- використання пропускної здатності фізичного каналу між обладнанням користувача та крайовим комутатором АТМ-мережі;
- цілісність віртуального каналу.

Характеристики точності стосовно умов використання АТМ-обладнання мають враховувати якість передавання даних щодо:

- виникнення помилок у потоці прийнятих чарунок підчас передавання трафіку через віртуальний канал;
- отримання зайвих чарунок у загальному потоці чарунок, які передаються віртуальним каналом.

Гарантованість передавання даних через канали мереж ПД характеризуються можливістю загублення чарунок у загальному потоці чарунок, які передаються віртуальним каналом.

IV Висновок

Отже, під час вибору показників відповідності стосовно обладнання АТМ доцільно користуватися узагальненими мережними параметрами і характеристиками, наведеними в [1]. Під час вибору множини показників відповідності достатньо враховувати тільки ті узагальнені мережні характеристики, які відповідають фазі передачі даних. Оскільки різні класи трафіку передаються віртуальними каналами мереж АТМ за допомогою служб різних сервісних категорій, які використовують різні механізми маршрутизації, керування з'єднаннями, резервування ресурсів мережі і підтримки необхідної якості обслуговування, а тому визначаються різними наборами параметрів трафіку і QoS, зробимо висновок про необхідність вибору показників відповідності для контролю працездатності обладнання АТМ окремо для віртуальних каналів кожної з сервісних категорій.

Література: ***1.*** *International Telecommunications Union, Telecommunication Standardization Sector, "General Quality of Service Parameters for Communication via Public Data Networks", Rec. X.140, September 1992, <http://www.itu.int/itu-t>.* ***2.*** *ATM Forum, Traffic Management Specification Version 4.1, AF-TM-0121.000, March 1999, <http://www.atmforum.org>.*

УДК 681.3.004

ФОРМАЛІЗАЦІЯ ПРОЦЕСІВ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ОБЧИСЛЮВАЛЬНИХ СИСТЕМАХ

Сергій Хамула, Володимир Ковбаса, Юрій Кулинич*

Об'єднаний інститут при Національній академії оборони України

**Центр АСУ Головного штабу ВМС України*

Анотація: **Розглянуто підхід до формалізації процесів забезпечення безпеки інформації, що грунтується на використанні властивостей мереж Петрі і їх проблемно-орієнтованих розширень.**

Summary: **We have considered the approach to the formalization of the processes aimed at ensuring the security of information based on the use of properties of the Petri nets and on their problimatically orientated extensions.**

Ключові слова: **Система захисту інформації, система підтримки прийняття рішень, мережі Петрі.**

I Вступ

Відомо [1, 2], що для досягнення необхідного рівня захищеності інформації процесами захисту потрібно постійно керувати. Тобто, досягнення необхідного рівня захищеності має здійснюватися з мінімальними і зіставлюваними з цінністю інформації витратами сил і засобів захисту. Тому, одним з основних структурних елементів будь-якої системи захисту інформації (СЗІ) слід вважати підсистему управління безпекою (ПУБ), призначену для синхронізації і координації функціонування засобів захисту інформації [3, 4]. Більш детально класифікацію задач, які покладаються на ПУБ наведено на рис. 1.

В свою чергу, процес управління СЗІ розглядається, звичайно, як задача адаптаційного управління і базується на концепції централізації функцій управління та застосування спеціалізованих систем підтримки прийняття рішень (СППР). Доцільність використання СППР в ПУБ обумовлена необхідністю оперативного реагування на спроби несанкціонованого доступу (НСД) до інформації або відмови засобів захисту з метою попередження порушень безпеки інформації і мінімізації можливих втрат у випадку їх здійснення. Основою для розробки таких СППР є формалізація процесів забезпечення безпеки інформації [4].

Аналіз останніх досліджень і публікацій вказує на те, що проблема захисту інформації в інформаційно-обчислювальних системах (ІОС) із значною кількістю одночасно працюючих абонентів та складною структурою інформаційно-логічних зв'язків ще далека від остаточного розв'язання. Основою більшості із зазначених робіт є теоретичні моделі, запропоновані в [5 – 8]. Ці моделі в недостатній мірі враховують топологічні особливості і специфіку контролю стану ІОС, а також їх функціонування в умовах ризику, при невідомих імовірностях реалізації загроз інформації і різних величинах збитку від реалізації цих загроз.

