УДК 004.621.3:519.816 **С.В. Зибін**

МЕТОД ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ ФУНКЦІОНУВАННЯ СППР В СКЛАДІ ПРОГРАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Дана робота присвячена методу імітаційного моделювання функціонування систем підтримки прийняття рішень в складі комплексної системи технічного захисту. Метод побудовано з використанням мережевих моделей мереж Петрі, Мерліна та Е-мереж.

Ключові слова: програма безпеки, захист, СППР, система підтримки прийняття рішень, моделювання, Петрі, Мерлін.

Розробка складних систем й оцінка якості їх функціонування передбачає розв'язання широкого кола різнопланових завдань. Причому інтенсивне застосування засобів обчислювальної техніки й автоматизації постійно корегує погляди на діяльність цих систем, до складу яких входять системи підтримки прийняття рішень.

Підвищення якості й скорочення часу прийняття рішень при керуванні складними системами різного призначення в сучасний час неможливе без розробки ефективних комплексних програмних і апаратних засобів. Особливо гостро стоїть ця проблема в системах підтримки прийняття рішень, щодо забезпечення безпеки інформації. Системах технічного захисту працюють у режимі реального часу, де дефіцит часу відчувається особливо сильно, а наслідки при несвоєчасному або неправильному ухваленні рішення можуть бути катастрофічними.

У зв'язку з цим існує потреба у застосуванні систем підтримки прийняття рішень, основним завданням яких є надання допомоги фахівцям у процесі прийняття раціонального й оптимального рішення в складних ситуаціях, які виникають при функціонуванні систем технічного захисту. Причому оцінка якості вибору рішень і їх параметрів повинні здійснюватися на базі моделей, які б дозволили оцінювати застосування однієї й тієї ж системи в різних умовах експлуатації.

Підвищення ефективності математичного моделювання систем технічного захисту можна забезпечити за рахунок моделювання, як комплексної системи в цілому, так і підсистем, які входять до її складу. Ця необхідність стимулює розробку моделей і алгоритмів, що допускають вирішення складних завдань керування системою.

Тому синтез системи технічного захисту і підтримки прийняття рішень для них, які будуються на основі засобів обчислювальної техніки повинен здійснюватися відповідно до наступних критеріїв:

- декомпозиція процесу керування, тобто можливість реалізації будь-якої складної операції на послідовності більш простих;
- модульність побудови систем;
- магістральний спосіб обміну інформацією, який дозволяє мінімізувати кількість зав'язків;
- можливість масштабування обчислювальної потужності за рахунок використання розподілених систем.

Розробка, аналіз й дослідження математичних моделей систем технічного захисту і підтримки прийняття рішень, які являються невід'ємною частиною програм інформаційної безпеки, вимагає значних часових витрат. Застосування мереж Петрі для таких цілей дозволяє прискорити процес розв'язання подібних задач.

По своєму призначенню, структурі й функціям, що виконуються системам підтримки прийняття рішень являються невід'ємною складовою частиною систем технічного захисту, які працюються в режимі реального часу. Тому питання синтезу систем підтримки прийняття рішень слід розглядати з урахуванням взаємодії алгоритмів роботи таких систем із алгоритмами функціонування систем захисту інформації.

Для сучасних систем керування системами технічного захисту, що працюють у режимі реального часі, найбільш типовою є трьохрівнева структура обчислювальних засобів.

На першому рівні знаходиться універсальна обчислювальна машина, що має потужний потенціал для засобів обробки інформації, в тому числі розподілених засобів; на другому – спеціалізовані обчислювальні пристрої; на третьому – персональні обчислювальні пристрої, які входять до автоматизованих робочих місць.

При формуванні інформаційної моделі та способів її керування основними функціями обчислювальних засобів являються збір і обробка інформації від функціональних програм. Однією з важливих функцій є формування й видача керуючих і інформаційних масивів на об'єкти керування, а також приймання й використання інформаційних повідомлень, що вводяться.

