УДК 004. 056.53
DOI: 10.31673/2409-7292.2025.011077

Лаптєв О.А., Пономаренко В. В.

ПІДГОТОВЧИЙ ЕТАП СТРУКТУРНОГО ПРОЕКТУВАННЯ ЗАХИЩЕНИХ ІНФОРМАЦІЙНИХ МЕРЕЖ.

Впровадження нових інформаційних технологій неможливе без забезпечення інформаційної безпеки, яка охоплює різні аспекти. Незважаючи на прогрес у сфері телекомунікацій та мультимедіа, досі не існує єдиного математичного підходу до аналізу й обробки даних про інформаційні об'єкти та мережі. Це ускладнює обґрунтований вибір технологій і методів проектування мереж. Тому важливим завданням є створення єдиного математичного підходу для оцінки стану та функціонування захищених мереж зв’язку. Це дозволить автоматизувати аналіз роботи інформаційних систем, враховуючи можливість виникнення природних і штучних каналів витоку інформації та різних видів впливів, а також забезпечити обробку наслідків таких подій, вибір шляхів відновлення мереж після атак і розробку ефективних систем захисту. Запропонований підхід має подолати різнорідність і складність формалізації цих процесів, зосереджуючись на обчислювально простому аналізі ключових параметрів, що описують функціонування захищених мереж. Саме цьому завданню присвячена дана робота.

Ключові слова: захищені інформаційні мережи, захист інформації, безпека мереж, структурне проектування, складні системи, реальний час.

Вступ

У процесі проектування складних систем широко застосовуються натурні експерименти, які дозволяють оцінити їхню поведінку в заданих умовах експлуатації. Проте проведення таких експериментів потребує значних матеріальних та фінансових ресурсів, що далеко не завжди є можливим. У зв’язку з цим попередній етап проектування передбачає використання комп’ютерного моделювання. Такий підхід базується на програмній реалізації математичної моделі, яка описує взаємодію компонентів системи між собою та із зовнішнім середовищем. Це дозволяє здійснити попередній вибір параметрів системи та прогнозувати її поведінку за різних умов експлуатації.

Зростання складності впровадження захищених інформаційних мереж підкреслює актуальність забезпечення їх живучості та безпеки. Сучасні захищені інформаційні мережи оснащені високорозвиненими системами передачі даних, включно із супутниковим зв’язком, що зумовлює широке застосування мікропроцесорів та одно кристальних мікрокомп’ютерів [1-4].

Досвід проектування захищених інформаційних мереж на основі сучасної елементної бази показав, що поряд із вирішенням спеціальних завдань ускладнюються інші етапи проектування, зокрема виникає потреба в радикальному перегляді існуючих принципів і підходів. У загальному випадку процес проектування захищених інформаційних мереж поділяється на три ключові етапи: системний, структурний і логічний, після завершення яких здійснюється технічна реалізація.

Сучасний підхід до проектування захищених інформаційних мереж має такі основні особливості:

— *принцип "знизу-вгору"*: побудова мережі починається з елементів і функціональних вузлів, а виконання основних етапів проектування розпочинається з логічного рівня. При цьому такі характеристики, як розрядність оброблюваних даних, система команд, специфіка обміну інформацією тощо, формуються на основі аналізу завдань, які визначають спеціалізацію захищених інформаційних мереж . Хоча деякі аспекти підходу "згори-вниз" також знаходять застосування, вони є допоміжними;

— *розробленість логічного етапу*: цей етап охоплює проектування окремих функціональних блоків, вузлів і пристроїв, завдяки наявності розвиненого математичного апарату та інструментів моделювання;

— *завершення процесу проектування*: основний акцент робиться на створенні захищених інформаційних мереж, виключаючи спеціалізовані задачі проектування резервних або специфічних систем.

Незважаючи на різноманітність підходів, проектування захищених інформаційних мереж супроводжується такими труднощами, а саме:

— необхідність розробки математичного апарату для системно-структурного проектування;

— обмежена застосовність класичних методів, зокрема через те, що вирішення завдань, таких як між абонентський зв’язок, стає можливим лише в межах підходу "згори-вниз".

Усі завдання мають системний характер і вимагають комплексного підходу. У межах системного підходу бракує обґрунтованих методів і математичних інструментів для проведення проектування мереж, що значно ускладнює побудову сучасних захищених інформаційних мереж.

Аналіз літературних джерел та формулювання проблеми.

