DOI: 10.18372/2310-5461.62.18709
УДК 004.056

В. О. Хорошко, д-р техн. наук, проф.
Національний авіаційний університет
orcid.org/0000-0001-6213-7086
e-mail: professor_va@ukr.net;

О. А. Лаптєв, д-р техн. наук, старш. наук. співр.
Київський національний університет
імені Тараса Шевченка
orcid.org/0000-0002-4194-402X
e -mail: olaptiev@knu.ua;

Ю. Є. Хохлачева, канд. техн. наук, проф.
Національний авіаційний університет
orcid.org/0000-0002-1883-8704
e -mail: yuliiahohlachova@gmail.com;

Аль-далваш Аблуллах Фоуад, аспірант,
Національний авіаційний університет
orcid.org/0000-0002-1003-9182
e -mail: abdullah.dalosh@gmail.com;

Ю. В. Пепа, канд. техн. наук., доцент,
Державний університет інформаційно-комунікаційних технологій
orcid.org/0000-0003-2073-1364
e -mail: yurka14@ukr.net

ОСОБЛИВОСТІ ПРОЕКТУВАННЯ ЗАХИЩЕНИХ ІНФОРМАЦІЙНИХ МЕРЕЖ

Вступ

В процесі проектування складних систем виконують натурні експерименти, які дають можливість оцінити їх поведінку у певних умовах експлуатації, але зазвичай, це вимагає витрат значних матеріальних і фінансових ресурсів, що не завжди можливо. Зважаючи на це, попередньо використовують комп'ютерне моделювання, яке засновується на програмній реалізації математичної моделі, що описує взаємодію складових частин системи між собою та зовнішнім середовищем експлуатації. Це дає можливість зробити попередній вибір параметрів системи та прогноз її поведінки в різних умовах.

Тенденція зростання складності впровадження захищених інформаційних мереж (ЗІМ) визначає актуальність забезпечення живучості та безпеки мережі. Компоненти більшості відомих систем розробляються з вузьким функціоналом, а оскільки сучасні ЗІМ мають високорозвинені системи передачі інформації, в тому числі з використанням супутникового зв'язку, то в них широко використовуються мікропроцесори (МП) і однокристальні мікрокомп'ютери [1–4].

Досвід проектування ЗІМ з використанням сучасної елементної бази для вирішення спеціальних завдань показав, що водночас ускладнюються інші етапи проектування, а також виникає необхідність кардинальної зміни існуючих принципів і стереотипів проектування. Нагадаємо, що виділяють три основних етапи проектування ЗІМ: системний, структурний та логічний, після виконання яких безпосередньо переходять до технічного. Причому, в нинішньому підході до проектування є три важливі моменти:

1. Принцип проектування та дослідження ЗІМ «знизу-вгору» (побудова мережі з елементів і функціональних вузлів) є основним, а реалізація вищевказаних етапів проектування починається з логічного. При цьому такі вимоги, як розрядність оброблюваних даних, вибір системи команд, специфіка обміну інформацією та інші формуються на основі аналізу задач, які визначають спеціалізацію ЗІМ. Однак деякі особливості проектування «згори-вниз» в даному випадку слід розглядати як не основні.

2. Найбільш пророблениими є задачі логічного етапу (проектування окремих блоків і вузлів, функціонально закінчених пристроїв та ін.), що пов'язано з наявністю розвиненого математичного апарату і засобів моделювання.

3. Процес проектування завершується створенням ЗІМ (виключаючи задачі проектування резервних та інших мереж і систем спеціального призначення).

Крім того, створення ЗІМ стикається з певними труднощами:

– проблема вибору та розробки математичного апарату для етапів системно-структурного проектування;

– неможливість застосування перевірених методів і прийомів класичного підходу до проектування, які пов’язані з тим, що рішення таких структурних задач, як міжабонентський зв’язок та ін., можливе тільки на основі результатів проектування системи «згори-вниз» і стає глобальним, а це відповідає системному підходу.

У той же час в системному підході відсутні обґрунтовані методи і математичний апарат для досліджень.

Аналіз останніх досліджень і публікацій

Процес впровадження нових інформаційних технологій у всі сфери життя суспільства неможливий без вирішення питань інформаційної безпеки. Безпека структурується у абсолютно різних, але пов'язаних між собою аспектами [1, 2]. Широкомасштабне використання обчислювальної техніки та телекомунікаційних систем, перехід до цифрових технології, збільшення обсягів оброблюваної інформації та розширення кола користувачів призводить до якісно нових можливостей несанкціонованого доступу до інформації. Додатково приводить до їх високої вразливості. У сучасних умовах, що вимагають захисту не тільки державної та військової, а й промислової, комерційної, фінансової таємниць, захист інформації в цілому та захист інформації в мережах зв'язку, зокрема, стає все більш складною проблемою [3].

Сучасний прогрес у галузі глобальних мереж та засобів мультимедіа призвів до розробки численних методів, призначених для забезпечення безпечної передачі інформації по каналах телекомунікацій та використання їх у неоголошених цілях, методів синтезу різних інформаційних об'єктів та розробки їх нових математичних моделей [4, 5]. Однак ці методи часто не мають теоретичної основи, опис їх властивостей, переваг та недоліків спирається лише на практичний досвід їх використання, що не гарантує їх успішної роботи при застосуванні, наприклад, у позаштатних ситуаціях. Математичний апарат, що використовується в галузі інформаційної безпеки, досі залишився досить обмеженим, спираючись головним чином на теорію інформації, теорію ймовірності, математичну статистику, теорію ігор, а останнім часом – на теорію штучних нейронних мереж, і використовувався в різних підобластях області інформаційної безпеки практично незалежно[6–9]. До теперішнього часу не існує єдиного математичного підходу до аналізу та обробки даних про інформаційні об'єкти, мережі передачі інформації та методи їх проектування. Причиною цього, очевидно, є складність та різнорідність інформаційних об'єктів, більшість з яких погано формалізуються, потребують адаптації безпосередньо у процесі функціонування, управління та проектування. Зважаючи на відсутність єдиного математичного апарату, до цього моменту не існувало методів для проведення апріорного аналізу властивостей цих об'єктів, порівняння різних технологій функціонування систем зв'язку, що в загальному випадку позбавляло можливості обґрунтованого вибору технології функціонування мережі зв'язку або методу її проектування.