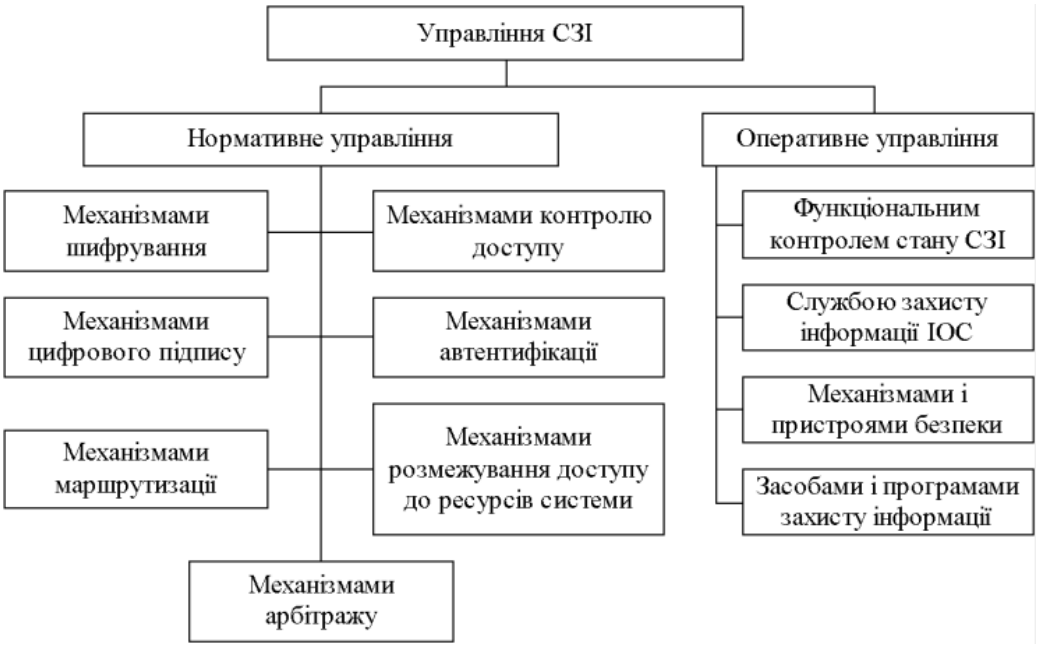

Рисунок 1 – Класифікація задач, які покладаються на ПУБ

II Постановка завдання

Завдяки складності і високому рівню абстракції, в притаманних згаданим моделям, побудувати захист і отримати кількісні показники його ефективності в конкретних системах до цього часу не вдалось. В процесі проектування систем розробники змушені керуватись стандартами і нормативними документами, в яких наведено лише набір захисних функцій і сформульовані вимоги щодо їх реалізації, проте методики побудови (синтезу) СЗІ відсутні. Критерієм експертної оцінки відповідності захисту тому чи іншому класу є кількість зазначених функцій і повнота виконання наведених вимог. Такі критерії і методи оцінки мають вельми низьку точність результатів [9].

Метою даної статті є розгляд підходу до формалізації процесів забезпечення безпеки інформації, який ґрунтується на використанні мереж Петрі і їх проблемно-орієнтованих розширень. Останні дозволяють описати структуру системи і отримати якісну оцінку її функціонування, а згадані розширення мереж Петрі – ще й кількісні показники ефективності функціонування систем.

III Основна частина

Нехай функціонування СЗІ відбувається у середовищі, що описується кортежем:

$$Q(t) = \langle Y(t), H(t) \rangle,$$

де $Y(t)$ – керовані характеристики середовища: потоки даних, повноваження абонентів, параметри криптографічних протоколів; $H(t)$ – некеровані характеристики середовища: відмови елементів системи, спроби НСД до інформації і елементів системи.

Стан СЗІ $X(t)$ в процесі функціонування залежить від стану середовища, а також від реалізації управління:

$$X(t) = \langle U_{\text{і}}(t), U_{\text{î}}(t) \rangle,$$

де $U_{н}(t)$ – нормативне управління СЗІ; $U_{о}(t)$ – оперативне управління СЗІ.

Декомпозиція факторів управління СЗІ $U(t)$ на оперативне і нормативне дозволяє більш ефективно вирішувати задачі управління СЗІ в умовах невизначеності місця і часу спроб НСД, а також в комбінованих ІОС зі змінною структурою, для яких нормативне управління СЗІ малоефективне. Це пов'язано з тим, що при зміні конфігурації мережі або при переміщенні абонентів вузлами мережі відбувається істотна зміна алгоритмів нормативного управління.