Процес впровадження нових інформаційних технологій у всі сфери суспільного життя є неможливим без вирішення ключових питань інформаційної безпеки, яка охоплює різні, але взаємопов’язані аспекти [1, 2]. Масштабне використання обчислювальної техніки, телекомунікаційних систем і цифрових технологій, поряд зі зростанням обсягів оброблюваної інформації та розширенням кола користувачів, створює нові можливості для несанкціонованого доступу до інформації. Це, своєю чергою, значно підвищує вразливість таких систем. У сучасних умовах, коли необхідно забезпечувати захист не лише державної чи військової інформації, але й промислової, комерційної та фінансової таємниць, питання захисту інформації загалом та в мережах зв’язку зокрема набувають особливої актуальності [3].

Сучасний розвиток глобальних мереж та мультимедійних технологій сприяв створенню численних методів, спрямованих на забезпечення безпечної передачі інформації по каналах телекомунікацій, синтез інформаційних об’єктів та розробку нових математичних моделей [4, 5]. Однак більшість із цих методів базуються на практичному досвіді застосування і часто не мають достатньо розвиненої теоретичної основи. Їх ефективність у позаштатних ситуаціях залишається під сумнівом через відсутність гарантованого опису їх властивостей, переваг та недоліків.

Математичний апарат, який застосовується в галузі інформаційної безпеки, залишається обмеженим. Він базується на теорії інформації, ймовірностей, математичній статистиці, теорії ігор, а останнім часом – на штучних нейронних мережах. Ці підходи використовуються окремо в різних під областях інформаційної безпеки, не утворюючи єдиного цілісного підходу [6–9]. На сьогодні не існує універсального математичного методу для аналізу та обробки даних про інформаційні об’єкти, мережі передачі інформації чи методи їх проектування. Основною причиною цього є складність і різнорідність інформаційних об’єктів, які часто важко формалізувати та адаптувати в умовах функціонування, управління чи проектування.

Відсутність єдиного математичного апарату унеможливлює апріорний аналіз властивостей інформаційних об’єктів, порівняння технологій функціонування систем зв’язку та обґрунтований вибір технологій чи методів проектування мереж зв’язку. Це створює перешкоди для створення ефективних і надійних систем захисту інформації.

На основі аналізу наукових праць, дисертацій, патентів, монографій та практичних розробок встановлено у межах системного підходу бракує обґрунтованих методів і математичних інструментів для проведення проектування мереж, що значно ускладнює побудову сучасних захищених інформаційних мереж. Виникає актуальне наукове завдання по обґрунтовані методів та математичного апарату побудові захищених інформаційних мереж. Вирішенню цього наукового завдання і присвячена дана робота.

© Лаптєв О.А., Пономаренко В. В. (2025). Підготовчий етап структурного проектування захищених інформаційних мереж. Сучасний захист інформації, 1(61), 121–126.
https://doi.org/10.31673/2409-7292.2025.011077.

Мета роботи та цілі дослідження

Основною метою дослідження є обґрунтування методів та математичного апарату побудові захищених інформаційних мереж, а саме розробка підходів до системного проектування та складання специфікацій, необхідних для реалізації наступного етапу – структурного проектування захищених інформаційних мереж

Виклад основного матеріалу

Існуючі методи проектування і побудови захищених інформаційних мереж 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 [10–13].

Початковий етап проектування пропонується виконувати наступним шляхом:

Перший етап. 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 на обробку, які позначимо наступним чином:

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

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

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

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

Обмеження накладаються на «жорсткі» вимогами реального часу при обробці інформаційного потоку

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

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

«Нежорсткі» вимоги реального часу 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) $T = \{T_1, T_2, ..., T_n\}$, але часові проміжки T^*, протягом яких ІБ повинні бути оброблені, визначаються як

$$T^* = HOK\left[\{T_i\}\right]; \qquad \forall\left(i = \overline{1,n}\right). \tag{2}$$

Другій етап. Проводиться комплексний аналіз функцій обробки ІБ, структурування оброблюваних даних в захищених інформаційних мережах та виділення елементарних функцій обробки, орієнтованих на обробку окремих інформаційних блоків 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 елементарних функцій обробки

$$\forall\left(\phi_j^i \in \Phi_i\right)\left(\alpha_j^i \leftarrow \phi_j^i\right). \tag{3}$$

Після верифікації всіх алгоритмів встановлюються інформаційно-керуючі зв'язки між елементарними функціями обробки і зовнішнім середовищем – абонентами (джерелами і приймачами), нарешті, будується мультограф функцій, які виконуються в захищених інформаційних мережах (рис. 1).

