радіоелектроніки. – Харків, 2013. – 35 с. 9. Грицик В. В. Обробка складних зображень та їх розпізнавання в інформаційно-аналітичних системах комп'ютерного зору / В. В. Грицик // Доповіді НАН України. Секція інформатики та кібернетики. – 2009. – № 3. – С. 49–54. 10. Грицик В. В., Грицик В. В., Зозуля А. М. Дослідження паралельних алгоритмів на ООС на систолічних системах. – ДНДІІІ. – Препринт № Д1. – 2009. – 23 с. 11. Грицик В. В., Грицик В. В., Зозуля А. М. Дослідження паралельного опрацювання інформації визначення основних імовірнісних хаорактористик марківських процесів на систолічних системах ООС. – ДНДІІІ. – Препринт № Д2. – 2009. – 35 с. 13. Параллельная обработка информации: в 5 т. – Т. 5: Проблемно-ориентированные и специализированные средства обработки информации / под ред. Б. Н. Малиновского, В. В. Грицыка; АН УССР. Физ.-мех. ин-т. – К.: Наук. думка, 1985. – 504 с.

УДК 004.942

Н. М. Іванущак[1], В. В. Пасічник[2]
[1]Чернівецький національний університет імені Юрія Федьковича,
[2]Національний університет "Львівська політехніка",
кафедра інформаційних систем та мереж.

УЗАГАЛЬНЕНА МОДЕЛЬ ЕВОЛЮЦІЇ МЕРЕЖЕВОГО АНСАМБЛЮ В УМОВАХ ДЕСТАБІЛІЗАЦІЙНИХ ЗАГРОЗ

Розроблено нову математичну модель генерування структури локальних комп'ютерних мереж та узагальнену модель еволюції мережевого ансамблю в умовах дестабілізаційних загроз, розв'язано задачу про стійкість мереж до випадкових та спрямованих атак.

Ключові слова: комп'ютерні мережі, стохастичний граф, системи аналізу захищеності.

In this paper we have developed a new mathematical model for generating the structure of local computer networks and the generalized model for the evolution of network ensemble in conditions of destabilizing threat to solve the problem of the stability of networks to random and targeted attacks.

Key words: computer networks, stochastic graph, system security analysis.

Вступ

Проблеми статистичного дослідження локальних комп'ютерних мереж, моделювання на їх основі топології та процесів розвитку цих систем, прогнозування динаміки їх подальшої структуризації, дослідження стійкості до спрямованих атак і розповсюдження комп'ютерних вірусів залишаються актуальними в умовах дестабілізаційних загроз. Дослідження структури та динаміки росту комп'ютерних систем створює умови для їх ефективного розвитку і захисту. Задачі статистичного опису таких систем для свого розв'язання потребують застосування нового математичного апарату та переходу від імітаційного до ймовірнісного моделювання, що полягає в багатоетапному проведенні випробувань реалізованої ймовірнісної моделі і подальшій статистичній обробці результатів моделювання з метою визначення шуканих характеристик аналізованого процесу у вигляді оцінок його параметрів. Окрім суто наукових і технологічних причин підвищеної уваги до них є і суто прагматична. Річ у тім, що такі системи мають системотвірний компонент, тобто їх структура і динаміка активно впливають на ті процеси, які ними контролюються.

Загальна постановка проблеми

Метою роботи є розв'язання задачі, яка має суттєве значення для створення нових методів математичного моделювання, а саме – дослідження і обґрунтування підходів, які дають змогу ідентифікувати структуру і параметри моделей локальних комп'ютерних мереж на основі даних спостережень; розроблення методів та засобів математичного моделювання процесів розвитку структур інфокомунікаційних мереж (на прикладі комп'ютерних мереж). Наукова новизна роботи полягає у математичному моделюванні реальних локальних комп'ютерних мереж з урахуванням їх ймовірнісних характеристик для підвищення ефективності їх функціонування і захищеності їхніх елементів від спрямованих атак.

Аналіз останніх досліджень та публікацій

Розвиток методів і технологій ймовірнісного моделювання процесів росту та структуризації комп'ютерних мереж стимулює інтерес дослідників до вивчення *теорії складних мереж* (*Complex Networks*), в межах якої пропонуються підходи до розв'язання обчислювально складних задач, які є характерними для сучасних систем. Властивості багатьох реальних комп'ютерних, біологічних і соціальних мереж суттєво відрізняються від властивостей класичних випадкових графів з рівноймовірними зв'язками між вузлами, і тому вони будуються на основі зв'язаних структур та степеневих розподілів [1–6]. Теорія складних мереж як область дискретної математики вивчає характеристики мереж, враховуючи не тільки їх топологію, але і статистичні феномени, розподіл ваг вузлів і ребер, ефекти протікання, провідності тощо.

Виділяють три основні напрямки у теорії складних мереж:

– дослідження аналізом статистичних властивостей, які характеризують поведінку мереж;

– створення моделей мереж;

– прогнозування розвитку мереж при зміні їх структурних властивостей.

Зростаюча складність комп'ютерних мереж і механізмів захисту, збільшення кількості уразливості і потенційних помилок у їх використанні, а також можливостей реалізації атак зумовлює необхідність розроблення громіздких автоматизованих засобів (систем) аналізу захищеності.

