DOI: 10.35681/1560-9189.2023.25.2.300525

УДК 004.5

О. В. Никифоров[1], В. Г. Путятін[2], С. А. Куценко[2]
[1]Науковий центр Повітряних Сил Харківського національного університету
Повітряних Сил ім. І. Кожедуба
вул. Сумська, 77/79, 61023 Харків, Україна
[2]Інститут проблем реєстрації інформації НАН України
вул. М. Шпака, 2, 03113 Київ, Україна

Математичні моделі та методи для вирішення деяких питань інформаційної безпеки

Наведено інструментарій моделювання щодо інформаційної безпеки, представлений такими трьома основними напрямками: розроблення методів і моделей контролю поточного стану системи та прийняття рішень з оперативного управління інформаційною безпекою; розроблення методів і моделей підтримки прийняття рішень щодо організаційного управління і проєктування систем інформаційної безпеки; розроблення методів і моделей самоорганізації системи.

Ключові слова: *алгоритм, засоби, захист інформації, інформаційна безпека, мережі, методи, моделі, нейромережі, онтологія.*

Вступ

Проблеми забезпечення інформаційної безпеки складних інформаційних систем, включаючи територіально-розподілені інформаційні комп'ютерні системи (ТРІКС), що діють у єдиному інформаційному просторі, мають багато аспектів щодо їхнього вирішення.

Особливості ТРІКС (широкий спектр програмно-апаратних засобів та інформаційних технологій, що застосовуються; функціонально-структурна складність; територіальна розподіленість компонентів тощо) зумовлюють їхню уразливість від безлічі зовнішніх і внутрішніх загроз різної природи. Порушення функціонування ТРІКС, особливо тих, які працюють у критичних галузях, призводить до виникнення високих ризиків у життєдіяльності суб'єктів та об'єктів суспільства, до зниження їхньої працездатності та інформаційної безпеки, а в деяких випадках — до зупинення діяльності або навіть руйнування об'єктів критичної інфраструктури. Побудова ефективної системи інформаційної безпеки є обов'язковою умовою для зниження ризику реалізації подібних негативних сценаріїв.

Актуальність дослідження визначається тим, що існує велике різноманіття методів і математичних моделей, які застосовуються при моделюванні та побудові

систем захисту. Це призводить до того, що при формулюванні початкової задачі конкретного наукового дослідження за проблематикою інформаційної безпеки має місце велика невизначеність стосовно вибору доцільних методів та ефективних математичних моделей.

Мета статті

Метою статті є аналіз актуальної проблематики наукових досліджень стосовно забезпечення інформаційної безпеки ТРІКС та огляд основних методів і математичних моделей, які придатні для вирішення наукових задач у цій сфері.

У статті представлено напрямки застосування, можливості, переваги та недоліки основних методів і моделей, а також інструментальні засоби для їхньої реалізації, у тому числі засоби моделювання загроз, що має допомогти науковцям і розробникам визначитись, який саме підхід доцільно використовувати при моделюванні та побудові ефективної системи інформаційної безпеки для захисту систем, подібних до ТРІКС, від негативних впливів.

1. Актуальні напрямки наукових досліджень при вирішенні проблеми інформаційної безпеки та методи і моделі, що їх забезпечують

Для вирішення проблем захисту ТРІКС від негативних впливів, моделювання та побудови системи інформаційної безпеки можна виділити такі актуальні напрями та завдання наукових досліджень (рис. 1):

1) *розроблення методів і моделей контролю поточного стану системи і прийняття рішень з оперативного управління інформаційною безпекою:*

а) формування динамічних зон і порогів, що характеризують різні стани ТРІКС (динамічні вектори індикації);

б) розроблення ідеології і стратегії виконання адаптивного контролю векторів індикації, прогнозування тенденцій зміни їхніх значень;

в) розроблення методів та алгоритмів адаптивного одиночного та групового контролю та прогнозування значень компонентів векторів індикації;

г) розроблення методів та алгоритмів розпізнавання та ідентифікації приналежності станів системи динамічним зонам і порогам на підставі аналізу поточних і прогнозованих значень окремих компонентів і векторів індикації у цілому;

д) розроблення методів та алгоритмів діагностування систем на основі аналізу результатів ідентифікації за всіма векторами індикації;

2) *розроблення методів і моделей підтримки прийняття рішень щодо організаційного управління і проєктування систем інформаційної безпеки:*

а) вибір рішень із множини альтернатив на підставі аналізу стану та поведінки системи та з урахуванням вимог управління, ресурсних обмежень, квантифікованих оцінок близьких і віддалених наслідків прийнятих рішень;

б) декомпозиція (деталізація) прийнятих рішень відповідно до ієрархічного рівня управління системи;

в) підтримка прийняття рішень щодо самоорганізації системи в процесі її функціонування;

3) *розроблення принципів, методів і засобів самоорганізації:*

а) розроблення адаптивних моделей для опису структури та поведінки системи, прогнозування значень її параметрів;

б) розроблення адаптивних моделей для формування підмножини контрольованих параметрів і зон їхнього контролю залежно від вимог до стійкості функціонування системи;

в) розроблення адаптивних моделей для контролю працездатності та діагностування порушень працездатності;

г) розроблення методів і засобів самоорганізації та саморозвитку сімейств моделей для опису структури, поведінки, прогнозування, контролю та діагностування з урахуванням забезпечення заданої стійкості в умовах впливу зовнішнього середовища.

