УДК 681.321;322:621.395

Гончарук Д.С., Кононович В.Г.

СТРУКТУРНА ЖИВУЧІСТЬ ТА ІНФОРМАЦІЙНА БЕЗПЕКА ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Постановка проблеми

Останні десятиліття телекомунікаційні технології стрімко розвивались слідом за інформаційними технологіями. Роль телекомунікаційних мереж у функціонуванні систем управління державою, економікою, бізнесом значно зросла, але одночасно збільшились уразливість їх інформаційних ресурсів. Життєдіяльність суспільства, його інформаційна безпека залежить від стабільного функціонування, живучості, надійності та готовності телекомунікаційних мереж. Це вимагає перегляду проблем забезпечення живучості мереж в умовах розвитку та впровадження нових телекомунікаційних технологій.

Аналіз досягнень та публікацій

Телекомунікаційні мережі являють собою організаційно-технічну сукупність, яка складається з комплексів взаємозв'язаного й узгодженого за завданням, місцем і часом дії телекомунікаційного обладнання – вузлів комутації та з'єднуючих їх каналів зв'язку. Різним аспектам живучості систем, телекомунікаційних мереж та систем захисту присвячені роботи Горицького В.М. [1], Додонова А.Г., Горбачик Е.С. [2], Романова О.І., Павлова І.М. [3], Рижакова В.А., Саковича Л.М. [4] та інших. Проаналізувавши дані роботи, можна сказати, що сьогодні ще низка питань стабільної інформаційної безпеки та живучості телекомунікаційних мереж залишаються невирішеними. Разом з тим, у оглядових роботах ряду авторів [5,6] фіксується, що розвиненість, складність та зростаюча роль телекомунікаційних мереж, як критичного державного ресурсу, ведуть до зміни парадигми інформаційної безпеки та підходів до побудови системи захисту. Процес забезпечення інформаційної безпеки все більше пересікається з процесами управління якістю надавання телекомунікаційних послуг, де захищеність та готовність інформаційних ресурсів є складовою частиною оцінки якості; управління економічною ефективністю, де є взаємозв'язок між інформаційними та економічними ризиками та задачами технічної експлуатації в частині забезпечення вимог до збереження мінімального набору критично важливих функцій, до живучості інформаційних систем, до запасу стійкості при дії дестабілізуючих факторів зовнішнього середовища.

Ціль статті

Метою даної статті є дослідження живучості та готовності телекомунікаційних мереж, як критичної властивості інформаційно-комунікаційних мереж, та структурної надійності мереж в умовах переходу до нових телекомунікаційних технологій, вирішення задачі вибору оптимальної топології мереж за цими критеріями.

Викладення основного матеріалу

Під живучістю телекомунікаційної мережі розуміються такі властивості мережі, що характеризують стійкість системи до відмовлень її елементів. Властивість живучості в нормальних умовах функціонування системи виявляється як певні властивості надлишковості, адаптивності, відмовостійкості. В критичних умовах ці властивості дозволяють системі зберігатись як цілому в умовах цілеспрямованих чи випадкових несприятливих впливів та зберігати працездатність при руйнуванні елементів мережі. У загальному випадку *живучість* визначається як властивість складних систем адаптуватись у непередбачуваних ситуаціях, протистояти несприятливим впливам, які не були передбачені умовами експлуатації, і досягати цілі функціонування за рахунок зміни поведінки та структури системи. Під поняттям „несприятливий вплив" розуміють відмови, збої і

порушення у роботі програм та обладнання, атаки на систему, катастрофічні впливи природного або техногенного походження. До засобів забезпечення живучості відносяться використання внутрішніх ресурсів, перебудова структури, зміни функцій та алгоритмів функціонування окремих підсистем тощо. Для інтелектуальних систем засобом забезпечення живучості може бути зміна поведінки системи або її окремих частин.