Аналіз отриманих наукових результатів

Ймовірнісна модель комп'ютерної мережі

Комп'ютерна мережа подається у вигляді графу G, який визначається як сукупність (V,E) кінцевої множини вершин V, $\dim(V)=N$, і множини ребер E, яка складається із невпорядкованих пар (u,v) де $u,v\in V$ і $u\neq v$. Кожна вершина характеризується своїм ступенем, тобто кількістю інцидентних їй ребер. Впорядкований список ступенів вершин утворює ступеневу послідовність.

Інтегральною характеристикою комп'ютерної мережі є закон розподілу ступенів p_k, який задає ймовірність того, що випадково вибрана вершина має ступінь приєднання k. Ступеневу послідовність для неорієнтованого графу зручно подати у формі

$$d=\left(k_1^{n_1},k_2^{n_2},...,k_s^{n_s}\right),$$

де числа k_i є ступенями вершин, а показник n_i визначає кількість повторів числа k_i у послідовності. Дискретний розподіл ступенів вершин p_k пов'язується зі ступеневою послідовністю d у формі

$$p_k \overset{def}{=} P[x=k_i]=n_i/N\,.$$

У моделі випадкових графів [7] ребро, яке інцидентне довільним двом вершинам, присутнє або відсутнє з рівною ймовірністю, а тому розподіл p_k буде біноміальним або (у границі за N) пуассонівським. Однак більшість реальних мереж має структуру, відмінну від структури

випадкових графів, що позначається на характері розподілу ступенів вершин. Зокрема, у багатьох реальних мережах емпіричний розподіл ступенів вершин інтерпретується в термінах ступеневого розподілу $p_k = k^{-\gamma}$. Цей розподіл характеризується єдиним параметром γ, який визначає швидкість спадання "хвоста" розподілу. Для здійснення процесу моделювання локальних комп'ютерних мереж використовувались характеристики реальних мереж інтернет-провайдерів в м. Чернівцях: "BW-Star & FoxNet", "КТМ" та "DSS-Group". Ступінь вузла k задає кількість ребер інцидентних конкретній вершині, а n_k – кількість вершин у графі із заданим k. За цими даними побудовано розподіл ступенів вершин. На рис. 1 наведено апроксимацію "хвостів" розподілів ступенів вершин досліджуваних мереж та встановлені для них значення параметра степеневого розподілу: $p_k = k^{-2.4}$ для мережі "BW-Star & Fox Net" та $p_k = k^{-.2.1}$ для мережі "DSS-Group".

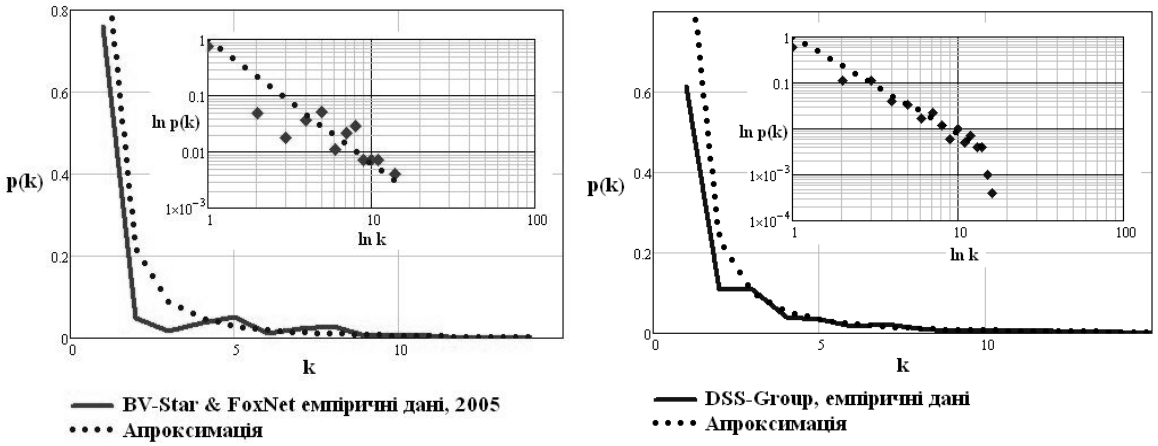

Рис.1. Апроксимація "хвостів" розподілів ступенів вершин досліджуваних мереж

Алгоритм побудови ймовірнісної моделі розвитку комп'ютерної мережі

Для побудови моделі розвитку комп'ютерної мережі, параметри якої близькі до тих, які спостерігаються у реальній, пропонується така архітектура мережі. Нехай мережа складається з N вузлів (вершин); s – кількість класів вершин; $i \in \{1,2,3,...,s\}$ – позначає конкретний клас вершин; n_i – кількість вершин *i*-го класу; k_i – ступінь вершини *i*.

Початково розподіл ступенів вершин p_k задано, тому базою для процедури побудови цієї безмасштабної мережі є такий алгоритм:

- сформуємо ступеневу послідовність d, вибираючи s чисел n_i згідно із заданим розподілом p_k, де $i = \overline{1,s}$;
- кожній вершині i графа присвоїмо k_i "заготовок" (кінців) для майбутніх ребер;
- зі ступеневої послідовності випадково вилучаються пари "заготовок". Вони з'єднуються ребром у тому випадку, якщо нове ребро не приведе до утворення ребер-циклів (петель) або мультиребер. Якщо ребро згенеровано, то відповідні індекси із ступеневої послідовності видаляються;
- попередній крок повторюється доти, поки ступенева послідовність не стане порожньою;
- циклічно випадково укладають граф розміщенням вершин з найбільшими ступенями приєднання в центрі графу, а вершини з меншими ступенями радіально розташовують від центру до периферії в послідовності зменшення їхніх ступенів;
- зв'язки між вузлами заповнюють послідовно, починаючи з вершин з найбільшою кількістю ребер.

