без D5, збереже як абсолютну більшість своїх членів, так і наявність усіх ієрархічних ланок.

Одним з основних питань при моделюванні груп супротивника й активних дій над ними є питання про те, коли розглянуту структуру можна вважати зруйнованою, або знищеною.

Розглянемо можливий розв'язок для задачі 1. Для розв'язку цієї задачі по графовій моделі групи визначається множина усіх простих, або «командних», ланцюгів, початок і кінець яких відповідає лідерові й безпосередньому виконавцеві відповідно. По отриманій множині визначається сукупність вузлів графа, кожний з яких є присутнім хоча б в одному ланцюзі, причому кожний ланцюг вносить у цю сукупність єдиний вузол. Видалення із графа такої сукупності (cutset), зруйнує в ньому всі існуючі «командні» ланцюги. У цьому випадку робиться висновок про знищення групи супротивника.

Розглянемо можливий алгоритм для здійснення руйнування групи супротивника, використовуючи в якості моделі запропонований вище зважений неорієнтований граф. Для цього побудуємо для графа-моделі кореневу структуру рівнів (КСР) з коренем у вузлі, що має найбільшу вагу, тобто, що відповідає лідерові (варіант, коли значення максимальної ваги відповідає декільком вершинам, розглядається нижче). Для зручності подальшого викладу позначимо цей вузол . КСР  є розбивка множини вершин *V* графа:

,

така, що  , де - множина вузлів графа, що не належать , але суміжних хоча б з одним вузлом з . Ексцентриситет  вузла  стосовно структури рівнів називається довжиною , а ширина  структури визначається як

.

Для графа, представленого на рис.2, коренева структура рівнів, описана вище, буде мати вигляд, представлений на рис.3.

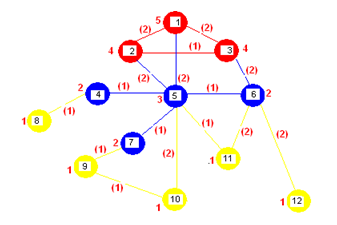


Рис.2. Модель групи супротивника у вигляді зваженого графа

Усі «командні» ланцюги - це очевидно прості ланцюги графа, що виходять із нульового рівня кореневої структури й закінчуються або вершиною, ступінь якої дорівнює 1, або вершиною, що лежить в останньому рівні КСР; якщо  - дві послідовні вершини такого ланцюга, то номер рівня в КСР, що містить , не більше номера рівня, у який потрапила вершина . Вузли, що потрапили в один рівень структури, визначать ту сукупність, видалення якої приведе до розпаду графа на компоненти за рахунок розриву всіх ланцюгів зв'язку, тобто до блокування групи супротивника. Спосіб побудови КСР приведе до того, що лідери будуть «відрізані» від безпосередніх виконавців, що позбавить можливості організованих активних дій дану групу.

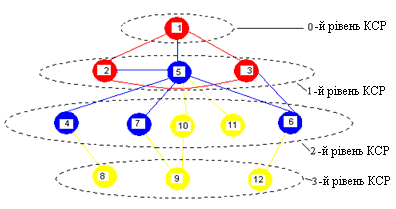


Рис.3. Коренева структура рівней

Нехай є кілька вершин з максимальною вагою. Тоді при побудові КСР роль «кореня» буде відігравати не один вузол: усі вершини графа з максимальними ваговими значеннями, що відповідають лідерам супротивника, розміщуються на нульовому рівні структури. Інші кроки для виділення відокремлюючої множини графа залишаються без зміни.

Вузли якого рівня вибрати, щоб завдати більшої шкоди групі супротивника при блокуванні відповідних членів?

Для чисельної оцінки збитку, що завдається кримінальному угрупованню, скористаємося матрицею суміжності графа-моделі. Для графа, представленого на рис.2, ця матриця має вигляд:

**5 2 2 0 2 0 0 0 0 0 0 0**

**2 4 1 0 2 0 0 0 0 0 0 0**

**2 1 4 0 0 2 0 0 0 0 0 0**

**0 0 0 2 1 0 1 1 0 0 0 0**

**2 2 0 1 3 1 1 0 0 2 1 0**

**PROT= 0 0 2 0 1 2 0 0 0 0 2 2**

**0 0 0 1 1 0 2 0 1 0 0 0**

**0 0 0 1 0 0 0 1 0 0 0 0**

**0 0 0 0 0 0 1 0 1 1 0 0**

**0 0 0 0 2 0 0 0 1 1 0 0**

**0 0 0 0 1 2 0 0 0 0 1 0**

**0 0 0 0 0 2 0 0 0 0 0 1**

(на головній діагоналі - вагові коефіцієнти вершин, позадіагональні елементи - вагові коефіцієнти ребер). У силу неорієнтованості графа матриця є симетричною. Вона повністю визначає граф, а тому характеризує всю групу супротивника. Кожна з характеристик такої матриці є характеристикою й реальної людської групи.

Назвемо ***ваговою енергією групи супротивника*** ()енергію сигналу, цифровим представленням якого є матриця суміжності графової моделі супротивника:

,

де - евклідова матрична норма. Виключення певного члена групи (певної вершини графа разом з інцидентними ребрами) для матриці суміжності буде виражатися у видаленні з неї рядка й стовпця, номера яких відповідають номеру виключеної вершини. Енергію групи після виключення з неї членів  будемо позначати (). Цей числовий показник буде використовуватися для порівняння результатів передбачуваного блокування тих або інших членів групи супротивника. Залежно від підсумків порівняння робиться висновок про доцільність блокування конкретної сукупності членів групи.

Звичайно, такий алгоритм не гарантує відокремлення лідерів від безпосередніх виконавців, але розбивка на зв'язні компоненти в кожному разі приведе до ослаблення групи й потребує певного часу на її відновлення.

**Питання**

1. Чим обумовлене традиційне використання теорії графів для представлення групи людей із вказівкою взаємних відносин між ними?
2. Як будується граф, що представляє модель групи людей?
3. Для розв'язку яких задач традиційно використовуються графові моделі супротивника?
4. Що таке зважений граф?
5. Як визначається вага вершини, ребра в графовій моделі групи супротивника?
6. Як операції над графами використовуються для моделювання процесу руйнування групи супротивника?
7. Що таке коренева структура рівней графа?
8. Що таке вагова енергія групи супротивника?