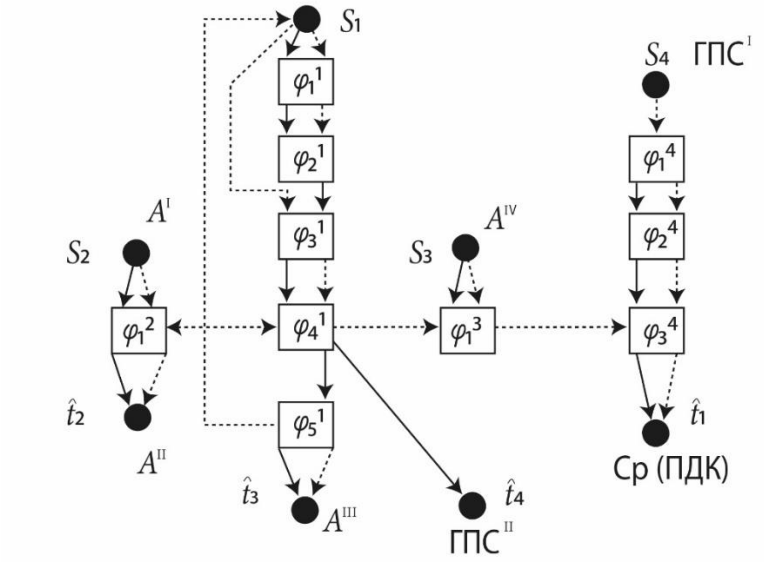

Рис. 1. Функціональний мультограф захищеної інформаційної мережи [15]

На рис. 1 прийняті такі позначки:

⟶ – керуючі зв'язки;

⇢ – інформаційні зв'язки;

Ср – сервер;

ПРК – приймальний канал;

ПДК – канал передачі інформації;

СОС – спеціальна обчислювальна система;

ГПС – генератор пакетів сигналів, що задають синхронне формування і передачу інформаційних блоків;

А – абонент з закінченими пристроями.

Можна вважати, що система обробки сигналів 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 системи обробки сигналів , є сукупність функцій для обробки отримуваних інформаційних блоків

$$\Phi_1 = \left(\phi_1^1, \phi_2^1, \phi_3^1, \phi_4^1, \phi_5^1\right), \tag{4}$$

де ϕ_1^1 – функція синхронності; ϕ_2^1 – функція контролю синхронності; ϕ_3^1 – функція декодування записів інформаційних блоків; ϕ_4^1 – функція ідентифікації інструкцій; ϕ_5^1 – функція трансляції та відображення інформаційних блоків 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 інформаційних блоків - ϕ_2^4; трансляція інформаційних блоків в ПДК Ср - ϕ_3^4

Третій етап. Здійснюється вибір МП та оцінюється їх продуктивність за класом задач, для чого доцільно використовувати метод бенчмарковських програм. В якості бенчмарковських програм для Ср захисту інформаційної мережи 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.

Четвертий етап. Проводиться кодування алгоритмів елементарних функцій обробки і створення прикладного програмного забезпечення

$$\forall\left(\alpha_j^i \in A\right)\times\left(m_j^i \leftarrow \alpha_j^i\right). \tag{5}$$

Візьмемо наступну ієрархію в позначенні ППЗ:

m_j^i – окрема підпрограма обробки інформаційних блоків;

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

$M = \left\{M_1,...,M_e\right\}$ – комплект ППЗ, що реалізовано в захищених інформаційних мережах.

Заключний етап. Проводиться аналіз процесу інформації. Метою під етапу є виявлення елементарних процесів обробки, під якими ми будемо розуміти процеси, пов'язані з реалізацією окремих підпрограм $m_j^i \in M_i$. Будемо вважати, що кожен елементарний процес обробки складається з трьох фаз: введення інформаційних блоків або результат обробки інформаційних блоків, реалізація власної підпрограми m_j^i і виведення результату виконання підпрограми.

При цьому параметри елементарних процесів обробки визначаються

$$\forall\left(m_j^i \in M_i\right)\left(g_j^i \leftarrow m_j^i; g_j^i = \left(x_j^i, y_j^i, \mu_j^i\right)\right), \tag{6}$$

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 вирішується мінімальна кількість модулів обробки і зв'язків між ними, а також зв'язків з абонентами, розподіл функцій, що можуть бути реалізовані між модулями обробки та визначення специфікацій швидкодії роботи для мереж потоку обміну.

