Snodgrass R.T. – Information Systems Vol. 19, No. 7, 1994. – P. 513–547. 8. Paolo Terenziani, Richard T. Snodgrass. Reconciling Point-based and Interval-based Semantics in Temporal Relational Databases: A Proper Treatment of the Telic/Atelic Distinction/ Paolo Terenziani, Richard T. Snodgrass – IEEE Transactions on Knowledge and Data Engineering, 16(5) – May, 2004. 9. D. Toman. Point-Based Temporal Extensions of SQL and Their Efficient Implementation. Temporal Databases: Research and Practice/ D. Toman. – Springer, 1st edition. – July 1, 1998 10. What are temporal databases? [електронний ресурс] – http://www.timeconsult.com/TemporalData/TemporalDB.html. 11. Базаркин А.Н. Разработка темпоральной модели данных в медицинской информационной системе // Программные продукты и системы, 2009, № 2 – С. 34–40. 12. Костенко Б.Б., Кузнецов С.Д. История и актуальные проблемы темпоральных баз данных [електронний ресурс] – http://citforum.ru/database/articles/temporal/. 13. Порай Д.С., Соловьев А.В., Корольков Г.В. Реализация концепции темпоральной базы данных средствами реляционной СУБД // Документооборот. Концепции и инструментарий / ред. В.Л. Арлазаров, Н.Е. Емельянов: Эдиториал УРСС, 2004. – С. 92–109, Тр. Института системного анализа Российской академии наук. 14. Темпоральные базы данных [електронний ресурс] – http://www.chair36.msiu.ru/articles/3/html/node56.html. 15. Григорович В.Г., Шілінг А.Ю. Темпоральні бази даних: історія та основні характеристики // Матеріали сьомої Всеукраїнської науково-практичної інтернет-конференції «Сучасність, наука, час». – м. Київ, 18–20 листопада 2010 р. Режим доступу: http://intkonf.org/kf-mn-grigorovich-vg-shiling-ayu-temporalni-bazi-danih-istoriya-ta-osnovni-harakteristiki/. 16. Григорович В.Г., Косовська О.Ю. Темпоральні бази даних та методи представлення даних // Комп'ютерні науки та інженерія. Матеріали четвертої Міжнародної конференції молодих вчених CSE – 2010. – Львів: Видавництво Львівської політехніки. – С 68–69.

УДК 004.056, 004.75

В.Б. Дудикевич, Ю.Р. Гарасим
Національний університет "Львівська політехніка",
Кафедра захисту інформації

ДОСЛІДЖЕННЯ МОДЕЛІ ОЦІНЮВАННЯ ЖИВУЧОСТІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ КОРПОРАТИВНИХ МЕРЕЖ ЗВ'ЯЗКУ ЗА ДОПОМОГОЮ МЕРЕЖ ПЕТРІ

Розглянуто актуальну науково-практичну проблему розроблення моделей і методів оцінювання живучості систем захисту інформації корпоративних мереж зв'язку. Розроблено та проаналізовано модель оцінки живучості систем захисту інформації корпоративних мереж зв'язку.

Ключові слова: властивість живучості, оцінка живучості, системи захисту інформації.

The work is devoted to enterprise communication networks information security systems survivability assessment models and methods development as an actual scientific and practical problem solution. Within the paper enterprise communication networks information security systems survivability assessment model was developed and investigated.

Key words: survivability, survivability assessment, information security system.

Вступ

Для підвищення ефективності процесу забезпечення живучості систем захисту інформації (СЗІ) корпоративних мереж зв'язку (КМЗ) на етапі проектування та експлуатації виникла необхідність розробити адекватні моделі та методи її оцінювання. Ці моделі та методи повинні

враховувати особливості процесу проектування, побудови та функціонування як корпоративних мереж зв'язку [1–7], так і самої системи захисту інформації [8–12].

Для систем з настільки складною архітектурою і великою кількістю гетерогенних компонентів [13–18] оцінити живучість – доволі складна проблема, навіть якщо відомими є всі необхідні метрики для усіх елементів, що входять до складу цієї СЗІ корпоративної мережі зв'язку. Крім цього, в умовах безперервно і динамічно мінливих вимог з боку зовнішнього середовища та швидкого морального старіння інфокомунікаційних активів організації таке завдання взагалі видається нерозв'язним. Тому доцільно переосмислити підходи до цієї проблеми, як відповідь на потребу в розробленні простих і доволі ефективних з інженерного погляду моделей, методів та методик, що забезпечуватимуть швидку достовірну оцінку основних характеристик властивості живучості сучасних СЗІ КМЗ.

1. Структурна схема моделі оцінки живучості систем захисту інформації корпоративних мереж зв'язку

Модель оцінки живучості систем захисту інформації корпоративних мереж зв'язку [19] є сукупністю досить великої кількості окремих моделей різного призначення, що використовують для опису процесів як детерміновані, так і ймовірнісні методи (рис. 1).

Блок дестабілізуючих факторів (ДФ). За областю впливу розрізнятимемо точкові та просторові моделі ДФ. У точкових моделях вважатимемо, що ДФ точно виражає один або декілька функціональних елементів СЗІ КМЗ. В останньому випадку область впливу ДФ – група точок, в яких розташовані структурні елементи системи захисту. Кількість елементів в СЗІ КМЗ завжди більша, ніж кількість точок в області впливу ДФ. Тому для кожного елемента або групи елементів задамо ймовірність потрапляння в область впливу ДФ. При одноточковій області задамо розподіл $\{a_i, i=1,...,N\}$, де N – кількість елементів системи, a_i – ймовірність того, що i-й елемент потрапить в область впливу ДФ. Одним із можливих розподілів є рівномірний розподіл $a_i = 1/N$. Для багатоточкової області задамо розподіл $\{b_i = P(X=i), i=1,...,N\}$, де b_i – ймовірність того, що в область впливу потрапить рівно i елементів СЗІ. В моделі використовуватимемо усічений біноміальний розподіл

$$b_i = C_N{}^i p^i (1-p)^{N-i} \Big/ (1-p)^N, i=1,...,N,$$

де p – ймовірність виживаності одиничного елемента у точковій моделі та усічений пуассонівський розподіл:

$$b_i = \frac{a^i}{i!} \Bigg/ \sum_{j=1}^{N} \frac{a^j}{j!}, a = -\ln p.$$

У просторових моделях задамо двовимірний розподіл декартових координат епіцентра ДФ $p_2(x_0, y_0)$ та розподіл радіуса кола $p_0(r_0)$, в якому діє ДФ.