Основну функцію по формуванню інформаційної моделі і по керуванню нею виконують обчислювальні засоби кінцевих пристроїв. Найбільш типовими із цих функцій, як правило, є наступні [1]:

- функція по формуванню інформаційної моделі;
- функція по керування інформаційною моделлю.

Реалізація підтримки прийняття рішень у системах технічного захисту не змінює основних функцій обчислювальних засобів, пов'язаних з формуванням інформаційної моделі. Імітаційна модель дозволяє оцінити ефективність роботи системи й усувати конфліктні ситуації. В цьому випадку функціонування системи стає ситуаційним.

Для оцінки ефективності функціонування системи підтримки прийняття рішень у складі системи технічного захисту необхідно виконати моделювання процесу роботи системи.

Основними цілями моделювання являються:

- уточнення технічного рішення по вибору засобів обчислювальної техніки і розподіл функцій між ними;
- перевірка узгодженості функціонування технічних засобів СППР;
- оцінка ефективності роботи програми інформаційної безпеки, яка включає в себе систему підтримки прийняття рішень.

Структурна схема імітаційної моделі, що виконує описані вище задачі, наведена на рис. 1.

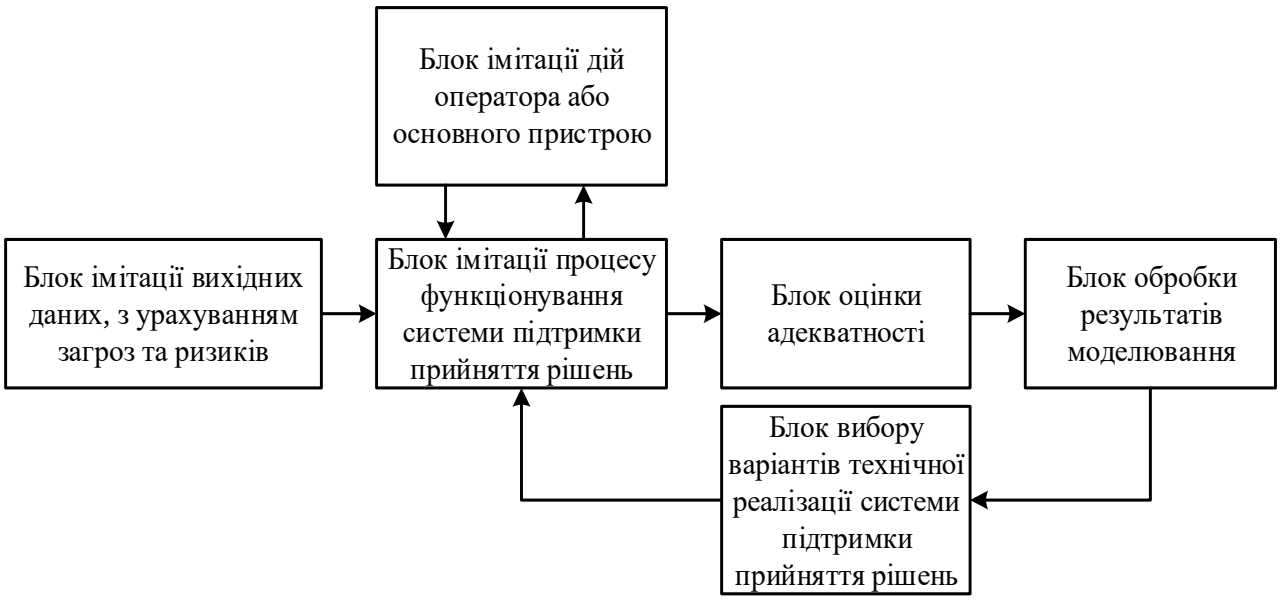

Рис. 1. Структурна схема імітаційної моделі функціонування системи

Для оцінки ефективності системи підтримки прийняття рішень із урахуванням загроз та ризиків при усуненні конфліктних ситуацій у моделі необхідно враховувати дії обслуговуючого персоналу й зловмисників.