Алгоритм побудови ймовірнісної моделі забезпечує об'єднання всіх вузлів у єдину структуру стохастичного графу, що відображає факт обов'язкового приєднання всіх користувачів у реальну локальну комп'ютерну мережу.

Програмна реалізація

Результатом програмної реалізації запропонованого алгоритму є власне комп'ютерна мережа, зображена у вигляді стохастичного графу з відомою кількістю вершин і заданим розподілом ймовірностей їх приєднання.

Адекватність описання моделлю реальної структури, роботу алгоритму моделювання проілюстровано за допомогою генерації графу з використанням характеристик реальних комп'ютерних мереж BW-Star & Fox Net та DSS-Group в м. Чернівцях. Для цих комп'ютерних мереж визначено розподіли таких числових характеристик:

1. n_k – кількість вершин у мережі, k – ступінь їхнього приєднання у мережу;
2. $d = \left(k_1^{n_1}, k_2^{n_2}, ..., k_s^{n_s}\right)$ – впорядкований список ступенів вершин у вигляді ступеневої послідовності для моделювання стохастичного графу;
3. $p_1, p_2, p_3, ..., p_s$ – ймовірності приєднання у мережу вершин з різними ступенями k_i ($i = \overline{1, s}$) відповідно.

За емпіричними розподілами ступенів вершин $p_k = k^{-\gamma}$ здійснювалася вибірка, на її основі модельовано мережі з подальшою можливістю порівняння результатів моделювання з характеристиками досліджуваних мереж та оцінювання адекватності описання моделлю реальної структури.

Здійснивши апроксимацію "хвостів" розподілів ймовірностей приєднання у мережу вершин з різними ступенями k, що проілюстровано на рис. 1, та визначивши тим самим показники γ для різних локальних комп'ютерних мереж, зокрема $\gamma = 2{,}4$ для мережі "BW-Star & Fox Net", $\gamma = 2{,}6$ для мережі "КТМ" та $\gamma = 2{,}1$ для мережі "DSS-Group", модельовано ці мережі за відомим показниковим $p_k = k^{-\gamma}$ розподілом ймовірностей приєднання користувачів у мережу з відповідними γ. На рис. 2 проілюстровано приклад візуалізації стохастичного графу, який відображає властивості досліджуваних комп'ютерних мереж. Для динамічної візуалізації використовувався алгоритм укладання графу, який, на нашу думку, найінформативніше зображає структуру та властивості комп'ютерних мереж.

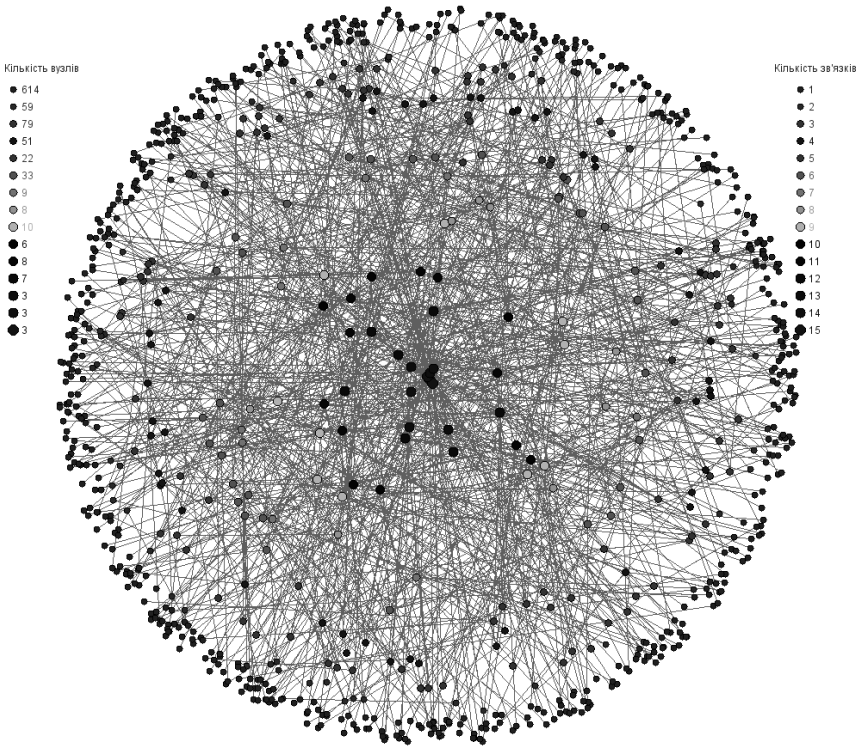

Рис. 2. Графічне зображення топології мережі "BW-Star & Fox Net" за законом залежності $p_k = k^{-\gamma}$*:* $\gamma = 2{,}4$, $N = 915$

На рис. 2 вершини з різними ступенями приєднання k зображено різними кольорами, їхню кількість у згенерованій мережі винесено на панель ліворуч, кількість зв'язків, які відповідають кожній вершині, відображено на панелі праворуч.