Висновки

У результаті проведеного дослідження запропоновано метод структурного проектування. Запропонований метод вирішує такі основні структурні та неструктурні задачі:

- визначення мінімальної кількості модулів обробки і зв'язків між ними, а також зв'язків з абонентами;
- розподіл функцій, що можуть бути реалізовані між модулями обробки ;
- визначення специфікацій швидкодії роботи для мереж потоку обміну.

Це значно скорочує час на проектування та побудову системи захисту інформації та дозволяє вирішувати завдання побудови захищених мереж передачі даних у значно

© Лаптєв О.А., Пономаренко В. В. (2025). Підготовчий етап структурного проектування захищених інформаційних мереж. Сучасний захист інформації, 1(61), 121–126.
https://doi.org/10.31673/2409-7292.2025.011077.

скорочений час. Що особливо актуально в період війни з росією, коли порушення інформаційних мереж відбувається з великою інтенсивністю.

Перелік посилань

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

2. Бобало Ю.Я., Дудикевич В.Б., Павлов І.М. та ін. Проектування комплексних систем захисту інформації. Видавництво Львівської політехніки, 2020. – 320 с.

3. Кулаков Ю.О., Луцький Г.М. Комп'ютерні мережі. За ред. Ю.С. Ковстанюка. – К.: Видавництво «Юніор», 2005. – 400 с.

4. Ю.В. Щербина, Н.Ф. Казакова, О.О. Фразе-Фразенко, О.А. Лаптєв, А.В. Собчук. 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. https://doi.org/10.3390/axioms12121074 WoS

6. Barabash O., Laptiev O., Grushina O. The conceptual model of the intelligent network. *Сучасний захист інформації*, No4 (56), 2023, P. 1-9. https://doi.org/ 10.31673/2409-7292.2023.030202

7. Лаптєв О., Зозуля С. Метод виключення відомих сигналів при сканування заданого радіодіапазону. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка».* Том 2 № 22 (2023). С. 31–38. https://doi.org/10.28925/2663-4023.2023.22.3138

8. В.В. Собчук, І.М. Циганівська, О.А. Лаптєв, В.М. Журавльов. Планування технологічних ланцюжків засобами скінченно частково впорядкованих множин. *Наукоємні технології.* Том 60 № 4 (2023) С. 372-385. https://doi.org/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 Contro*l. Yogyakarta, Indonesia, 2019. Vol. 17, № 4. P. 2025 – 2038. https://doi.org/10.12928/TELKOM-NIKA.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)"*, October 17-19, 2017, Kyiv, Ukraine: National Aviation University, 2017. P. 108-111.

12. Лаптев О.А., Собчук В.В., Саланди И.П., Сачук Ю.В. Математична модель структури інформаційної сеті на основі нестаціонарної ієрархічної та стаціонарної гиперсети. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка.* К.: ВІКНУ, Вип. 64, 2019. С. 124 – 132.

13. Lubov Berkman, Oleg Barabash, Olga Tkachenko , Andri Musienko, Oleksand Laptiev, Ivanna Salanda. The Intelligent Control System for infocommunication networks. International *Journal of Emerging Trends in Engineering Research (IJETER)* Volume 8. No. 5, May 2020. Scopus Indexed - ISSN 2347 – 3983. P.1920 – 1925.

14. Стефурак О.Р., Тихонов Ю.О., Лаптєв О.А., Зозуля С.А. Удосконалення стохастичної моделі з метою визначення загроз пошкодження або несанкціонованого витоку інформації. *Сучасний захист інформації: науково-технічний журнал.* К.: ДУТ, 2020. № 2(42)., С 19 – 26.

15. Barabash O., Laptiev O., Grushina O. The conceptual model of the intelligent network. Сучасний захист інформації, No4 (56), 2023, P. 1-9.
https://doi.org/ 10.31673/2409-7292.2023.030202

16. Дробик О. В., Лаптєв О. А., Пархоменко І. І., Богуславська О. В., Пепа Ю. В., Пономаренко В. В. Розпізнавання радіосигналів на основі апроксимації спектральної функції у базисі передатних функцій резонансних ланок другого порядку. *Сучасний захист інформації.* 2024. №2. С.13-23. https://doi.org/ 10.31673/2409-7292.2024.020002

17. Лаптєв, О. А., Колесник, В. В., Ровда, В. В., & Половінкін, М. І. Метод підвищення захисту особистих даних за рахунок синтезу резильєнтних віртуальних спільнот. 2024. *Сучасний захист інформації.* 4(60). С. 141–146. https://doi.org/10.31673/2409-7292.2024.040015

Надійшла 05.02.2025