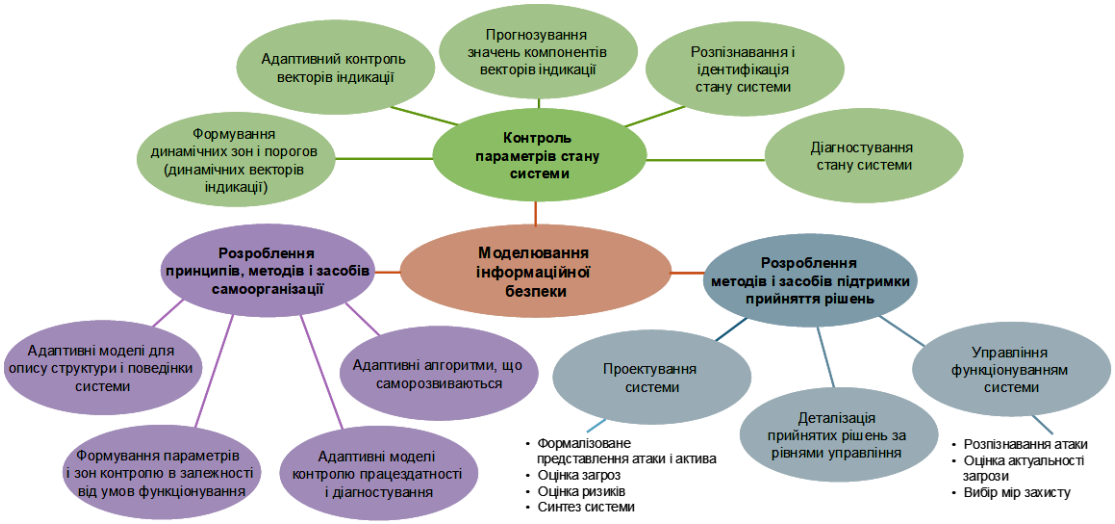

Рис. 1. Основні напрямки та групи актуальних наукових завдань при вирішенні проблем інформаційної безпеки ТРІКС

Для вирішення наукових завдань за зазначеними напрямками використовуються різноманітні математичні моделі та підходи.

Так, за напрямом контролю параметрів стану системи широко представлені методи data mining (регресійний і кореляційний аналіз, аналіз часових рядів) [1, 2].

Для груп завдань формування динамічних зон критеріїв управління безпекою, адаптивного контролю та прогнозування стану можуть бути застосовані:

— методи концептуального проєктування [3, 4];

— мережі Петрі [5-7];

— когнітивні карти, кінцеві автомати [8];

— моделі теорії ігор [9, 10];

— марковські ланцюги, байєсовські графи [11; 12].

Для групи завдань розпізнавання, ідентифікації станів і діагностики систем використовуються:

— онтологічне моделювання та логічний висновок [13];

— розпізнавання багатопараметричних об’єктів і виведення експертних правил [14];

— нейромережі [15, 16].

Для вирішення завдань розробки методів і засобів підтримки прийняття рішень (проєктування систем; деталізація (розгортання) прийнятих рішень; управління процесом функціонування систем захисту інформації) застосовуються:

— функціональне моделювання [17];

— динамічне моделювання [18], розфарбовані мережі Петрі;

— об'єктно-орієнтовані методи та моделі аналізу ризиків і загроз: STRIDE-моделі (Spoofing, Tampering, Repudiation, Information disclosure (privacy breach or data leak), Denial of service, Elevation of privilege) [19–23];

— методологія PASTA (Process for Attack Simulation and Threat Analysis) [24, 25];

— методологія LINDDUN (Linkability, Identifiability, Non Repudiation, Detectability, Disclosure of Information, Unawareness, Non-Compliance) [26, 27];

— система оцінки CVSS (Common Vulnerability Scoring System) [28–30];

— метод моделювання Attack trees [31, 32];

— метод моделювання Persona non Grata [33];

— метод моделювання hTMM [34];

— методологія Quantitative TMM (Threat Modeling Method) [35];

— система оцінки OCTAVE [36];

— методологія Trike [37];

— методологія VAST modeling [38];

— методи моделювання Security Cards [39, 40];

— методи розподілення обмежених ресурсів [41];

— моделі розмежування доступу [42-44];

— розпізнавання багатопараметричних об'єктів і виведення експертних правил [45];

— нейромережі;

— онтологічне моделювання [46];

— матрична модель безпеки [47, 48].

Для групи завдань щодо вирішення проблеми самоорганізації (адаптивні моделі опису поведінки та структури; адаптація зон контролю (критеріїв безпеки); адаптація моделі діагностики; адаптація або саморозвиток алгоритмів), крім онтологічних і матричних моделей безпеки також можуть бути застосовані методи тензорного перетворення мереж [49].

2. Стисла характеристика математичних моделей і методів, що застосовуються для забезпечення інформаційної безпеки

2.1. Нейромережеві моделі

Нейромережеві моделі [50], які спочатку застосовувалися для моделювання процесів розпізнавання графічних зображень, на цей час знайшли широке використання і в галузі розпізнавання багатопараметричних об'єктів, а також регулювання параметрів роботи складних систем. Таке їхнє застосування є ефективним стосовно вирішення задач управління інформаційною безпекою. За допомогою нейромереж успішно вирішуються завдання класифікації загроз, вибору параметрів заходів захисту, регулювання режимів роботи інформаційних систем.

Штучні нейронні мережі відрізняються за методами налаштувань (навчання) і за формою структури. На цей час відомі такі методи налаштувань нейромереж:

1) з учителем:

— метод зворотного розповсюдження помилки (ЗРП);

— генетичний алгоритм (ГА);

2) без учителя:

— ітеративний алгоритм Уідроу-Хоффа з мінливим кроком;

— модифікований метод найменших квадратів (ММНК);

— метод послідовного навчання.

Метод зворотного розповсюдження помилки (ЗРП)

Процес навчання за допомогою методу ЗРП передбачає виконання таких дій: визначення чергової навчаючої пари з навчальної вибірки та подання її на вхід нейромережі; обчислення виходу мережі; обчислення помилки; корегування вагових коефіцієнтів мережі так, щоб мінімізувати помилку; повторення попередніх кроків до тих пір, доки помилка на всій навчальній множині не досягне придатного значення.