За законом розподілу інтенсивності ДФ розрізнятимемо ДФ з нескінченною інтенсивністю, з постійною інтенсивністю I за всією площею області дії, спадною від епіцентра за визначеним законом $I(r, j)$ інтенсивністю, в окремому випадку, за законом Релея:

$$I(r, j) = I_0 \exp(-r^2 / a{r_0}^2),$$

де I_0 – максимальна інтенсивність в епіцентрі; r_0 – радіус кола – області дії ДФ; a – постійний параметр, r і j – полярні координати точки при розташуванні початку координат в епіцентрі.

За тривалістю дії розрізнятимемо імпульсні ДФ (нульова тривалість), з постійною t і з випадковою тривалістю T, яку задамо розподілом $F_T(t) = P(T > t)$. За постійної тривалості амплітуду збурень I_0 задамо як функцію часу за допомогою формул:

$$I_0(t) = {I_0}^0 (1 - t/t); I_0(t) = {I_0}^0 \exp(-t^2 / b^t 2), \quad (1)$$

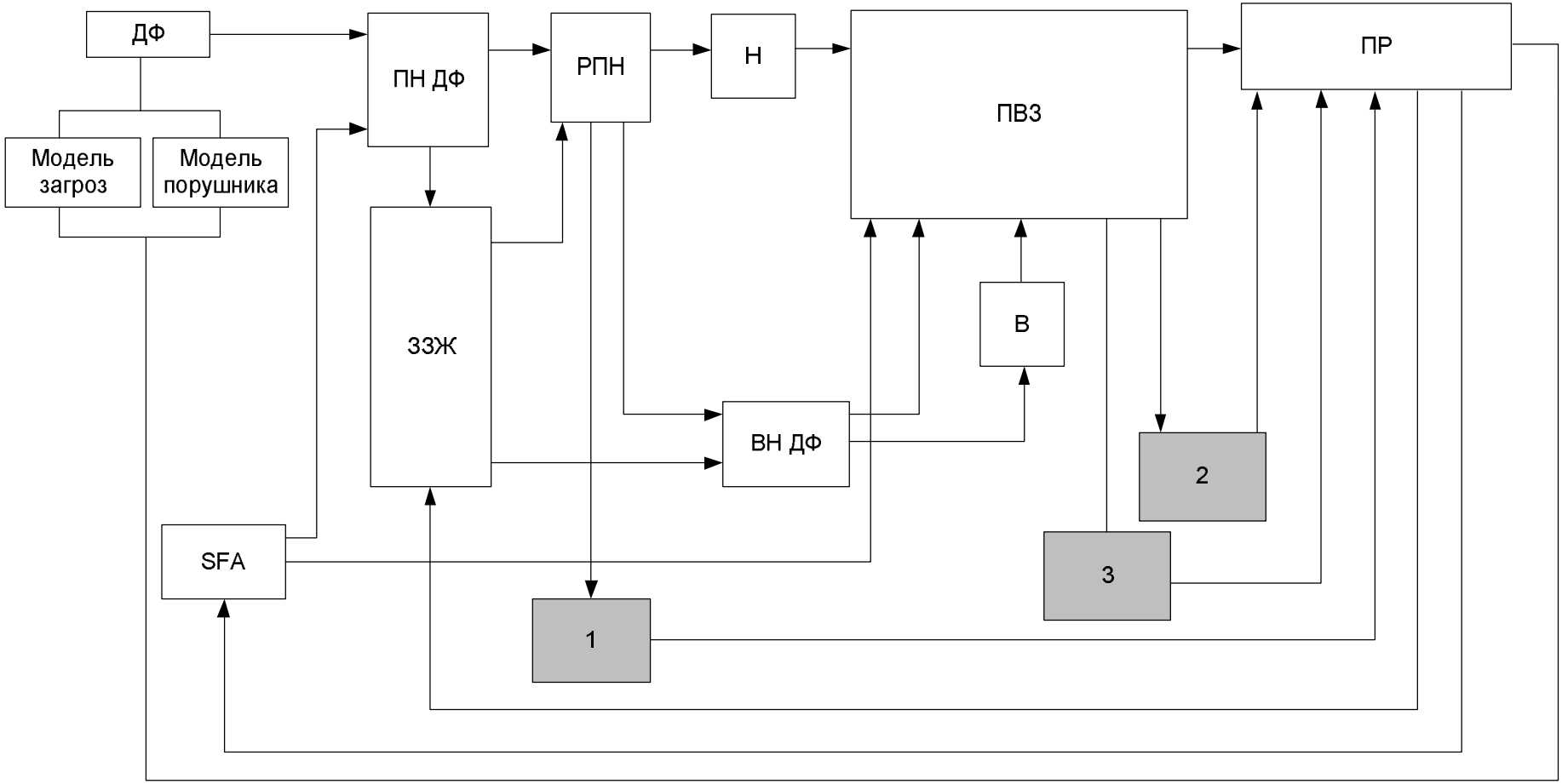

Рис 1. Структурна схема моделі оцінки живучості систем захисту інформації корпоративних мереж зв'язку
(1 – оцінка живучості за станом системи, 2 – оцінка живучості за результатами виконання завдання; 3 – потокова модель)

де $b = 0{,}3...0{,}5$ – параметр. Аналогічні залежності будуть і за випадкової тривалості, але тоді в (1) t замінятимемо на випадкову величину T.

При багатократному ДФ найпростішими стратегіями вибору характеристик наступного ДФ є стратегія незалежних ДФ (стратегія 1) і стратегія з вилученням вражених елементів із області впливу наступного ДФ (стратегія 2). За сукупністю зазначених характеристик можна створити різні моделі. Деякі з них наведемо в табл. 1.

Блок SFA (наприклад, модель захищеної КМЗ). SFA-модель описує технічну і функціонально-алгоритмічну структури системи захисту, зокрема моделі функціонування і характеристик функціональних елементів, топології системи, маршрутів інформаційних, матеріальних і енергетичних потоків, функціональну і структурну ієрархію, дерева цілей функціонування.

