3. Голубничий А.Г. Оценка скрытности передачи данных на основании анализа структуры спектра сигналов / А.Г. Голубничий // Інтегровані інформаційні технології та системи: наук.-практ. конф., 21-23 листопада 2005 р.: матеріали. – К., 2005. – С. 139-141.

4. Закон України "Про Національну систему конфіденційного зв'язку". – Офіц. вид. – Відомості Верховної Ради (ВВР). – 2002. – № 15. – С. 103.

5. Пат. 82053 Україна, МПК Н 04 J 11/00. Спосіб багатоканальної передачі дискретної інформації / Голубничий О.Г., Любімов О.Д.; заявники та власники Голубничий О.Г., Любімов О.Д. – № 20040402844; заявл. 19.04.04; опубл. 11.03.08; Бюл. № 5.

6. Борисов В.И. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты / Борисов В.И., Зинчук В.М., Лимарев А.Е. – М.: РадиоСофт, 2008. – 512 с.

7. Применение режима СИЧ в перспективных войсковых радиостанциях УКВ-связи [Електронний ресурс] / Клименко Н.Н. – Режим доступу: http://www.qrz.ru/vhf/klimenko/u1_7.shtml

8. Помехозащищенность систем радиосвязи с расширением спектра сигналов модуляцией несущей псевдослучайной последовательностью / [В.И. Борисов, В.М. Зинчук, А.Е. Лимарев и др.]. – М.: Радио и связь, 2003. – 640 с.

9. Мазурков М.И. Метод защиты информации на основе совершенных двоичных решёток / М.И. Мазурков, В.Я. Чечельницкий, П. Мурр // Радиоэлектроника. – 2008. – Том 51. – № 11. – С. 53-57.

10. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99. – 1999. – 53 с.

11. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма: ГОСТ Р 34.10-94.

Рецензент: Хорошко В.О.
Надійшла 17.06.2011

УДК 004.7

Дудикевич В.Б., Гарасим Ю.Р., Нечипор В.В.
(Національний університет «Львівська політехніка»)

МЕТОДИ МОДЕЛЮВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ КОРПОРАТИВНИХ МЕРЕЖ ЗВ'ЯЗКУ

Вступ

Імітаційне математичне моделювання дозволяє отримати важливу інформацію про структуру та дослідити динамічну поведінку складних систем, до яких відносимо й системи захисту інформації (СЗІ), визначити та детально проаналізувати вразливі ділянки, промоделювати процес несанкціонованого втручання у роботу СЗІ зловмисником та дослідити ймовірні наслідки втручання або наслідок впливу дестабілізуючих факторів. Результати аналізу потенційно небезпечних ділянок використовуються у визначенні необхідних заходів захисту.

Постановка проблеми. На цей час практично відсутні методи, моделі та методики проектування (а, відповідно, моделювання) СЗІ для корпоративних мереж зв'язку (КМЗ). Проблема ускладнюється й відсутністю адекватних математичних моделей таких систем, вибір математичного апарату для дослідження СЗІ в КМЗ здійснюється необґрунтовано. Робота присвячена вирішенню цих завдань.

Аналіз останніх досліджень і публікацій. Проблемам методів моделювання складних систем присвячені наступні роботи: Девянин П.М. [1], Малюк А.А. [2], Павлов В.А., Пятунин А.Н. [3], Кульгин М. [4], Шеннон Р. [5], Бенькович Е.С. [6]. В роботі Цибулин А.М, Шипилева А.В. [7] розглянуто проблему моделювання поведінки зловмисника в КМЗ з використання апарату мереж Петрі-Маркова, запропоновано використання матриці станів для кількісної оцінки вразливих ділянок КМЗ. В роботі Омарова О.М. [8] запропоновано функціональне розширення мереж Петрі для усунення недоліків при моделюванні

паралельних алгоритмів. Проте, вони не враховують особливостей побудови СЗІ в КМЗ та вимог до їх експлуатації.