Центральним блоком моделі є блок імітації процесу функціонування системи підтримки прийняття рішень. Для імітації процесів, що відбуваються в засобах обчислювальної техніки, широко використовуються: теорія масового обслуговування, ймовірнісні графи, мережі Петрі і т.д. [1, 2].

Класичну мережу Петрі можна представити у наступному вигляді – $P=(D, B, G, \Theta, M_0)$,

де B – кінцева множина позицій $B=\{b_i\}$, $i = \overline{1,n}$;

D – кінцева множина переходів $D=\{d_j\}$, $j = \overline{1,k}$;

$G:D\times B \rightarrow \{0,1\}$ – пряма функція інцидентності;

Θ: $B\times D \rightarrow \{0,1\}$ – зворотна функція інцидентності;

M_0: $B \rightarrow Z$ – початкова розмітка (маркування), що задає початковий розподіл міток по позиціях мережі;

$Z=\{0,1,2,...\}$ – множина невід'ємних цілих чисел.

Для кожного переходу $d_j \in D$ можна визначити множину вхідних $\Theta(t_j)$ та вихідних $I(t_j)$ позицій:

$$\Theta(t_j)=\{b_i \in B/\Theta(b_i, d_j) = 1\},$$

$$I(t_j)=\{b_i \in B/G(d_j, b_i) = 1\},$$

де $i = \overline{1,n}$; $j = \overline{1,k}$.

Аналогічно вводяться визначення множини вхідних $I(b_i)$ та вихідних $\Theta(b_i)$ переходів позиції

$$I(b_j)=\{d_j \in D/G(d_j, b_i) = 1\},$$

$$\Theta(b_j)=\{d_j \in D/\Theta(b_i, d_j) = 1\}.$$

Маркування мережі представляється вектором

$$M = \begin{vmatrix} m(b_1) \\ m(b_2) \\ \dots \\ m(b_n) \end{vmatrix},$$

де $m(b_i)$ – число міток в позиції b_i.

Мережа Петрі функціонує переходячи від розмітки до розмітки. Зміна розміток відбувається в результаті спрацьовування одного з переходів $d_j \in D$ мережі. Необхідною умовою спрацьовування одного із переходів d_j являється $\forall\, b_i \in B\ [m(b_i) - \Theta(b_i,d_j) \geq 0]$. Перехід d_j, для якого виконується зазначена умова, визначається як такий, що перебуває в стані готовності до спрацьовування або як збуджений перехід.

Спрацьовування переходу d_j змінює розмітку M_ξ на $M_{\xi+1}$, тобто перехід d_j вилучає по одній мітці з кожної своєї вхідної позиції й додає по одній мітці в кожну з вихідних позицій.

Основним недоліком класичних мереж Петрі являється відсутність часу в описі динаміки процесу функціонування системи, яка моделюється. Усунути цей недолік можна за допомогою двох розширень мереж Петрі: часові мережі й мережі Мерліна, які дозволяють відбити в моделі часові параметри системи [2].

Мережу P_s з урахуванням часового параметру можна за допомогою $P_s=(D, B, G, \Theta, M_0, J, \vartheta)$,

де

$J=(\tau_1,\dots, \tau_i,\dots)$ – зростаюча послідовність дійсних чисел (часова база);

ϑ:$B\times J \rightarrow$ J – функція часових затримок.

Факт часу враховується в цій мережі шляхом впровадження пасивного стану мітки в позиції. При надходженні мітки в позицію b_i вона залишається в пасивному стані на час $\vartheta(b_i, \tau_s)$ і тільки після цього переходить в активний стан.

Мережа Мерліна задається співвідношенням $P_y=(D, B, G, \Theta, M_0, J^*, J^{**})$,

де $J^*=\{\tau_i^*\}$ – множина часів мінімальної затримки для переходів $d_j \in D$;

$J^{**}=\{\tau_i^{**}\}$ – множина часів максимальної затримки для переходів $d_j \in D$.