Розглянемо детальніше чотири характеристики моделі: розміри елементів, їхню надійність, стійкість і топологію системи. За розмірами елементи можуть бути точковими, лінійними, плоскими з межею у вигляді довільного контуру, об'ємні з межею у вигляді однозв'язної поверхні. За рівнем надійності елементів розрізнятимемо моделі з ідеально надійними елементами і моделі з обмеженою надійністю елементів. Перший випадок є ідеалізованим, який використовуватимемо для оцінки живучості за станом системи. За рівнем стійкості розрізняємо елементи з нульовою і ненульовою стійкістю. Перший випадок є ідеалізованим та призначений для того, щоб в моделі оцінки живучості СЗІ КМЗ вважати непрацездатними всі елементи, що потрапили в зону впливу ДФ. У другому випадку ймовірність порушення працездатності залежить від інтенсивності ДФ і розміру тієї частини площі (або об'єму) елемента, яка потрапила в зону впливу ДФ.

За топологією системи розрізнятимемо моделі з довільною і заданою топологією. Модель першого типу використовуємо при точкових елементах і точкових ДФ. При просторових ДФ і плоских або об'ємних елементах використовуємо модель другого типу.

Таблиця 1

Моделі дестабілізуючих факторів за сукупністю характеристик

Фактори	Модель ДФ						
	1	2	3	4	5	6	7
Область дії	точка	точка	група точок	група точок	площа	площа	площа
Інтенсивність	∞	∞	∞	∞	∞	I_0	I_0
Тривалість дії	імп.	імп.	імп.	імп.	імп.	t	t
Стратегія	1	2	1	2	1	1	2

Блок первинних наслідків (ПН) ДФ отримуємо у результаті взаємодії моделі працездатності з моделлю SFA, завдяки чому враховуємо аспект вразливостей моделі СЗІ КМЗ та ДФ, які через них впливають на систему захисту. В цій моделі не враховуємо управлінські впливи з боку засобів забезпечення живучості (ЗЗЖ).

Блок ЗЗЖ відображає характеристики засобів контролю, аварійного захисту, рекон-фігурування і управління. Алгоритми прийняття рішень про боротьбу за живучість, що входять в цю модель, формують управлінські дії, спрямовані на зміну структури і параметрів системи і на використання внутрішніх резервів, що створюють для роботи в умовах впливу ДФ. У цій моделі враховуємо також характеристики зовнішніх ЗЗЖ.

Блок розвитку первинних наслідків (РПН) ДФ отримуємо в результаті поєднання моделі ПН і моделі ЗЗЖ, що дає змогу знайти траєкторію керованого перехідного процесу з урахуванням дій ЗЗЖ. Кінцевою метою аналізу моделі РПН є визначення нового стійкого стану системи. Оскільки деякі характеристики ЗЗЖ є ймовірнісними, результати аналізу моделі РПН також можна подати в ймовірнісній формі.

Блок надійності (Н) містить інформацію про безвідмовність і ремонтопридатність елементів, систему технічного обслуговування, про реакцію системи на окремі відмови елементів, про вплив

різних факторів ДФ на безвідмовність елементів. Цю модель застосовуємо для оцінки живучості за наслідками виконання завдання.

Блок вторинних наслідків (ВН) ДФ відображає ті віддалені наслідки ДФ, які можуть виникати в системі внаслідок скорочення обсягу функцій, що виконуються, і погіршення технічних характеристик. До вторинних наслідків можна зарахувати збільшення часу виконання функцій, швидкості старіння і зносу елементів, додаткове розмноження помилок в СЗІ КМЗ, підвищену витрату енергії і матеріалів для виконання тих самих функцій й інші наслідки, що призводять до скорочення резервів у системі, які залишилися після впливу ДФ, і подальшого погіршення технічних характеристик.

Блок відновлення (В) містить опис аварійних ресурсів, правил і способів їх використання в умовах впливу ДФ з метою відновлення технічної і функціонально-алгоритмічної структури тієї частини системи, яка зайнята у виконанні встановленого завдання. Її можна трактувати як модель розвитку системи після закінчення впливу ДФ.

Блок процесів виконання завдання (ПВЗ) отримуємо в результаті об'єднання п'яти моделей (SFA, H, B, BH). Аналіз цієї моделі дає змогу оцінити живучість за наслідками виконання завдання.

На етапі проектування та експлуатації захищеної КМЗ використовується також *блок прийняття рішення (ПР)* про способи підвищення живучості, якщо оцінки показують її незадовільний рівень. Модель допомагає встановити поради щодо зміни структури і параметрів системи, а також додаткового розвитку ЗЗЖ.

2. Аналіз процесу оцінки живучості систем захисту інформації за допомогою мережі Петрі

Проаналізувавши оцінки живучості систем захисту інформації за допомогою мереж Петрі, можна у зручній графічній формі дослідити коректність реалізації процесу оцінки та експлуатаційні властивості моделі. Теорію мереж Петрі широко використовують для аналізу процесу моделювання та його оцінки [20–24].

Однією з найважливіших якостей системи захисту інформації корпоративних мереж зв'язку на етапі проектування є її функціональна коректність. Це означає, що вона проявляє певні кількісні або якісні властивості. Переконавшись, що СЗІ КМЗ поводить себе належно («правильно»), важливим завданням є забезпечити, щоб система відповідала певним продуктивно-пов'язаним (або кількісним) цілям. Хоч користувачі системи захисту вважають забезпечення коректності її роботи де-факто, саме кількісні властивості доволі часто визначають перевагу однієї системи над іншою [24].

Теорія мереж Петрі дає змогу розв'язати задачі якісного характеру [23], які виникають під час дослідження процесу оцінки СЗІ КМЗ: чи виконує система ті функції, для яких вона призначена; чи функціонує вона ефективно; чи можуть в ній виникати помилки та аварійні ситуації; чи містить вона потенційно вузькі місця; чи можна спростити систему або замінити її окремі компоненти і підсистеми на досконаліші, не порушуючи її загального функціонування; чи можна з таких систем сконструювати складнішу, яка відповідатиме заданим вимогам, тощо.