Будь-яка телекомунікаційна транспортна мережа має елементи – вузли комутації та лінії передачі; структуру та технологію – комутацію каналів (КК) чи комутацію пакетів (КП) з різними способами керування. У телекомунікаційних мережах з комутацією каналів для передачі повідомлення спочатку формується наскрізний канал, який існує весь час передачі повідомлення поки не буде подано сигнал роз'єднання. Основним засобом забезпечення живучості є зміна алгоритмів маршрутизації (трасування) з'єднань з використанням обхідних маршрутів у відповідь на несприятливий вплив, який виражається у руйнуванні чи відмові частин мережі – вузлів комутації та з'єднувальних ліній. Такий метод характеризується значними додатковими витратами і обмеженістю у виборі варіантів обхідних маршрутів. На практиці були реалізовані варіанти обхідних маршрутів другого і третього вибору.

З переходом до мереж з комутацією пакетів живучість мереж різко зростає. Фізично наскрізний канал не створюється, повідомлення поділяється на пакети і кожен з пакетів передається мережею самостійно своїм маршрутом. На кожному з вузлів пакет передається, якщо є хоча б один канал у потрібному напрямі. На місці прийому всі пакети знову збираються у повідомлення. Повідомлення буде передане навіть коли більша частина мережі зруйнована, якщо знайдеться хоча б один віртуальний маршрут.

Для телекомунікаційних мереж, які є розподіленими інформаційними системами розрізняють *функціональну і структурну живучість*. Останнім часом сформовано ще й поняття *інформаційної живучості*. Під функціональною живучістю розуміють здатність системи виконувати із заданою якістю ціль функціонування при наявності несприятливих впливів. Структурна живучість – це здатність системи підтримувати необхідну для виконання із заданою якістю цілі функціонування й системну структуру при наявності несприятливих впливів. Інформаційна живучість безпосередньо зв'язана з інформаційною безпекою й розуміється як здатність системи забезпечувати доступність, цілісність та конфіденційність інформації на рівні, який дозволяє виконувати із заданою якістю ціль функціонування незалежно від зовнішніх і внутрішніх несприятливих інформаційних впливів і порушень у використанні інформаційних ресурсів.

Нова парадигма інформаційної безпеки телекомунікаційних мереж

На розвиток моделі інформаційної безпеки телекомунікаційних мереж впливають ряд нових факторів і серед них: зростання ролі телекомунікаційних мереж у критичних фізичних та інформаційних ресурсах держави; особливості функціонування телекомунікаційних мереж, як взаємо зв'язаної сукупності об'єктів інформаційної діяльності; відсутність повної глобальної спостережності сучасних мереж внаслідок необмеженості мережного середовища; відсутність у середовищі функціонування єдиної політики безпеки; суміщення централізованого та децентралізованого управління; необхідність посиленого розвитку певних функцій телекомунікаційних мереж та телекомунікаційних послуг в світлі впровадження систем електронного уряду, електронного документообігу, електронного цифрового підпису, розвитку електронної торгівлі тощо.

В сучасних інфраструктурах країни телекомунікації мають виключну роль. Національна безпека України залежить від цілісності, надійності й готовності критичних фізичних та інформаційних інфраструктур. Поняття «критичної інфраструктури» включає в себе сукупність фізичних або віртуальних систем і засобів, важливих для держави настільки, що їх вихід з ладу або знищення можуть привести до згубних наслідків у області економіки, оборони, охорони здоров'я та національної безпеки. Стає великою залежність військових

технологій від загроз інформаційним технологіям і вразливості останніх. Програмно-математичний вплив на інформаційно-комунікаційні системи, так звані комп'ютерні атаки, засоби інформаційного протиборства направлені на використання, модифікацію, підміну або знищення інформації, яка міститься у комп'ютерах та інформаційних мережах, зниження ефективності функціонування або виведення з ладу самих комп'ютерів та інформаційних мереж. До них відносяться засоби несанкціонованого доступу, комп'ютерні віруси, програмні закладки, «логічні бомби» та «троянські коні», нейтралізатори тестових програм, навмисне створені приховані інтерфейси для входу в інформаційну систему з корисними або диверсійно-підривними намірами, створення непомітних завад інтелектуального впливу на системи зв'язку, збирання та обробка інформації шляхом блокування, підміни у повідомленнях ключових елементів, введення у повідомлення хибних ключових елементів.

