6. Якщо $p' = \phi$, то $\Pi(z) := TLV$, перейти на крок 1, інакше в множині $\omega(TLV)$ знайти сукупність всіх пошукових образів текстів по пошуковому розпорядженню p_1'. Виключити p_1' з множини p' пронумерувати розпорядження, які залишились числами 1,2,... Якщо хоч би один текст знайдено, позначити їх множину через $\Pi(z)$ і перейти на крок 2, інакше на крок 6.

7. Кінець алгоритму.

Висновки.

Розглянутий метод пошуку призначений для комплексного підвищення ефективності діагностування сучасних електронно-обчислювальних пристроїв і систем. Він використовується в діагностичних інформаційних системах при пошуку опису тексто-графічної інформації про об'єкти діагностування і властиві їм несправності.

Література

1. Муляр І. В., Джулій В. М. Представлення моделі ООБД інформаційного забезпечення тестового діагностування мікропроцесорних пристроів // Вісник ТУП. – 2004. – № 2. Частина 1, том 1 – С.79– 83.

2. Муляр І.В., Джулій В.М. Інформаційні процеси та моделі їх представлення при тестовому комбінованому діагностуванні // Вимірювальна та обчислювальна техніка в технологічних процесах. – 1999. – № 4.

3. Муляр І.В., Джулій В.М. Гіпертекстова модель представлення інформації в базах діагностичних даних. // Вісник ТУП. – 2001. – № 1. – С.189– 191.

4. Локазюк В. М, Муляр І. В., Джулій В. М. Архітектура автоматизованої системи інтелектуалізації баз даних процесу тестового комбінованого діагностування // Вісник ТУП. – 2002. – № 3. – С.97– 100.

Надійшла 9.9.2009 р.

УДК 004.056

О.А. МЯСІЩЕВ, А.В. ДЖУЛІЙ
Хмельницький національний університет

НАПРЯМКИ ВИРІШЕННЯ ПРОБЛЕМ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖАХ

У даній статті розглядаються концепції безпеки захисту інформації в мережах, основні етапи забезпечення безпеки. Система інформаційної безпеки підприємства повинна враховувати появу нових технологій і сервісів, а також задовольняти загальним вимогам, поставленим сьогодні до будь-яких елементів корпоративної інформаційної системи. Наявність централізованих засобів керування продуктами безпеки є обов'язковою умовою для можливості їхнього застосування в корпоративному масштабі.

In this article conceptions of safety and defense of information are examined in networks, basic stages of providing of safety. The system of informative safety of enterprise must take into account appearance of new technologies and services, and also satisfy general requirements put today to any elements of the corporate informative system Presence the centralized facilities of management safety products is necessary condition for possibility of their application in a corporate scale.

Ключові слова: захист інформації в мережах.

Вступ. Сучасні системи захисту інформації повинні відповідати запитам сучасного бізнесу в умовах росту числа погроз безпеки інформації, що виходять із самої корпоративної мережі. Усе більше співробітників змушені працювати із чутливими ресурсами інформаційної системи, перебуваючи поза її межами. Неухильно зростає швидкість появи нових корпоративних додатків. Збільшуються масштаби й складність мереж. Із цих причин традиційна концепція побудови систем безпеки корпоративної мережі у вигляді захисту тільки зовнішніх каналів зв'язку офіс-офіс (LAN-LAN) уже недостатня. Сучасні системи безпеки повинні захищати не окремі елементи мережі, а інформацію у вигляді інформаційних ресурсів і потоків незалежно від місця й часу їхнього виникнення [1].

Концепція інформаційної безпеки. Інформаційна безпека є складовою частиною інформаційних технологій – області, що розвивається надзвичайно високими темпами. Розробка сучасної системи інформаційної безпеки вимагає, з одного боку, відстеження швидких змін в інформаційних технологіях і погрозах, що з'являються, а з іншого боку – обліку реальних характеристик апаратного й програмного забезпечення корпоративних мереж і систем. Процедура придбання пристроїв інформаційної безпеки не складна. Істотно більш складним є рішення проблем: як захищати і які засоби безпеки застосовувати? Це рішення охоплює й керування інформаційною безпекою, включаючи планування, розробку політики безпеки й проектування необхідних процедур безпеки [1, 2].