Спрацьовування будь-якого переходу d_j мережі Мерліна може настати через час не менше τ_i^* після його збудження й не більше τ_i^{**}.

Подальшим розширенням мереж Петрі являються так звані оцінні мережі або Е-мережі, що дозволяють відображати залежність процесів обробки від типу задач, що вирішуються, тобто враховуючі пріоритетність обробки інформації [2]. Однак вони не враховують одну важливу особливість обробки інформації, а саме, її ймовірнісний характер. Тому на основі часових мереж і Е-мереж як апарата для імітаційного моделювання функціонування систем підтримки прийняття рішень слід застосовувати модифіковані часові мережі Петрі, що дозволяють враховувати ймовірнісний характер обробки інформації.

Модифікована часова мережа Петрі задається сукупністю множин $\widetilde{P_s} = \{D, B, G, \Theta, M_0, J, f(D_i)\}$,

де

$B=\{B_{SP}, B_\tau, B_R, B_P\}$ – множина позицій, що складаються із неперетинних підмножин B_{SP} звичайних позицій;

B_τ – часові позиції;

B_R – керуючі позиції;

B_P – зліченні позиції;

$D=\{D_{SP}, D_Y, D_F, D_R, D_P\}$ – множина базових переходів, вміст яких розглянемо далі;

$J=\{\tau_i\}$ – час перебування мітки в позиції B_τ;

$f(D_i)$ – функція, що визначає наявність мітки в керуючій позиції B_R.

Для модифікованої часової мережі Петрі визначено п'ять основних типів переходів [3], логіка роботи яких задається вказівкою дозволених змін розміток. Спрацьовування переходу типу D_{SP} (звичайний перехід) відбувається при наявності мітки у вхідній позиції B_1 і відсутності мітки у вихідній позиції B_2, тобто $(1,0) \xrightarrow{D_{sp}} (0,1)$.

Для переходу D_F (розгалуження) маємо $(1,0,0) \xrightarrow{D_F} (0,1,1)$, а перехід об'єднання D_y описується $(1,1,0) \xrightarrow{D_y} (0,0,1)$.

Керуючий перехід типу D_R (розгалуження за умовою) визначається наступним чином:

$$(0,1,0,0) \rightarrow (0,0,1,0),$$

$$(1,1,0,0) \rightarrow (0,0,0,1).$$

Зліченний перехід D_P задається співвідношенням $(p, 1, 0) \rightarrow (n\text{-}1,0,1)$, де $n \geq 1$).

Наведені п'ять основних типів переходів дозволяють виконати моделювання різних ситуацій, що зустрічаються при обробці інформації. Перехід D_{SP} моделює подію, що наступає при виконанні однієї умови. У випадку наявності двох або більше умов використовується перехід D_Y. Розгалуження потоку інформації відображається переходом D_F. При необхідності зміни напрямку потоку інформації з деякої умови використовується перехід типу D_R. При організації лічильника застосовується T_P.

Позиції в модифікованої часової мережі Петрі являються також декількох типів:

- B_{SP} – звичайна позиція, мітка з якої видаляється відразу після дозволу вихідного переходу;
- B_τ – часова позиція, мітка з якої видаляється тільки після закінчення часу τ;
- B_R – керуюча позиція, у якій мітка з'являється по результату обчислення функції $f(b_i)$ і зникає при спрацьовуванні вихідного переходу;

• B_P – зліченна позиція, кількість міток якої визначається лічильником циклу виконання ділянок програми.

Функціонування модифікованої часової мережі Петрі являє собою послідовне виконання трьох фаз [3].

Фаза псевдоготовності є присутнім при всіх переходах. Протягом цієї фази відбувається перевірка переходів на дозволеність, тобто наявність у всіх вхідних позиціях хоча б однієї мітки. Виключення становить керуючий перехід D_R, у якому достатньо мітки в одній позиції.

