УДК 004.722.056:004.724

М. Ю. Костяк, Л. Т. Пархуць
Національний університет "Львівська політехніка",
кафедра захисту інформації

ОСОБЛИВОСТІ ПРОЕКТУВАННЯ ЗАХИЩЕНИХ ІНФОРМАЦІЙНИХ МЕРЕЖ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

© Костяк М. Ю., Пархуць Л. Т., 2016

Розглянуто особливості проектування захищених інформаційних мереж спеціального призначення. Вказано особливості архітектури побудови таких мереж, розглянуто питання управління процесом обміну інформацією та вибору оптимального алгоритму функціонування захищених інформаційних мереж.

Ключові слова: захист інформації у комп'ютерній мережі, проектування захищених мереж, управління процесом обміну інформацією.

The article discusses the features of protected information networks design for special purposes. There were indicated the features of architecture of building such networks, the problem of process control of information exchange and choosing the optimal algorithm operation of protected information networks.

Key words: information protection in computer networks, protected networks design, managing the exchange of information.

Вступ

Масове використання комп'ютерних мереж для опрацювання, зберігання та передачі інформації, віддаленого управління стратегічними та потенційно небезпечними об'єктами, керування транспортом, життєвим циклом у приватних будівлях тощо, значно розширило можливості несанкціонованого доступу та дій над інформацією. Необхідність захисту не лише державної та військової, а й промислової, комерційної, фінансової таємниць, захист інформації загалом та захист інформації в автоматизованих системах стає щоразу актуальнішою і складнішою проблемою.

Події останніх років свідчать, що мережі загального користування Інтернет не можуть забезпечити гарантований захист інформації з обмеженим доступом. Тому усе більшого поширення, зокрема в Україні, набувають спеціальні захищені інформаційні мережі (ЗІМ).

ЗІМ мають певні особливості порівняно з мережею Інтернет. Вони розподілені нерівномірно за щільністю абонентів на території обслуговування, абоненти мають різні пріоритети та права, інформаційні повідомлення мають різні рівні важливості і пріоритету в обслуговуванні, повинні працювати постійно і безвідмовно у надзвичайних ситуаціях та забезпечувати відповідний рівень захисту інформації.

Сьогодні не має єдиного математичного підходу до вирішення проблеми проектування, оптимізації архітектури та технології функціонування ЗІМ. Причиною цього є складність і неоднорідність ЗІМ та їх параметрів, більшість з яких погано формалізуються, вимагають адаптації в процесі функціонування, а використовуваний в галузі інформаційної безпеки математичний апарат не є довершеним.

Зважаючи на відсутність єдиного математичного апарата не існує і загальної методології проведення апріорного аналізу властивостей ЗІМ, порівняння алгоритмів їх функціонування, що загалом позбавляє можливості обгрунтованого вибору архітектури та алгоритмів функціонування елементів та вузлів ЗІМ. Тому надзвичайно актуальним є подальший розвиток теорії оптимізації архітектури та технології функціонування ЗІМ.

Особливості архітектури захищених інформаційних мереж

Архітектура захищених інформаційних мереж – це організаційно-технічне об'єднання окремих підсистем, яке містить інформацію про характерні принципи побудови системи та зв'язки: внутрішні – між підсистемами та зовнішні – із надсистемами, їхній поточний стан та тенденції перспективного розвитку. Архітектура мережі забезпечує динаміку розвитку системи, її здатність до нарощування номенклатури комунікаційних послуг, можливість широкого впровадження сучасних спеціалізованих та універсальних додатків [1].

Функціональна архітектура ЗІМ визначає склад функціональних підсистем та комплексів завдань, які забезпечують реалізацію процесів. Відповідно до функціональної архітектури, формуються організаційні компоненти ЗІМ, насамперед це є мережа комунікацій, робочі станції та автоматизовані робочі місця кінцевих користувачів і серверна підсистема мережі, визначається їхня взаємодія.

Інформаційно-технологічна архітектура включає апаратно-програмну платформу реалізації ЗІМ, організаційну форму бази даних, архітектуру та топологію комп'ютерної мережі, засобів телекомунікації, комплекс технічних засобів обробки даних. Визначається інформаційно-технологічна архітектура ЗІМ програмними та технічними засобами, які використовуються зокрема засобами телекомунікації та системами управління базами даних [1].