Під *інформаційною безпекою* розуміється захищеність інформації й підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, спрямованих на завдання збитків власникам або користувачам інформації й підтримуючої інфраструктури. Природа цих впливів може бути найрізноманітніша. Це й спроби проникнення зловмисників, і помилки персоналу, і вихід з ладу апаратних і програмних засобів, а також стихійні лиха (землетрус, ураган, пожежа й т.п.) [2].

Інформаційна безпека є одним з найважливіших аспектів інтегральної безпеки незалежно від розглянутого рівня – національного, галузевого, корпоративного або персонального. Слід зазначити, що інформаційна безпека не зводиться винятково до захисту інформації, це принципово більш широке поняття. Суб'єкт інформаційних відношень може постраждати (понести матеріальні або моральні збитки) не тільки від несанкціонованого доступу до інформації, але й від поломки системи, що викликала перерву в роботі. Крім того, трактування проблем, пов'язаних з інформаційною безпекою, для різних категорій суб'єктів може істотно розрізнятися. Наприклад, досить зіставити такі різні категорії суб'єктів, як режимні державні організації й комерційні структури. Інформаційна безпека представляє собою багатогранну сферу діяльності, у якій успіх можливий тільки при систематичному, комплексному підході.

У забезпеченні інформаційної безпеки виступають три основні категорії суб'єктів: державні організації, комерційні структури, окремі громадяни. Спектр інтересів суб'єктів, пов'язаних з використанням інформаційних систем, можна підрозділити на наступні основні категорії [2]:

- доступність (можливість за прийнятний час одержати необхідну інформаційну послугу);
- цілісність (актуальність і несуперечність інформації, її захищеність від руйнування й несанкціонованої зміни);
- конфіденційність (захист від несанкціонованого ознайомлення).

Політики безпеки в мережах. Розробка політики безпеки є ключовим етапом побудови захищеної інформаційної системи або мережі [3]. Слід зазначити, що складання політики або політик безпеки є тільки початком здійснення загальної програми забезпечення безпеки організації. Детальна програма забезпечення безпеки необхідна для створення ефективної системи безпеки організації на основі розробленої політики безпеки.

Основними етапами забезпечення безпеки є наступні:

- визначення цінності технологічних і інформаційних активів організації;
- оцінка ризиків цих активів (спочатку шляхом ідентифікації тих погроз, для яких кожний актив є цільовим об'єктом, а потім оцінкою ймовірності того, що ці погрози будуть реалізовані на практиці);
- установлення рівня безпеки, що визначає захист кожного активу, тобто мір безпеки, які можна вважати рентабельними для застосування;
- формування політики безпеки організації на базі попередніх етапів;
- залучення необхідних фінансових ресурсів для реалізації політики безпеки, придбання й установка необхідних засобів безпеки;
- проведення роз'яснювальних заходів і навчання персоналу для підтримки співробітниками й керівництвом необхідних мір безпеки;
- регулярний контроль покрокової реалізації плану безпеки з метою виявлення поточних проблем, обліку зміни зовнішнього оточення й внесення необхідних змін до складу персоналу.

Досвід показав, що в цілому організації одержують істотну вигоду від реалізації добре розробленої методології розв'язання зазначених вище задач.

Політика безпеки повинна:

- указувати мету й причини, по яких потрібна політика;
- описувати, що саме охоплюється її складовими;
- визначити ролі, обов'язки й контакти;
- визначити, як будуть оброблятися порушення безпеки.

Політика безпеки повинна бути:

- реальною й здійсненою;
- лаконічною і доступною для розуміння;
- збалансованою по захисту й продуктивності.

Першими кроками по розробці політики безпеки є наступні:

- створення команди по розробці політики;
- ухвалення рішення про область дії й цілях політики. В області дії повинно зазначатись, хто охоплюється цією політикою;
- ухвалення рішення про особливості розроблювальної політики;
- визначення особи або органа для роботи як офіційного інтерпретатора політики.