Корегування вагових коефіцієнтів мережі здійснюється пропорційно значенню помилки відклику. Для цього спочатку визначається помилка вихідного нейрону

$$\delta_j = \Delta_j \cdot F'(S_j) = (t_j - S_j) \cdot \left[S_j \ (1 - S_j) \right], \tag{1}$$

де δ_j — помилка *j*-го нейрону, що належить вихідному шару нейромережі; t_j — значення вихідної функції в *j*-му нейроні (термі) згідно навчальної вибірки; S_j — значення вихідної функції відповідного нейрону, яке сформовано мережею при визначених вагових коефіцієнтах; $F'(S_j)$ — похідна сигмоїдальної порогової функції нейрону, що запропонована Мамдані.

Потім, зворотним ходом, визначаються помилки для нейронів внутрішніх шарів і вхідного шару:

$$\delta_k = \left[S_k (1 - S_k) \right] \cdot \delta_j w_{k,j}, \tag{2}$$

де δ_k — помилка *k*-го нейрону, що утворює підмножину нейронів, виходи яких є входами для *j*-го нейрону; $w_{k,j}$ — ваговий коефіцієнт, встановлений для зв'язку *k*-го нейрону з *j*-м нейроном.

Значення поправок для вагових коефіцієнтів обчислюються як

$$\Delta w_{i,k} = \eta \cdot \delta_i S_k, \tag{3}$$

де η — коефіцієнт швидкості навчання ($\eta = 0{,}01 \div 1$).

Існують комерційні програмні продукти для налаштування нейромереж за допомогою методу ЗРП [51].

Генетичні алгоритми (ГА)

В основу генетичних алгоритмів покладено механізм природного відбору (еволюції) [52]. Ітерації процесу пошуку рішення здійснюються шляхом відтворення зі старої популяції альтернатив нової популяції з подальшим відбором перс-

пективних альтернатив. Частоти вибору альтернатив залежать від їхніх властивостей (ступеня пристосованості особи).

При підборі вагових коефіцієнтів нейронних мереж за допомогою ГА знаходиться початкове рішення (первинне значення вектора вагових коефіцієнтів), яке досить близьке до оптимального. Існує комерційний програмний продукт Evolver [53], який реалізує початкову оптимізацію вагових коефіцієнтів за допомогою ГА. Далі відбувається поліпшення коефіцієнтів за допомогою методу ЗРП.

Ітеративний алгоритм Уідроу-Хоффа з мінливим кроком

Уідроу і Хофф модифікували персептронний алгоритм Ф. Розенблатта, додатково увівши сигмоїдальну функцію активації.

Процедура Уідроу-Хоффа розроблена для «чорної скриньки», в якій між входами та виходами існують лише прямі зв'язки. Процедура навчання для нейромережі із кількома вихідними нейронами складається з двох фаз, що чергуються. У першій фазі на входах задається вхідний вектор, а на виходах — необхідний вихідний вектор. Потім усі вагові коефіцієнти мережі збільшуються на малу величину δ. У другій фазі на вході формується той самий вхідний вектор, але вихід розраховується нейронною мережею. При цьому потрібно дотримуватися такого правила: вихід активізується лише тоді, коли сума ваги його зв'язків з активними входами є позитивною. Після цього вагові коефіцієнти мережі зменшуються на величину δ. Якщо мережа виробила правильний вихідний вектор, то ці зменшення ваг точно компенсують їхнє збільшення, вироблені в першій фазі. Якщо мережа виробила вихідний вектор не такий, який потрібен, то зміна коефіцієнтів, що визначені у першій фазі, зберігається.

Для управління процесом покрокового змінення значень вагових коефіцієнтів нейромережі використовуються процедури покоординатного або градієнтного спуску, для знаходження безумовного екстремуму функції $\varepsilon^2(w_1,...,w_n)$, де $\varepsilon = d - r$, d, r — бажаний та обчислений за допомогою мережі вихідний сигнал:

$$\frac{d\left(\varepsilon^2\right)}{d\mathbf{W}} = 0, \tag{4}$$

де $\mathbf{W} = \{w_1,...,w_n\}$.

Перевагою алгоритму Уідроу-Хоффа є відсутність обмеження на вигляд функції належності (терму) та її розташування у нормованому інтервалі, а недоліком — недостатня швидкодія.

Модифікований метод найменших квадратів (ММНК)

ММНК [55] дозволяє підвищити швидкодію алгоритму Уідроу-Хоффа за рахунок обчислення вагових коефіцієнтів за одну ітерацію за умови лінійних термножин фазифікатора лінгвістичної змінної.

Головна відмінність ММНК полягає в тому, що замість використання ітераційної процедури покоординатного або градієнтного спуску використовується процедура одноразового розв'язання алгебраїчної системи рівнянь:

$$\frac{\partial\left(\varepsilon_k{}^2\right)}{\partial w_{i,k}} = 2\left(\sum_{j=1}^{n} w_{j,k}x_j - d_k\right) = 0, \quad i,k = 1,...,n, \tag{5}$$

де ε_k — помилка по виходу k-го нейрона; n — кількість нейронів нейромережі; d_k — встановлений вихід для k-го нейрону; $w_{j,k}$ — вагові коефіцієнти зв'язків нейромережі.

Матриця вагових коефіцієнтів є квадратною, з розмірністю $n \times n$. Для відсутніх зв'язків відповідні синаптичні сигнали x_j набувають нульових значень.

ММНК застосовується лише для лінійних терм, піддіапазони яких рівні та рівномірно розташовані в нормованому інтервалі. Число терм терм-множини фазифікатора завжди повинно дорівнювати числу підінтервалів розбиття нормованого інтервалу. У разі, коли відбувається регулювання терм, ММНК не застосовується.

Метод послідовного навчання

Метод адаптації з послідовним навчанням [56, 57] належить до методів послідовної ідентифікації лінійних систем у реальному часі, який заснований на принципі навчання з моделлю і в якому отримана модель імпульсної характеристики. Цей метод має збіжність трохи нижче, ніж ММНК. Його зручно застосовувати для процесів з параметрами, що повільно змінюються. Основна перевага методу послідовного навчання полягає у простоті алгоритму адаптації.