Сьогодні склались типові інформаційно-технологічні структури комп'ютерних інформаційних систем та відповідні структури ЗІМ:

1) централізована обробка даних, коли на одному комп'ютері встановлені та функціонують засоби: інтерфейсу, що забезпечує інтерактивний режим роботи користувача; змістовної обробки – програми додатків; організації та використання баз даних;

2) файл-серверна розподілена обробка даних: на робочій станції знаходяться засоби інтерфейсу та програми додатків, на сервері зберігаються файли бази даних;

3) клієнт-серверна дворівнева розподілена обробка даних: на робочій станції знаходяться лише засоби інтерфейсу, на сервері додатків – програми додатків, а на сервері баз даних зберігаються СУБД та файли бази даних.

Наявність виділених рівнів у технологічній структурі дає можливість варіювання апаратних та програмних засобів для реалізації структурних складових інформаційно-технологічної архітектури ЗІМ: вибір операційних систем, СУБД, інтерфейсів користувачів, серверів та робочих станцій.

Під час проектування ЗІМ виділяється певне коло завдань, виконання яких є першочерговим. Процес проектування є спрощеним моделюванням майбутнього, а тому передбачити усі можливі фактори, врахувати усі потреби, які можуть виникнути, фактично неможливо.

У процесі проектування чи створення нової мережі для будь-якого відомства чи підприємства необхідно враховувати такі основні чинники [2]:

1) необхідний розмір мережі (у найближчому майбутньому та за прогнозом на перспективу);

2) необхідна структура, ієрархія та основні частини мережі (за підрозділами підприємства, а також за кімнатами, поверхами та будівлями підприємства);

3) основні напрямки та інтенсивність інформаційних потоків (в найближчому майбутньому та за прогнозом на перспективу);

4) технічні характеристики обладнання (комп'ютерів, адаптерів, кабелів, репітерів, концентраторів, комутаторів) та його вартість;

5) можливості прокладання кабельної системи у приміщеннях та між ними, а також заходи щодо забезпечення цілісності кабелю;

6) забезпечення обслуговування мережі та контролю за її безвідмовністю та безпекою;

7) вимоги до програмних заходів з допустимого розміру мережі, швидкості, гнучкості, розмежування прав доступу, вартості, можливостей контролю за обміном інформацією тощо;

8) необхідність підключення до глобальних мереж чи до інших корпоративних мереж.

Захищену інформаційну мережу можна розглядати як складну систему, що складається з кількох шарів, які взаємодіють між собою. Основу цієї системи становить множина комп'ютерів

(центрів зберігання та обробки інформації), і транспортна підсистема, яка забезпечує надійну передачу інформаційних пакетів між комп'ютерами. Над транспортною системою працює множина мережевих операційних систем, яка організовує роботу програмного забезпечення у комп'ютерах та надає через транспортну систему ресурси свого комп'ютера для спільного користування.

На наступному рівні працюють системні сервіси, які, користуючись СУБД, як інструментом для пошуку потрібної інформації серед мільйонів та мільярдів байт, які зберігаються на дисках, надають кінцевим користувачам цю інформацію у зручній для прийняття рішення формі, а також виконують деякі спільні для підприємств усіх типів процедури обробки інформації.

До цих сервісів належать служба World Wide Web, система електронної пошти, системи колективної роботи тощо [2].

Верхній рівень ЗІМ являють спеціальні програмні системи, які виконують задачі, специфічні для цього підприємства чи підприємств такого типу. Прикладами таких систем можуть бути системи автоматизації банку, організації бухгалтерського обліку, автоматизованого проектування, управління технологічними процесами тощо. Остаточна мета ЗІМ втілена у прикладних програмах верхнього рівня, але для їхньої успішної роботи абсолютно необхідно, щоб підсистеми інших шарів чітко виконували свої функції [3].

Стратегічні рішення, як правило, впливають на вигляд мережі загалом та стосуються кількох шарів мережевої "піраміди", хоча спершу належать лише до одного конкретного шару або навіть окремої підсистеми цього шару. Такий взаємний вплив продуктів та рішень необхідно обов'язково враховувати під час планування технічної політики розвитку мережі, інакше можна зіткнутися з необхідністю термінової та непередбаченої заміни, наприклад, мережевої технології, через те, що нова прикладна програма відчуває гострий дефіцит пропускної здатності для свого трафіка [4].

Управління процесом обміну інформацією та вибір оптимального алгоритму функціонування ЗІМ

Існує велика кількість варіантів побудови мереж інтегрального обслуговування, що пов'язує задану множину користувачів мережі. Вони відрізняються топологічною структурою, алгоритмами управління, продуктивністю каналів зв'язку і пристроїв комутації, надійністю, захищеністю, живучістю, витратами на створення і експлуатацію тощо.