До всіх розроблюваних політик безпеки доцільно застосовувати уніфікований процес проектування з однаковими вимогами до політики. Цей процес точно визначав би, хто створює початковий ескіз політики, які групи потрібні для розгляду й побудови кожної політики, якими повинні бути процеси твердження й реалізації політики.

Після аналізу й систематизації вимог бізнес-команда по розробці політики безпеки переходить до аналізу й оцінки ризиків. Використання інформаційних систем і мереж пов'язане з певною сукупністю ризиків. *Аналіз ризиків* є найважливішим етапом формування політики безпеки. Іноді цей етап називають

також аналізом вразливостей або оцінкою погроз.

На етапі аналізу ризиків здійснюються наступні дії:

- ідентифікація й оцінка вартості технологічних і інформаційних активів;
- постулювання й аналіз тих погроз, для яких даний актив є цільовим об'єктом;
- оцінка ймовірності того, що погроза буде реалізована на практиці;
- оцінка ризиків цих активів.

Оцінка ризику виявляє як найцінніші, так і найбільш уразливі активи, вона дозволяє точно встановити, на які проблеми потрібно звернути особливу увагу. Після оцінки ризиків активів можна переходити до встановлення рівня безпеки, що визначає захист кожного активу, тобто мір безпеки, які можна вважати рентабельними для застосування. Вартість захисту конкретного активу не повинна перевищувати вартості самого активу. Необхідно скласти докладний перелік всіх активів, що включає такі матеріальні об'єкти, як сервери й робочі станції, і такі нематеріальні об'єкти, як дані й програмне забезпечення. Повинні бути ідентифіковані директорії, які містять конфіденційні файли або файли цільового призначення. Після ідентифікації цих активів повинно бути проведене визначення вартості заміни кожного активу з метою призначення пріоритетів у переліку активів.

Для контролю ефективності діяльності в області безпеки й для обліку змін обстановки необхідна періодична переоцінка ризиків. Після проведення описаної вище попередньої роботи можна переходити до безпосереднього складання політики безпеки. У політиці безпеки організації повинні бути визначені використовувані стандарти, правила й процеси безпеки. *Стандарти* вказують, які критерії повинно використовувати керування безпекою. *Правила* докладно описують принципи й способи керування безпекою. *Процеси* повинні здійснювати точну реалізацію правил відповідно до прийнятих стандартів. Крім того, політика безпеки повинна визначити значимі для безпеки ролі й указати відповідальність цих ролей. Ролі встановлюються під час формулювання процесів. Як правило, процес складається з однієї або більше дій, де кожна дія включає чотири компоненти (рис. 1):

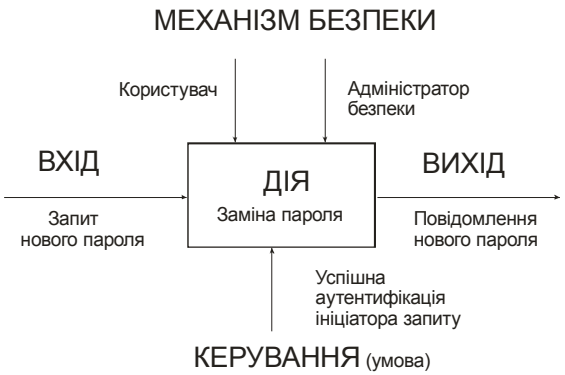

Рис. 1. Графічне подання дії в рамках процесу

1. ВХІД, наприклад, запит користувачем нового пароля.

2. МЕХАНІЗМ БЕЗПЕКИ – реалізує дану дію й указує засоби або ролі, за допомогою яких ця дія виконується. Іншими словами, він визначає, які ролі залучені в цю конкретну дію. У нашому прикладі такими ролями є користувач, що запитує новий пароль, і адміністратор безпеки.

3. КЕРУВАННЯ – описує алгоритм або умови, які керують цією дією. Наприклад, стандарт може задати наступну умову: при запиті нового пароля ініціатор запиту повинен успішно пройти аутентифікацію.