Із проведених досліджень видно, що для малих значень параметра розподілу γ мережа кластеризується в один більший зв'язаний кластер, аніж у випадку з більшими значеннями γ.

Визначення оптимальної стратегії захисту локальних мереж від спрямованих атак

Запропонована вище абстрактна модель комп'ютерної мережі дає змогу здійснювати прогностичні оцінки атакувальних дій різних категорій порушників з реалізації найпоширеніших сценаріїв загроз безпеки мережі, а саме спрямованих та випадкових атак на вузли. Це прогнозування не потребує великої ресурсовитратності, властивої автоматизованим системам аналізу захищеності.

Аналіз реальних безмасштабних мереж WWW та Інтернету, метаболізму та мереж харчування демонструє неабияку їхню стійкість до вилучення вузлів: тобто ці мережі виявляють несподіваний ступінь стійкості за випадкових уражень. З іншого боку, під час спланованих сценаріїв нанесення шкоди або вірусних атак мережа стає надзвичайно уразливою.

Випадковий вибір атакувального вузла характеризує випадкову атаку (відмова, збій, R-атака). Послідовне знищення вузлів з максимальною зв'язаністю є класичною стратегією цілеспрямованих атак (I-атак). Зазвичай наслідки атак досліджуваних мереж аналізують за допомогою широкого набору метрик: реєструють зміни діаметра, коефіцієнта кластерності, розміру максимального кластера і його відносних величин. У реальному житті виникають складніші ситуації, тобто вузли і зв'язки комп'ютерних мереж різної топології, що мають різну уразливість, піддаються неоднорідним випадковим і цілеспрямованим загрозам, причому в різноманітних комбінаціях.

Розроблено узагальнену агентну модель еволюції мережевого ансамблю в умовах дестабілізаційних загроз. Основними компонентами описової конструкції мережі є ***модель загроз*** та ***модель безпеки*** [8].

Сформований стохастичний граф, що відображає структуру реальної мережі, подається на вхід ***моделі загроз***. Імітаційне моделювання дестабілізаційних загроз полягає у проведенні над графом двох сценаріїв атак: "природної" ліквідації вершин і ребер, тобто випадкової R-атаки, та ліквідації вершин з найбільшими ступенями, тобто I-атаки. Частка вузлів, що містяться у найбільшому кластері мережі, визначає відносний розмір максимального кластера S:

$$S = 1 - \sum_{k=1}^{k_{\max}} \frac{k \cdot n_{del}(k)}{N}, \qquad (1)$$

де $n_{del}(k)$ – кількість видалених вершин ступеня k; N – загальна кількість вершин у мережі.

Розвиток цієї моделі дає змогу імітувати атаки у вигляді комбінованих загроз (R-випадкової та I-цілеспрямованої) незахищеним вузлам мережі в прямій (R-загрози + I-загрози) та зворотній (I-загрози + R-загрози) послідовності.

На рис. 3 подано результати зміни відносного розміру максимального кластера залежно від кількості атакованих вузлів безмасштабних комп'ютерних мереж "BW-Star & FoxNet", "КТМ" та "DSS-Group" м. Чернівці. Видно, що для будь-якої з наведених мереж атакувальна комбінація I-R є ефективнішою, ніж R-I.

Модель безпеки [8] враховує, що основною мірою безпеки є ризик:

$$R = \rho_{th} \cdot \rho_v \cdot Pl, \qquad (2)$$

де R – ризик; ρ_{th} і ρ_v – відповідні ймовірності загрози та уразливості; Pl –ціна втрати.

Модель забезпечує вивчення складніших атак на системи, ніж у їх традиційному трактуванні для теорії комплексних мереж шляхом зіставлення опису джерел загроз, близьких до реальних. На відміну від багатьох відомих методів, де наслідком атаки завжди є знищення вузла чи зв'язка, цей підхід дає можливість для кожного вузла ввести параметр уразливості (або захищеності).

Елементам мережі приписують величини їх уразливості, в загальному випадку, з $\rho_v(i)$, відмінними від 1, які визначаються об'ємом фінансових вкладів F_i в безпеку *i*-го елемента:

$$\rho_v(i) = f(F_i). \tag{3}$$

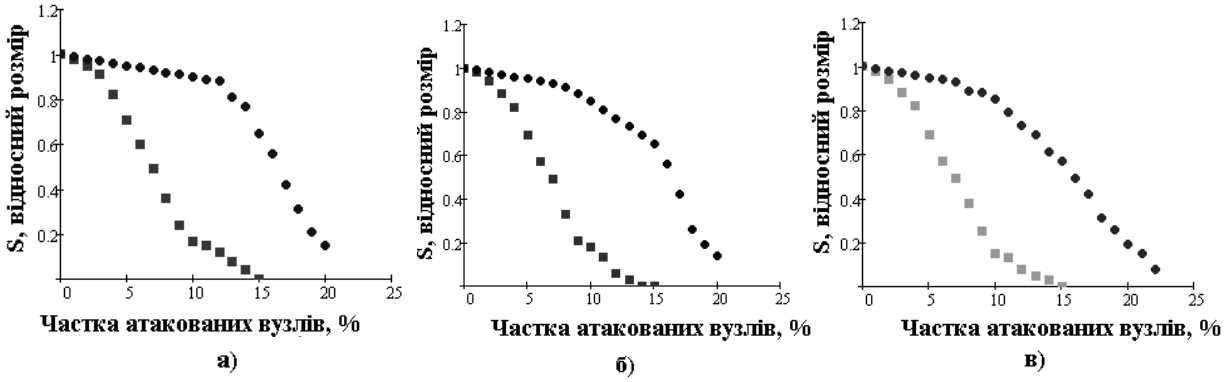

Рис. 3. Залежність відносного розміру максимального кластера в мережах "BW-Star & FoxNet" (а), "КТМ" (б) та "DSS-Group" (в) від кількості атакованих вузлів, що піддаються атакаму різній послідовності: I+R (■) та R+I (●)

Ціна втрати – рівень спаду працездатності мережі у випадку вилучення вузла і всіх суміжних ребер – визначається вибором елемента із множини метрик M -х індикаторів працездатності, які визначають головні цільові характеристики мережевих ансамблів. Наприклад, як елементи множини M можуть використовувати значення коефіцієнта кластерності, посередництва, максимальний розмір кластера, найкоротші шляхи тощо.

Як комп'ютерний експеримент проводили дослідження реакції відповідних змодельованих стохастичних графів, що відображають структури реальних комп'ютерних мереж "BW-Star & FoxNet", "КТМ" та "DSS-Group", на цілеспрямовані загрози захищених елементів – вузлів. Вважають, що ймовірність успішної атаки на вузол змінюється тільки зі зміною $\rho_v(i)$, яка експоненційно зменшується зі збільшенням "товщини" захисного бар'єра d_i, який, своєю чергою, визначається традиційним комплексом заходів безпеки: правовими, організаційними, технічними, фізичними і математичними. Величина d_i визначається об'ємом затрат, тобто $d_i \sim F_i$, і в такому випадку:

$$\rho_v(i) \sim \exp(-\mu F_i), \tag{4}$$

де μ – коефіцієнт, який задає ефективність використання фінансових затрат.

На практиці різні елементи мережі – вузли і зв'язки – захищені (фінансуються) по-різному. Так, зазвичай найвищий рівень захисту мають найважливіші агенти мережі, тоді як захист листів стохастичного графу (кінцевих споживачів) може бути повністю відсутній. Вважаючи, що стратегія безпеки визначає розподіл ресурсів між вузлами, досліджено реакції мережі на загрози для випадків відсутності фінансування та трьох можливих стратегій розподілу інвестицій для захисту, які залежать від ступеня вузла (за однакового сумарного об'єму):

а) відсутність інвестицій $F0_i = 0$;

б) низька захищеність усіх вузлів мережі $F1_i = 1/\mu$;

в) середня захищеність вузлів із високими та середніми ступенями $F2_i = k_i/(C_1 \cdot \mu)$;

г) максимальний рівень захисту вузлів із високими ступенями $F3_i = k_i^2/(C_2 \cdot \mu)$;

$$\sum_{i=1}^{1000} F1_i = \sum_{i=1}^{1000} F2_i = \sum_{i=1}^{1000} F3_i .$$

Коефіцієнти C_1 та C_2 відіграють роль нормувальних констант і визначають їх згідно з виразом $C_i = \frac{F_i}{N_k}$, де N_k – кількість вузлів з високими та середніми ступенями для C_1 або кількість вузлів лише з високими ступенями для C_2.

Для тестової мережі, що містить 1000 вершин, використано класичну стратегію цілеспрямованих атак з послідовними атаками на вузли максимального ступеня. Результати розрахунків зміни відносного розміру максимального кластера для цих чотирьох варіантів захисної стратегії наведено на рис. 4.

Видно, що стратегія надмірного захисту вузлів максимальної зв'язаності (тобто $F_i \sim k_i^2$) не є оптимальною, оскільки цей сценарій приводить до того, що на захист елементів меншого ступеня просто не вистачає коштів.

Ефективність визначення оптимальної стратегії захисту мережі зумовлена не лише вибором її топології, розподілом ресурсів для захисту її елементів, а й максимально точним оцінюванням стратегії та дій атакувальної сторони [9].

Із рис. 4 видно, що оптимальною стратегією захисту локальних комп'ютерних мереж є стратегія захищеності вузлів із високими та середніми ступенями. Тому для вивчення властивостей, пов'язаних з надійністю, захистом від уразливості локальних комп'ютерних мереж, реалізовано процедуру виділення "опорної мережі", що полягає у багатоетапному відрізанні листів початкового графу (рис. 5).