Мережі Петрі є популярним графічним формалізмом процесу моделювання, який може допомогти розробникам систем захисту забезпечити правильність, коректність і продуктивність процесу під час її проектування та розроблення. Незважаючи на те, що теорія мереж Петрі спочатку була розроблена для дослідження якісних властивостей складних систем, представлення паралелізму і синхронізації процесів, нині вони дають змогу здійснювати й кількісний аналіз [24].

У структурному представленні мережею Петрі є дводольний орієнтований граф, який складається із множини позицій (places) і множини переходів (transitions). Графічно позиції позначають у вигляді «кругів», а переходи – «бар'єрами». Умови-позиції та події-переходи пов'язані відношенням безпосередньої залежності (безпосереднім причинно-наслідковим зв'язком), яке позначають за допомогою напрямлених дуг, які скеровані із позицій в переходи та навпаки.

Дуги графа є (щодо переходів) вхідними дугами (стрілка дуги з позицій до переходів), вихідними дугами (стрілка дуги з переходів у позиції) та дугою-інгібітором (позначають дугою з

колом із позицій до переходів). Багатократні (вхідні, вихідні або інгібіторні) дуги між позиціями та переходами дозволені із вказанням числа, яке позначає їхню кратність.

У середині позиції є маркери, які позначають у вигляді чорних точок, що відображають значення станів або об'єктів. Зокрема, розташування маркерів у певних позиціях називають маркуванням. Система розпочинає роботу в деякий момент із певним набором маркерів, який називають початковим маркуванням.

Перехід називають активним лише за умови наявності принаймні стількох маркерів у обидвох позиціях на його вході, якою є кратність вхідних дуг, та якщо кожна інгібіторна позиція містить менше маркерів, ніж кратність інгібіторної дуги. Активний перехід може спрацювати, тобто відбувається видалення по одному маркера з усіх вхідних позицій та створення одного маркера у кожній вихідній позиції (рис. 2) [24].

Якщо два (або більше) переходи можуть спрацювати і вони не мають спільних позицій, то їхні спрацювання є незалежними діями, що відбуваються в будь-якій послідовності або паралельно.

Якщо декілька переходів можуть спрацювати і мають спільну вхідну позицію, тоді спрацьовує лише один з них. Може виявитися, що, спрацювавши, цей перехід позбавить можливості спрацювати інші переходи. Тобто в мережі моделюють конфлікт між подіями, коли реалізація однієї події може перешкоджати можливості реалізації інших. У теорії мереж Петрі не вказано, як фактично необхідно вирішувати цей конфлікт. Вважають, що рішення про те, яка подія із конфліктних повинна реалізуватися, приймають за межами формалізму мережі, тобто поведінка мережі має невизначений недетермінований характер.

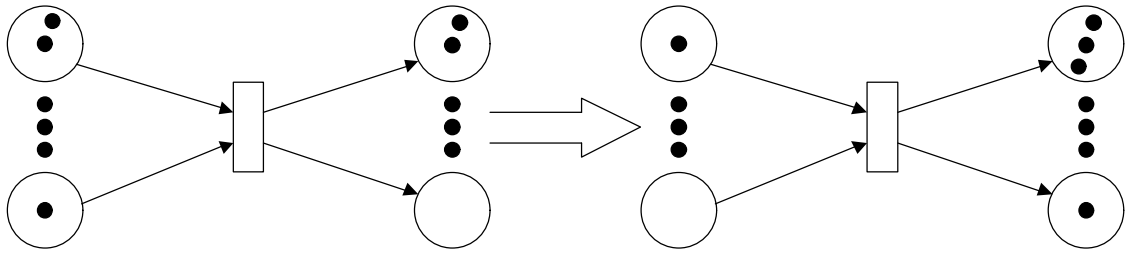

Рис. 2. Зразок роботи переходу мережі Петрі

В процесі функціонування мережі відбувається зміна розмітки позицій як результат спрацьовування її переходів. Мережа зупиняється, якщо жоден із її переходів не є активним [23].

Формально, процес оцінки живучості СЗІ КМЗ подамо графом мережі Петрі і наведемо визначення.

Мережа дослідження процесу оцінки живучості СЗІ КМЗ – це мережа з набором основних параметрів (P,T,F): P – непорожня множина елементів мережі, які називають позиціями; T – непорожня множина елементів мережі, які називають переходами; $F \subseteq P \times T \cup T \times P$ – відношення інцидентності; $W : F \to N\{0\}$ та $M_0 : P \to N$ – дві функції, які називають кратністю дуг та початковим маркуванням відповідно [22, 23].

Мета спеціальної теорії мереж Петрі – автоматичний аналіз властивостей мереж, їхній автоматичний синтез та перетворення, на основі чого можна побудувати практичні алгоритми аналізу, синтезу і перетворення дискретних систем, які моделюють мережами. В окремому випадку важливим завданням є пошук алгоритмів, за допомогою яких для будь-якої представленої мережі можна встановити, чи має вона необхідні для проектувальників СЗІ властивості – чи є вона обмеженою, живою, стійкою тощо. Насамперед необхідно довідатися про існування таких алгоритмів. Ці запитання сформуємо як масові алгоритмічні проблеми для мереж: проблема обмеженості (чи існує алгоритм, за яким можна дізнатися про те, чи є мережа обмеженою), проблема потенційної живучості переходів, проблема живучості мереж, проблема стійкості, проблема безпечності [20–24].

Разом із описаними вище графічним та теоретико-множинним визначенням мережі Петрі, широко використовують матричне представлення мережі. Позиції та переходи $P = \{p_i \mid i = \overline{1,m}\}$,

$T = \{t_j \mid j = \overline{1,n}\}$ нумерують так, що $|P| = m$, $|T| = n$. Відношення A представляють матрицями інцидентності B (вхідна) та D (вихідна) або, для мереж без петель, матрицею C (інгібіторна):

$$B = \left\| b_{i,j} \right\|, i = \overline{1,m}, j = \overline{1,n}, b_{i,j} = A(p_i, t_j);$$

$$D = \left\| d_{i,j} \right\|, i = \overline{1,m}, j = \overline{1,n}, d_{i,j} = A(t_j, p_i);$$

$$C = D - B.$$

Маркування мережі подамо вектором:

$$\overline{M} = (M(p_1), M(p_2), ..., M(p_m)).$$

У цьому випадку мережа Петрі однозначно задає набір $(B, D, \overline{M_0})$ для мереж без петель – $(C, \overline{M_0})$.