4. ВИХІД – є результатом цієї дії. У нашому прикладі таким виходом буде повідомлення користувачеві нового пароля.

Пов'язуючи разом всі дії, що входять у процес, ми одержуємо точне подання результуючого процесу й ролей, необхідних для його виконання. У даному прикладі процес складається з однієї дії – відновлення пароля користувача; ролі ідентифікуються як Користувач і Адміністратор безпеки. Стандарти, правила й процеси повинні бути документовані в рамках політики для цілей аудиту.

У політику безпеки організації можна виділити базову структуру, що звичайно називають базовою політикою безпеки. Опис базової політики безпеки представляє собою високорівневий документ, що встановлює, як організація обробляє інформацію, хто може одержати до неї доступ і як це можна зробити. У цьому документі визначаються дозволені й заборонені дії, а також вказуються необхідні засоби керування в рамках реалізованої архітектури безпеки. З базовою політикою безпеки, що виконує роль основної структури, узгоджуються спеціалізовані політики й процедури безпеки.

Спадний підхід, реалізований базовою політикою безпеки, дає можливість поступово й послідовно виконувати роботу зі створення системи безпеки, не намагаючись відразу виконати її на 100 %. Ця базова структура дозволяє в будь-який час ознайомитися з політикою безпеки в повному обсязі й з'ясувати поточний стан безпеки в організації [2].

Політика безпеки організації включає наступні елементи:

- огляд політики безпеки;
- опис базової політики безпеки;

- посібник з архітектури безпеки;
- спеціалізовані політики безпеки;
- процедури безпеки (рис. 2).

Огляд політики безпеки розкриває мету політики безпеки, описує структуру цього документа, докладно викладає, хто за що відповідає, установлює процедури й передбачувані тимчасові рамки для внесення змін. Залежно від масштабу організації політика безпеки може містити більше або менше розділів.

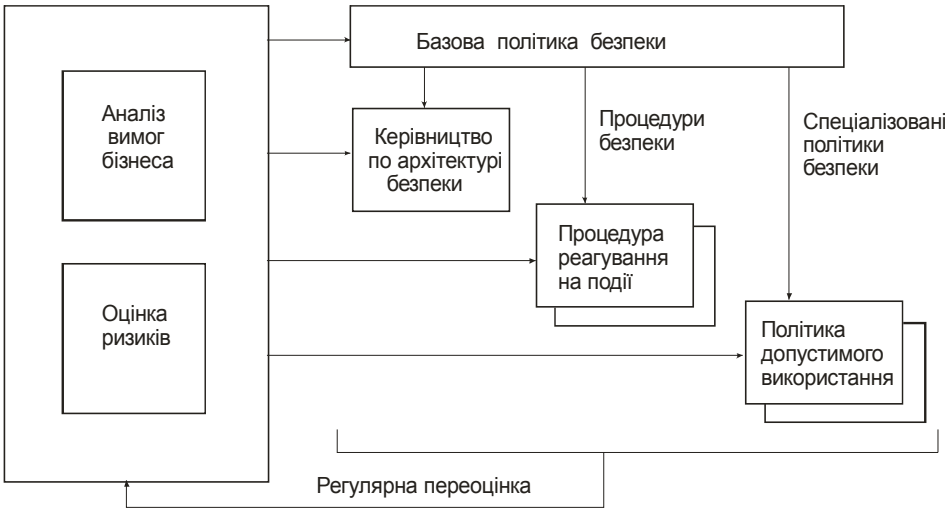

Рис. 2. Схема розробки політики безпеки

Моделі керування безпекою. Напрямки вирішення проблем захисту інформації в мережах. У більшості комп'ютерних середовищ засоби безпеки використовуються головним чином для керування ідентифікаторами ID користувачів і керування доступами до ресурсів. Ці дії часто носять рутинний, повторюваний характер. Вони необхідні для задоволення запитів ресурсів користувачами й підтримки встановленого рівня сервісу.