На підставі проведеного аналізу, результатів вивчення наукових публікацій за темою дослідження, дисертацій, патентів, монографій та практичних розробок встановлено, що на сучасному етапі розвитку прогресивних інформаційних технологій існує об’єктивне протиріччя між математичними моделями та методами забезпечення функціонування систем захисту інформації та необхідністю ефективного та надійного забезпечення функціонування систем захисту інформації для мереж передачі даних.

Основною ***метою*** статті є системне проектування і складання специфікацій, які необхідні для проведення наступного етапу проектування – структурного.

Виклад основного матеріалу

Існуючі методи проектування і побудови ЗІМ засновані на концептуальному підході, який розглядає процес проектування, як проектування переліку функцій з технічного завдання на архітектуру конкретної інформаційної мережі. Іншими словами, на заданій елементній основі, що має властивість функціональної або структурної повноти, в рамках стандартної архітектури організовується комплекс взаємопов’язаних компонентів, що реалізує весь набір функцій, перерахованих в проектному технічному завданні, включаючи функції захисту. Чітке створення захищеної інформаційної мережі здійснюється шляхом доповнення існуючих загальносистемних і прикладних функцій реальної мережі функціями забезпечення інформаційної безпеки з урахуванням архітектурних особливостей початкової мережі.

Основною метою статті є системне проектування і складання специфікацій, які необхідні для проведення наступного етапу проектування – структурного. Для цього виділимо п’ять типів специфікацій і, відповідно, п’ять підетапів системного проектування ЗІМ [10].

Підетап 1. Визначаємо загальну кількість джерел інформації (S) та потоків інформації (Ω): даних, сигналів, запитів абонентів на ініціацію програми, а також приймачів результатів їх обробки ($П$). Джерела і потоки інформації поділимо на періодичні та асинхронні, а серед них – з «жорсткими» вимогами реального часу (ВРЧ) на обробку, які позначимо наступним чином:

$\bar{S} \leftrightarrow \bar{\Omega}$ – джерела періодичних потоків з «нежорсткими» ВРЧ;

$\bar{\bar{S}} \leftrightarrow \bar{\Omega}$ – джерела періодичних потоків з «жорсткими» ВРЧ;

$\tilde{S} \leftrightarrow \tilde{\Omega}$ – джерела асинхронних потоків з «нежорсткими» ВРЧ;

$\tilde{\tilde{S}} \leftrightarrow \tilde{\Omega}$ – джерела асинхронних потоків з «жорсткими» ВРЧ.

Обмеження накладаються на «жорсткі» ВРЧ при обробці інформаційного потоку

$$\forall(d_i \in D)\big(r_i \le t_{p+1} - t_p\big),$$

де d_i – мінімальний, неподільний при обробці інформаційний блок (ІБ) або запит абонента; τ_i – максимально допустимий час обробки d_i; t_p, t_{p+1} – моменти часу надходження поточного і наступного ІБ.

«Нежорсткі» ВРЧ підпадають під обмеження при обробці потоком інформації, тобто відсутні вимоги тупикових ситуацій. Якщо врахувати, що для потоків задані періоди слідування ІБ, або мінімально допустимі інтервали слідування ІБ (для асинхронних потоків) $T = \{T_1, T_2, \dots, T_n\}$, але часові проміжки T^*, протягом яких ІБ повинні бути оброблені, визначаються як:

$$T^* = HOK[\{T_i\}]; \qquad \forall\big(i = \overline{1,n}\big).$$

Підетап 2. Проводиться комплексний аналіз функцій обробки ІБ, структурування оброблюваних даних в ЗІМ та виділення елементарних функцій обробки (ЕФО), орієнтованих на обробку окремих ІБ для кожний з інформаційних потоків $\phi_j^i \in \Phi_i$, де Φ_i – повний набір функцій з обробки інформаційного потоку.

Потім проводиться детальна розробка алгоритмів реалізації ЕФО:

$$\forall\big(\phi_j^i \in \Phi_i\big)\big(\alpha_j^i \leftarrow \phi_j^i\big).$$

Після верифікації всіх алгоритмів встановлюються інформаційно-керуючі зв'язки між ЕФО і зовнішнім середовищем – абонентами (джерелами і приймачами), нарешті, будується мультиграф функцій, які виконуються ЗІМ (рис. 1).

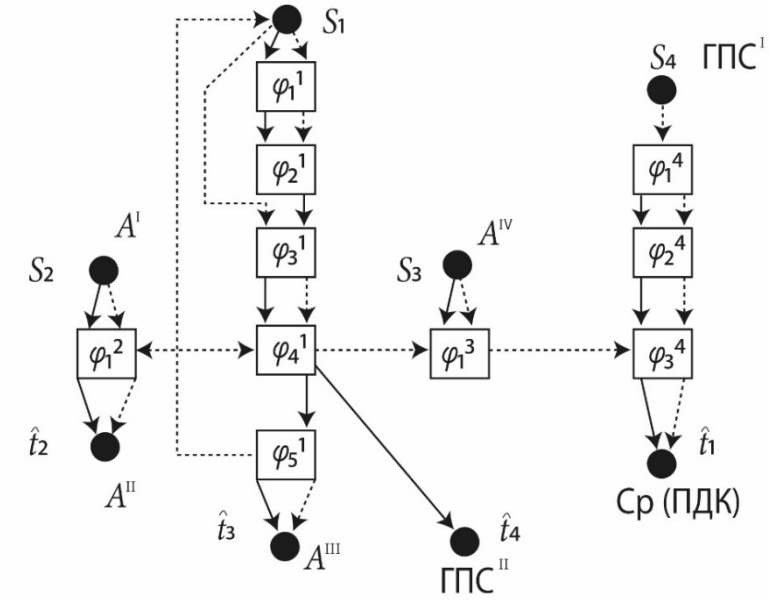


Рис. 1. Функціональний мультиграф ЗІМ

На рис. 1 прийняті такі позначки:

⟶ – керуючі зв'язки;

⇢ – інформаційні зв'язки;

Ср – сервер з приймальним каналом (ПРК) і передавальним каналом (ПДК); СОС – спеціальна обчислювальна система; ГПС – генератор пакетів сигналів, що задають синхронне формування і передачу ІБ; А – абонент з закінченими пристроями.