Завади інтелектуального впливу треба враховувати у системах забезпечення безпеки суспільно політичних відносин в рамках забезпечення національної безпеки. Вони базуються на автоматизованому аналізі структури повідомлень, слідкуванні за ключовими словами, синтезі мови у реальному масштабі часу. Небезпека таких загроз у тому, що фальсифікація може проводитись не лише власником чи розпорядником інформації, за що він має нести відповідальність перед законом, а й противником, приховано, під час передачі інформації телекомунікаційною мережею. Навмисне руйнування, переривання або перекручення даних у цифровій формі або потоків інформації приводять до широкомасштабних наслідків у політичному, релігійному або ідеологічному планах. Інформація викрадається, перекручується, обмежується, фільтрується з метою впливу (або виключення впливу) на психіку людини, психологію великих мас людей, суспільну свідомість з метою примусити їх думати і діяти в напрямі, потрібному для того, хто організує та здійснює цей вплив.

Можна вважати, що рівень небезпечності загроз цільового інформаційного впливу прямо пропорційний рівню технологічного розвитку мереж та масштабам застосування комп'ютерів у системах управління мережею, галуззю і державою в цілому. З огляду на телекомунікаційні мережі зростає важливість вимог забезпечення цілісності та достовірності передачі інформації, захисту від порушень правил маршрутизації, точності й своєчасності доставки інформації (мінімальної затримки повідомлень), а також захисту від несанкціонованого доступу до інформаційних ресурсів мереж та забезпечення фізичної безпеки інформаційної інфраструктури.

Безпека інфраструктури держави в цілому залежить від рівня безпеки державних і комерційних інформаційних та телекомунікаційних систем. Живучість цих систем визначає мобілізаційну готовність збройних сил, промисловості, економіки, народного господарства і суспільства в цілому як до ведення війни, так і до ліквідації наслідків терористичних актів, стихійних лих і техногенних катастроф. Для збереження мінімального набору критично важливих функцій інформаційно-телекомунікаційна система повинна мати певний запас живучості та стійкості до зовнішніх дестабілізуючих впливів середовища. Тому при розробці *систем інформаційної безпеки телекомунікаційних мереж* необхідно враховувати невизначеність умов їх функціонування при використанні глобальних мереж. Реалізація нової парадигми інформаційної безпеки, з урахуванням усіх перелічених факторів, має дати гарантію, що, навіть при несанкціонованому проникненні в контур керування, втраті частини ресурсів та перенавантаження трафіку, комплекс організаційно-технічних заходів захисту забезпечить виконання найбільш важливих задач.

Серед критичних інфраструктур телекомунікаційні мережі, поряд з інформаційними технологіями, системами управління виробництвом, системами електропостачання та базами даних, займають особливе місце. Телекомунікаційні мережі можна вважати найкритичнішою інфраструктурою країни. Вирішальне значення має розробка заходів із захисту, дублювання, мобільності, сполучення, відновлення й безпеки телекомунікаційних систем країни для використання в інтересах управління державою критичних інформаційних послуг та телекомунікаційних ресурсів як у надзвичайних умовах, так і в режимі нормального

функціонування. Законом України «Про телекомунікації» ставляться вимоги забезпечення живучості, що передбачає підтримання таких властивостей як надійність функціонування телекомунікаційної, сталість, доступність інформаційних ресурсів, цілісність структури, відновлюваність.

Забезпечення надійності й готовності телекомунікаційних мереж

Ефективним методом аналізу і синтезу телекомунікаційної мережі є метод розрахунків, що використовує теорію графів, гіпермереж та інших теорій, які використовують структурні моделі систем. При використанні таких методів основною метою є постановка і вирішення математичних (теоретико-графових) задач аналізу і синтезу телекомунікаційних мереж, на базі яких може бути створена методика комплексного проектування структури мережі. Дана методика припускає рішення цієї задачі в декілька етапів: оцінки необхідних параметрів телекомунікаційної мережі і розробка на їх базі спрощеної моделі мережі; вибору оптимального методу аналізу і синтезу структури мережі та оптимальної топології з урахуванням сукупності обмежень, що задаються; аналізу проблеми забезпечення надійності і живучості телекомунікаційної мережі. Як критерії ефективності розглядаються економічні критерії, критерії якості передачі, критерії живучості, зокрема надійності мереж.