Достатня безпека системи може бути отримана тільки в тому випадку, якщо реалізується раціональна політика безпеки. Ця політика використовує точно певні ролі безпеки й щодня виконувані операції аудиту й контролю [4].

При створенні системи безпеки повинні застосовуватися методи й технології, що погоджуються з політикою безпеки. Це дозволяє знизити чисто адміністративні витрати й у той же час направити зусилля на використання більш ефективних операцій безпеки.

Адміністративно-організаційна модель керування безпекою, заснована на застосуванні таких категорій, як робочі функції й групи користувачів, дозволяє підвищити рівень безпеки й зменшити адміністративні витрати. *Робоча функція* визначає набір можливостей, необхідних для виконання заданої бізнес-діяльності; вона описує ресурси (файли, бази даних, програму, термінал). Робоча функція встановлює доступ з певними повноваженнями. Опис робочої функції відповідає на запитання: що я можу робити і з якими ресурсами? Іноді опис робочої функції називають *роллю*. *Група користувачів* визначає набір користувачів з подібними обов'язками усередині організації. У нашому випадку це поняття описує користувачів, що працюють в однаковій авторизації. Якщо ці групи зв'язуються з робочими функціями, членство в різних групах впливає на функції будь-якого конкретного користувача.

Якщо зв'язати ідентифікатор користувача із групами користувачів, а групи користувачів – з робочими функціями (ролями), то виходить ефективна модель для керування безпекою. Звичайно, користувачі можуть належати не до однієї, а до декількох груп, а кожна група може включати кілька ролей (рис. 3).

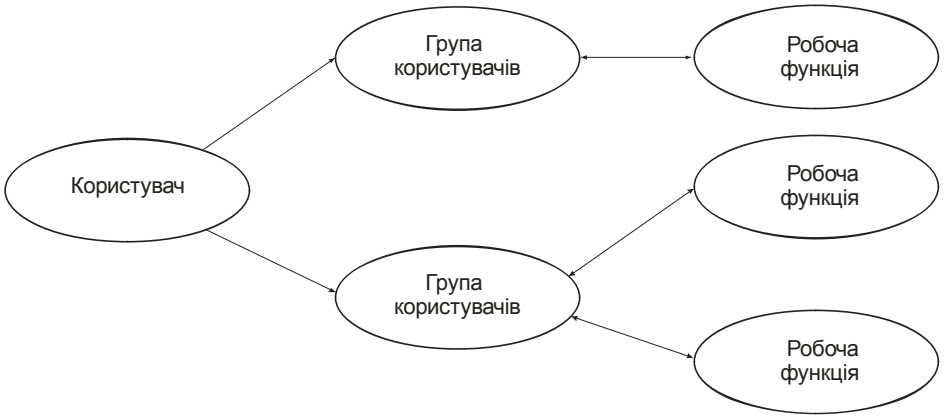

Рис. 3. Модель керування безпекою

При використанні даної моделі немає необхідності керувати доступом користувачів поодинці. Краще керувати відразу асоціацією (групою) користувачів, що набагато ефективніше. Додавання користувача в групу, переміщення користувача з однієї групи в іншу або видалення користувача із групи – сукупність цих нескладних операцій забезпечує зручне й коректне керування доступом користувача до необхідного набору ресурсів. Ці ресурси можуть бути розподілені по багатьох різних системах, навіть різних типах платформ.

Адміністративно-організаційна модель керування безпекою, запропонована вище, може бути реалізована різним чином залежно від використовуваного сервісу безпеки. Застосовується як традиційний підхід, заснований на групах, так і підхід, заснований на ролях. Розглянемо розходження між цими підходами.

Підхід, заснований на групах, визначає, хто може одержати доступ до ресурсу і при якому дозволі. Популярна реалізація цього підходу заснована на використанні списків керування доступом ACL (Access Control Lists) до об'єктів. Списки ACL точно вказують користувачів і групи з їхніми правами доступу до об'єктів. Цей підхід широко розповсюджений серед існуючих сервісів безпеки. Зокрема, цей підхід використовують UNIX, RACF і NT.