Нехай $R(t) = R(X(t))$ – критерій ефективності СЗІ, визначений на контрольованих станах ІОС і СЗІ. Стан СЗІ $X(t)$ залежить від $Q(t), U_{о}(t), U_{н}(t)$, тому можливо отримати залежність:

$$X(t) = S(Q(t), U(t)),$$

де *S* – модель СЗІ.

В цьому випадку мета управління полягає у вирішенні задачі:

$$U^{*}(t) = \arg \max_{U(t) \in \Delta} R[S(Q(t), U(t))],$$

де Δ – обмеження, що накладаються на вибір управління $U^{*}(t)$, пов'язані з можливостями СЗІ і вимогами до якості забезпечення безпеки інформації.

Складність апріорного вирішення даної задачі на стадії проектування СЗІ і ІОС в цілому обумовлена невизначеністю характеристик $H(t)$, тобто не визначенням місця, з якого здійснюються спроби НСД, оснащеності порушника (складу технічних засобів, що ним застосовуються), часу доступу до технічних або програмних засобів ІОС. Осереднення по даним характеристикам вводити неможливо, бо вони мають нестаціонарний характер. Тому, задачу синтезу управління СЗІ $U^{*}(t)$ необхідно вирішувати оперативно в масштабі реального часу. В даному випадку управління зводиться до виявлення критичних, з точки зору НСД, ситуацій, локалізації місця їх виникнення і виробленню оптимальних рішень з мінімізації можливих втрат.

Такий підхід потребує розробки формальної моделі СЗІ, яка має використовуватись як основа функціонування СППР. Як таку модель пропонується застосовувати мережну модель СЗІ, розглянуту в [4, 10].

Підвищити оперативність функціонування СППР можливо шляхом введення в модель управління елементів програмного управління (використання оперативних планів нормативного $\pi_{н}$ і оперативного $\pi_{о}$ управління): $\pi = \langle \pi_{н}, \pi_{о} \rangle$.

В загальному випадку в $n+1$-й момент часу управління визначається як

$$U_{n+1} = W(U_n, \Delta_n, R_n, \pi_n),$$

де W – оператор рекурентного управління; U_n, Δ_n, R_n – значення параметрів U, Δ, R в *n*-ий момент часу.

Оператор рекурентного управління має ієрархічну структуру і являє собою кортеж:

$$W = \langle W_{о}^{'}, W_{н}^{'}, W_{о}, W_{н}, W_{е} \rangle,$$

де $W_{о}^{'}$ – підоператор планування операцій оперативного управління СЗІ: $\pi_{о} = W_{о}^{'}(X)$; $W_{о}$ – підоператор оперативного управління СЗІ: $U_{о} = W_{о}(X, \pi_{о})$; $W_{н}^{'}$ – підоператор планування операцій нормативного управління СЗІ: $\pi_{н} = W_{н}^{'}(X, U_{о})$; $W_{н}$ – підоператор нормативного управління СЗІ: $U_{н} = W_{н}(X, \pi_{н})$; $W_{е}$ – підоператор управління характеристиками СЗІ: $\Delta = W_{е}(t)$.

На нульовому рівні здійснюється динамічна корекція характеристик СЗІ (вимог до якості захисту інформації, складу операцій з захисту інформації та ін.); на першому та другому рівнях – планування операцій оперативного і нормативного управління засобами захисту інформації, а на третьому і четвертому рівнях – реалізація цих планів. Далі функціонування СППР буде розглядатись в рамках даної моделі управління СЗІ.

Вирішення завдань з управління СЗІ ґрунтується на використанні моделі об'єкту управління, яка визначає оптимальний стан СЗІ відповідно до вимог, висунутих до неї. Необхідність представлення складних процесів захисту інформації призводить до необхідності використання специфічних засобів опису моделі СЗІ.

Одним з можливих підходів до опису моделі СЗІ є використання мереж Петрі з їх проблемно-орієнтованими розширеннями [11].

В загальному випадку позиції і переходи моделі на базі мережі Петрі задають структурні відношення між елементами СЗІ. На множині позицій задаються функції, що визначають наявність в кожній позиції відповідних властивостей захисту інформації. Крім того, існує деяке правило управління, яке задає у часі порядок зміни властивостей позицій мережі і відображає зміну поточного стану СЗІ.

Мережна модель СЗІ має описувати структуру процесів обробки інформації і конкретні алгоритми функціонування елементів ІОС і СЗІ (наприклад, процеси збору і обробки даних у вузлах мережі, протоколи встановлення з'єднань), представляти у реальному масштабі часу логіку функціонування паралельних процесів за умов здійснення нормативного управління СЗІ (наприклад, розподіл ключової інформації, процеси ідентифікації та автентифікації користувачів), надавати можливість проводити виявлення і аналіз нештатних ситуацій (спроб НСД, відмов елементів СЗІ) в ІОС, оцінку і пошук оптимальних рішень з реалізації управління і необхідному коригуванню моделі СЗІ.