Якщо перехід дозволений, він вступає у фазу готовності, протягом якої відбувається визначення результату часу знаходження міток у вхідних часових позиціях. Після закінчення цього часу перехід входить в активну фазу. Якщо перехід B_{SP}, то він входить в активну фазу відразу.

В активній фазі змінюється розмітка відповідно до управління переходу.

Таким чином, апарат модифікованої часової мережі Петрі дозволяє будувати досить повні моделі функціонування алгоритмів, що відображають їхню структуру, логіку роботи й часові характеристики.

Для ефективного використання широкого спектра можливостей апаратних мереж Петрі необхідне створення на базі апаратних мереж Петрі системи спеціального математичного забезпечення з набором засобів опису, введення, трансляції, компонування, компіляції, налагодження, імітації моделі, обробки результатів моделювання й аналізу.

При побудові системи імітаційного моделювання на мережах Петрі істотну роль відіграє вибір:

• опису вихідних моделей;

• способу внутрішньомашинного (внутрішньосистемного) представлення описаної моделі й на його основі організації алгоритму моделювання.

Внутрішньосистемне представлення мереж Петрі може бути організоване у вигляді матриць або у вигляді спискових структур.

При наявності системи підтримки прийняття рішень у складі системи технічного захисту внутрішньосистемне представлення в матричній формі мереж Петрі може бути описано двома матрицями: матрицею інцидентності E розмірності $p \times d$, де p – число вершин місць, d – число вершин переходів моделі, і матрицею руху міток F розмірністю, які визначаються наступним чином [4]:

1) $E(i,j) = 1$, якщо $B_i \in B^I_{t_j}$; $E(i,j) = 0$, якщо $B_i \notin B^I_{t_j}$;

2) $F(i,j) = \alpha+\beta$, де $\alpha = 1$, якщо $B_i \in B^I_{t_j}$;

$\alpha = 0$, якщо $B_i \notin B^I_{t_j}$;

$\beta = -1$, якщо $B_i \in O^o_{t_j}$;

$\beta = 0$, якщо $B_i \notin O^o_{t_j}$.

Позначимо A^j – j-й стовбець матриці A.

Тоді можна стверджувати:

а) перехід t_j може бути запущений, якщо $E^j - d_0^{-(k)}$;

б) наступна розмітка після спрацьовування t обчислюється по формулах

$$d_0^{-(k+1)} = d_0^{-(k)} + F^{(j)}$$

$$-\left[E^j \to d_0^{-(k)}\right] \equiv \left[E^j d_0^{-(k)}\right] = \left[E^j / d_0^{-(k)} = 0\right].$$

Отже, умова запуску переходу t_j полягає у виконанні умови $E^j d_0^{-(k)} = 0$, а наступна розмітка обчислюється в такий спосіб:

$$d_0^{-(k+1)} = d_0^{-(k)} \oplus C^j,$$

де

$\oplus$ – позначення операції виключне АБО;

C(i,j) = 1, якщо $F(i,j) \neq 0$;

C(i,j) = 0, якщо *F(i,j) = 0.*

Тут всі операції виконуються над векторами булевих змінних, що дозволяє досить ефективно реалізовувати цей спосіб з використанням обчислювальної техніки.

Для підвищення швидкодії впровадимо представлення кожного з переходів t_v одним із місць $B_\varepsilon^\tau \in B_{t_v}^1$. Для запуску переходу t_v необхідно (але недостатньо) виконання умови $d(B_\varepsilon^\tau) = 1$.

Визначимо вектор булевих змінних R розмірності $d \times 1$, а також матриці A і W розмірністю $d \times d$:

- $R(j) = 1$, якщо $d(B_i^\tau) = 1, B_i^\tau \in B_{t_j}^1$;
- $W(i,j) = 1$, якщо t_j і t_i представлені одним й тим самим місцем B_i^τ;
- $A(i,j) = 1$, якщо t_j представлено місцем $B_i^\tau \in \Theta_{t_j}$.

Тоді після спрацювання t_j наступна розмітка обчислюється по формулі $R^+ = R \oplus A^j \oplus W^j$ і моделюється алгоритмом. Крім того $R^+ = R \oplus L^j$.