Мета роботи – аналіз та вибір ефективної системи імітаційного комп'ютерного моделювання, представлення можливостей математичного апарату в задачах захисту КМЗ з метою подальшого її використання при побудові СЗІ в КМЗ.

Математичні методи моделювання складних систем

Нижче розглянемо декілька найпоширеніших методів математичного моделювання складних систем та дослідимо їх на предмет можливості та ефективності застосування для моделювання СЗІ в КМЗ.

Теорія графів – розділ дискретної математики, що вивчає властивості графів. В загальному випадку, граф представляється як множина вершин (вузлів), які з'єднуються ребрами. В моделюванні використовують орієнтований граф (граф, ребрам якого присвоєно напрям). Зокрема дводольний орієнтований граф використовується в мережах Петрі, в теорії масового обслуговування використовується граф станів [9].

Теорія масового обслуговування (ТМО) – прикладна математична дисципліна, що займається дослідженням показників продуктивності технічних засобів (систем масового обслуговування (СМО)), що призначені для обробки заявок на обслуговування [10]. Метою ТМО є розроблення рекомендацій щодо раціональної побудови СМО, організації їх роботи і регулюванню потоку заявок для забезпечення високої ефективності функціонування складної системи. Теорія масового обслуговування дозволяє дослідити механізм виникнення черг на пристроях обслуговування, визначити основні характеристики системи: інтенсивність вхідного потоку заявок, середній час обслуговування заявки, інтенсивність потоку обслуговування, інтенсивність завантаженості каналу, ймовірність виникнення відмови від обслуговування, середню довжину черги. При цьому важливу роль відіграє характер надходження потоку заявок, кількість каналів обслуговування, наявність буферу пам'яті, принцип надходження заявки з буферу до пристрою обслуговування, кількість етапів обслуговування.

Марківські процеси – це випадкові процеси, конкретні значення яких у момент часу $t+1$ залежать від значень у момент часу t, але не залежать від його значень у моменти часу $t-1$. Використання марківських процесів у моделюванні дозволяє дослідити складні системи за багатьма параметрами, зокрема: досяжність, зворотність, ергодичність станів системи за допомогою матриці переходу, що повністю визначає ймовірності переходів та станів системи на n-му кроці [11].

Теорія мереж Петрі знайшла широке застосування при проектуванні та аналізі динамічних дискретних систем [12]. Мережею Петрі є дводольний орієнтований граф, який складається з вершин двох типів – позицій і переходів, які з'єднані між собою дугами. Умовою спрацювання переходу є наявність у відповідній позиції маркера. Перевагою мереж Петрі для моделювання СЗІ в КМЗ є строгий математичний опис, що дозволяє досліджувати моделі з використанням обчислювальної техніки; можливість аналізу системи на обмеженість, досяжність маркування та активність переходів, оберненість тощо; використання причинно-наслідкових зв'язків між подіями для представлення алгоритмів; дослідження як послідовних, так і паралельних процесів [13]. Під час аналізу використовується графічний, матричний методи представлення результатів, метод побудови графу маркування.

Математичний апарат теорії мереж Петрі

В теорії мереж Петрі умови моделюються позиціями, події – переходами, при цьому входи переходів є передумовами, а виходи – постумовами. Виконання умови представляється маркером у відповідній позиції. Запуск переходу видаляє маркери-дозволи і формує нові

маркери, які відображають виконання пост-умов. Мережі Петрі дозволяють моделювати паралельні або одночасні події, таким чином мережі Петрі є ефективнішими при моделюванні систем з розподіленим управлінням, в яких декілька процесів відбуваються одночасно. Мережі Петрі формально представляються як $N=(P,T,M,\Phi)$, де P – множина усіх позицій, T – множина усіх переходів, M – функція маркування, Φ – функція кратності ребер, $\Phi(t)=[\Phi(p_1,t),\Phi(p_2,t),...,\Phi(p_n,t)]$ – кратність дуги із позиції в перехід, $\Phi(t)=[\Phi(p,t_1),\Phi(p,t_2),...,\Phi(p,t_n)]$ – кратність дуги із переходу в позицію. Важливими задачами аналізу мереж Петрі є дослідження основних властивостей мережі:

- безпечність: позиція $p_i \in P$ мережі Петрі $N=(P,T,M,\Phi)$ з початковим маркуванням M_0 є безпечною, якщо $M(p_i)\le 1$ для будь-якої $M \in R(N,M)$;
- обмеженість: позиція $p_i \in P$ мережі Петрі $N=(P,T,M,\Phi)$ з початковим маркуванням M_0 є k-безпечною, якщо $M(p_i)\le k$ для усіх $M \in R(N,M)$.
- консервативність: мережа є консервативною, якщо сума маркерів у всіх її позиціях залишається незмінною при роботі мережі $\forall M_1,M_2 \in R(N)\sum_{p\in P}M_1(p)=\sum_{p\in P}M_2(p)$.
- досяжність маркування: маркування M мережі Петрі є досяжним, якщо існує комбінація $R(N,T)$ така, що переводить мережу із стану M_0 в стан M. Мережа має властивість перекриття, якщо для даного маркування M існує M' таке, що $M' \in R(N,M)$ та $M' \ge M$.
- потенційна живучість: перехід називається потенційно живим при маркуванні $M \in R(N)$, якщо існує досяжне з M маркування M', при якому перехід t може спрацювати.
- живучість: перехід є живим, якщо він є потенційно живим в будь-якому досяжному маркуванні $M' \in R(N), \exists M' \in R(N,M): M' \ge F(t)$.
- тупик (deadlock): маркування M мережі називається t-тупиковим, якщо перехід $t \in T$ не є потенційно живим; маркування M мережі називається тупиковим, якщо воно t-тупикове для усіх переходів мережі.
- стійкість: перехід t називається стійким у мережі N, якщо $\forall t' \in T\{t\}, \forall M \in R(N): (M \ge F(t)) \wedge (M \ge F(t')) \Rightarrow (M \ge F(t)+F(t'))$ тобто, якщо перехід t може спрацювати, тоді жоден інший перехід спрацювавши не може позбавити його такої можливості.
- мережа N є стійка, якщо всі її переходи стійкі.

При функціонуванні мережі Петрі виникає наступна невизначеність: якщо декілька переходів можуть спрацювати, тоді спрацьовує будь-який з них. В реальних імітаційних моделях СЗІ в КМЗ переходи мають різний пріоритет спрацювання в залежності від вразливості ланки та прийнятих заходів захисту. Для моделювання такого процесу введемо множину пріоритетів PR: кожному переходу t відповідатиме пріоритет $pr(t)$. Таким чином перехід t спрацьовує в тому випадку, якщо для будь-якого іншого переходу t' виконується умова $pr(t') \le pr(t)$.

Процес імітаційного моделювання систем захисту інформації в корпоративних мережах зв'язку

Моделювання типових систем захисту інформації в КМЗ здійснимо в програмному середовищі pipe 3.0 (проект MSc Group, Department of Computing at Imperial College London), яке, на відміну від інших, дозволяє будувати граф мережі, аналізувати його на безпечність, обмеженість та на активні/мертві переходи, містить повний набір модулів аналізу поведінки

та властивостей мереж, статистику продуктивності та деякі прості функції: порівняння та класифікація [14].

Розглянемо декілька прикладів імітаційного моделювання процесу функціонування СЗІ в КМЗ. Модель атаки зловмисника на сервер авторизації користувачів захищеної КМЗ у вигляді мережі Петрі наведено на рис. 1.

