УДК 004.056, 004.75

В.Б. Дудикевич[1], Ю.Р. Гарасим[2], В.В. Нечипор[1]

vdudykev@polynet.lviv.ua„ igarasym@space-it.com.ua, nechypor.vv@gmail.com

[1]*Національний університет «Львівська політехніка», Львів*
[2]*Space IT, Київ*

ВИКОРИСТАННЯ ТЕОРІЇ НЕЧІТКИХ МНОЖИН В ЗАДАЧАХ ОЦІНКИ ЖИВУЧОСТІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

На етапі проектування системи захисту інформації (СЗІ) в корпоративній мережі зв'язку (КМЗ), що має властивість живучості, важливим завданням є отримання точної і оперативної оцінки ризиків. У зв'язку з відсутністю достатнього об'єму статистичних даних про ймовірність реалізації загроз інформаційної безпеки відсутня й єдина розвинена загальноприйнята методологія кількісної оцінки ризиків. В роботі використано методи якісної оцінки ризиків, які запропоновані в міжнародних стандартах серії ISO 17799 та ISO 27001, що набули широкого розповсюдження у світовій практиці.

Система захисту інформації в КМЗ часто є розподіленою інформаційною системою, яка функціонує за умов невизначеності впливу чинників дестабілізації [1]. Використання теорії нечітких множин для опису структури, прогнозування її параметрів на етапі побудови адаптивної моделі СЗІ дає змогу оцінити загальні характеристики системи з подальшим розробленням рішень щодо підвищення ефективності і оптимізації режимів її роботи.

Показник живучості СЗІ визначається через функцію живучості, тобто, через сукупність значень функції, характерних для кожної конкретної топології СЗІ [2]. Розраховуючи функції живучості, кожну із скінченної кількості загроз ($i=\overline{1,n}$) описуємо за допомогою теорії нечітких множин. Загрози представляємо функцією від двох параметрів – ймовірності появи $P_{загр}$ (виражена якісно через експертні оцінки) і можливим зниженням показника живучості системи $\Delta d^{загр}$ (може виражатися як якісними так і кількісними показниками, залежно від прийнятих показників ефективності виконання системою своїх функції).

На етапі математичного моделювання представимо систему у вигляді дводольного графа. Кожен з вузлів системи характеризується показниками якості функціонування, критичністю інформації, що обробляється, ефективністю засобів захисту та вектором загроз.

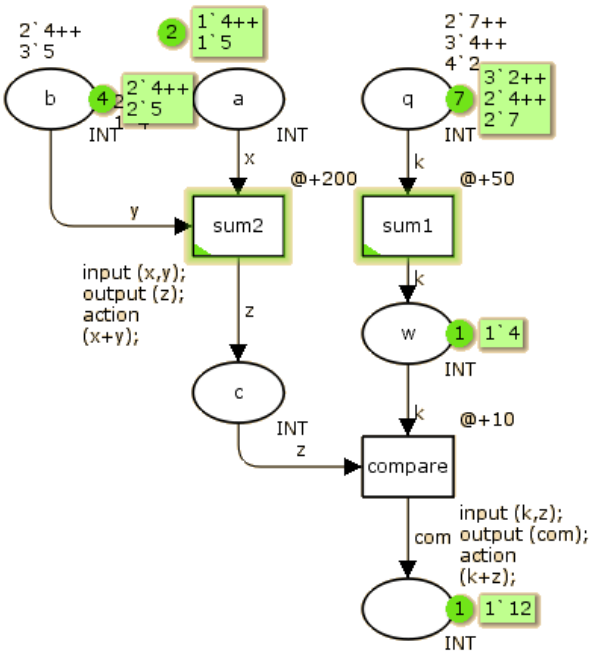

Рис. 1. Елементарна модель системи захисту інформації

Вибір раціональної топології системи захисту інформації відбувається на основі сумарного показника відвернених загроз $\overline{W}$, який розраховуємо для кожної з можливих початкових топологій системи.

$$\overline{W} = F(P_{i\,загр}; \Delta d_i^{загр}; P_{i\,загр}^{нейтр}; i=\overline{1,n}),$$

де $P_{i\,загр}^{нейтр}$ – ймовірність знешкодження i-ої загрози.

Список літератури

1. Нечипор В. В. Методи моделювання систем захисту інформації для корпоративних мереж зв'язку / В. Б. Дудикевич, Ю. Р. Гарасим, В. В. Нечипор // Науково-технічний журнал «Сучасний захист інформації». – № 4. – 2011. – С. 54-60.

2. Нечипор В. В. Оцінка живучості систем захисту інформації за допомогою CPN TOOLS / В. В. Нечипор, Ю. Р. Гарасим // Збірник тез VIII Міжнародної науково-технічної конференції студентства та молоді «Світ інформації та телекомунікацій». – Київ, 2011. – С. 104-105.