Тут $L^j = A^j \oplus W^j$ дозволяє заощаджувати об'єм пам'яті, що використовується. При такому підході можна скоротити час виконання програми з одночасним зменшенням об'єму пам'яті, що використовується. Це відбувається за рахунок матриці L і вектора R. Для зниження обсягу пам'яті, що використовується доцільно використовувати внутрішньосистемне представлення моделей у вигляді стекових структур, тому що E, F, L являються розрідженими матриці. У результаті розмір пам'яті, що використовується лінійно залежить від значень d и p, тоді як у випадку матричного представлення цей розмір пропорційний $d \times p$.

Одним із способів досягнення компромісу між складністю й вірогідністю математичної моделі є спрощення еквівалентне об'єкту мережі, яке відбувається за допомогою маршрутів функціонування системи [5] на основі апарата нечітких відносин у просторі, який обумовлений базою системи технічного захисту і підтримки прийняття рішень, яка може розширюватися. У цю же базу даних заносяться відомості про поведінку системи за наявності ризиків, загроз та зовнішніх впливів. Моделі, одержані таким способом мають керовану розмірність і на основі строгих математичних правил перетворюються або в компактний, або в розширений вид. Вірогідність моделі системи технічного захисту і підтримки прийняття рішень у ній є не вихідним, а вхідним параметром для моделювання. Звідси витікає й головна перевага такого підходу. Маршрутна модель із вірогідністю, що заздалегідь задається, дозволяє прогнозувати динаміку розвитку подій навколо програми інформаційної безпеки за наявності загроз та ризиків, а також стан.

Розглянемо більш докладно принципи побудови маршрутів, маршрутних моделей і моделюючого інформаційного середовища. Приймемо за X універсальну множину можливих співвідношень об’єкту, що моделюється. Нехай X моделюється з необхідною вірогідністю φ множиною описів N_0, що складається з елементів $\bar{n}$.

Тому:

$$N_0 \leq x;$$

$$N_0 = \{N/\bar{N} \in X, \mu(\bar{N}) \geq 1 - \varphi\}, \quad (1)$$

де $\mu(N)$ – функція приналежності опису $\bar{N}$ множині X.

Маршрут, як відображення марківського процесу з нечіткими початковими умовами стосовно нечіткої множини описів N_0, являється множиною рівня $\alpha \neq 1 - \varphi$;

$$N = \{\bar{N}/N_0\,, \mu(\bar{N}) > \alpha\} \quad (2)$$

Однак враховуючи правила впорядкування елементів в N_0 маршрут можна представити у вигляді $A\bar{B}P = (B, D, KS)$, де N_0 відображує характер компонента ABP.

Будемо вважати, що множина відносин, що відповідають "нормальному" маршруту N_H, визначається як:

$$N_H = \{\bar{N}/\bar{N} \in N_0, \mu_H(\bar{N}) > \beta\}, \quad (3)$$

де β – параметр, який задається, стійкості системи технічного захисту до зовнішніх впливів.

У той же час для "експериментального" маршруту N_E справедливо наступне твердження

$$N_{\mathrm{E}} = \{N/\bar{N} \in N_0, \mu_{\mathrm{E}}(\bar{N}) > \beta^1\}, \quad (4)$$

де β^1 – параметр, що задається, границі нестійкості системи технічного захисту.