Вирішимо задачу пошуку оптимальної топології телекомунікаційної мережі за критерієм живучості. Будемо відрізняти формальну і фізичну топологію мереж. Під формальною топологією мережі будемо розуміти математичну модель мережі у вигляді неорієнтованого графа, де мережа представлена вершинами графа (вузлами комутації), з'єднаних між собою ребрами графа (каналами зв'язку). Фізична топологія визначається архітектурою технології, за якою побудовані фрагменти мережі. Вона залежить від конкретних архітектурно-технологічних рішень, прийнятих у цифрових системах передачі. По суті фізична топологія – це топологія вторинної мережі, побудованої на базі первинної мережі магістральних каналів. Така топологія може бути описана за допомогою методів теорії гіперграфів. Питання вибору фізичної топології з урахуванням особливостей архітектури цифрових систем передавання буде предметом розгляду наступної роботи.

Сукупність вимог, які пред'являються існуючим або проектованим мережам, називаються критеріями ефективності телекомунікаційної мережі. Таким чином, критерії ефективності - це умови, відповідно до яких приймається рішення щодо ефективності функціонування мережі. Як сказано вище, розрізняють три види критеріїв: критерії якості і надійності функціонування, економічні критерії, критерії живучості. З погляду телекомунікаційної безпеки критерії якості й економічні показники не є першочерговими, тому при розгляді різних топології мережі важливим показником є критерій живучості, на підставі якого далі проводяться відповідні розрахунки.

Важливим критерієм живучості є надійність, яку також поділяють на функціональну та структурну надійність. Функціональна надійність характеризується тим, що при послідовній відмові елементів із заданою інтенсивністю мережа залишається в працездатному стані в плині заданого часу. Враховується також таке поняття як, час наробітку на відмовлення. Звичайно розрізняють повне відмовлення працездатності і часткове відмовлення працездатності. Всі інші поняття, зв'язані з відмовленням працездатності, характеризуються динамікою переходу з одного стану в інший. Об'єктивною характеристикою є ймовірність P технічної готовності мережі до передавання інформації між вузлами зв'язку принаймні в одному напрямі зв'язку. У теорії надійності ця характеристика визначається як ймовірність зв'язності, або ймовірність справного стану хоча б одного з можливих напрямів зв'язку.

Серед параметрів, які характеризують живучість телекомунікаційних мереж виділимо структурну надійність [4], під якою розуміють здатність забезпечувати зв'язність вузлів мережі з якістю, не нижчої від заданої. Основним показником такої якості є ймовірність

зв'язності двох- і багатополюсних систем зв'язку. Структурною надійністю ще називають сукупність програмних, апаратних, програмно-апаратних та організаційних засобів, спрямованих на забезпечення неперервної роботи усієї мережі в цілому. Розрахунок величини структурної надійності розглядається у численних роботах з теорії надійності, зокрема у роботах [4, 7]. Структурна надійність оцінюється імовірністю виходу із ладу елементів мережі, при якому унеможливлюється з'єднання двох або більше вузлів.

Дослідимо докладніше проблему надійності та цілісності структури, як показників живучості телекомунікаційної мережі. Вказаних показників замало для всебічної оцінки живучості та ефективності телекомунікаційних мереж. Доводиться використовувати ще й інші показники та формувати різного роду інтегральні показники. В даній роботі залучимо для попереднього порівняння мереж такий показник, як загальна довжина магістралей, які з'єднують між собою вузли мережі, для яких проводяться розрахунки.

При створенні теоретичної моделі необхідно дати математичне описання, оскільки при застосуванні теорії графів не завжди можливо точно описати структуру мережі. При аналізі мереж, крім методів теорії графів, необхідно користуватися також різними емпіричними прийомами дослідження. Структура телекомунікаційної мережі може бути задана графом:

$$C = (X, R) = <X_{11},\ldots, X_{ij}; R_1,\ldots, R_k; G>, \quad (1)$$

де $X = (x_1,\ldots,x_n)$ – множина вершин, а $R = (r_1,\ldots,r_m)$ – множина гілок; $X_{11},\ldots, X_{ij}$ $R_1,\ldots, R_i$ – множина типів зв'язків між вузлами $R_1,\ldots, R_i$.