Введемо фундаментальні характеристики поведінки мережі Петрі. Для цього використаємо такі допоміжні позначення: позначимо, що перехід $t \in T$ є активним (дозволений) в маркуванні $\overline{M}$ як $\overline{M} \to^t$; спрацювання переходу $t \in T$ позначимо як $\overline{M} \to^t \overline{M'}$. Аналогічні позначення використовуватимемо також для послідовності спрацьовувань переходів $s \in T^* (s = t_{j_1}, t_{j2}, ..., t_{jk})$: послідовність $s \in T^*$ спрацьовує у маркуванні $\overline{M} : \overline{M} \to^s \overline{M'}$. Фундаментальними характеристиками поведінки мережі Петрі є вільний вибір маркування мережі $L(N) = \{s \mid \overline{M_0} \to^s\}$ та множина досяжних маркувань мережі $R(N) = \{\overline{M} \mid \exists s \in T^* : \mid \overline{M_0} \to^s \overline{M} \mid\}$.

Набір основних властивостей мереж Петрі сформувався як набір характеристик, які властиві об'єкту дослідження, що є корисними або небажаними (яких необхідно уникати). Тому властивості умовно розділимо на позитивні та негативні. Необхідність побудови методів для визначення того, чи має мережа потрібну властивість, сформулюємо у вигляді задач (проблем). Розрізнятимемо поведінкові та структурні властивості мереж. Поведінкові властивості пов'язані із конкретним початковим маркуванням. Структурні властивості виконуються за будь-якого початкового маркування.

Для процесу оцінки живучості СЗІ КМЗ (рис. 1), який представлено мережею Петрі (рис. 4), доцільно дослідити такі основні властивості [25]:

- досяжність маркування: для заданої мережі Петрі N і маркування $\overline{M}$ визначити, чи виконується умова $\overline{M} \in R(N)$;
- покриття: для заданої мережі Петрі N і маркування $\overline{M}$ встановити, чи містить $R(N)$ певне маркування $\overline{M'}$ таке, що $\overline{M'} \geq \overline{M}$;
- потенційна живучість: перехід $t \in T$ є потенційно живим, якщо існує дозволена послідовність спрацювань, що містить цей перехід: $\exists s \in T : \overline{M_0} \to^s \& t \in s$;
- живучість: перехід є живим, якщо він є потенційно живим у будь-якому досяжному маркуванні; $t \in T$ є живим, якщо $\forall \overline{M} \in R(N), \exists s \in T^* : \overline{M} \to^s \& t \in s$; мережа Петрі є живою, якщо живими є всі її переходи;
- тупик (deadlock): маркування $\overline{M}$ мережі називають t-тупиковим, якщо перехід $t \in T$ не є в ній потенційно живим; маркування $\overline{M}$ мережі називають тупиковим, якщо вона t-тупикова для усіх переходів мережі. Інколи розглядають таку властивість, як безтупиковість, що означає відсутність у мережі тупиків. Ця властивість є слабшою, ніж живучість. Хоча мережа й може функціонувати нескінченно, але при цьому певні переходи не можуть бути активними. Тому властивість тупиковості часто розглядають як негативну;

• обмеженість: позиція $p \in P$ обмежена (l-обмежена), якщо існує таке ціле число l, що маркування позиції не перевищує його: $\forall \overline{M} \in R(N): M(p) \le l$. Мережа є обмеженою, якщо обмеженими є всі її позиції;

• безпечність: безпечною називають *1*-обмежену мережу;

• консервативність: консервативною називають мережу, яка зберігає зважену суму маркерів щодо певного вектора міри $\overline{w}$ з натуральними компонентами: $\overline{w}\overline{M} = \overline{w}\overline{M_0} = const$. Строго консервативною називають мережу, сума маркерів якої постійна, тобто консервативну мережу щодо одиничного вектора міри;

• повторюваність: послідовність спрацювання переходів s повторювана, якщо її можна запустити довільну кількість разів; тобто із $\overline{M} \to^{s}$ випливає $\overline{M} \to^{s^*}$;

• стаціонарна повторюваність: послідовність спрацювань переходів s стаціонарно повторювана, якщо вона повторювана і приводить мережу в початкове маркування: $\overline{M} \to^{s} \overline{M}$;

• стійкість: мережа є стійкою, якщо для двох будь-яких дозволених переходів спрацювання одного із них не призводить до заборони спрацювання іншого:

$$\forall t, t' \in T, \overline{M} \in R(N): (\overline{M} \to^{t} \overline{M^1} \,\&\, \overline{M} \to^{t'} \overline{M^2}) \Rightarrow (\overline{M^1} \to^{t} \,\&\, \overline{M^2} \to^{t'});$$

• оборотність: мережа є оборотною, якщо для $\forall M \in R(G, \overline{M_0})$ виконується $M_0 \in R(G, \overline{M})$;

• стан прийому: маркування називають станом прийому (базовим станом), якщо вона досяжна із будь-якого досяжного в мережі маркування.

Для представлення процесу оцінки живучості СЗІ КМЗ у вигляді мережі Петрі: 1) визначимо події, що виникають у системі захисту; 2) встановимо умови, за яких виникає кожна з подій; 3) з'ясуємо зміни, які відбуваються в системі під час здійснення кожної події; 4) відобразимо графічно зв'язки між подіями та умовами.

Представимо модель процесу оцінки живучості СЗІ КМЗ (рис. 1) у вигляді мережі Петрі (рис. 4) та дослідимо її у програмному середовищі Pipe v.3.0 (Проект MSc Group, Department of Computing at Imperial College London). Результати роботи програми наведено нижче. Програмне середовище Pipe v.3.0 (із відкритим програмним кодом) є платформонезалежним засобом для створення та аналізу мереж Петрі (містить повний набір модулів аналізу поведінки та властивостей мереж, статистику продуктивності та деякі прості функції: порівняння та класифікацію) [24].