Можна вважати, що СОС вирішує проблему безперервної обробки інформаційних потоків від абонентів. Аналіз показав, що найбільш складним за змістом і трудомісткістю для реалізації, що вимагає до 90 % обчислювальних ресурсів СОС, є сукупність функцій для обробки отримуваних ІБ:

$$\Phi_1 = (\phi_1^1, \phi_2^1, \phi_3^1, \phi_4^1, \phi_5^1),$$

де ϕ_1^1 – функція синхронності; ϕ_2^1 – функція контролю синхронності; ϕ_3^1 – функція декодування записів ІБ; ϕ_4^1 – функція ідентифікації інструкцій; ϕ_5^1 – функція трансляції та відображення ІБ на А.

Функції $\Phi_2 = \phi_1^2$ та $\Phi_3 = \phi_1^3$ орієнтовані на обслуговування А. Набір функцій для обробки пакетів сигналів ГПС складається з трьох функцій: кодування запитів (ϕ_1^4); формування ІБ (ϕ_2^4); трансляція ІБ в ПДК Ср (ϕ_3^4).

Підетап 3. Здійснюється вибір МП та оцінюється їх продуктивність за класом задач, для чого доцільно використовувати метод бенчмарковських програм. В якості бенчмарковських програм для Ср ЗІМ рекомендується вибирати програми реалізації алгоритмів контролю синхронізму та/або декодування записів полів: $\alpha_2^1 \leftarrow \phi_2^1$; $\alpha_3^1 \leftarrow \phi_3^1$. Вказані алгоритми найбільш повно відображають вимоги класу задач і системи команд, а також розрядності оброблюваних даних.

Підетап 4. Проводиться кодування алгоритмів ЕФО і створення прикладного програмного забезпечення (ППЗ):

$$\forall\left(\alpha_j^i \in A\right) \times \left(m_j^i \leftarrow \alpha_j^i\right).$$

Візьмемо наступну ієрархію в позначенні ППЗ:

m_j^i – окрема підпрограма обробки ІБ;

$M_i = \{m_1^i, \ldots, m_n^i\}$ – програма обробки потоку інформації Ω_i;

$M = \{M_1, \ldots, M_e\}$ – комплект ППЗ, що реалізовано в ЗІМ.

Підетап 5. Проводиться аналіз процесу інформації. Метою підетапу є виявлення елементарних процесів обробки (ЕПО), під якими ми будемо розуміти процеси, пов'язані з реалізацією окремих підпрограм $m_j^i \in M_i$. Будемо вважати, що кожен ЕПО складається з трьох фаз: введення ІБ або результат обробки ІБ, реалізація власної підпрограми m_j^i і виведення результату виконання підпрограми.

При цьому параметри ЕПО визначаються:

$$\forall\left(m_j^i \in M_i\right)\left(g_j^i \leftarrow m_j^i; g_j^i = \left(x_j^i, y_j^i, \mu_j^i\right)\right),$$

де x_j^i і y_j^i – кількість циклів вводу і виводу вхідних даних і результату при реалізації підпрограми m_j^i; μ_j^i – максимальна кількість команд (з урахуванням циклів) при реалізації підпрограми m_j^i.

Необхідно відмітити, що для деяких підпрограм немає першої та/або третьої фази, тоді $x_j^i = 0$ і $y_j^i = 0$.

На етапі структурного проектування вирішуються такі основні структурні та неструктурні задачі:

– визначення мінімальної кількості модулів обробки (МО) і зв'язків між ними, а також зв'язків з абонентами;

– розподіл функцій, що можуть бути реалізовані між МО;

– визначення специфікацій швидкодії роботи для МП обміну.

Для вирішення цих завдань головним питанням є вибір моделі. Слід зазначити, що в області створення захищених систем з періодично повторюваним навантаженням застосування імовірнісних моделей, найчастіше побудованих на основі математичного апарату теорії масового обслуговування, вкрай ускладнене [5].

Серед детермінованих моделей найбільш перспективними є моделі і методи теорії мереж з детермінованими потоками в гілках (МДПГ). Однак аналіз показав, що відомі варіанти МДПГ не мають достатніх ресурсів для моделювання часових аспектів процесів. Для вирішення цих завдань запропоновано варіант МДПГ-мережі з дискретними детермінованими потоками у гілках (МДДП).

Перш за все, встановимо ступінь деталізації представлення як структури ЗІМ, так і процесів, що відбуваються в ній. Найбільш оптимальними і часто використовуваними є М1, М2, М3 – ступені деталізації представлення мережі на системному етапі проектування. У цьому випадку для розподіленої ЗІМ ці компоненти означають:

– компоненти М1–МП (однокристальні мікрокомп'ютери без доступу до мережі і даних або пристрій для апаратної реалізації функцій – спеціалізовані МП);

– компоненти М2 – буферні пристрої для організації передачі інформації про безпеку між компонентами М1;

– компоненти М3 – комутатори інформаційних потоків (загальна шина, мультиплексори, демультиплексори).