Кожному мережному вузлу буде відповідати вершина графа G, а кожному каналу зв'язку – гілка графа G. Характеристика елементів телекомунікаційної мережі, в такому випадку, відповідає параметрам відповідних вершин і гілок графа G.

Основними способами забезпечення надійності мережі є підвищення надійності всіх її компонентів, а головне, застосування резервування. Найбільш підходящою структурою мережі на початковому етапі її розвитку була радіально-вузлова структура (рис. 1). В цій структурі розрізняють вузли 1-го, 2-го і 3-го рівня. В рамках такої структури резервування вузлів і каналів передачі приводить до схеми (рис. 2), де показані основний та резервний головні вузли і пунктиром додаткові резервні канали. На кожен вузол резервні канали повинні входити з різних напрямів, але не повинні проходити по одним і тим же магістралям або системам передачі, бо відмови та збої в каналах у межах одної системи передачі чи магістрального кабелю сильно корельовані.

У радіально-вузловій структурі вузли 2-го рівня для підвищення надійності з'єднуються по принципу „кожен з кожним". Вузли нижніх рівнів приєднуються за радіальним принципом (рис. 3). Радіально-вузлова схема є, так би мовити, віртуальною схемою у трьох мірному просторі, яку для реалізації треба проектувати на площину і реалізувати на базі первинної мережі магістральних каналів передачі. Реально канали та вузли розташовуються на поверхні земної кулі і утворюють досить складну топологію. Наприклад, система подвійного резервування на 3-му рівні приводить до схеми (рис. 4), де траси пролягання основних та резервних каналів між вузлами 2-го і 3-го рівнів на площині утворюють трикутники і чотирикутники. Схеми потрійного та вищих ступенів резервування приводять ще до більш заплутаних схем.

Радіально-вузлова структура мережі мала суттєву перевагу при комутації каналів. При комутації каналів вирішальною була вимога обмеження числа пере-приймальних ділянок. Для всіх вузлів нижнього рівня це число однакове. У мережах передачі (комутації) пакетів така вимога не застосовується, хоча впливає на величину затримки повідомлень. Радально-вузлова структура не гнучка. Наявність головного вузла знижує надійність усієї мережі. Руйнування чи відмова головних вузлів означає розпад мережі на не зв□язані між собою фрагменти. З появою технологій комутації пакетів відкрились можливості суттєво підвищити живучість мереж у порівнянні з мережами комутації каналів. Тому доцільно розглядати й

інші топології мереж.

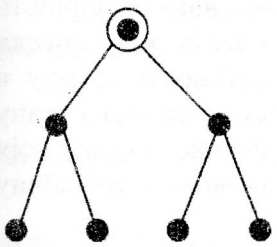

Рис. 1

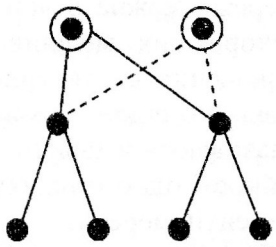

Рис. 2

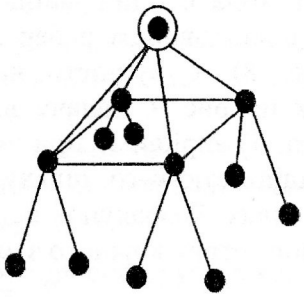

Рис. 3

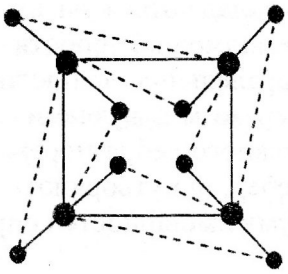

Рис. 4

Останнім часом, все більший розвиток має принцип організації інформаційних, телекомунікаційних, обчислювальних та інших критичних ресурсів по типу «матриці», коли забезпечується гнучкий, безпечний і централізований розподіл ресурсів в інтересах так званих «віртуальних організацій», які створюються під вирішення виникаючих задач в складній динамічній обстановці [6]. Наприклад, Пентагон створює глобальну інформаційну матрицю (Global Information Grid), за допомогою якої, уже починаючи з 2005 р., буде здійснювати у реальному часі керування мобільними і компактними змішаними формуваннями у будь-якому районі земної кулі.