Розглянемо наявність необхідних властивостей у мережній моделі СЗІ, побудованій засобами мереж Петрі.

Перша вимога задовольняється тим, що інтерпретація семантичного змісту переходу відокремлена від опису мережі. При описі процесів захисту інформації мережами Петрі може бути використаний підхід, аналогічний опису протоколів і механізмів управління доступом [12]. В цьому випадку переходи і позиції мережі зіставляються елементам СЗІ і далі задаються відображення операцій з захисту інформації на елементи СЗІ. Наприклад, нехай будь-який засіб захисту генерує і розсилає ключову інформацію, тоді процесу генерації ключів відповідає один перехід, процесу розсилки – інший, а самому засобу захисту – позиція. В результаті формується мережа, що моделює СЗІ як на рівні узагальнених операцій, так і на рівні функціонування її елементів. Позиції мережі при цьому відповідають елементам СЗІ або виділеним станам СЗІ, а переходи – операціям, що виконуються.

Друга вимога задовольняється використанням при моделюванні фактору реального часу. Прив'язка функціонування мережі Петрі до реальних часових співвідношень надає можливість отримання еталонної моделі СЗІ, можливості якої синхронізовані у часі з процесами захисту інформації.

Сформульовані вимоги дозволяють більш конкретно визначити клас мережних моделей СЗІ і перейти до опису основаних на цих моделях алгоритмів функціонування СППР і процедур управління безпекою інформації в ІОС.

Нехай m – число операцій з захисту інформації, що реалізуються СЗІ, а n – число переходів мережної моделі СЗІ. Тоді мережна модель СЗІ може бути представлена у вигляді кортежу

$$S = \langle N, O, G, f, D, K, L, V, M, M_o \rangle,$$

де N – мережа Петрі, що характеризує структуру і моделює функціонування СЗІ; O – множина операцій, що виконуються СЗІ; G – матриця можливості призначення операції з захисту інформації на переходи мережної моделі СЗІ (розмірність матриці $m \times n$); f – навантажувальне відображення, яке задає управління на мережі, причому $f = \{f_1, f_2\}$, де f_1 – умови запуску на виконання операцій, а f_2 – зміни маркувань позицій мережі після виконання операцій (відображення f_1 може бути представлене тривимірною матрицею F_1; елемент матриці $F_1[i, j, k]$ відповідає маркуванню k-ої позиції, яка задовольняє умовам збудження j-го переходу за умов призначення на нього i-ої операції; відповідно F_2 – тривимірна матриця, елементи якої відповідають маркуванням, які вміщуються у вихідні позиції переходів після їх спрацьовування за умов виконання призначеної операції); D – матриця $m \times n$ тривалості виконання операцій з захисту інформації елементами СЗІ (або часових затримок спрацьовування переходів); K – матриця $m \times n$ поточного призначення операцій з захисту інформації на елементи СЗІ; L – матриця $m \times n$, що містить інформацію про працюючі в даний момент переходи; V – матриця $m \times n$, що характеризує час, який залишився до завершення операцій на переходах; M, M_o – поточне і початкове маркування мережі.

Аналіз властивостей мережних моделей СЗІ може здійснюватись шляхом дослідження матричного представлення мережі [11], при якому аналіз здійснюється завдяки вирішенню рекурентного рівняння, яке задає динаміку мережі на базі матриць наступності і передування, а також шляхом задання початкового маркування.

Припустимо, що матриця K зафіксована для заданого моменту часу. Тоді умова збудження переходу зображується логічним рівнянням:

$$\forall p_i \in I(t_j) \exists M(p_i): \left[K(O_m, t_j) = 1 \,\&\, F_1(O_m, t_j, p_i) = M(p_i)\right] \Rightarrow U_k(t_j) = 1, \qquad (1)$$

де p_i – позиція мережі Петрі; U_k – керуючий вектор (якщо $U_{kj} = 1$, то перехід t_j є збудженим); I – множина вхідних позицій переходу t_j.

Дана умова визначає можливість активізації виконання переходу. В противному випадку $U_k(t_j) = 0$.

За умов спрацьовування переходів відбувається передача мічень відповідно до відображень f_1 з вхідних позицій у вихідні, що визначається відображенням f_2.