Нехай X – компонентами ЗІМ будуть джерела інформаційних потоків і приймачі результатів їх обробки, а М1 – зв'язки між ними, тоді структурна модель ЗІМ є графом $G = (V, \Gamma)$, в якому $V = X$ – множина вершин; $\Gamma = R$ – множина спрямованих гілок. Припустимо, що функціонування компоненти М1 полягає в реалізації компонента Ф – деякого набору ЕФО. Простіше кажучи, можна вважати, що реалізація окремо взятої ЕФО складається з трьох фаз, які безперервно слідують одна за одною: введення ІБ (початкова фаза), реалізація $\phi_j^i \in \Phi$ (основна фаза), виведення ІБ – результат обробки (результуюча фаза).

Припустимо, що функція компонента М2 полягає в реалізації елементарних процесів передачі

ІБ, кожен з яких складається з двох фаз: прийманню ІБ (початкова фаза) і виведенню ІБ (фаза результату). Важливою деталлю є те, що для двох з'єднаних компонент М1 і М2 результуюча фаза головного компонента (відносно напрямку передачі ІБ) є одночасно початковою фазою реалізації ЕФО для наступного компонента.

Припустимо, що серед функцій компонент М3 існує лише два типи: або з n входами і одним виходом $(n+1)$ (М3 – (загальна шина, мультиплексори) або з одним входом і m виходами $(m+1)$ (М3 – (загальна шина, демультиплексори). Можна вважати, що єдиною функцією компонент М3 є об'єднання (розподіл) ІБ, що передається між компонентами М1 та/або М2. При цьому часові параметри відповідних початкової та результуючої фаз реалізації ЕФО визначаються тільки взаємними процесами пов'язаних компонент М1 або М2.

Підводячи підсумок вищезгаданого спрощеного аналізу властивостей процесів, що відбуваються в компонентах ЗІМ: М1, М2 і М3, приймемо наступні положення [6, 7]:

1. Компоненти М1 і М2 відносяться до групи інтегруючих функцій, їх структурною моделлю є вершина графа з однією гілкою на вході і однією на виході, а також петлями, що представляють відповідну кількість основних фаз ЕФО. Цей тип вершин в графі буде називатися інерційною і позначатися $v_j^i \in V$, де i – індекс умовної приналежності до потоку оброблюваної інформації; j – порядковий номер.

2. Компоненти М3 належать до групи безінерційних компонент, їх структурною моделлю є вершина графа або з n гілками, інцидентними по входу і однією гілкою на виході або з однією гілкою, інцидентною по входу і m гілкою на виході. Цей тип вершин в графі буде називатися безінерційною і позначатися $v_s^i \in V$, серед яких виділяють типи вершин: $(nx1)v_s$ і $(1xm)v_s$.

Процедуру введення в структурну модель (граф G) неструктурованої інформації назвемо зважуванням графа, а зважений граф $G=(F,V,D)$ назвемо мережею. Ваги F, орієнтовані на моделювання різних специфікацій продуктивності і є інформаційними потоками. Для зважування вершин інерційного і безінерційного типів введемо ряд понять і визначень.

Визначення 1. Складовою МДДП гілки $b \in \Gamma$ мережі G є вага, що присвоюється гілці b і визначається:

$$f = \left(d_j^i; \tau_j^i; t_j^i\right),$$

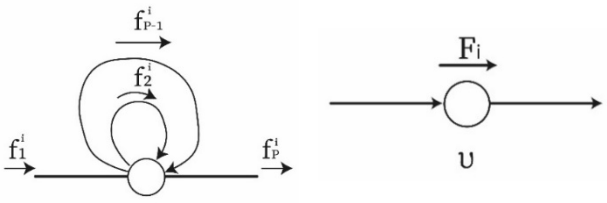
де d_j^i – значення детермінованого потоку (ДДП) (одиниця вимірювання інформації); τ_j^i – тривалість ДДП (одиниця вимірювання часу); t_j^i – початок ДДП (одиниця вимірювання часу).

Визначення 2. Дискретний детермінований потік вершини $v \in V$ мережі G є вагою, приписаною вершині v і визначається кортежем:

$$F_j = \left(f_1^i, f_2^i, \ldots, f_{p-1}^i, f_p^i, T_i\right),$$

де f_1^i – початковий ДДП, приписаний до гілки, інцидентної по входу вершині $v \in V$; $f_2^i, \ldots, f_{p-1}^i$ – основні ДДП, приписані $(p-2)$ – петлям вершин; f_p^i – результуючий ДДП, приписаний до гілки, інцидентної гілки по входу вершині; T_i – період потоку; i – номер потоку.

Позначення зважених гілок (рис. 2, *а*) і вершин показано на рис. 2, *б*.



а *б*

Рис. 2. Зважування гілки (*а*) і вершини (*б*)

Визначення 3. Мережею G_i^1 називають мережу G, структурна частина якої обмежена однією інерційною вершиною τ безпосередньо з'єднаною з нею безінерційними вершинами v_s, а також тими вершинами типу S і T, які безпосередньо пов'язані із заданими вершинами v_s типу.

Відмітимо, що інерційна вершина може бути зважена декількома потоками $F=(F_1,\ldots,F_n)$.

Існує особливість зважування гілок падаючих вершин v_s. Так як всі вершини $1xm$ v_s типу ДДП в гілках інцидентні по виходу і є вихідними ДДП потоками $F=(F_1,\ldots,F_n)$, що примикають до зважених суміжних вершин v_s з інерційними вершинами $v_1,\ldots,v_m$. Припустимо, що ДДП f_1 є ваговою гілкою інцидентною по входу v_s і складається з m частин. Тоді, враховуючи, що f_1 є результуючим ДДП f_p^i інерційної вершини, суміжної з v_s, приймемо:

$$f_p^i = \left(f_1', \ldots, f_\lambda', \ldots, f_m'\right),$$

де $f_\lambda' = (d_\lambda', \tau_\lambda', t_\lambda')$ – частина результуючого ДДП; d_λ' – розмір деталі ДДП $\sum_{\lambda=1}^m d_\lambda' = d_p^i$; τ_λ' – тривалість частини ДДП $\sum_{\lambda=1}^m \tau_\lambda' = \tau_p^i$; t_λ' – початок частини ДДП $t_\lambda' = t_p^i + \sum_{j=1}^{\lambda-1} \tau_j^i$.