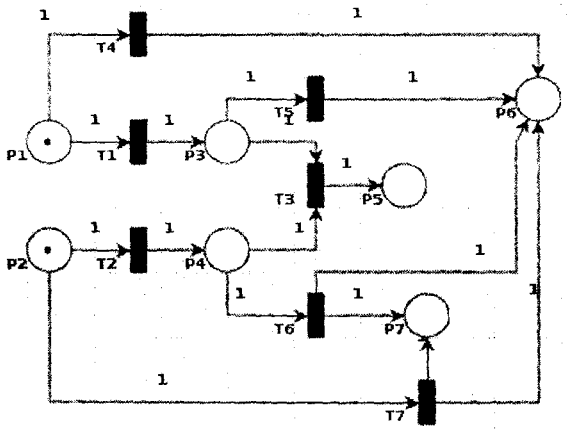

Рис. 1. Модель атаки зловмисника на сервер авторизації користувачів захищеної корпоративної мережі зв'язку, яка представлена за допомогою мережі Петрі

Опис процесу функціонування мережі Петрі, яка представляє атаку на сервер авторизації в КМЗ:

Позиції: P1 – користувач встановив з'єднання із КМЗ загального користування; P2 – зловмисник встановив з'єднання із КМЗ; P3 – користувач встановив з'єднання з абонентом КМЗ і почав обмін даними; P4 – зловмисник отримав доступ до лінії зв'язку сервера авторизації; P5 – зловмисник отримав ім'я та пароль користувача; P6 – атака нейтралізована; P7 – умови для перехоплення пакетів відсутні.

Переходи: T1 – встановлення з'єднання між сервером авторизації та абонентом; T2 – отримання зловмисником доступу до сервера авторизації; T3 – перехоплення пакетів користувача; T4, T5, T6, T7 – виявлення та нейтралізація атаки.

При матричному представленні результатів імітаційного моделювання та розрахунку мереж Петрі використовуються матриці інцидентності, що відображають кратність вхідних дуг переходів (дуга із позицій в перехід) – $'\Phi(t)$.

Відповідно «1» в позиції [1,1] матриці означає, що з позиції під номером $p1$ в перехід $t1$ йде дуга одиничної кратності. Матриця інциндентності $\Phi'(t)$ характеризує кратність вихідних дуг переходів. Матриця маркування M_0 відображає початкове маркування системи (кількість маркерів в позиціях на початковому етапі моделювання).

За допомогою пріоритетів переходів задаємо ймовірності виконання кожної події. При впровадженні належних методів та заходів захисту пріоритети переходів, що відповідають за виявлення та нейтралізацію атаки зростає і, відповідно, ймовірність вдалих дій зловмисника зменшується. Матриці інцидентності для $'\Phi(t)$ та $\Phi'(t)$ наведемо нижче:

$'\Phi(t)$ $\Phi'(t)$

i/j	1	2	3	4	5	6	7
1	1			1			
2		1					1
3			1		1		
4			1			1	
5							
6							
7							

M_0

i	1	2	3	4	5	6	7
	1	1	0	0	0	0	0

i/j	1	2	3	4	5	6	7
1							
2							
3	1						
4		1					
5			1				
6				1	1	1	1
7						1	1

Пріоритети переходів

i	1	2	3	4	5	6	7
	1	1	0	1	0	0	0

Результати імітаційного моделювання вказують на те, що система немає властивості живучості, є обмеженою та в ній наявні «дедлоки». Найкоротшим шляхом до «дедлоку» є виконання переходів T1, T2, T5, T6. Стан СЗІ в КМЗ після вдалих дій зловмисника показано на рис. 2:

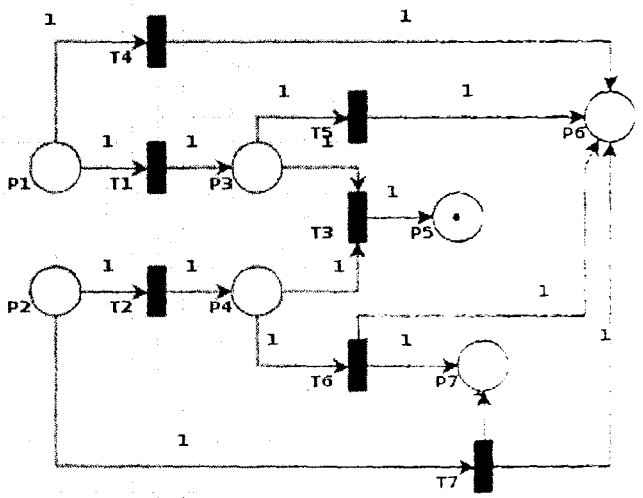

Рис. 2. Представлення реалізованої атаки зловмисника на захищену корпоративну мережу зв'язку у вигляді мережі Петрі