При розширенні й звуженні множин моделюючих відносин слід керуватися наступними принципами:

- розширення нормального маршруту з урахуванням експеременталього маршруту

$$N_1 = \{\bar{N}/N \in N_0, N_1(\bar{N})\}, \quad (5)$$

$$\text{де } N_1(\bar{N}) = \begin{cases} 0, \text{ якщо } \left[\mu_E(\bar{N}) X_{\mu_E}(\bar{N})\right] < \beta \\ \max[\mu_E(\bar{N})], \text{ якщо } \left[\mu_E(\bar{N}) V_{\mu_H}(\bar{N})\right] \geq \beta \end{cases}$$

- звуження експеременталього маршруту з урахуванням нормального маршруту

$$M_2 = \{\bar{N}/N \in \overline{N_0}, N_2(\bar{N})\}, \quad (6)$$

$$\text{де } N_2(\bar{N}) = \begin{cases} 0, \text{ якщо } \left[N_E(\bar{N}) V_{\mu_H}(N)\right] \geq \beta \\ \max[N_E(N), N_H(N)], \text{ якщо } [N_E(N) N_H(N)] < \beta \end{cases}$$

З умов (5) і (6) випливає

$$\lim_{\beta \to 0} N_1 = \lim_{\beta \to 0} N_2 = N_0 \quad (7)$$

Швидкість переходів і вірогідність розміщень для позицій моделюючої мережі Петрі є мірою інформативності відповідним їм відносин.

При $\beta = 1$ в мережі Петрі, які синтезуються на маршрутних множинах, увійдуть найбільше "живі" переходи мереж Петрі, побудовані на N_0 [6]. По мірі зростання кількості вузлів мережі Петрі функція приналежності переходу множині "живих" переходів убуває. Замінивши поняття швидкість на експертну оцінку приналежності переходу множині "живих" переходів, вдається відійти від безпосереднього розв'язання питання про можливість спрацьовування того або іншого переходу.

Для множин станів типу маршрутних множин вихідний стан позначимо через N_p, а досяжне з нього як N_p^+. Тоді прогноз як лінійний оператор описується в такий спосіб:

$$F = N_p^- = N_p^+, \tag{8}$$

де F – лінійний оператор прогнозу:

$$N_p^- \underline{W} \text{ и } N_p^+ \underline{W} M_1.$$

Прогноз як функціонал визначається в базисі N_0 як функція приналежності стану N_p^- множині оцінок технічного стану системи технічного захисту. Аспекти прогнозу мають свої прогнози в *ABP* і формалізується як лінійний оператор у просторі, який породжується N_0 і як функціонал, обумовлений лінійною формою в просторі N_0.

Зі співвідношення (8) витікає, що прогноз як лінійний оператор і як функціонал утворює дерево можливостей, тому що по визначенню з виразів (5) і (6) випливає, що потужність N_1, більше ніж N_2. При машинній реалізації це приводить до рішення задач комбінаторного типу й до експонентного росту розмірностей моделі. Внаслідок цього проводимо відсікання гілок, тобто приймаємо до розгляду тільки ті гілки дерева можливостей, функція приналежності яких N_0 не менш β. Основою для реалізації приведеного підходу на ПЕОМ служить виділення й аналіз так званих стаціонарних станів системи технічного захисту. Стосовно N_0 множина стаціонарних станів визначається як

$$N_0 \leq N_W$$

$$N_W\{\overline{N}/N \in N^0, N^W(\overline{N})\} \cong 1,$$

де N_W – множина стаціонарних станів.

Всі елементи N_W є корінням нормального маршруту при відсутності зовнішніх впливів. Зовнішні впливи утворюють простір збурювань, базисом якого являється елементарний вплив [7]. Кожному елементу N_W відповідає нечітко обмежений підпростір простору збурювань. Іншими словами, елементам N_W присвоюються чутливість до елементів базису простору збурювань, тим самим даючи початок елементам множин. Множина станів кожного стаціонарного стану веде свій початок з множини елементів, по одному на кожний нульовий елемент базису підпростору збурювань. Відносини між множинами й множиною стаціонарних станів поля

$$N_Э \cap N_W = N_H \cap N_W = N_W.$$

Інакше кажучи, базисні впливи породжують символи дерев можливості.

Аналіз стаціонарних станів системи технічного захисту повинен виявити взаємозв'язок між ними. У випадку великої складності системи застосовуються підтримка прийняття рішень, експертні оцінки якої визначають взаємозв'язки елементів N_0. Результатом аналізу являється нормальний маршрут стаціонарних станів, який є основою для побудови дерева ймовірності й прогнозування технічного стану системи технічного захисту і рівня захищеності.