Таблиця 2

Результати моделювання мережі Петрі (1000 спрацювань переходів)

Позиція	Середня кількість маркерів	Інтервал довіри 95% (+/-)
В	0.04595	0.01096
ВН ДФ	0.08591	0.01021
ДФ	0.05295	0.00436
ЗЗЖ	0.09790	0.00932
Модель загроз	0.05395	0.00436
Модель оцінки № 1	0.02697	0.00399
Модель оцінки № 2	0.04695	0.00534
Модель оцінки № 3	0.04296	0.01024
Модель порушника	0.05395	0.00436
Модель СЗІ КМЗ	0.04895	0.00667
Н	0.01399	0.01151
ПВЗ	0.12587	0.00881
Переглянути модель загроз та порушника	0.05295	0.00436
ПН ДФ	0.07592	0.01094
ПР	0.15285	0.00685
РПН	0.07592	0.01385

Аналіз моделювання показав, що мережа Петрі, яка відображає процес оцінки живучості СЗІ КМЗ, є коректною, її можна використати на етапі проектування та експлуатації, оскільки у неї є такі властивості:

- обмеженість, оскільки кількість маркерів в ній не перевищує ціле число, що уможливлює її апаратну реалізацію;
- безпечність, оскільки кількість маркерів в ній не перевищує 1, що є важливою властивістю для мереж Петрі, які повинні моделювати реальний пристрій або процес;
- мережа є потенційно живою, оскільки кожний із переходів може спрацювати (табл. 2);
- мережа має властивість досяжності маркування та покриття (рис. 3);

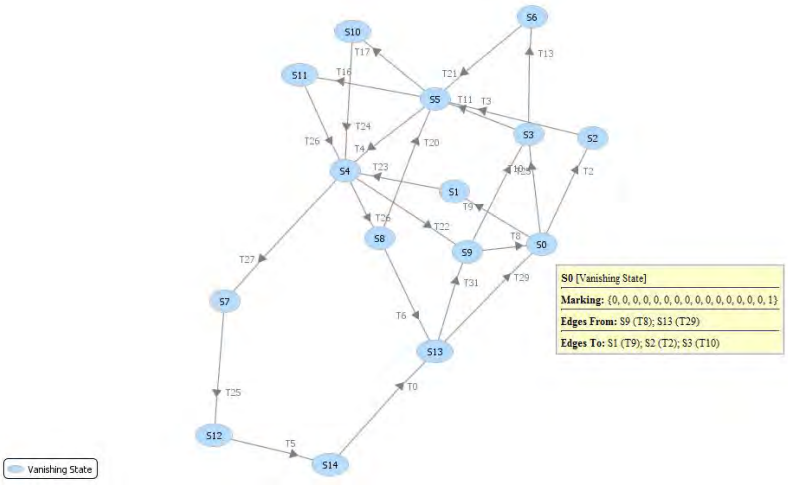

Рис. 3. Граф досяжності/покриття мережі Петрі

Таблиця 3

Вхідна матриця інцидентності *B*

Позиція/ Перехід	T0	T10	T11	T13	T16	T17	T2	T20	T21	T22	T23	T24	T25	T26	T26	T27	T28	T29	T3	T31	T4	T5	T6	T8	T9
В	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ВН ДФ	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
ДФ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
ЗЗЖ	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
Модель загроз	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
Модель оцінки №1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Модель оцінки №2	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Модель оцінки №3	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Модель порушника	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
Модель СЗІ КМЗ	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
Н	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ПВЗ	0	0	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
Переглянути модель загроз та порушника	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
ПН ДФ	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
ПР	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	0	0	0	0	1	0	0	0	0
РПН	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0

- мережа є живою, оскільки в ній немає тупикових маркувань;
- стійкість, оскільки спрацювання будь-якого переходу не блокує інших;
- активність, тобто у ній відсутні взаємні блокування, що випливає із матриць інцидентності (табл. 3, 4, 5, 6);

Таблиця 4

Вихідна матриця інцидентності D

Позиція/ Перехід	T0	T10	T11	T13	T16	T17	T2	T20	T21	T22	T23	T24	T25	T26	T26	T27	T28	T29	T3	T31	T4	T5	T6	T8	T9
В	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ВН ДФ	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ДФ	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ЗЗЖ	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0
Модель загроз	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
Модель оцінки №1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Модель оцінки №2	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
Модель оцінки №3	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
Модель порушника	0	0	0	0	0	0	0	0	0	0	0	0	0		0	0	0	0	0	0	0	1	0	0	0
Модель СЗІ КМЗ	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0		1	0	0
Н	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
ПВЗ	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
Переглянути модель загроз та порушника	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
ПН ДФ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0
ПР	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0
РПН	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Таблиця 5

Вихідна матриця інцидентності C

Позиція/ Перехід	T0	T10	T11	T13	T16	T17	T2	T20	T21	T22	T23	T24	T25	T26	T26	T27	T28	T29	T3	T31	T4	T5	T6	T8	T9
В	0	0	0	1	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ВН ДФ	0	1	-1	-1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
ДФ	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
ЗЗЖ	0	0	0	0	0	0	0	0	0	1	0	0	-1	0	0	0	0	0	0	1	0	0	0	-1	0
Модель загроз	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	-1	0	0	0
Модель оцінки №1	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Модель оцінки №2	0	0	0	0	0	1	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0
Модель оцінки №3	0	0	0	0	1	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0
Модель порушника	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	-1	0	0	0
Модель СЗІ КМЗ	0	0	0	0	0	0	0	-1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	-1	0	0
Н	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0
ПВЗ	0	0	1	0	-1	-1	0	1	1	0	0	0	0	0	0	0	0	1	0	-1	0	0	0	0	0
Переглянути модель загроз та порушника	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	1	0	0	0	0	0	0	0	0	0
ПН ДФ	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	-1	0	0	1	0	0
ПР	0	0	0	0	0	0	0	0	0	-1	1	1	0	1	-1	-1	0	0	0	0	1	0	0	0	0
РПН	0	-1	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	-1

Таблиця 6

Інгібіторна матриця H

Позиція/ Перехід	T0	T10	T11	T13	T16	T17	T2	T20	T21	T22	T23	T24	T25	T26	T26	T27	T28	T29	T3	T31	T4	T5	T6	T8	T9
В	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ВН ДФ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ДФ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ЗЗЖ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Модель загроз	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Модель оцінки №1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Модель оцінки №2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Модель оцінки №3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Модель порушника	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Модель СЗІ КМЗ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Н	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ПВЗ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Переглянути модель загроз та порушника	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ПН ДФ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ПР	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
РПН	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

• мережа не є консервативною, оскільки систему $\overline{\overline{wM}} = \overline{\overline{wM_0}}$ неможливо розв'язати в цілих невід'ємних числах;

• початкове маркування $M_0 = [0000100010000000]$ є досяжним у мережі.