Для вирішення задач дослідження процесів обробки інформації в ЗІМ, для випадків, коли є «жорсткі» і «нежорсткі» ВРЧ, приймемо ряд теорем.

Теорема 1. Потік F_i вершини $v \in V$ мережі G є «жорстко» врівноваженим, якщо виконується умова:

$$\sum_{j=1}^{k} \tau_j^i \prec T_i - t_1^i. \quad (1)$$

Причому потік F_i є максимальним, якщо є рівність:

$$\sum_{j=1}^{k} \tau_j^i = T_i - t_1^i. \quad (2)$$

У цьому випадку, якщо для деякої вершини вираз (1) не виконується, то така вершина буде називатися «жорсткою» і неврівноваженою. Відмітимо, що теорема визначає закони існування ЗІМ з достатньою пропускною здатністю для випадку обробки потоку інформації з «жорсткими» ВРЧ.

Для визначення «жорстких» урівноважених вершин, зважених декількома потоками $F = (F_1, \dots, F_k)$, необхідно враховувати можливий вибір процедур для обслуговування запитів на обробку ІБ в ЗІМ. У цьому випадку найпростіше співвідношення буде для циклічної процедури обслуговування ЗІМ.

Теорема 2. Вершина $v \in V$ мережі G є «жорстко» урівноваженою в рамках моделі ЗІМ з циклічною процедурою обслуговування, якщо для потоків F, що врівноважують вершину v при виконанні наступних умов:

$$\forall (F_i \in F)\left(\sum_{i=1}^{n} \sum_{j=1}^{k} \tau_j^i \pi \, min_F\left[T_i - t_j^i\right]\right) \quad (3)$$

і потоки максимальні, якщо має місце

$$\forall (F_i \in F)\left(\sum_{i=1}^{n} \sum_{j=1}^{k} \tau_j^i \, min\left[T_i - t_j^i\right]\right).$$

Отримання виразів для визначення «жорстко» урівноважених вершин в рамках моделі ЗІМ з іншими процедурами обслуговування (абсолютними і відносними) є складним і тягне за собою постановку і рішення задачі нелінійного програмування. У загальному випадку, якщо періоди $T_i \in F_i$ всіх потоків, що урівноважують вершину, дорівнюють між собою, то вирази (2) і (3) справедливі також і для моделювання ЗІМ з абсолютними і відносними процедурами обслуговування.

Розглянемо аналогічні співвідношення для випадків моделювання ЗІМ з «нежорсткими» ВРЧ.

Теорема 3. Вершина $v \in V$ мережі G не «жорстко» урівноважена, якщо для потоків F, що урівноважують вершину, виконується умова:

$$\forall (F_i \in F)\left(\sum_{i=1}^{n} \sum_{j=1}^{k} \tau_j^i k_i \pi T^*\right),$$

де $T^* = HOK[\{T_i\}]$;

$$\forall (F_i \in F)\left(k_i = \frac{T^*}{T_i}\right),$$

при цьому потік F є максимальним, якщо має місце

$$\forall (F_i \in F)\left(\sum_{i=1}^{n} \sum_{j=1}^{k} \tau_j^i k_i = T^*\right).$$

Найбільший інтерес представляє випадок моделювання ЗІМ, які здійснюють обробку інформаційних потоків, частина з яких підпорядкована «жорстким» ВРЧ, а інші – не «жорстким» ВРЧ. Розділимо всі потоки і вершини на підмножини «жорстких» і не «жорстких» потоків $F = \{F^{\alpha}, F^{\beta}\}$.

Теорема 4. Вершина $v \in V$ мережі G повністю урівноважена, якщо для потоків $F = \{F^{\alpha}, F^{\beta}\}$, які урівноважують вершину, виконується наступна умова:

$$\begin{cases} \forall (F_i \in F^{\alpha})\left(\sum_{j=1}^{k} \tau_j^k \prec T_i - t_j^i\right); \\ \forall (F_{\lambda} \in F^{\beta})\left(\sum_{i=1}^{n} \sum_{j=1} k_i \tau_j^i \prec T^*\right), \end{cases} \quad (4)$$

де $T^* = HOK[\{T_i\}]$;

$$\forall (F_{\lambda} \in F)\left(k_{\lambda} = \frac{T^*}{T_i}\right). \quad (5)$$

Введені визначення дозволяють будувати моделі розподіленої ЗІМ системного етапу проектування з урахуванням різних вимог реального часу та можливих процедур обслуговування запитів в ЗІМ. Для побудови мережі з ДДП в гілках необхідний наступний набір вхідних даних:

– граф $G = (V, D)$, в якому є вершини заданих типів (S – джерела, P – приймачі; v – інерційні вершини; $(n \times 1)v_s$ і $(1 \times m)v_s$ – безінерційні вершини);

– $f = (d, \tau, t)$ значення ДДП;

– розбиття R всієї множини ДДП на групи – метод або правило, за яким задається відповідність груп ДДП і інерційних вершин.

Інформація неструктурного характеру легко визначається за даними системної стадії проектування. Наприклад, $\tau \in f$ тривалість ДДП визначається за такими формулами:

$$\tau^1 = \frac{x}{P_{\text{ц}}}; \rightarrow \tau^2 = \frac{\mu}{P_{\text{ср}}}; \rightarrow \tau^3 = \frac{y}{P_{\text{ц}}}, \quad (6)$$

де $\{x \in g, \mu \in g, y \in g\}$ – параметри ЗІМ; P_u – продуктивність МП під час циклів входу та/або виводу інформації; P_{sr} – продуктивність МП при реалізації програм.

Для ДДП, які відображаються відповідно до мультиграфа, що реалізовує функції ЗІМ, задано $t_j^1 = 0$, а для розрахунку $t_j^i < f_j^i$ інших ДДП використовується той факт, що окремі фази, як і ЕФО безперервно слідують одна за одною.