Система підтримки прийняття рішень у складі програми інформаційної безпеки включає себе у вузлові моменти функціонування системи технічного захисту, тому вона відбиває характер поведінки елементів і підсистем згідно із алгоритмом. Таким чином, система підтримки прийняття рішень являється моделлю штатної роботипрограми інформаційної безпеки. Прогнозованість технічного стану такої програми спирається на марківський характер функціонування підсистем, з однієї сторони й на систему оцінок і рекомендацій системи підтримки прийняття рішень з іншої сторони.

Для коректного визначення якостей функціонування програми інформаційної безпеки із урахуванням рекомендацій системи підтримки прийняття рішень необхідне задоволення й виконання наступних вимог [5]:

- система оцінок технічного стану і якості функціонування повинна містити пріоритети відповідних вихідних гілок мереж Петрі стаціонарних станів, що виражаються у вигляді функцій приналежності станів вихідної гілки множині технічних станів і умов функціонування програми інформаційної безпеки;
- глибина дослідження і деталізацій технічних станів і якості (умов) функціонування програми інформаційної безпеки визначається заданою вірогідністю φ.

З урахуванням цих вимог модель реалізується на основі виразів (1) ÷ (8), являє собою модель, побудовану на асоціативних принципах. Залежно від необхідної вірогідності моделювання глибини пошуку в базі даних і підключення вузлів мережі Петрі може змінитися в широких межах, тому що дані в базі даних упорядковані у вигляді множини дерев, які перетинаються. Перетинання дерев слід розуміти як нечітке відношення [8]. Вузол перетинання являє собою нечіткі множини, яким придана міра у вигляді функції приналежності вузла дерева вузлу асоціації. Залежно від перехідних вимог асоціації можуть розширитися, розділитися або утворювати з іншими асоціаціями нову, більш широку асоціацію. Зведені в базу даних маршрути організують асоціативний доступ до характерних станів програми інформаційної безпеки, одночасно доповнюючи інформацію, що міститься в базі даних, новою необхідною й при цьому видаляючи стару, непотрібну.

Виходячи із цього засоби інтелектуалізації процесів ухвалення рішення є в теперішний час найбільш важливим і практично необхідним елементом у сфері інформаційних технологій, які являються основою інформаційної безпеки.

Література

1. Герасимов Б.М. Системы поддержки принятия решений: проектирование, применение, оценка эффективности / Герасимов Б.М., Дивизинюк М. М., Субач И. Ю. – Севастополь: НИЦ ВС Украины "Государственный океанариум".- 2004. – 320 с.

2. Питерсон Дж. Теория сетей Петри и моделирующие системы / Питерсон Дж. – М.: Мир, 1984. – 264с.

3. Котов В.Е. Сети Петри / Котов В.Е. – М.: Наука, 1984. – 160с.

4. Капустян М.В. Применение сетей Петри для оценки технического состояния систем защиты информации /Капустян М.В., Хорошко В.А., Чирков Д.В. // Сучасний захист інформації, № 1, 2011. – С. 10-15.

5. Тискина Е.О. Проектирование систем защиты информации и систем поддержки принятия решений для них / Тискина Е.О., Хорошко В.А. // Сучасний захист інформації, Спецвипуск, 2010. – С. 25-31.

6. Моржов С.В. Применение сетей Петри для моделирования параллельных процессов / Моржов С.В., Хорошко В.А. // Проблемы управления и информатика, № 2, 2004. – С. 86-94.

7. Кобозева А.А. Анализ информационной безопасности / Кобозева А.А., Хорошко В.А. – К.: Изд. ГУИКТ, 2009. – 215 с.

Майника Э. Алгоритмы оптимизации на сетях и графах / Майника Э. – М.: Мир, 1981. – 323 с.

Надійшла 08.12.2016 р. Рецензент: д.т.н., проф. Дружинін В.А.