При використанні цього підходу необхідно визначити групи, прикріпити їх до об'єктів у якості отримуючих право доступу й потім зв'язати із цими групами користувальницькі ідентифікатори ID. Цей підхід добре працює, але є продукто-орієнтованим, сугубо технічним і слабко зв'язаним зі структурою компанії.

Підхід, заснований на ролях і групах, орієнтується на застосуванні концепції ролей. Адміністратор безпеки визначає ролі й призначає для кожної ролі права доступу до об'єктів. Такий підхід абстрагується від механізму керування доступом, реалізованого в кінцевій точці. Оскільки конкретний тип роботи може вимагати різні ролі (або робочі функції), а різні типи роботи спричиняють обов'язки, що перекриваються (ролі, робочі функції), то на додаток до ролей можна також використати концепцію груп.

Спільне використання концепцій ролей і груп забезпечує краще наближення до реального функціонування організації. Користувачі призначаються в групи відповідно до тієї роботи, що вони повинні виконувати, а групам призначаються ролі згідно з тими робочими функціями, які властиві конкретному типу роботи. Перевага цього підходу полягає в тому, що адміністратор безпеки працює з більш звичними концепціями, близькими до реального життя, що відповідають принципам функціонування його компанії.

Підтримка масових і різноманітних зв'язків підприємства через Internet з одночасним забезпеченням безпеки цих комунікацій є сьогодні основним фактором, що впливає на розвиток корпоративної інформаційної системи підприємства. Однією із найбільш актуальних задач, що стоїть зараз перед розроблювачами й постачальниками інформаційних технологій, є рішення проблем інформаційної безпеки, пов'язаної із широким поширенням Internet, intranet, extranet. Слід зазначити, що засоби злому комп'ютерних мереж і розкрадання інформації розвиваються так само швидко, як і всі високотехнологічні комп'ютерні галузі. У цих умовах забезпечення інформаційної безпеки є пріоритетним завданням для керівництва компанії, оскільки від збереження конфіденційності, цілісності й доступності корпоративних інформаційних ресурсів багато в чому залежить якість і оперативність прийняття стратегічних рішень і ефективність їхньої реалізації.

Створювана система інформаційної безпеки підприємства повинна враховувати появу нових технологій і сервісів, а також задовольняти загальним вимогам, пропонованим сьогодні до будь-яких елементів корпоративної інформаційної системи [5]:

- використання інтегрованих рішень;
- забезпечення масштабування в широких межах;
- застосування відкритих стандартів.

Для того, щоб забезпечити надійний захист ресурсів корпоративної інформаційної системи на сьогодні і на найближче майбутнє, у системі інформаційної безпеки повинні бути реалізовані самі прогресивні й перспективні технології інформаційної безпеки. До них відносяться:

- *комплексний підхід до формування інформаційної безпеки, що* забезпечує раціональне об'єднання технологій і засобів інформаційного захисту;
- *застосування захищених віртуальних мереж VPN* для захисту інформації, переданої по відкритих каналах зв'язку;
- *криптографічне перетворення даних* для забезпечення цілісності, дійсності й конфіденційності інформації;
- *застосування міжмережевих екранів* для захисту корпоративної мережі від зовнішніх погроз при підключенні до загальнодоступних мереж зв'язку;
- *керування доступом на рівні користувачів* і захист від несанкціонованого доступу до інформації;
- *гарантована ідентифікація користувачів* шляхом застосування токенів (смарт-карт, touch-memory, ключі для USB-портів і т.п.) та інших засобів аутентифікації;
- *підтримка інфраструктури керування відкритими ключами РКІ,*
- *захист інформації на файловому рівні* (шляхом шифрування файлів і каталогів) для забезпечення її надійного зберігання;

- *захист від вірусів* з використанням спеціалізованих комплексів антивірусної профілактики й захисту;
- *технологія виявлення вторгнень* (Intrusion Detection) і активного дослідження захищеності інформаційних ресурсів;
- *централізоване керування засобами інформаційної безпеки.*

Наявність централізованих засобів керування продуктами безпеки є обов'язковою вимогою для можливості їхнього застосування в корпоративному масштабі. Необхідно зауважити, що системи централізованого керування продуктами безпеки різних виробників поки не сумісні одна з одною.