При вирішенні задач синтезу структур ЗІМ необхідно визначати еквівалентні операції перетворення в мережі.

Визначення 4. Під операцією склеювання в мережі G вершин v_1 з v, які розділені вершиною типу v_s, будемо розуміти:

1. В структурному плані – це видалення вершини v_1 з графа і додавання петель видаленої вершини до вершини, що склеюється v;

2. Зважування доданих петель основними ДДП видаленої вершини;

3. Додавання вихідного та результуючого ДДП видаленої вершини, як частини вихідного та результуючого ДДП вершини, що підлягають склеюванню.

Визначення 5. Операція склеювання буде називатися еквівалентною, якщо в результаті перетворення всі вершини мережі залишаться повністю збалансованими.

Графічна ілюстрація операції склеювання показана на рис. 3 *а*, *б*.

Складність розв'язання задачі синтезу моделі ЗІМ полягає в тому, що граф G спочатку не визначений. У цьому випадку можна задати граф G, зважити його за допомогою обчисленого ДДП і, виконуючи еквівалентні операції склеювання, домогтися зменшення кількості інерційних вершин, тим самим формуючи структурну модель ЗІМ.

У зв'язку з цим можуть бути запропоновані два принципово різних методи синтезу моделі ЗІМ:

– метод декомпозиції мережі з однією інерційною вершиною;

– метод згортки моделі екстремально розподіленої ЗІМ.

Перший метод заснований на припущенні, що можлива одномодульна реалізація ЗІМ. Тоді повинна існувати мережа з єдиною інерційною вершиною v, пов'язаною з однією вершиною типу $(1 \times m)v_s$, які, в свою чергу, з'єднані з джерелами і приймачами, при цьому вершина v повинна бути повністю збалансована.

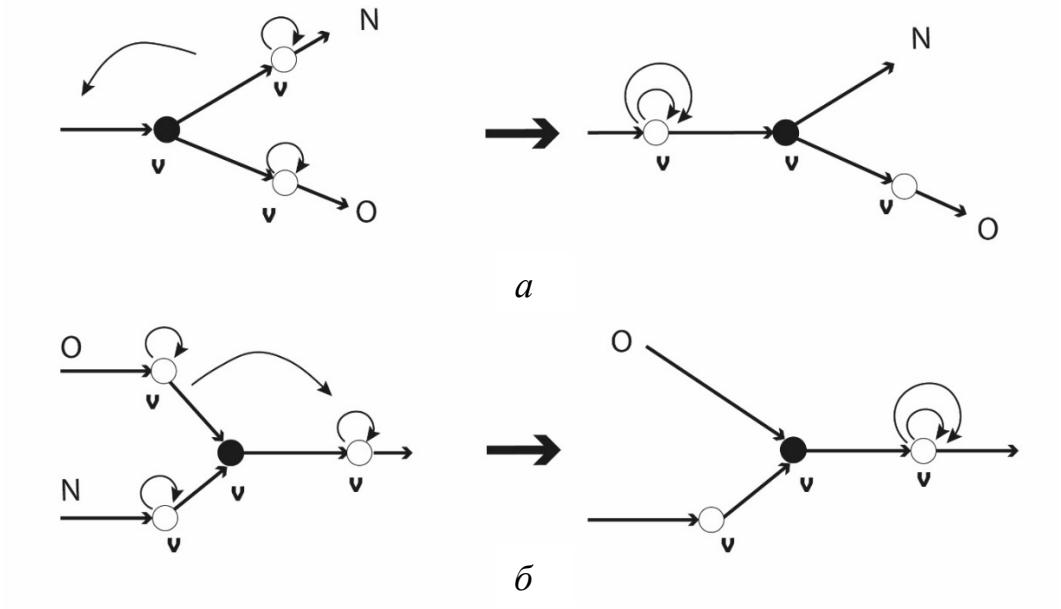


Рис. 3. Синтез моделі ЗІМ: склеювання вершин: перший метод (*а*), другий метод (*б*)

Для перевірки цього припущення обчислюються ДДП, яка моделює ЕФО, будується потік $F = (F_1, \ldots, F_n)$, за яким зважується інерційна вершина і перевіряються співвідношення (4) і (5). Якщо результат позитивний, то гіпотеза про можливість реалізації одномодульної ЗІМ підтверджується, в іншому випадку потрібна декомпозиція мережі на мінімальну кількість зв'язаних підмереж $\{G_i{}'\}$, в яких безінерційні вершини $v \in G_i{}'$ є збалансованими. Зв'язаність підмереж визначається на основі аналізу розподілу ДДП по підмережах. Проте, як показує досвід, реалізація одномодульної ЗІМ нездійсненна через ВРЧ, а процедура декомпозиції складно формалізується, тому другий спосіб синтезу мережі є більш перспективним.

Метод згортки заснований на гіпотезі про існування такої розподіленої ЗІМ з однією ЕФО, а структура міжмодульного інтерфейсу відповідає структурі мультиграфа реалізованих функцій.

При реалізації методу пропонується наступний алгоритм:

1. Складання вихідного графа G. Вихідний граф G будується шляхом перетворення мультиграфа функції ЗІМ за правилом: вершини, що відображають ЕФО, замінюються інерційними вершинами $\{v_i\}$; джерела та приймачі інформації – вершинами, джерелами S, а вершини – приймачами P, при цьому, якщо ці вершини з'єднані входом та/або виходом з більш ніж однією вершиною, то ці зв'язки реалізуються шляхом введення безінерційних вершин типу $(n \times 1)v_s$ та/або $(1 \times m)v_s$.

2. Розрахунок ДДП. За допомогою виразу (6) обчислюються ДДП, що моделює реалізацію окремих ЕФО.