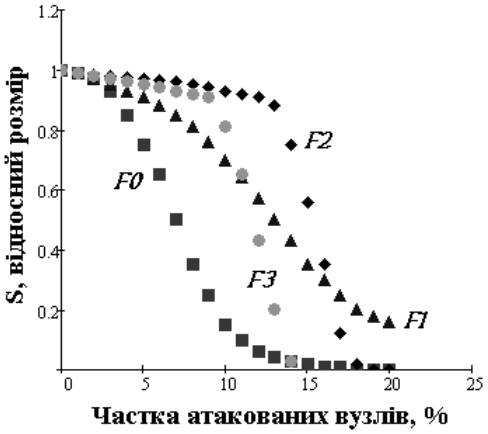

Рис. 4. Залежність відносного розміру максимального кластера в мережі від кількості атакованих вузлів за різних захисних стратегій розподілу інвестицій: $F0_i = 0$, $F1 = 1/\mu$, $F2_i = 4.1k_i/\mu$, $F3_i = 28k_i^2/\mu$

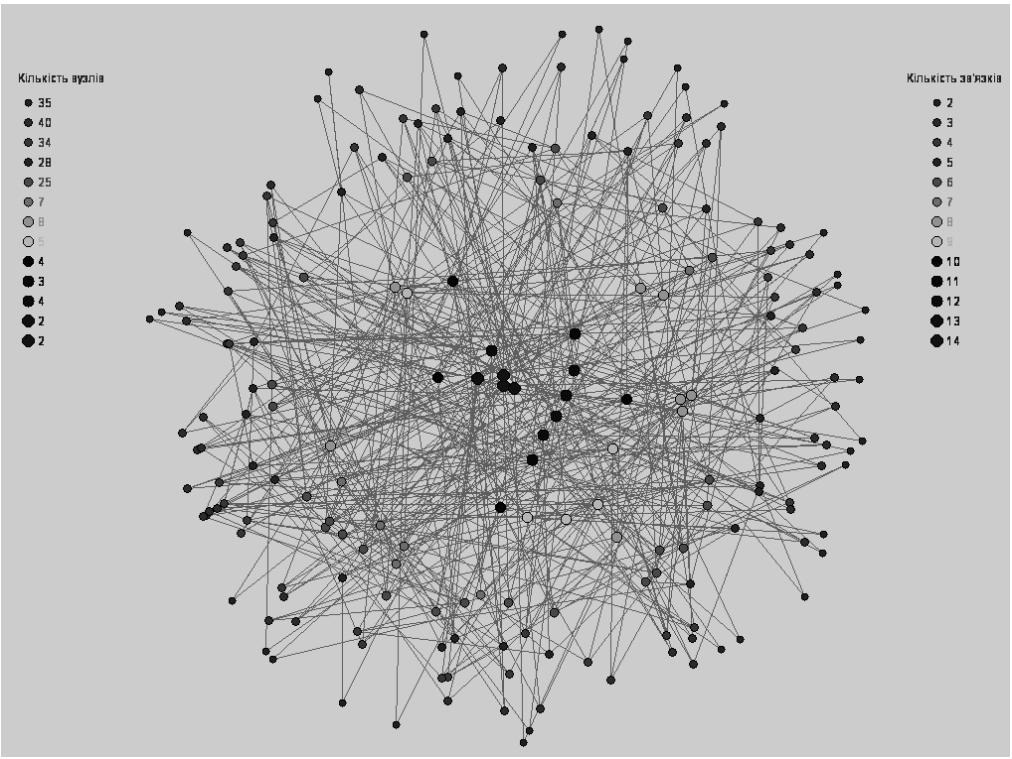

Рис. 5. Опорна мережа інтернет-провайдера "BW-Star & FoxNet"

Побудова опорної мережі інтернет-провайдера “BW-Star & FoxNet” складалася з таких кроків: на першому етапі з отриманого графу видалено 614 листів, на другому – 85 листів, на третьому – 16, а на четвертому – 3 листи. У результаті отримано опорну мережу, що складається з 197 вузлів, кожен з яких має ступінь, не менший ніж 2 (рис. 5).

Опорні мережі різних інтернет-провайдерів виявилися безмасштабними, залежність розподілу ступенів їхніх вузлів з високою точністю апроксимується степеневою функцією. Вивчено і наведено нові наближені до реальності приклади поведінки комп’ютерних мереж у полі загроз, які дають можливість ефективно підійти до розв’язання широкого спектра задач стійкості практично значущих мережевих конструкцій.

Динамічна модель розповсюдження вірусів у комп’ютерних мережах

Для інтернет-провайдерів комп’ютерних мереж особливої актуальності набувають дослідження розповсюдження комп’ютерних вірусів мережею [8], оскільки відсутність антивірусного програмного забезпечення на комп’ютерах користувачів може призвести до лавинного зараження користувачів (так званої епідемії), і, як наслідок, до збоїв у роботі мережевих служб. Маючи інформацію про топологію мереж і поширення вірусів у них (з використанням змодельованих стохастичних графів), можна рекомендувати оптимальну стратегію імунізації (розроблення антивірусних проектів), яка здатна зупинити поширення вірусів та підвищити надійність функціонування мережевих структурних елементів.

Наведемо епідеміологічну модель у вигляді пари $\{G,\Gamma\}$, де G – граф, який визначається як сукупність (V,E) множини вершин V та ребер E, а Γ – еволюційний оператор, що відображає зміну станів мережі через дискретні проміжки часу t:

$$\begin{aligned} \langle V,E\rangle_{t+1} &= \Gamma\langle V,E\rangle_t; \\ \langle V,E\rangle_{t=0} &\overset{def}{=} \langle V_0,E_0\rangle. \end{aligned} \tag{5}$$

Для змодельованих стохастичних графів запускається процес розповсюдження віртуального вірусу для дослідження стійкості локальних комп’ютерних мереж до вірусних атак. Кожен вузол у мережі може перебувати в одному з трьох можливих станів: сприйнятливий, інфікований, а також відновлений (імунний) (рис. 6).