Розглянемо можливі топології матричної мережі та оцінимо їх з позицій сумарної довжини каналів та структурної надійності. Для спрощення задачі будемо розглядати покриття території прямокутної форми правильними багатокутниками. Легко показати, що для потрійного резервування необхідне покриття шестикутниками (рис. 5), для резервування з чотирьох напрямів необхідне покриття чотирикутниками (рис. 6), для резервування з шести напрямів – трикутниками (рис. 7). Покриття п'ятикутниками можливе лише для сфери з цілком певним діаметром (прикладом служить - футбольний м'яч).

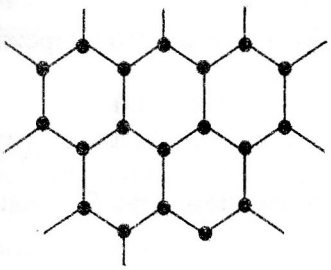

Рис. 5

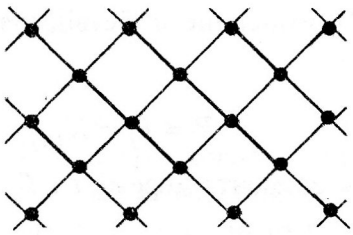

Рис. 6

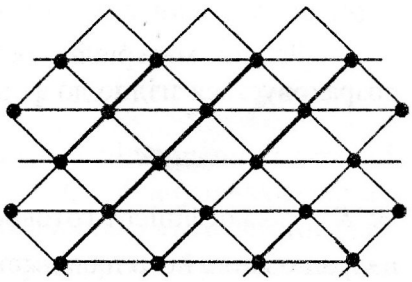

Рис. 7

Для розрахунків приймемо, що територія має форму прямокутника з площею $S = 600 \cdot 1000$=600 000 кв. км., що близько до загальної площі України, а вузлирівномірно розподілені цією площею. Кількість вузлів $N = 38$, однакова для всіх варіантів. Розрахуємо показник структурної надійності для довільного вибраного двополюсника, що представляє собою сукупність можливих шляхів, які з'єднують термінали двох абонентів, відстань між якими фіксована. Місця включення терміналів двох абонентів виберемо так. Прямокутну територію поділимо на дві рівні частини. У кожному з нових утворених прямокутників виберемо по вузлу X_i та Y_j, які розташовані найближче до центрів цих прямокутників. Далі побудуємо двополюсники шляхів, які з'єднують вибрані вузли для кожної з топологій, що порівнюються.

Подія зв'язності у двохполюсних мережах настає тоді, коли між вибраною парою вершин X_i та Y_j існує хоча б один ланцюг. Шляхи можливого з'єднання цих вузлів розкладаються на прості послідовності ребер мережі, кожне з яких має свою імовірність безвідмовної роботи (рис. 8). Сукупність найкоротших можливих шляхів має вигляд паралельних ланцюгів, як на рис 9. Задачу визначення структурної надійності зв'язку в мережі між вузлами X_i та Y_j вирішимо при умові, що відомі ймовірності справного стану кожного ребра мережі. Надійністю k–го шляху називають ймовірність справного стану всіх ребер, що утворюють цей шлях. Розрахунок надійності одного шляху становить алгебраїчну суму ймовірностей справного стану кожного з елементів мережі:

$$P_{i,j} = \sum (p_i + p_j), \tag{2}$$

де P_i - імовірність виходу з ладу комутаційного вузла мережі; P_j - імовірність виходу з ладу лінії, яка з'єднує вузли мережі; $P_{i,j}$ - сумарна імовірність виходу з ладу послідовно з'єднаного відрізка мережі.

Надійністю зв'язку від X_i до Y_j є ймовірність справного стану принаймні одного шляху із заданої їх множини m_{ij}. Для порушення зв'язку від X_i до Y_j достатньо, щоб вийшли з ладу всі ребра хоча б одного перерізу s_{ij} із множини перерізів S_{ij}, що відповідає множині m_{ij} шляхів. Ймовірність справного стану принаймні одного шляху виглядає як добуток елементів які входять в структуру мережі. Таким чином, структурна надійність виглядає як:

$$P_k = \prod p_{i,j}, \tag{3}$$

де P_k - імовірність виходу з ладу сегмента мережі, який з'єднує рознесені у просторі комутаційні вузли.