Множину можливих варіантів можна подати у вигляді об'єднання двох підмножин. Перша підмножина включає варіанти, що забезпечують виконання вимог користувачів захищених інформаційних мереж, друга – варіанти, які не забезпечують виконання відповідних вимог. Основним завданням проектування захищених інформаційних мереж є вибір варіанта, який належить до першої підмножини і вимагає мінімальних витрат на побудову мережі.

У процесі проектування захищених інформаційних мереж можна виділити два основні етапи: системне та інженерне проектування. Системне проектування полягає у виборі топологічної структури ЗІМ, продуктивності мережі, методів і алгоритмів управління функціонуванням мережі і її елементів, а інженерне проектування полягає в реалізації апаратно-програмних вирішень, відповідно до результатів системного проектування [2].

Під час розроблення системи управління можна виділити такі часткові завдання, які виконуються послідовно:

1) вибір методів і розроблення алгоритмів управління процесом обміну інформацією у мережі;

2) розроблення, верифікація та оптимізація протоколів обміну інформацією у мережі;

3) визначення вимог, розроблення структури і алгоритмів функціонування пристроїв комутації;

4) забезпечення необхідного рівня захисту інформації.

Кожне з цих завдань може виконуватися неодноразово, якщо результати виконання інших свідчитимуть про необхідність повторних рішень. Розглянемо докладніше ці часткові завдання проектування, без виконання яких неможливо розв'язати задачу аналізу і синтезу алгоритмів керування обміном інформацією у мережі.

Основні особливості обробки і передачі інформації у ЗІМ інтегрального обслуговування можуть розглядатися на основі двох типів повторюваних процесів, а саме: процесів взаємодії між парою пунктів мережі інтегрального обслуговування і процесів, що відбуваються у пристроях комутації. Це можливо внаслідок того, що процес обробки і передачі інформації складається з повторюваних циклів. Пакет (запит на з'єднання) надходить у пристрій комутації, до якого підключений відправник, обробляється у ньому і передається далі через проміжні пристрої комутації до вузла, до якого підключений одержувач. Цикли обробки є подібними у кожному пристрої комутації.

Тому управління процесом обміну інформації повинно містити управління потоками по входу пристрою комутації, всередині нього і по виходу з нього. Управління по входу пристрою комутації включає процедури управління інтенсивністю переданих по мережі потоків. Управління у пристрої комутації є маршрутизацію потоків, а управління виходу з нього – сукупністю процедур управління структурою мережі.

Останній різновид управління є потужним засобом збільшення продуктивності мережі інтегрального обслуговування і поліпшення якості обслуговування запитів користувачів. Однак реалізація управління структурою мережі інтегрального обслуговування може зажадати дорогих засобів. Тому під керуванням процесом обміну інформацією в мережі інтегрального обслуговування розумітимемо комплекс методів управління вибором маршрутів (маршрутизації) та інтенсивністю переданих по мережі потоків.

Алгоритми управління процесом обміну інформацією разом з протоколами транспортної мережі і алгоритмами комутації становлять основу функціонального програмного забезпечення пристроїв комутації [5, 6]. З погляду системного проектування ЗІМ інтегрального обслуговування важливо оцінити ефективність введення конкретної версії кожного з алгоритмів. Попереднє рішення про використання того чи іншого алгоритму, як правило, приймається на основі доволі наближених аналітичних моделей.

За вибору конкретної версії повинні враховуватися витрати ресурсів на реалізацію алгоритму у процесі функціонування ЗІМ інтегрального обслуговування. Витрати ресурсів пов'язані з необхідністю залучення обчислювальних потужностей пристроїв комутації і передачі службової інформації каналами зв'язку.

Під час виконання завдання розроблення, верифікації та оптимізації протоколів ЗІМ інтегрального обслуговування проводиться остаточна розбивка функцій управління за рівнями програмної структури мережі, здійснюється формалізація і верифікація протоколів і оптимізуються їхні параметри.

Вихідними даними у завданні розроблення структури і алгоритмів функціонування пристроїв комутації використовуються: топологічна структура мережі; параметри потоків інформації, що надходить на входи пристрою комутації; алгоритми управління процесом обміну інформацією; алгоритм комутації; функції витрат на обладнання пристрою комутації. Завдання полягає у виборі такої структури і алгоритмів функціонування пристрою комутації, за яких вузол мав би мінімальну вартість під час виконання вимог до якості обслуговування користувачів.

Мета роботи – дослідити ефективність методів управління маршрутизацією та інтенсивністю потоків інформації у захищених інформаційних мережах інтегрального обслуговування великої розмірності із заданою топологічною структурою і розробити оптимальні алгоритми керування процесом обміну інформацією.