Процес виявлення та нейтралізації атаки зловмисника на СЗІ в КМЗ зображено на рис. 3. Результати імітаційного моделювання вказують на потенційну досяжність ланки обміну інформації. Для зменшення вразливості СЗІ в КМЗ впровадимо систему-приманку «honeypot» (позиція P7). Метою впровадження системи-приманки (рис. 4) є отримання даних про типову поведінку зловмисника для подальшої її аналізу та впровадження відповідних методів та засобів захисту в систему захисту інформації для корпоративної мережі зв'язку. В результаті проведеного імітаційного моделювання переконуємося у нездатності реалізації вищезазначеної атаки на СЗІ в КМЗ.

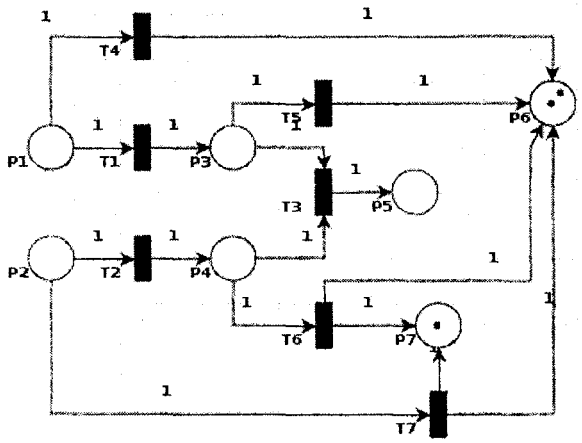

Рис. 3. Представлення процесу виявлення та нейтралізації атаки зловмисника на захищену корпоративну мережу зв'язку у вигляді мережі Петрі

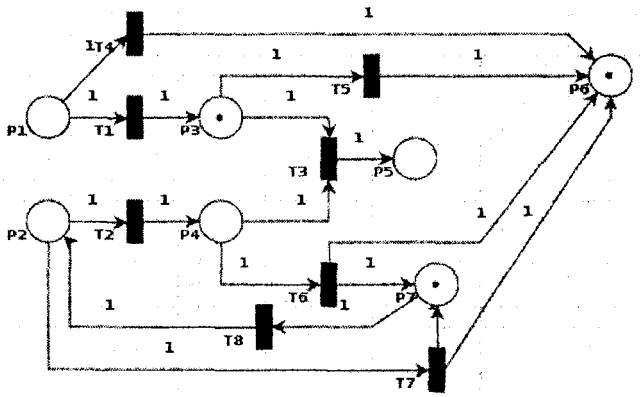

Рис. 4. Представлення моделі захищеної системи зв'язку з впровадженням системи-приманки у вигляді мережі Петрі

Висновки

В роботі досліджуються можливості використання математичного апарату в задачах моделювання захищених мереж зв'язку, представлено основні переваги теорії мереж Петрі для моделювання таких систем та з її допомогою представлено процес атаки зловмисника на захищений вузол зв'язку, та реалізацію системи приманки. На основі отриманих результатів запропоновано інтеграцію системи виявлення та запобігання атак honeypot з метою підвищення рівня захищеності вузла зв'язку.

Предметом подальших досліджень є створення математичної моделі типової СЗІ в КМЗ, вдосконалення методів моделювання за допомогою використання розширеного апарату мереж Петрі, що дозволить моделювати нові та робити оцінки вже існуючих СЗІ з метою підвищення їх надійності, живучості та стійкості до атак.

Список використаних джерел

1. Девянин П. Н. Модели безопасности компьютерных систем / П. Н. Девянин. – М. : Издательский центр «Академия», 2005. – 144 с.