3. Поділ ДДП на мінімальну кількість груп. Мета розбиття полягає в тому, щоб виділити таке мінімальну кількість груп ДДП, щоб F – потоки, що складаються з них, задовольняли б співвідношенням (4) і (5). Для цього кожному з періодичних потоків вибирається послідовність ДДП, починаючи з першого, за умови дотримання заданих співвідношень. Асинхронні потоки враховуються додаванням до основного ДДП додаткового потоку з тривалістю, визначеною виразом:

$$\tau^g = \frac{\tau^{(2)} \times T_n}{T_a},$$

де $\tau^{(2)} \in f^{(2)}$ – тривалість ДДП асинхронного потоку; T_n – період потоку; T_a – мінімальний інтервал слідування безпечного асинхронного потоку.

4. Формування мережі – це створення моделі розподіленої ЗІМ. Мережа формується шляхом склеювання вершин інерційного типу всередині виділених підграфів. Таким чином формуються взаємопов'язані підмережі $\{G_i'\}$, кількість яких дорівнює мінімально виділеній кількості груп ДДП.

Операція склеювання на підграфі G_i' вершин ν_1' і ν_2' формує підмережуG_1'' (рис. 4) з інерційною вершиною ν_1 та ін. В результаті отримуємо мережу (рис. 4), в яку додатково введені інерційні вершини ν_1' і ν_2', які моделюють роботу буферних пристроїв для організації міжмодульного обміну.

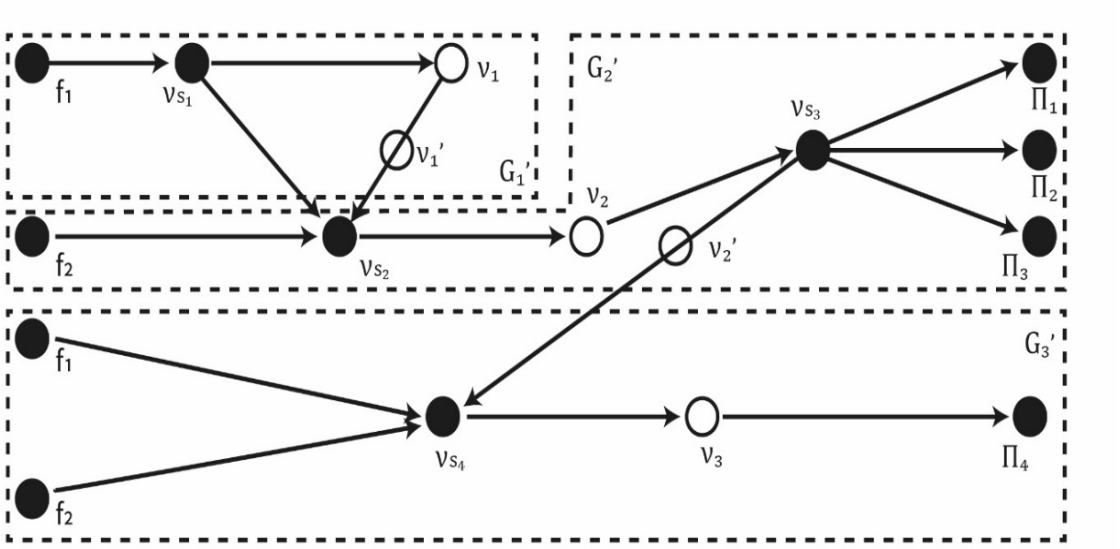


Рис. 4. Синтез моделі ЗІМ та її формування

Відображення компонентів М1, М2, М3 мережі G здійснюється функціональними модулями $\{\nu_{s1}, \nu_1\}$; $\{\nu_{s2}, \nu_2, \nu_{s3}\}$; $\{\nu_{s4}, \nu_3\}$, які відображаються зі стандартним складом елементів, причому вершини відображають ν_1' і ν_2' буферні пристрої.

Висновки

У результаті проведеного дослідження запропоновано метод проектування мережі з дискретними детермінованими потоками у гілках. Цей метод легко формалізується на першому системному етапі, при системному проектуванні. Розроблено та запропоновано модель мережі з детермінованими потоками в гілках. Ця модель також дозволяє формалізувати процедуру синтезу структурної моделі захисту інформаційних мереж. Що значно скорочує час на проектування та побудову системи захисту інформації.

ЛІТЕРАТУРА

[1] Павлов І. М., Хорошко В. О. Проектування комплексних систем захисту інформації. Київ: ВІТІ – ДУІКТ, 2011. 245 с.

[2] Бобало Ю. Я., Дудикевич В. Б., Павлов І. М. та ін. Проектування комплексних систем захисту інформації. Львів: Видавництво «Львівська політехніка», 2020. 320 с.

[3] Кулаков Ю. О., Луцкий Г. М. Комп'ютерні мережі. За ред. Ю. С. Ковстанюка. Київ: Видавництво «Юніор», 2005. 400 с.

[4] Щербина Ю. В., Казакова Н. Ф., Фразе-Фразенко О. О., Лаптєв О. А., Собчук А. В. Вибір джерела випадковості для комп'ютерного моделювання. *Наукоємні технології*. Том 59. № 3. 2023. С. 233–238. doi: 10.18372/2310-5461.59. 17944.

[5] Boryseiko O., Laptiev O., Perehuda O., Ryzhov A. Optimizing Energy Conversion in a Piezo Disk Using a Controlled Supply of Electrical Load. *Axioms*. 2023. № 12, 1074. doi: 10.3390/axioms12121074.