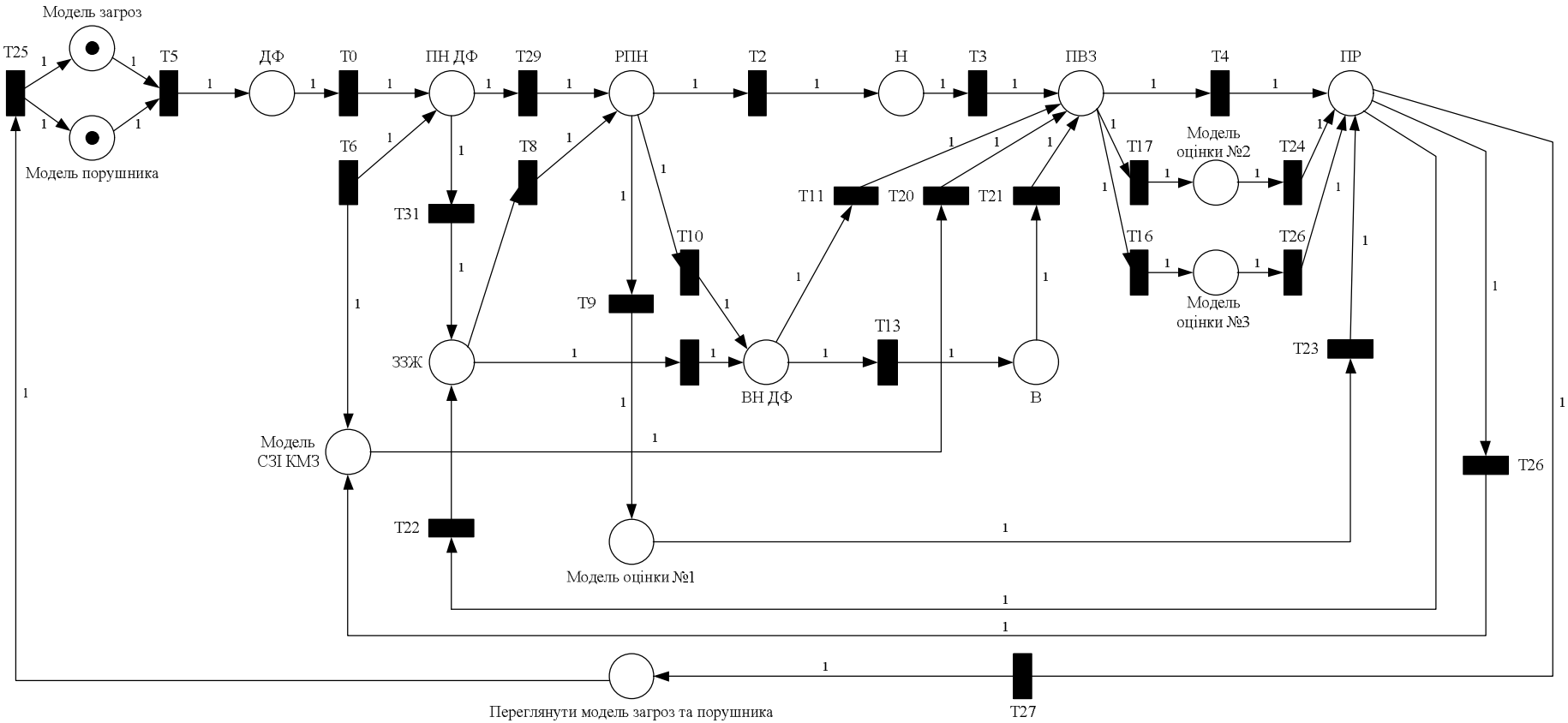

Рис. 4. Процес оцінки живучості систем захисту інформації корпоративних мереж зв'язку у вигляді мережі Петрі

Висновки

Розширення галузі застосування систем захисту інформації пов'язане з підвищенням вимог до швидкодії, точності, надійності, достовірності отриманих результатів. Якщо в одних випадках відмова або недостовірний результат може викликати лише незначні незручності у роботі, то в інших (наприклад, в оборонних структурах держави, банківській системі, захищених корпоративних мережах зв'язку) серйозність наслідків відмов не викликає сумнівів. Галузь застосування, яку характеризують невизначеністю умов функціонування, впливу дестабілізуючих факторів та недопустимістю відмов, пояснює актуальність створення систем захисту інформації не лише надійних, але й таких, що матимуть властивість живучості.

Вирішуючи актуальну науково-практичну проблему розроблення моделей і методів оцінки живучості СЗІ КМЗ для покращення показників якості її функціонування в умовах впливу дестабілізуючих факторів на етапі проектування та експлуатації, в межах роботи розроблено та проаналізовано модель оцінки живучості систем захисту інформації корпоративних мереж зв'язку, яка відрізняється від інших урахуванням особливостей функціонування СЗІ КМЗ, моделі загроз та порушника, використанням потокової моделі оцінки живучості, що забезпечує вирішення проблеми перерозподілу потоків інформації після впливу ДФ для виконання цільової функції (захисту інформації). Доведено коректність реалізації моделі оцінки живучості СЗІ КМЗ за допомогою теорії мереж Петрі.