Сформульоване завдання органічно пов'язане з іншими частковими завданнями, що виникають під час побудовя ЗІМ. Оскільки розглядаються мережі інтегрального обслуговування великої розмірності, в багатьох випадках виникає необхідність переходу до зонового управління процесом обміну інформацією [6, 7]. У зв'язку з цим завдання розпадається на два підзавдання: виділення зон управління і розроблення внутрізонових алгоритмів управління процесом обміну інформацією.

Виконання цих завдань включає два підетапи:

1) дослідження ефективності методів адаптивного управління процесом обміну інформацією – аналіз;

2) вибір оптимального алгоритму щодо вибраного критерію – синтез.

На етапі аналізу передбачається виконати такі завдання:

1. Розробити узагальнену модель процесу обміну інформацією у мережах інтегрального обслуговування, на підставі якої можна буде побудувати часткові моделі для оцінки ефективності процесу обміну інформацією.

2. Розробити та обґрунтувати критерій оцінки ефективності алгоритмів керування процесом обміну інформацією у мережі, що дає змогу враховувати продуктивність мережі і показники якості обслуговування запитів користувачів під час реалізації у мережі різних методів управління.

3. Побудувати аналітичну модель процесу обміну інформацією у мережах інтегрального обслуговування зі статичним керуванням з використанням розробленого критерію і апарата теорії масового обслуговування. Результати, одержані на цьому етапі, можуть бути використані для наближеної оцінки показників якості функціонування мереж інтегрального обслуговування під час використання у них алгоритмів адаптивного управління.

4. Побудувати аналітичну модель для оцінки ефективності методів адаптивного управління процесом обміну інформацією за непрямими показниками, які характеризують ступінь наближення заданого методу до методу ідеального спостерігача. На цьому етапі проводиться оцінка витрат на реалізацію методів адаптивного управління, що виражається у погіршенні показників якості функціонування мережі за рахунок наявності службової інформації і необхідності її обробки у пристрої комутації.

5. Розробити і машинно реалізувати імітаційну модель процесу обміну інформацією у мережах інтегрального обслуговування, необхідної для отримання експериментальної оцінки ефективності конкретних реалізацій методів адаптивного управління. В результаті виконання цього завдання уточнюються значення оцінок, отриманих на другому і третьому етапах розробки.

Висновок

Спираючись на розроблену узагальнену модель процесу функціонування мереж спеціального призначення та обрані критерії оцінки ефективності, в роботі розглянуто особливості проектування захищених інформаційних мереж спеціального призначення. Вказано особливості архітектури побудови таких мереж, розглянуто питання управління процесом обміну інформацією та вибору оптимального алгоритму функціонування захищених інформаційних мереж.

Використання запропонованих підходів на етапі проектування чи модернізації існуючих мереж дасть змогу створити мережу з оптимальною архітектурою та оптимальним трафіком передачі інформації, а також сприятиме підвищенню ефективності функціонування інформаційної мережі.

1. Конахович Г. Ф. Захист інформації в мережах передачі даних / Г. Ф. Конахович, О. Г. Корченко, О. К. Юдін. – К.: Видавництво ТОВ "НВП "ІНТЕРСЕРВІС", 2009. – 716 с. 2. Поповский В. В. Математические основы управления и адаптации в телекоммуникационных системах / В. В. Поповский, В. Ф. Олейник. – Харьков: СМИТ, 2011. – 362 с. 3. Соколов А. В. Защита информации в распределенных корпоративных сетях и системах / А. В. Соколов, В. Ф. Шаньгин. – М.: ДМК Пресс, 2002. – 656 с. 4. Соколов А. В. Защита информации в распределенных корпоративных сетях и системах / А. В. Соколов, В. Ф. Шаньгин. – М.: ДМК Пресс, 2002. – 656 с. 5. Костяк М. Ю. Управління обміном інформацією в захищеній локальній мережі / М. Ю. Костяк // VI Міжнар. наук.-техн. конф. "Світ інформації та телекомунікацій-2009". (28–29 квітня 2009 р. Київ: матер. конференції. – К.: ДУІКТ, 2009. – С. 80–81. 6. Костяк М. Ю. Алгоритми внутрішньозонової маршрутизації в захищеній локальній мережі / М. Ю. Костяк, Л. Т. Пархуць // Інформаційна безпека. – 2009. – № 1. – С. 38–43. 7. Дудикевич В. Б. Ієрархічна зонова адресація і маршрутизація в захищеній інформаційній мережі / В. Б. Дудикевич, М. Ю. Костяк, Л. Т. Пархуць, В. О. Хорошко // Вісник СНУ ім. В. Даля. – 2009. – № 6 (136), Ч. 1. – С. 143–149.