У методі послідовного навчання розглядається лінійна система з випадковим входом $x(t)$, виходом $S(t)$ і імпульсною характеристикою $g(t)$. Зв'язок між входом і виходом описується інтегралом згортки:

$$S(t) = \int_0^t g(\tau) \cdot x(t-\tau) d\tau , \tag{6}$$

де $x(t-\tau)$ — вимірювана величина.

У дискретній формі інтеграл згортки має вигляд

$$S_j = \sum_{i=1}^{n} g_i x_{j-i} . \tag{7}$$

Визначення імпульсної реакції g_i виконується шляхом ітераційних обчислень векторів $\phi_1^{(j)},...,\phi_n^{(j)}$, $\forall j = n+1, n+2,...$, які мають, відповідно, наближатися до $g_1,...,g_n$ у (7), де j позначає номер ітерації. Тоді оцінка виходу моделі (нейрона) S_j^{M} при використанні $\phi_i^{(j)}$ дорівнює за аналогією з (7):

$$S_j^{\mathrm{M}} = \sum_{i=1}^{n} \phi_i^{(j)} x_{j-i} , \tag{8}$$

де n — кількість входів (синаптичних зв'язків) нейрона.

Увівши позначення:

$$\mathbf{g} = [g_1,...,g_i,...,g_n]^{\mathrm{T}} ,$$
$$\boldsymbol{\varphi}_j = \left[\phi_1^{(j)},...,\phi_i^{(j)},...,\phi_n^{(j)}\right]^{\mathrm{T}} ,$$
$$\mathbf{x}_j = [x_{j-1},...,x_{j-i},...,x_{j-n}]^{\mathrm{T}} ,$$

(7) і (8) можуть бути записані як

$$S_j = \mathbf{g}^{\mathrm{T}}\mathbf{x}_j, \tag{9}$$

$$S_j^{\mathrm{M}} = \boldsymbol{\varphi}_j^{\mathrm{T}}\mathbf{x}_j. \tag{10}$$

Помилка виходу моделі (нейрона) набуде вигляду

$$S_j - S_j^{\mathrm{M}} = \left(\mathbf{g} - \boldsymbol{\varphi}_j\right)^{\mathrm{T}}\mathbf{x}_j = \mathbf{x}_j^{\mathrm{T}}\left(\mathbf{g} - \boldsymbol{\varphi}_j\right) = \mathbf{x}_j^{\mathrm{T}}\Delta\boldsymbol{\varphi}_j, \tag{11}$$

де $\Delta\boldsymbol{\varphi}_j = \boldsymbol{\varphi}_{j+1} - \boldsymbol{\varphi}_j$ — корекція вектора $\boldsymbol{\varphi}_j$ і його наступної ідентифікації $\boldsymbol{\varphi}_{j+1}$ з урахуванням помилки $\left(S_j - S_j^{\mathrm{M}}\right)$.

Якщо припустити, що

$$\Delta\boldsymbol{\varphi}_j = \left(S_j - S_j^{\mathrm{M}}\right)\frac{\mathbf{x}_j}{\mathbf{x}_j^{\mathrm{T}}\mathbf{x}_j}, \tag{12}$$

то рекурентне співвідношення для обчислення оцінок вагових коефіцієнтів набуде вигляду:

$$\boldsymbol{\varphi}_{j+1} = \boldsymbol{\varphi}_j + \left(S_j - S_j^{\mathrm{M}}\right)\frac{\mathbf{x}_j}{\mathbf{x}_j^{\mathrm{T}}\mathbf{x}_j}, \quad S_1^{\mathrm{M}} = 0. \tag{13}$$

З коефіцієнтом корекції помилки рекурентне співвідношення запишеться як

$$\boldsymbol{\varphi}_{j+1} = \boldsymbol{\varphi}_j + C\left(S_j - S_j^{\mathrm{M}}\right)\frac{\mathbf{x}_j}{\mathbf{x}_j^{\mathrm{T}}\mathbf{x}_j}, \quad 0 \prec C \prec 2. \tag{14}$$

Метод адаптації з послідовним навчанням має високу збіжність (достатньо двох, трьох ітерацій). При цьому він може використовуватись як при лінійних, так і при нелінійних термах нейронів.

Щодо структури нейромереж, які застосовуються для розв'язання задач безпеки інформації, то найбільш розповсюдженими є нейромережі класифікації. Такі мережі мають багатошарову довільну структуру, яка визначається структурою онтологічної мережі області, що розглядається [58]. Найбільш часто для класифікації використовується архітектура нейромережі прямого поширення, на вхідні нейрони яких подаються значення ознак об'єкта, що класифікується, а на виході формується мітка або числовий код класу. Зазвичай використовуються багатошарові персептрони. У таких мережах елементи вектора ознак надходять на вхідні нейрони та розподіляються на всі нейрони першого прихованого шару штучної нейронної мережі. Структура мережі, яка найкраще апроксимує функцію поділу класів у просторі ознак, наперед невідома. Тому доводиться підбирати її експериментально або використовувати досвід попередніх рішень за аналогією.

2.2. Когнітивні карти

Когнітивна карта — це суб'єктивна картина, яка має, перш за все, просторові координати та в якій локалізовані окремі предмети, що сприймаються. Виділяють

когнітивну карту-шлях, як послідовне представлення зв'язків між об'єктами за визначеним маршрутом, і карту-огляд, як одночасне представлення просторового розташування об'єктів.

Когнітивна карта виглядає як орієнтований граф, ребра якого мають вагу. Різні інтерпретації вершин графа, його ребер і їхні ваги, а також різні функції, що визначають вплив зв'язків на фактори, призводять до різних когнітивних моделей та методів їхнього аналізу.