1. Дудикевич В. Б. Концептуальні моделі захисту інформації для технологій стаціонарного, стільникового, супутникового зв'язку / В. Б. Дудикевич, Ю. Р. Гарасим, Г. В. Микитин // Вісник Національного університету «Львівська політехніка» «Автоматика, вимірювання та керування». – Львів, 2010. – № (665). – С. 18–26. 2. Steiglitz K. The design of minimum-cost survivable networks / K. Steiglitz, Weiner P., D. J. Kleitman // IEEE Transactions on circuit theory. – Vol. 16. – No. 4. – 1969. – 455–460 pp. 3. Додонов А. Г. Корпоративные информационные системы: обеспечение живучести / А. Г. Додонов, Д. В. Флейтман // Математичні машини і системи. – 2004. – № 4. – С. 118-130. 4. Можаев А. С. Технология автоматизированного структурно-логического моделирования надежности, живучести, безопасности, эффективности и риска функционирования систем / А. С. Можаев // Приборы и системы. Управление, Контроль, Диагностика. – СПб : ООО Издательство «НАУЧТЕХЛИТИЗДАТ», 2008. – С. 1–14. 5. Зиновьев П. А. Вопросы теории и практики создания и развития корпоративных систем в отрасли связи / П. А. Зиновьев, И. З. Насыров. – 2002. – С. 3–43. 6. Зиновьев П. А. О методологических особенностях системного проектирования корпоративных информационных систем / П. А. Зиновьев. – 1999. – С. 3–30. 7. Зегжда Д. П. Принципы и методы создания защищенных систем обработки информации : автореф. дис. на соискание ученой степени докт. техн. наук 05.13.19 / Зегжда Дмитрий Петрович; Санкт-Петербургский государственный политехнический университет: СПб, 2002. – 39 с. 8. Павлов І. М. Методики проектної оцінки надійності та живучості комплексної системи захисту інформації мобільних систем зв'язку і автоматизації : автореф. дис. на здобуття наукового ступеня канд. тех. наук: 05.13.21 / Павлов Ігор Миколайович; Держ. ун-т інформаційно-комунікаційних технологій. – К., 2008. – 19 с. 9. Хорошко В. А. Методы и средства защиты информации / В. А. Хорошко, А. А. Чекатков. – К. : Юниор, 2003. – 503 с. 10. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты / В. В. Домарев. – К. : ООО «ДС», 2001. – 688 с. 11. Ленков С. В. Методы и средства защиты информации. Том 2. Информационная безопасность / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. – Арий, 2008. – 344 с. 12. Казакова Н. Ф. Повышение адаптивности и достоверности вероятностной модели оценки живучести системы защиты шифрования / Н. Ф. Казакова, Е. О. Тискина, В. А. Хорошко // Інформаційна безпека. – № 2 (2). – 2009. – С. 69–72. 13. US Patent Application Publication. Rule-based network survivability framework / Satyendra Yadan, Nilesh M. Bhide. – Pub. No.: US 2004/0111638 A1. – Jun. 10.2004. – 1–8 pp. 14. Knight J. C. Achieving Critical System Survivability through Software Architectures / J. C. Knight, E. A. Strunk. – Department of Computer Science, University of Virginia. – 2005. – 1–28 pp. 15. Liew S. C. A framework for characterizing disaster-based network survivability / S. C. Liew, K. W. Lu // IEEE Journal on selected areas in communications. –

Vol. 12. – No 1. – 1994. – 52–58 pp. 16. Liu Y. A general framework for network survivability quantification / Y. Liu, K. S. Trivedi // 12th GI/ITG conference on measuring, modelling and evaluation of computer and communication systems. – 2004. – 1–10 pp. 17. Kawamura R. Architectures for ATM network survivability / Ryutaro Kawamura // IEEE Communications Surveys. – 1998. – Vol. 1. – No. 1. – 1–11 pp. 18. Medhi D. Multi-Layered Network Survivability – Models, Analysis, Architecture, Framework and Implementation: An Overview / D. Medhi, D. Tipper. – 2000. – 1–21 pp. 19. Гарасим Ю. Розробка моделі оцінки живучості для систем захисту інформації / Ю. Гарасим // Комп'ютерні науки та інженерія: Матеріали IV Міжнародної конференції молодих вчених CSE-2010. – Львів : Видавництво Львівської політехніки, 2010. – С. 320–321. 20. David R. Petri Nets and Grafcet / R. David, H. Alla. – Prentice Hall, Cambridge, 1992. 21. Лескин А. А. Сети Петри в моделировании и управлении / А. А. Лескин, П. А. Мальцев, А. М. Спиридонов. – Л. : Наука, 1989. – 133 с. 22. Питерсон Дж. Теория сетей Петри и моделирование систем / Дж. Питерсон. – М., 1984. – 270 с. 23. Котов В. Е. Сети Петри / В. Е. Котов. – М. : Наука, 1984. – 157 с. 24. Bonet P. Pipe v.2.5: a Petri net tool for performance modeling / P. Bonet, Llado C., Puigjaner R. – 12 p. 25. Зайцев Д. А. Математические модели дискретных систем / Д. А. Зайцев. – Одесса: ОНАС им. А.С. Попова, 2004. – 40 с.

УДК 378

Н.О. Думанський
Національний університет "Львівська політехніка,
кафедра інформаційних систем та мереж

ВІДКРИТІ СИСТЕМИ ДИСТАНЦІЙНОГО НАВЧАННЯ

Розглянуто відкриті системи для створення дистанційних курсів. Проаналізовано їхні характеристики та функціонал.

Ключові слова: дистанційна освіта, електронне навчання.

The article deals with open systems to create distance learning courses. Analyzes their characteristics and functionality.

Key words: distance education, e-learning.

Вступ

Широкий розвиток дистанційної освіти сприяє створенню все нових і нових систем організації цього напряму освіти. Почало з'являтись як вільне програмне забезпечення, так і пропрієтарне. Оскільки пропрієтарне програмне забезпечення розвивається переважно в англомовному варіанті, доцільно було б розглянути вільне ПЗ, оскільки, якщо його перекладу на українську мову і не існує, його можна перекласти без порушення авторських прав. Першопрохідцем в цій галузі була система Moodle. Її досить широко використовують на теренах нашої держави. Але не варто забувати і про інші програмні продукти формування дистанційних курсів. Адже в них міститься багато цікавих реалізацій деяких функцій навчально-виховного процесу. Функціональні можливості вільних систем дистанційного навчання не поступаються, а в дечому навіть і перевищують пропрієтарні аналоги. Розвиток вільного ПЗ ґрунтується на спільному створенні системи спільнотою вибраного продукту. Програмісти – дописують та виправляють код, а прості користувачі, в цьому випадку, виконують роль тестерів. Такий метод написання програм є досить дієвим, оскільки дають змогу знайти і виправити ті помилки, з якими дійсно стикається користувач системи.