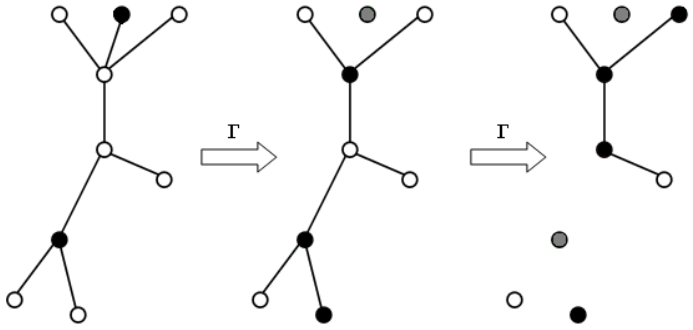

Рис. 6. Схематична модель розповсюдження вірусу у мережі.
Чорні кружечки позначають заражені вузли, сірі – імунізовані вузли

Обчислення проводять через дискретні проміжки часу, тобто на кожному часовому кроці кожний інфікований вузол передає вірус до кожного зі своїх сусідів з певною ймовірністю (δ). Після передачі вірусу – в тому самому часовому кроці – кожен інфікований вузол відновлюється і отримує імунітет до вірусу з іншою ймовірністю (ν). Цей метод використовує випадкові змінні для створення стохастичної поведінки. Щоразу перед можливим зараженням вузла одного зі своїх сусідів з рівномірного розподілу $\{0,1\}$ вибирають випадкову величину U. Якщо $U<\delta$ вірус передається, якщо $U>\delta$ зараження не відбувається. Той самий принцип використовують і для ν.

Щоб спростити подання, вважатимемо, що епідемія розпочинається з одного випадково вибраного вузла.

Епідеміологічні параметри, що можуть варіюватися:

– ефективність вірусу, тобто ймовірність того, що вузол заражатиме сусідів, з якими з'єднаний (δ);
– ймовірність одужання / імунізації (ν);
– вузол, з якого розпочинається зараження.

Моделювання епідемії триватиме доти, доки кількість заражених вузлів не дорівнюватиме нулю. Тоді генерується вихідний файл, який містить кількість інфікованих індивідів на кожному часовому кроці, який може бути використаний згодом для оцінювання.

Оскільки модель є дискретною, то для визначення дискретних проміжків часу $t = n\Delta t$ використовують змінну n.

На $n+1$ кроці шанс будь-якого сприйнятливого вузла S_n не мати контакту з будь-яким з I_n інфікованих вузлів дорівнює $(1-\delta)^{I_n}$. Отже, ймовірність мати хоча б одне з'єднання і стати інфікованим – $1-(1-\delta)^{I_n}$.

На кожному наступному часовому кроці всі заражені вузли з попереднього часового кроку одужують, тому рівняння має вигляд:

$$I_{n+1} = S_n(1-(1-\delta)^{I_n}). \quad (6)$$

Кількість сприйнятливих вузлів на кожному часовому кроці дорівнює числу сприйнятливих вузлів на попередньому часовому кроці, крім тих, які стали інфікованими в цей момент часу:

$$S_{n+1} = S_n - S_n\left(1-(1-\delta)^{I_n}\right) = S_n(1-\delta)^{I_n}. \quad (7)$$

Кількість вузлів, що одужали, з урахуванням параметра імунізації ν, становить:

$$R_{n+1} = R_n + \nu I_n. \quad (8)$$

Отже, отримуємо таку систему рівнянь:

$$\begin{aligned} S_{n+1} &= S_n(1-\delta)^{I_n}; \\ I_{n+1} &= S_n(1-(1-\delta)^{I_n}); \\ R_{n+1} &= R_n + \nu I_n. \end{aligned} \quad (9)$$

Для дослідження ефективності запобігання розповсюдженню вірусів у комп'ютерній мережі проводять дві стратегії імунізації вузлів: випадкову та імунізацію сусідів. ***Випадкова імунізація*** полягає у випадковому введенні імунізованих індивідів у мережу. ***Імунізація сусідів*** ґрунтується на припущенні, що випадково вибраний сусід має більше зв'язків, аніж випадково вибраний вузол. Параметрами контролю є *імунізованість* Ω, яка визначається відношенням заражених вузлів мережі ω до загальної кількості вузлів N та кількість імунізованих вузлів φ.

Результати програмної реалізації запропонованого алгоритму дали змогу діагностувати процеси розповсюдження комп'ютерних вірусів у локальних комп'ютерних мережах і зробити низку висновків (рис. 7).