Література

1. Вихорев С. В., Березин А. С. Новые подходы к проектированию систем защиты информации // Документальная электросвязь. – 2006. – № 6. – С. 35-37.

2. Галицкий А. В., Рябко С. Д., Шаньган В. Ф. Защита информации в сети – анализ технологий и синтез решений. – М.: ДМК Пресс, 2004. – 616 с.: ил.

3. Козьминых С. И., Забияко С. В. Методологические принципы проектирования интегрированных систем безопасности // Конфидент. – 2002. – № 1. – С. 70-76.

4. Домарев В.В. Безопасность информационных технологий. Системный подход. – К.: ООО ТИД "ДС", -2004. – 992 с.

5. Мамаев М., Петренко С. Технологии защиты информации в Интернете: Специальный справочник. – СПб.: Питер, 2002. – 384 с.

Надійшла 18.9.2009 р.

УДК 519.852.35

Ю.М. ПАНОЧИШИН
Вінницький інститут економіки

ЗАДАЧА РОЗПОДІЛУ ПОТОКІВ У МЕРЕЖАХ ІЗ БАГАТЬМА ДЖЕРЕЛАМИ І СТОКАМИ

У статті формулюється задача розподілу потоків у мережах із багатьма джерелами і стоками та пропонується алгоритм її розв'язання. Проведені дослідження дадуть можливість підвищити якість проектування та ефективність експлуатації різноманітних мережних систем.

The flows distribution problem in networks with many sources and sinks is formulated and the algorithm of its solution is offered in the paper. The researches will enable to increase planning quality and exploitation efficiency of the different network systems.

Ключові слова: потоки в мережах, алгоритм розв'язання.

Вступ. Останнім часом значно зросла зацікавленість учених та практиків мережними і потоковими моделями. Це пов'язано із впровадженням та активним розвитком різноманітних територіально розподілених систем: трубопровідних, транспортних, телекомунікаційних та ін. Основою таких систем є певна мережа (мережа трубопроводів, доріг, каналів зв'язку тощо), в якій циркулюють певні потоки (потоки речовин, транспорту, даних тощо), тому задачі, які доводиться розв'язувати при проектуванні та експлуатації систем з мережною структурою, часто зводяться до розробки математичних моделей розподілу потоків та постановки і розв'язання відповідних оптимізаційних задач.

Відомі моделі розподілу потоків у мережах [1] базуються на поняттях теорії графів [2]. Це пов'язано з тим, що граф дає можливість наочно відобразити структуру мережі, а параметри його вузлів і дуг – представити основними числовими характеристиками її елементів. Набір характеристик залежить від природи модельованої системи, а також характеру розв'язуваних задач, однак у потокових моделях їх, як правило, представляють такими параметрами, як зовнішній потік у вузлі, потік по дузі, пропускна здатність дуги, вартість передавання одиниці потоку по дузі тощо.

Потокові задачі, як правило, зводяться до пошуку такого розподілу потоків у мережі, при якому б забезпечувався екстремум деякого критерію. При цьому мають враховуватися обмеження, що накладаються умовами збереження потоків у вузлах і неперевищення потоками пропускної здатності дуг. Типовими потоковими задачами є задача про потік мінімальної вартості, про максимальний потік, транспортна задача, задача про призначення та інші. Для їх розв'язання розроблено чимало ефективних алгоритмів, сформувався навіть відповідний напрям обчислювальних методів під назвою потокового програмування [1].

Не дивлячись на очевидний прогрес в області потокового моделювання, при проектуванні та експлуатації різноманітних територіально розподілених систем часто виникають задачі, які важко віднести до одного з відомих типів, а тим більше запропонувати ефективний алгоритм їх розв'язання. Так, наприклад, в системах водо-, газо-, теплопостачання, водовідведення, зрошувальних системах часто виникає задача