Історично першою когнітивною моделлю (картою) був знаковий граф Акселърода [59, 60]. Це граф, ребра якого мають вагу «+1» або «–1», скорочено: «+» або «–». Залежно від характеру впливів вершин (факторів) графа, він може бути неорієнтованим (має місце симетричний взаємний вплив) та орієнтованим (має місце вплив казуального типу: «причина – наслідок»).

Приклад знакового орієнтованого графа (орграфа) (когнітивної карти), що використовується для аналізу проблеми забезпечення інформаційної безпеки, наведено на рис. 2.

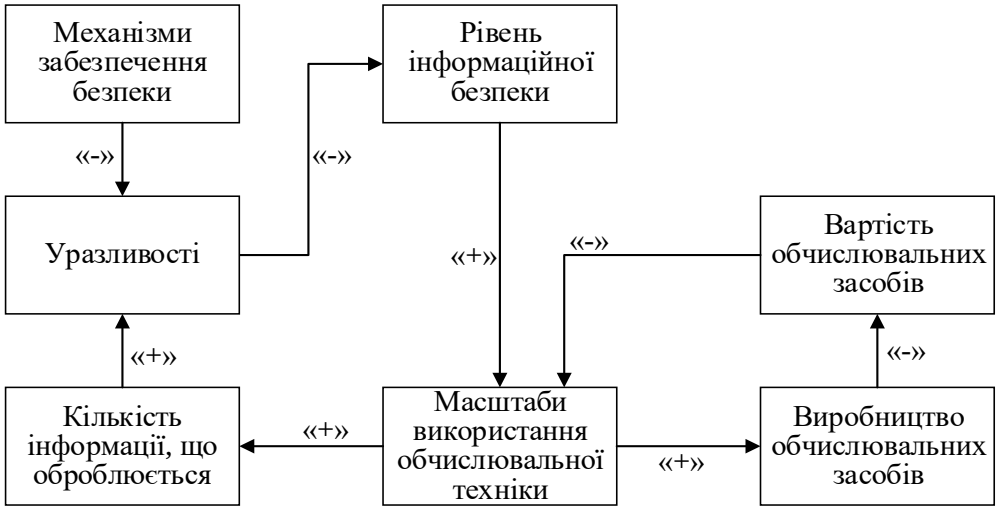

Рис. 2. Приклад когнітивної карти у вигляді знакового орграфа

Знак «+» позначає позитивний зв'язок, знак «–» — негативний. Вага шляху дорівнює добутку ваги ребер, які цей шлях утворюють. Тобто шлях має позитивний вплив, якщо кількість негативних ребер є парною, і негативний вплив, якщо кількість таких ребер є непарною. Позитивний зв'язок, при зростанні фактора-причини, призводить до зростання фактора-наслідку. Негативний зв'язок — до зменшення фактора-наслідку. Якщо між двома вершинами орграфа існує кілька шляхів впливу, які мають різні знаки, тоді питання про характер впливу одного фактора на інший залишається невизначеним.

Іншим видом когнітивних карт є нечіткі когнітивні карти (НКК) [61, 62]. Це такі карти, в яких, як і в знаковому графі, вершини представляють фактори (концепти), а ребра — зв'язки між факторами, що інтерпретуються як причинно-наслідкові (казуальні) зв'язки. Вага ребер — це або числа, задані на інтервалі [–1; 1], або лінгвістичні мінливі, що задані на впорядкованій шкалі, які характеризують силу

впливу фактора-причини та фактора-наслідку. Для аналізу НКК застосовується апарат нечіткої математики.

Суттєвим узагальненням НКК є когнітивна карта з нечіткими правилами (RBFCM — Rule Based Fuzzy Cognitive Maps) [63]. Нечіткі правила (продукції) мають форму речень виду: «Якщо, то», умовна частина яких представляє вираз нечіткої логіки над лінгвістичними значеннями факторів і відношеннями між ними. Наприклад: «Якщо $x_1 \in A_1$ і $x_2 \in A_2$ … , то $y \in B$ …», де x_1 , x_2 — вхідні мінливі, y — вихідна мінлива, A_1, A_2, B — нечіткі (лінгвістичні) значення. Посилання правила описує умови його застосування, а заключення правила — визначає функції належності лінгвістичних значень вихідним мінливим. Ребра графа відповідні відношенням впливу, які виражено за допомогою умовних частин правил. Кожному фактору ставиться у відповідність база правил, що складається з усіх продукцій, де є у заключенні цей фактор. На рис. 3 наведено приклад структури RBFCM.

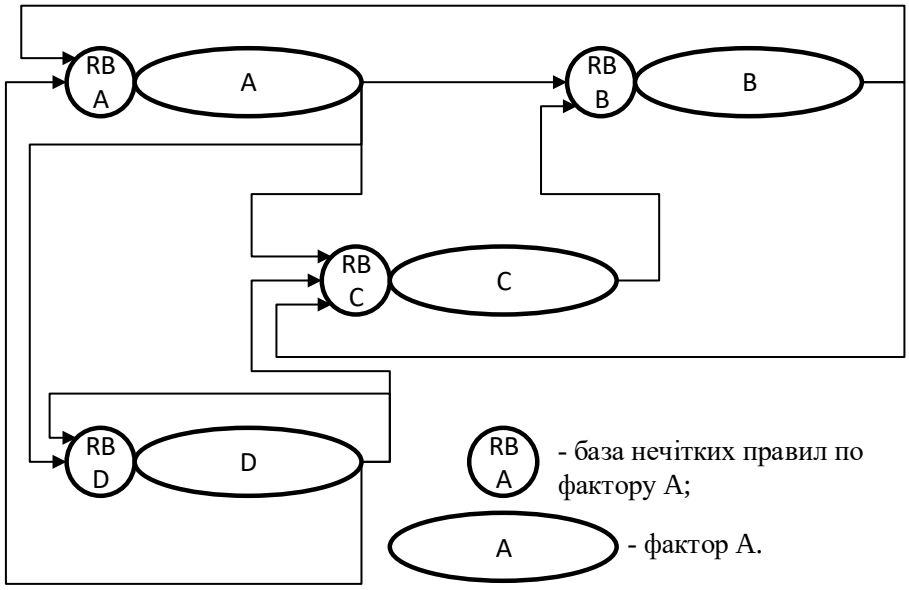

Рис. 3. Приклад структури RBFCM

Наукові задачі, які розв’язуються за допомогою математичних моделей когнітивних карт, є наступними:

1) статичний аналіз, а саме:

— задача оцінки сталості ситуації (системи);

— задача синтезу структури відношень (системи) за критерієм досягнення необхідного рівня сталості;

2) динамічний аналіз, а саме:

— задача прогнозування розвитку ситуації (пряма задача);

— задача оптимізації управлінських впливів, які забезпечують потрібну динаміку розвитку ситуації (зворотна задача).

Для розв’язання задач статичного аналізу досить ефективно застосовуються знакові когнітивні карти. При цьому невизначеності щодо оцінки характеру впливу на фактор, коли має місце кілька зв’язків з різними знаками, усуваються за рахунок

визначення величини сили впливу, яка залежна від довжини шляху відповідного зв'язку.

Для розв'язання задач динамічного аналізу більш придатні НКК і RBFCM. Це обумовлено тим, що при здійсненні динамічного аналізу потрібно оперувати не тільки характеристиками сили впливу казуальних зв'язків факторів, але й динамічними оцінками значень самих факторів.

Рішення прямої задачі має враховувати два суттєвих моменти.

По-перше, інтервали часу, якими оперують, є нечіткими, оскільки час реалізації впливу одних факторів на інші точно невідомий. Моменти часу $t+i$ розуміються не як точки на абсолютній шкалі часу, а як впорядковані за часом послідовні кроки прогнозу. При цьому цільовий стан $\mathbf{X}_{t+n}$ не обчислюється за ітеративною формулою

$$\mathbf{X}_{t+i} = \mathbf{X}_{t+i-1} + \mathbf{P}_{t+i}, \quad i = 1,...,n, \tag{14}$$

а є результатом узагальненої якісної оцінки всього процесу розвитку ситуації, що прогнозується від t до $t+n$. Шлях, яким система прийшла у поточний стан, є важливим.

По-друге, при обчисленні приростів і станів ситуації треба визначати не тільки наступне значення приросту, але й ступінь упевненості його вибору (консонанс). Тому при виборі позитивного (або негативного) приросту треба зберігати також відхилений негативний (або позитивний) приріст.

При розв'язанні зворотної задачі аналізуються шляхи розповсюдження впливів різної довжини. Для цього використовується нечітке транзитивне замикання $\mathbf{W}' = \{w'_{ij}\}$ матриці суміжності $\mathbf{W}$:

$$\mathbf{W}' = \{w'_{ij}\} : w'_{ij} = [w_{ij}, (w_{ij})_2, ..., (w_{ij})_n], \tag{15}$$

де $(w_{ij})_k = (w_{im} * (w_{mj})_{k-1})$. Символом * позначена операція оцінки приросту сили впливу при додаванні до шляху казуальних зв'язків когнітивної карти наступ-ного зв'язку w_{ij}.

Формалізованою постановкою зворотної задачі є рішення нечіткого реляційного рівняння:

$$\mathbf{U} \cdot \mathbf{W}' = \mathbf{G} \tag{16}$$

відносно вектора вхідних впливів $\mathbf{U}$, якщо визначені причинно-наслідкові зв'язки між факторами за допомогою матриці транзитивного замикання та заданий вектор потрібних значень факторів ситуації $\mathbf{G} = (g_1, g_2, ..., g_n)$.

Методи рішення рівняння (16) описано в [64].

Головною перевагою апарату когнітивних карт при проведенні досліджень і галузі інформаційної безпеки є можливість систематичного якісного (у сенсі — некількісного) врахування віддалених наслідків рішень, що приймаються, та виявлення побічних ефектів, які можуть перешкодити реалізації, здавалося би, очевидних рішень і які важко оцінити інтуїтивно при великій кількості факторів і різноманітності багаточисельних шляхів взаємодії між ними. В той же час слід пам'ятати, що результати аналізу, які, як правило, формуються в термінах лінгвіс-

тичних шкал, є достатньо приблизними в силу малої точності самих шкал. Вони відображають основні тенденції впливів, але виявляються ненадійними, наприклад, у разі приблизної рівності позитивних і негативних впливів. Індикатором такої ненадійності служать малі значення консонансів, що визначаються.

2.3. Кінцеві автомати (КА)

Кінцевий автомат (теорія алгоритмів) —– це математична абстракція, модель дискретного засобу, який має один вхід, один вихід і в кожний момент часу знаходиться в одному стані із множини можливих своїх станів. КА є частковим випадком абстрактного дискретного автомату, число можливих внутрішніх станів якого є кінцевим [65].

На вхід КА послідовно надходять вхідні впливи, на виході КА формуються вихідні сигнали. Вхідні та вихідні сигналі описуються вхідним і вихідним алфавітами, які, в загальному випадку, не перетинаються.

Відрізняють детерміновані і недетерміновані КА. Для детермінованих КА наступний стан однозначно визначається його поточним станом. З будь якого стану можливий перехід тільки в один стан. Для недетермінованих КА перехід в наступні стани відбувається з деякими ймовірностями. Можуть існувати мимовільні переходи з одного стану в інший без зовнішніх впливів, або КА може переходити в різні стани під впливом одного і того ж вхідного сигналу. Недетермінований КА є узагальненням детермінованого.

Процес функціонування КА описується діаграмою станів (графом переходів), яка подається як графічне представлення множини станів і функцій переходів у формі розміченого орієнтованого графа. Вершини графа відповідні станам КА, дуги — переходам між станами, а мітки дуг — правилам (способам), за якими здійснюються переходи.