2. Малюк А. А. Информационная безопасность: концептуальне и методологические основы защиты информации / А. А. Малюк. – М. : Горячая линия – Телеком, 2004. – 280 с

3. Павлов В. А. Основы построения и эксплуатации защищенных телекоммуникационных систем / В. А. Павлов, А. Н. Пятунин. – Воронеж : Воронежский государственный технический университет, 2004. – 67 с.

4. Кульгин М. Технологии корпоративных сетей. Энциклопедия / М. Кульгин. – СПб. : Издательство «Питер», 2000. – 704 с.

5. Шеннон Р. Имитационное моделирование систем – искусство и наука. Перевод с английского под. редакцией Е. К. Масловского / Р. Шеннон. – М. : Издательство «Мир», 1978. – 418 с.

6. Бенькович Е. С. Практическое моделирование динамических систем / Е. С. Бенькович, Ю. Б. Колесов, Ю. Б. Сениченков. – СПб. : БХВ-Петербург, 2002. – 464 с.

7. Цыбулин А. М. Математическая модель злоумышленника в корпоративной сети / А. М. Цыбулин, А. В. Шипилева. – Волгоградский государственный университет, Волгоград.

8. Омаров О. М. Моделирование параллельных алгоритмов с использованием сетей Петри / О. М. Омаров. – Дагестанский политехнический институт, г. Махачкала, Дагестан.

9. Березина Л. И. Графы и их применение / Л. И. Березина. – М. : Просвещение, 1979. – 143 с.

10. Томас. Л. Саати Элементы теории массового обслуживания и её приложения / Томас. Л. Саати. – Ленинградская типография. – №6. – 1965. – 505 с.

11. Дынкин Е. Б. Марковские процессы / Е. Б. Дынкин. – М., 1963. – 859 с.

12. Котов В. Е. Сети Петри / В. Е. Котов. – М. : Наука, 1984.

13. Дж. Питерсон. Теория сетей Петри и моделирования систем / Питерсон Дж. –М. : Мир, 1984.

14. Bonet P. Pipe v.2.5: a Petri net tool for performance modeling / P. Bonet, Llado C., Puigjaner R. – 12 p.

Рецензент: Щербак Л.М.
Надійшла 12.09.2011

УДК 004.236.321

Павлов І.М.
(КПІ)

ФУНКЦІОНАЛЬНА МОДЕЛЬ ПРОЦЕСУ АВТОМАТИЗОВАНОГО СУПРОВОЖДЕННЯ ТЕХНІЧНОГО ПРОЕКТУВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Проектно-конструкторський процес, яким є етап технічного проектування систем захисту інформації (СЗІ), носить ітераційний характер, причому результат одного етапу є постановкою задачі для іншого. Слід також пом'ятати, що кожний етап, в свою чергу, реалізується в вигляді визначеної послідовності проектних процедур і операцій [1 – 4].

Постановка загальної задачі створення нових технічних і програмних об'єктів СЗІ (ТПО СЗІ), їх концептуальное проектування є, в основному, творчими етапами і в цієй якості трудно піддаються формалізації, хоча є великий шляхи для досліджень в напряму автоматизації методик аналізу варіантів рішень і прийняття рішень на різних стадіях проектування. Для чого необхідно визначити критерії і показники.

Формалізація проектних рішень, в основному, можлива на етапі ескізного проектування [5 – 6], коли тільки створюється умозрительний ескіз проекту, коли необхідно прийняти принципове рішення про оформлення того або іншого проекту на створення СЗІ в інтересах захисту секретів або комерційної інформації. І тут необхідно не тільки мати знання про порядок створення СЗІ, про принципи та способи застосування СЗІ, а також необхідний постійній зв'язок замовника і розробника, щоб замовник уявляв: що він дійсно хоче захистити а розробник надасть для цього певні проектні механізми реалізації задуму замовника. При цьому збережіться "золота формула": при мінімальній вартості СЗІ (в залежності від захищаємої інформації) можливість максимального захисту інформації замовника.