[6] Barabash O., Laptiev O., Grushina O. The conceptual model of the intelligent network. *Сучасний захист інформації*. 2023. No 4 (56). P. 1–9. doi: 10.31673/2409-7292.2023.030202

[7] Лаптєв О., Зозуля С. Метод виключення відомих сигналів при скануванні заданого радіодіапазону. *Кібербезпека: освіта, наука, техніка*. 2023. Том 2. № 22. С. 31–38. doi: 10.28925/2663-4023.2023.22.3138

[8] Собчук В. В., Циганівська І. М., Лаптєв О. А., Журавльов В. М. Планування технологічних ланцюжків засобами скінченно частково впорядкованих множин. *Наукоємні технології*. 2023. Том 60. № 4. С. 372–385. doi: 10.18372/2310-5461.60.18266

[9] Barabash O., Musienko A., Sobchuk V., Lukova-Chuiko N., Svynchuk O. Distribution of Values of Cantor Type Fractal Functions with Specified Restrictions. Chapter in Book "Contemporary Approaches and Methods in Fundamental Mathematics and Mechanics". Editors Victor A. Sadovnichiy, Michael Z. Zgurovsky. Publisher Name: Springer, Cham, Switzerland AG 2021. P. 433–455. https://link.springer.com/book/10.1007/978-3-030-50302-4

[10] Boiko J., Tolubko V., Barabash O., Eromenko O., Havrylko Ye. Signal processing with frequency and phase shift keying modulation in telecommunications. *TELKOMNIKA. Telecommunication, Computing, Electronics and Control*. Yogyakarta, Indonesia, 2019. Vol. 17, No 4. P. 2025–2038. doi: 10.12928/TELKOMNIKA.v17i4.12168

[11] Barabash O. V., Dakhno N. B., Shevchenko H. V., Majsak T. V. Dynamic Models of Decision Support Systems for Controlling UAV by Two-Step Variational-Gradient Method. Proceedings of 2017 IEEE 4th International Conference «*Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD)*», (17–19 October, 2017), Kyiv, Ukraine. Kyiv: National Aviation University, 2017. P. 108–111.

Хорошко В. О., Лаптєв О. А., Хохлачева Ю. Є., Аль-Далваш Аблуллах Фоуад, Пепа Ю. В.

ОСОБЛИВОСТІ ПРОЕКТУВАННЯ ЗАХИЩЕНИХ ІНФОРМАЦІЙНИХ МЕРЕЖ

У статті розглядаються проблеми проектування захищених інформаційних мереж. Процес впровадження нових інформаційних технологій у всі сфери життя суспільства немислимий без вирішення питань інформаційної безпеки, яка структурується у абсолютно різних, але пов'язаних між собою різними аспектами. Сучасний прогрес у галузі глобальних мереж та засобів мультимедіа призвів до розробки численних методів, призначених для забезпечення безпечної передачі інформації по каналах телекомунікацій та використання їх у неоголошених цілях, методів синтезу різних інформаційних об'єктів та розробки їх нових математичних моделей. Математичний апарат, що використовується в галузі інформаційної безпеки, досі залишився досить обмеженим. До теперішнього часу не існує єдиного математичного підходу до аналізу та обробки даних про інформаційні об'єкти, мережі передачі інформації та методи їх проектування. Зважаючи на відсутність єдиного математичного апарату, до цього моменту не існувало методів для проведення апріорного аналізу властивостей цих об'єктів, порівняння різних технологій функціонування систем зв'язку, що в загальному випадку позбавляло можливості обґрунтованого вибору технології функціонування мережі зв'язку або методу її проектування. Тому надзвичайно актуальним для забезпечення можливості автоматизованого аналізу стану та функціонування захищених мереж зв'язку, в тому числі, аналізу функціонування інформаційної системи в цілому, з урахуванням можливості виникнення як природних, так і штучних каналів витоку інформації та різних видів впливів, автоматичної обробки результатів такої витоку та впливів, вибору шляху відновлення мережі після атаки, а також для вирішення питань синтезу та проектування систем захисту інформаційних мереж зв'язку із залученням сучасного математичного апарату є створення єдиного математичного підходу до проблеми оцінки стану інформаційних мереж зв'язку, що дозволяє б уникнути їх різнорідної та поганої формалізованості шляхом нескладного в обчислювальному сенсі аналізу лише певної групи математичних параметрів, що описують функціонування мереж зв'язку, що захищаються. Вирішуванню цій актуальної задачі і присвячена дана робота.

Ключові слова: *моделювання, захист інформації, безпека інформаційних мереж, захист мереж, теорія графів, складні системи.*

Khoroshko V., Laptiev O., Khokhlachova Yu., Al-Dalvash A., Pepa Y.

FEATURES OF SECURED INFORMATION NETWORK DESIGN

The article deals with the design problems of secure information networks. The process of introducing new information technologies into all spheres of social life is unthinkable without solving the issues of information security, which is structured in completely different but interconnected aspects. Modern progress in the field of global networks and multimedia tools has led to the development of numerous methods designed to ensure the safe transmission of information through telecommunications channels and their use for undeclared purposes, methods of synthesis of various information

objects and the development of their new mathematical models. The mathematical apparatus used in the field of information security has so far remained rather limited. Until now, there is no single mathematical approach to the analysis and processing of data about information objects, information transmission networks and their design methods. Due to the lack of a single mathematical apparatus, until now there were no methods for conducting an a priori analysis of the properties of these objects, comparing different technologies of the functioning of communication systems, which in general deprived the possibility of a reasonable choice of the technology of the functioning of the communication network or the method of its design. Therefore, it is extremely relevant to ensure the possibility of automated analysis of the state and functioning of protected communication networks, including the analysis of the functioning of the information system as a whole, taking into account the possibility of the emergence of both natural and artificial channels of information leakage and various types of influences, automatic processing of the results of such leakage and influences, choosing the way to restore the network after an attack, as well as to solve the issues of synthesis and design of protection systems of communication information networks with the involvement of modern mathematical apparatus is the creation of a unified mathematical approach to the problem of assessing the state of communication information networks, which would avoid their heterogeneous and poor formalizability by means of a computationally simple analysis of only a certain group of mathematical parameters describing the functioning of protected communication networks. This work is dedicated to solving this urgent problem.

Keywords: Modeling, information protection, security of information networks, network protection, graph theory, complex systems.

Стаття надійшла до редакції 07.05.2024 р.
Прийнято до друку 12.06.2024 р.