За аналогією з ординарними мережами Петрі динаміка мережної моделі СЗІ описується рівнянням стану мережі:

$$M_k = M_{k-1} + \left((KU_k)^T F_2 - (KU_k)^T F_1\right)U_k = M_{k-1} + (F_2 - F_1)KU_kU_k . \quad (2)$$

В даному рівнянні добуток $(KU_k)^T F_2$ характеризує переміщення міток у вихідні позиції переходів мережі, $(KU_k)^T F_1$ – переміщення міток з вхідних позицій. Добуток KU_k є керуючим вектором операцій, що виконуються (U_k – вектор-стовпець управління переходами).

Рівняння (2) описує динаміку мережної моделі СЗІ за умов відсутності часових обмежень на виконання операцій з захисту інформації. Якщо з переходами мережної моделі СЗІ зв'язати інтервали часу між моментами їх збудження і спрацювання, то можливо отримати повну мережну модель СЗІ, яка дозволяє дослідити у часі процеси, що вирішують задачі нормативного управління. При цьому, якщо терміни спрацьовування переходів однакові або кратні, то всі властивості мережної моделі залишаються незмінними, а зміна маркувань здійснюється з тактом, що дорівнює тривалості спрацьовування переходів або найменшому загальному дільнику цих тривалостей.

У випадку довільних інтервалів між тактами, зв'язаними із спрацьовуванням переходів, залишаються незмінними всі структурні властивості мережної моделі, бо введення часу позначається лише на правилах спрацьовування переходів, що задають динаміку мережі. Ці правила для часової мережі Петрі можуть бути представлені в наступному вигляді: умова збудження переходу аналогічна умові (1); умова завершення виконання переходу:

$$\forall t_i \exists O_m : \left[L(O_m, t_j) = 1 \,\&\, V(O_m, t_j) = 0\right] \Rightarrow U_k'(t_j) = 1,$$

тоді рівняння динаміки зміни маркування матиме вигляд:

$$M_k = M_{k-1} - (KU_k)^T F_1 U_k + (KU_k')^T F_2 U_k' .$$

IV Висновки

Таким чином, управління процесами забезпечення безпеки інформації в ІОС із значною кількістю одночасно працюючих абонентів і складною структурою інформаційно-логічних зв'язків базується на концепції централізації функцій управління і застосування спеціалізованих СППР. Розробка таких СППР ґрунтується на формалізації процесів забезпечення безпеки і припускає постійний збір, накопичення і обробку даних про стан ІОС з метою формування оптимальних рішень для попередження витоку конфіденційної інформації. Розглянутий в роботі підхід до формалізації процесів забезпечення безпеки інформації базується на використанні властивостей мереж Петрі і їх проблемно-орієнтованих розширень, що дозволяє вирішувати задачі як нормативного, так і оперативного управління сукупністю засобів захисту інформації в сучасних ІОС.

Література: ***1.*** *Мельников В. В. Защита информации в компьютерных системах. – М.: Финансы и статистика, 1997. – 368 с.* ***2.*** *Бриль В. М., Семенченко М. І. Основи безпеки інформаційних технологій. – К.: НТУУ "КПІ", 1999. – 107 с.* ***3.*** *Ухлинов Л. М., Мирошниченко Г. К. О формализации процессов защиты информации в вычислительных сетях // Автоматика и вычислительная техника. – 1992. – № 1. – С. 6-12.* ***4.*** *Ухлинов Л. М., Скиба В. Ю. Базовые модели системы поддержки принятия решений по управлению безопасностью (сохранностью) информации // Известия Академии наук. Теория и системы управления. – 1995. – № 1. – С. 139-148.* ***5.*** *Landwehr C. Formal models for computer security // ACM Computing surveys. – V. 13, № 3. – P. 247-278.* ***6.*** *Denning D. A lattice model of secure information flow // Communications of the ACM. – 1976. – V. 19, № 5. – P. 236-243.* ***7.*** *Landwehr C., Heitmeyer C., McLean J. A security model for military message systems // ACM Transactions on computer systems. – 1984. – V. 2, № 3. – P. 198-222.* ***8.*** *Shandhu R. The schematic protection model: it's definition and analisis for acyclie attenuating schems // Journal of the ACM. – 1988. – V. 35, № 2. – P. 404-432.* ***9.*** *Мельников В. В. Основы теории защиты информации в автоматизированных системах // Вопросы защиты информации. – 2000. – № 3. – С. 39-49.* ***10.*** *Хамула С. В. Використання мереж Петрі для створення моделей систем захисту інформації // Захист інформації. Збірник наукових праць. – вип. 5 – К.:*