За допомогою КА будуються моделі систем паралельної обробки інформації. Однак, щоб змінити число паралельних процесів, потрібні суттєві зміни. Крім того, спроба розробки складної моделі, що буде адекватною реальним процесам, призводить до швидкого зростання її розмірності (кількості станів КА) та обчислювальної складності. Деяке розв'язання цієї проблеми вдається отримати за допомогою використання моделі недетермінованого КА.

У термінах теорії КА може бути описана будь-яка система автоматичного або автоматизованого управління. Більшою мірою КА застосовуються для розв'язання задач проєктування систем управління інформаційною безпекою, формування регулярних множин навчальних вибірок, налаштування параметрів процесів навчання засобів класифікації і формування управлінських впливів у системах захисту інформації.

Існує спеціалізована графічна мова програмування SFC (Sequential Function Chart), яка використовується для програмування промислових логічних контролерів на основі моделей детермінованих і недетермінованих КА.

2.4. Мережі Петрі

Мережі Петрі [66] запропоновані як інструмент для опису асинхронних взаємодій у процесах і структурах з точками синхронізації і розгалуження. Графічна

схема, яка була запропонована Карлом Петрі, є подібною до схеми, що існує в системі моделювання GPSS у вигляді елементів розгалуження процесів Fork (вилка) та їхнього злиття Join.

Структура мережі Петрі подається у вигляді орієнтованого дводольного графа (біграфа). Множину вершин V дводольного графа розбивають на дві підмножини (частки), що не перетинаються: T і P, такі, що $V = T \cup P$, $T \cap P = \varnothing$. Вершини з T і P з'єднані між собою орієнтованими ребрами (дугами). В силу того, що з'єднання вершин у мережі має вигляд: $P \to T$ або $T \to P$, усі прості цикли біграфа мають парну довжину. Для моделювання процесів до графа вводяться динамічні елементи — мітки (марки). Розподіл марок за вершинами мережі називають її маркуванням.

Отже мережа Петрі — це наступна п'ятірка:

$$N = \{T, P, I, O, Mo\}, \tag{17}$$

де $P = \{p_i\}$, $i = 1,...,n$ — множина позицій (станів процесу); $T = \{t_j\}$, $j = 1,...,m$ — множина переходів між позиціями (станами); $I : T \times P \to \{0,1\}$ — функція слідування; $O : P \times T \to \{0,1\}$ — функція попереджування; $Mo : P \to Zo$ — початкове маркування, що визначає розподіл міток за позиціями мережі (станами процесу); Zo — множина натуральних чисел.

Маркування мережі подається як вектор

$$\mathbf{M} = |k(p_i)|, \tag{18}$$

де $k(p_i)$ — кількість міток в позиції p_i.

Перехід t_j з множини T збуджується маркуванням $\mathbf{M}$ і відбувається за умови, коли всі вхідні позиції переходу t_j мають мітки:

$$\forall p_i \in P\left[k(p_i) - O(p_i, t_j) \geq 0\right], \tag{19}$$

де $O(p_i, t_j)$ — кількість дуг (ребер) між p_i та t_j.

Спрацьовування переходу t_j призводить до того, що його позиції-попередники втрачають, а кожна з позицій-спадкоємців отримує по одній мітці.

Якщо в мережі задано початкове маркування, при якому хоча б один перехід виявляється збудженим, то у ній починається рух міток. Якщо в мережі одночасно виявляються збудженими кілька переходів, то порядок їхнього спрацьовування є не визначеним, тому може бути представлено кілька послідовностей спрацьовування переходів *t*.

Мовою мережі $L(N)$ зветься множина всіх кінцевих послідовностей переходів, що спрацьовують при заданому початковому маркуванні. Мова $L(N)$ представляє множину всіх можливих послідовностей дій, які виконуються паралельними процесами.

Для розширення сфери застосування мереж Петрі існують наступні розширення класичної моделі Петрі.

Часова мережа Петрі

Дозволяє більш адекватно моделювати процеси з їхньою розміткою за часом. Кожному переходу у відповідність ставиться час (тривалість) τ_j. Якщо перехід збуджується, то мітки, які обумовлюють запуск переходу, покидають вхідні позиції. У наступних (вихідних) позиціях мітки з'являються через час τ_j.

Формальне визначення часової мережі:

$$\mathrm{TN} = \{\mathrm{N}, \tau\}, \tag{20}$$

де N — класична мережа Петрі; $\tau : \mathrm{T} \to \mathrm{Ro}$ — функція часу спрацьовування переходів; Ro — множина позитивних раціональних чисел.

Мережа з пріоритетами переходів

Формальне визначення:

$$\mathrm{PRN} = \{\mathrm{N}, \mathrm{PR}\}, \tag{21}$$

де PR — відношення пріоритетності (порядку), що визначаються на множині переходів T.

Часова мережа з пріоритетами переходів

Поєднує (20) і (21).

Формальне визначення:

$$\mathrm{PRTN} = \{\mathrm{N}, \tau, \mathrm{PR}\}. \tag{22}$$

Розфарбована мережа Петрі

Моделі у формі розфарбованої мережі Петрі є природною інтерпретацією різноманітних реальних процесів і систем. За рівнем наочності вони відповідають багатокласним мережам з чергами без синхронізації-розмноження.

Міткам розфарбованої мережі привласнюють атрибути, які називають кольорами. Правила збудження переходів доповнюються умовами, які передба-чають вибір мітки за її кольором. Спрацьовування переходів супроводжується пересиланням в наступні (вихідні) позиції міток, для яких задаються (міняються) значення кольору.

Формалізоване визначення розфарбованої мережі Петрі:

$$\mathrm{CN} = \{\mathrm{N}, \mathrm{C}\}, \tag{23}$$

де $\mathrm{C} : \mathrm{T} \to \mathrm{Cl}$ — функція розфарбування, яка визначена на множині переходів; $\mathrm{Cl} = \{c_1, c_2, ..., c_j, ..., c_m\}$ — значення ознак кольору для визначених переходів з множини T.