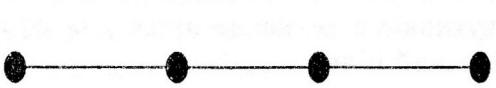

Рис. 8

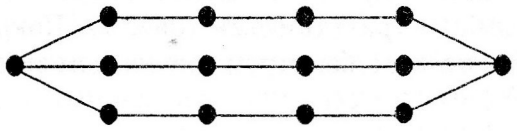

Рис. 9

Згідно матеріалів роботи [3] ймовірність безвідмовної роботи елементів мережі розраховується згідно до формули:

$$P_i = P_j = K_{Гi(j)} \varepsilon^{-\frac{t}{T_m}}, \tag{4}$$

де $K_{Гi(j)}$ - коефіцієнт готовності *i(j)* – елемента мережі; t t, T_m - час роботи елемента; T_m - час напрацювання його на відмову.

Коефіцієнт готовності залежіть від показників елемента, які є базовими на етапі розробки цього елемента:

$$K_{Гi(j)} = \frac{T_m}{T_m + T_в}, \tag{5}$$

де $T_в$ - середній час відновлення елемента після його відмови.

Результати розрахунків наведені у табл. 1.

Оцінимо сумарну довжину каналів зв'язку при різних варіантах топології матричної мережі зв'язку. Число вузлів мережі для різних варіантів не змінне. Для топології покриття площі шестикутниками (рис. 5), тобто для топології мережі резервуванням з трьох напрямків (потрійне резервування), сумарна довжина каналів складає величину:

$$L = 2 \cdot m \cdot l \cdot k, \tag{6}$$

де L – сумарна довжина каналів; m – кількість вузлів; l – довжина одного ребра; k – коефіцієнт поправки на довжину ребра відносно другого варіанту (рис. 6). $k_1 = 0,85$.

Для топології покриття площі чотирикутниками (рис. 6), тобто для топології мережі резервуванням з чотирьох напрямків, сумарна довжина каналів складає величину:

$$L = 2 \cdot m \cdot l. \qquad (7)$$

Для топології покриття площі трикутниками (рис. 7), тобто для топології мережі резервуванням з чотирьох напрямків, сумарна довжина каналів складає величину:

$$L = 3 \cdot m \cdot l \cdot k_3, \qquad (8)$$

де k_3 – коефіцієнт поправки на довжину ребра відносно другого варіанту, $k_3 = 0,75$.

Результати розрахунків зведені в табл. 1. Варіанти топології мереж розрізняються мнтодом резервування – з трьох напрямків (потрійне резервування), з чотирьох та з шести напрямів.

Таблиця 1. Порівняння топологій мереж

№ вар.	Кількість Вузлів	Степінь резервування	Сумарна довжина каналів	Імовірність виходу з ладу	Структурна надійність P_k
1	36	Потрійне	62	0.000038	0,48
2	36	З 4-х напрямів	71	0.000029	0,666
3	36	З 6-и напрямів	96	0.000019	0,998
4	6 +(6 *5)	Потрійне	153	0.000041	0,47

Для порівняння розрахована величина сумарної довжина каналів радіально-вузлової схеми при тих же S та N і методі потрійного резервування каналів до вузлів третього рівня. Для його варіанту прийнято таке допущення, що шість вузлів другого рівня розміщені рівномірно по всій площі і з'єднані по принципу «кожен з кожним». До кожного вузла другого рівня приєднано радіально по п'ять вузлів. Один вузол є головним з подвійним резервуванням. Результати розрахунку наведено в нижньому рядку табл. 1.

Висновки

За результатами розрахунків можна зробити такі висновки. З підвищенням степені резервування у мережі з матричною топологією загальна довжина з'єднувальних ліній збільшується не значно у порівнянні із збільшенням структурної надійності мережі. Таким чином, використання резервування із 6-и напрямків дозволяє організувати систему забезпечення безпеки, яка відповідає більш жорстким умовам живучості мереж. Формальна матрична топологія телекомунікаційних мереж має преваги у порівнянні з радіально вузловою резервованою структурою мережі за показниками структурної надійності. Нова парадигма побудови інформаційної безпеки приділяє суттєву роль питанням живучості телекомунікаційних мереж і врахування невизначеності умов їх функціонування.