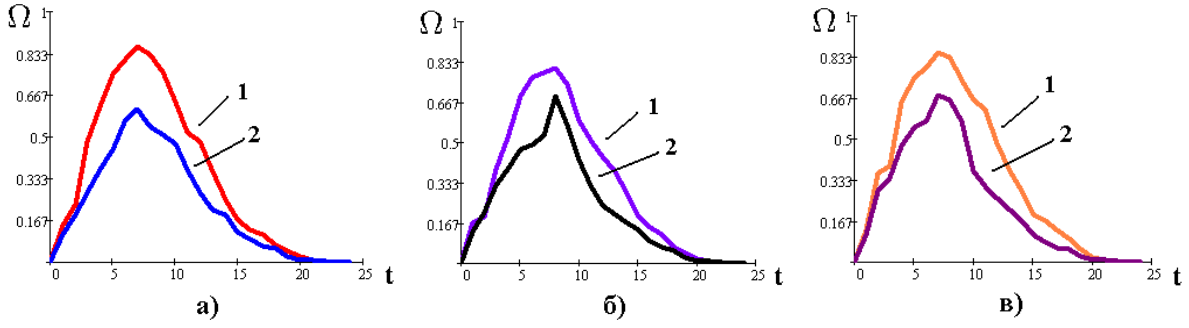

Рис. 7. Залежності Ω від часу t за випадкової імунізації (1) та імунізації сусідів (2) в мережах "BW-Star & FoxNet" (а), "КТМ" (б) та "DSS-Group" (в) для значень $\delta = 0.65$ та $\nu = 0.45$

Для трьох досліджуваних мереж інтернет-провайдерів “BW-Star & FoxNet”, “КТМ” та “DSS-Group” імунізація сусідів виявилася ефективнішою, ніж випадкова імунізація, оскільки вона приводить до значно меншого зараження вузлів, що є підставою для її рекомендації під час розроблення антивірусних проектів та систем аналізу захищеності комп’ютерних мереж.

Результати комп’ютерного експерименту дають можливість оцінити кількість імунізованих вузлів φ, яку необхідно ввести у мережу, щоб зупинити поширення комп’ютерних вірусів у ній. Вона визначається за допомогою згенерованого вихідного файла в момент часу $t_{кр}$, який відповідає максимуму залежності $\Omega(t)$. Для моменту часу $t > t_{кр}$ поширення епідемії сповільнюється і спадає завдяки процесам імунізації в ній (рис. 7).

У таблиці наведено мінімальну кількість імунізованих вузлів для мереж різних інтернет-провайдерів, необхідну для того, щоб зупинити процеси розповсюдження вірусів у їхніх структурах.

Мінімальна необхідна кількість імунізованих вузлів

	“BW-Star & FoxNet” *N=915*		“КТМ” *N=1604*		“DSS-Group” *N=2023*	
	$t_{кр}$	φ	$t_{кр}$	Φ	$t_{кр}$	φ
Випадкова імунізація	8	106	9	259	8	418
Імунізація сусідів	7	314	9	432	9	476

Для визначення значень δ та ν під час моделювання реальних систем необхідно керуватись експертними оцінками та статистичними даними для досягнення найвищої подібності між моделлю та системою.

Висновки та перспективи подальших наукових розвідок

На основі проведених досліджень обчислено інтегральні ймовірнісні характеристики реальних комп’ютерних мереж у різні часові проміжки, апроксимовано їх задля моделювання.

Вперше розроблено нову математичну модель генерування структури локальних комп’ютерних мереж із заданою функцією щільності розподілу ступенів вузлів. Відтворена в результаті моделювання мережа як стохастичний граф володіє параметрами, які близькі до реальної мережі, що уможливлює вивчення природи формування і розвитку мереж, виявлення нових закономірностей в них, моделювання задач зараження та імунізації, протидії мережевим атакам.

Запропоновані алгоритми моделювання сценаріїв атак використано для оцінювання уразливості комп’ютерних мереж та розв’язання задачі про їхню стійкість до випадкових та спрямованих атак. Розроблено узагальнену модель еволюції мережевого ансамблю в умовах дестабілізаційних загроз.

1. Головач Ю. Складні мережі / Ю. Головач, О. Олємской, К. фон Фербер, Т. Головач, О. Мриглод, І. Олємской, В. Пальчиков // Журнал фізичних досліджень. – 2006. – Т.10. – № 4. – С. 247–289. 2. Newman M.E.J. The Structure and Function of Complex Networks / M.E.J. Newman // SIAM Review. – 2003. – Vol. 45. – N. 2. – P. 167–256. 3. Erdős P. On the evolution of random graphs / P. Erdős, A. Renyi // Publications of the Mathematical Institute of the Hungarian Academy of Sciences. – 1960. – Vol. 5. – P. 17–61. 4. Frank O. Markov graphs / O. Frank, D. Strauss D // Journal of the American Statistical Association. – 1986. – Vol. 81. – P. 832–842. 5. Watts D. J. Collective dynamics of “small-world” networks / D. J. Watts, S. H. Strogatz // Nature. – 1998. – Vol. 393. – P. 440–442. 6. Barabasi A-L. Emergence of scaling in random networks / A.-L. Barabasi, R. Albert // Science. – 1999. – Vol. 286. – P. 509–512. 7. Albert R. Attack and error tolerance of complex networks / R. Albert, H. Jeong, A. Barabasi // Nature. – 2000. – Vol. 406. – Pp. 378–382. 8. Galindo F., Dmitrienko V., Caruso A., Rossodivita A., Tikhomirov A.A., Trufanov A. I., Shubnikov E. V. (2010). Modeling of Aggregate Attacks on Complex Networks. Information Security Technologies, Moscow, 3, 115-121. 9. Вовк О. Б. Аналіз та обґрунтування вибору методів дослідження інформаційного продукту / О. Б. Вовк // Вісник Нац. ун-ту Львівська політехніка. – 2014. – №783: Інформаційні системи та мережі. – С.293–302.