Напрямком подальших досліджень може бути розробка методики вибору оптимальної фізичної топології з урахуванням особливостей архітектури цифрових систем передавання.

Список літератури

1. Горицкий В.М., Павлов И.Н. Оценка вероятности безотказной работы комплексной системы защиты информации // Зв'язок, 2005. – № 5. – С. 50-56.

2. Додонов А.Г., Кузнецова М.Г., Горбачик Е.С. Введение в теорию живучести вычислительных систем. – К.: Наук. Думка, 1990. – 184 с.

3. Романов О.І., Лівенцев С.П., Павлов І.М. Методика оцінювання надійності комплексних систем захисту інформації у спеціальних телекомунікаційних системах // Зв'язок, 2005. – № 2. – С. 36-38.

4. Рижаков В.А., Сакович Л.М. Кількісне оцінювання структурної надійності систем зв'язку // Зв'язок, 2004. – № 4. – С. 53-57.

5. Леваков А. Анатомия информационной безопасности США. Jet Info online №6(109). -- 2002. *http://daily.sec.ru/dailypblshow.cfm?rid=9&pid=5503&pos= =13&stp= 10.*

6. Леваков А. В интересах внутренней безопасности США. Jet Info Специальный выпуск. 2004. – С. 36. *http://www.jetinfo.ru.*

7. Богуш В.М., Юдін О.К. Інформаційна безпека держави. - К.: МК-Прес, 2005. – 432 с.

Надійшла 29.09.2006

УДК 681.3

Дуткевич Т.В., Піскозуб А.З.

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ СИСТЕМ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ АТАК У ВИСОКОШВИДКІСНИХ КОРПОРАТИВНИХ МЕРЕЖАХ

1. Основні проблеми виявлення та запобігання атак в корпоративних мережах

Проблема безпеки корпоративних мереж набуває надзвичайної актуальності. Існуючі на сьогодні методи захисту: брандмауери, антивіруси, віртуальні мережі, системи виявлення та запобігання атак - не здатні у повній мірі задовольняти вимоги корпоративного інформаційного середовища. В умовах чіткої тенденції до масового використання сучасних засобів телекомунікації, зокрема мережі Internet, у бізнес-процесах та з іншого боку, зростання складності Internet загроз - вірусів і хробаків, DoS атак, атак на засоби електронної комерції, життєво важливим є забезпечення високого рівня захисту ресурсів корпоративних мереж. Тому виникає потреба у дослідженні проблем систем безпеки та розробки нових методів, здатних ефективно захищати ресурси корпоративних мереж [1].

Традиційні програмні та апаратні засоби не відповідають вимогам корпоративних мереж, оскільки вони не здатні ефективно аналізувати потік даних, не знижуючи при цьому загальної продуктивності мережі. Висока вартість комерційних кінцевих рішень не дозволяє широко впроваджувати їх у вітчизняні корпоративні мережі.

Дана проблема робить особливо актуальною розробку спеціалізованих засобів, зокрема систем виявлення та запобігання атак, в основі яких лежить рішення з відкритим кодом, для ефективного захисту високошвидкісного середовища корпоративної мережі.

Останні дослідження проведені групою дослідницьких лабораторій NSS відображають переваги тільки кінцевих продуктів окремих виробників. На скільки нам відомо, інших ґрунтовних досліджень особливостей підходів виробників до виявлення атак, результати яких доступні для публічного ознайомлення, немає. Наявні результати досліджень не можуть мати достатньої достовірності, оскільки, в більшості випадків, проводяться на замовлення виробників і як результат - недолікам приділяють недостатньо уваги. Перебільшення отриманих результатів призводить до хибного відчуття безпеки.

Невирішеними залишається ряд проблем. Серед них: відсутність стандартизованих методів оцінки продуктивності та ефективності систем виявлення та запобігання атак, відсутність єдиних підходів до виявлення атак, не зацікавленість більшості комерційних виробників у розвитку вільного програмного забезпечення, низька сумісність кінцевих