Пріоритетна розфарбована мережа Петрі

У розфарбованих мережах можна задавати пріоритетність обслуговування або захвату ресурсу для міток, які представляють потоки процесів. Для цього визначають відношення пріоритетності на множинах кольорів і переходів. Правила збудження переходу t_j реалізують пріоритетний вибір мітки за її кольором.

Формалізоване визначення мережі:

$$\mathrm{PRCN} = \{\mathrm{N}, \mathrm{C}, \mathrm{PR}\}, \tag{24}$$

де PR — відношення пріоритетності (порядку), що визначаються на множині $T \times Cl$.

Галузі застосування мереж Петрі включають дослідження телекомунікаційних мереж, мережевих протоколів, обчислювальних систем і обчислювальних процесів, виробничих і організаційних систем, проблем безпеки інформації. Мережі Петрі являють собою універсальний засіб формального опису поведінки дискретно-подійних систем.

Існують такі комерційні програмні продукти для створення імітаційних моделей динамічних процесів на основі застосування мереж Петрі [67]:

— ALPHA/Sim. Розфарбовані та часові мережі Петрі. Компоненти: графічний редактор; швидка імітація без графіки; аналіз продуктивності; імітація з анімацією;

— Cosmos (безкоштовно). Класична мережа Петрі. Компоненти: експорт/імпорт моделей із забезпеченням інтеграції з іншими засобами; швидка імітація без візуалізації;

— CPN-AMI (безкоштовно). Класична мережа Петрі. Компоненти: графічний редактор; анімація; швидка імітація; простори станів; інваріанти позицій; інваріанти переходів; структурний аналіз; експорт/імпорт моделей;

— CPN Tools (безкоштовно). Часова та класична мережі Петрі. Компоненти: графічний редактор; анімація; швидка імітація; простори станів; аналіз продуктивності; експорт/імпорт моделей;

— FLOWer. Класична мережа Петрі. Компоненти: графічний редактор; система управління робочими процесами; швидке прототипування;

— Fluid Survival Tool (безкоштовно). Класична мережа Петрі. Компоненти: простий аналіз продуктивності; вдосконалений аналіз продуктивності;

— GDLoolkit. Класична, часова, розфарбована та пріоритетна мережі Петрі. Компоненти: автоматичне розміщення елементів;

— Helena (безкоштовно). Класична, часова, розфарбована та пріоритетна мережі Петрі. Компоненти: простори станів; скорочення/стиснення моделей;

— INA (безкоштовно). Класична, часова, розфарбована та пріоритетна мережі Петрі. Компоненти: простори станів; інваріанти позицій; інваріанти переходів; скорочення/стиснення моделей; структурний аналіз; простий аналіз продуктивності; вдосконалений аналіз продуктивності; експорт/імпорт моделей;

— JPetriNet (безкоштовно). Класична мережа Петрі. Компоненти: графічний редактор; структурний аналіз;

— JSARP (безкоштовно). Класична мережа Петрі. Компоненти: графічний редактор; анімація потоку маркерів; швидка імітація; структурний аналіз;

— Mercury (безкоштовно). Класична мережа Петрі. Компоненти: інваріанти переходів; структурний аналіз; простий аналіз продуктивності; вдосконалений аналіз продуктивності; експорт/імпорт моделей;

— PACE. Класична, часова, розфарбована та пріоритетна мережі Петрі. Компоненти: графічний редактор; анімація потоку маркерів; швидка імітація; скорочення/стиснення моделей;

— PNetLab (безкоштовно). Класична та часова мережі Петрі. Компоненти: графічний редактор; анімація потоку маркерів; інваріанти позицій; інваріанти переходів; структурний аналіз; простий аналіз продуктивності; експорт/імпорт моделей.

2.5. Марковські та байесовські мережі

Марковські та байесовські мережі представляються у вигляді, відповідно, неорієнтованого та орієнтованого графу, кожній вершині якого відповідає ймовірнісна мінлива, а дуги характеризують залежності між цими мінливими. Особливістю марковської мережі є те, що залежності між мінливими (вершинами графа) вводяться за умови відсутності впливу на них попередніх станів системи. Враховується тільки поточний стан. Для байесовської мережі характерні відношення, які виводяться на основі ймовірного рівняння Байесу. Наприклад, байесовська мережа діагностує стан системи за наявністю або відсутністю симптомів на підставі параметрів залежності проявлення типів станів від значень симптомів. Отже, для використання байесовської мережі необхідний попередній етап її навчання.

Марковські ймовірнісні процеси, де вводиться умова про відсутність впливу передісторії імовірнісних подій на наступні події, органічно поєднуються з апаратом байесовських мереж. Утворені при цьому марковські мережі дуже зручні для опису ймовірнісних процесів у вигляді ймовірностей переходів між дискретними станами системи. Переходи системи з одного стану до іншого можливі у фіксовані моменти часу, в проміжках між якими система зберігає свій стан. Це дає можливість лінеаризації систем рівнянь, що описують поведінку системи. Суттєво спрощуються задачі аналізу та синтезу систем інформаційної безпеки.

Марковські мережі застосовуються, в основному, при моделюванні атак і прогнозуванні стану інформаційних систем [68]. Наприклад, алгоритм дій зловмисника щодо реалізації внутрішніх загроз з метою подолання захисних механізмів доступності, цілісності та конфіденційності інформації.

Інформаційна система в результаті дій порушника міняє свої стани у фіксовані моменти часу $T = \{t_1, \ldots, t_k\}$, які є етапами марковського процесу. За тими станами, в яких може знаходитися інформаційна система у різні моменти часу, створюється матриця перехідних імовірностей системи і будується граф станів при діях порушника (рис. 4).

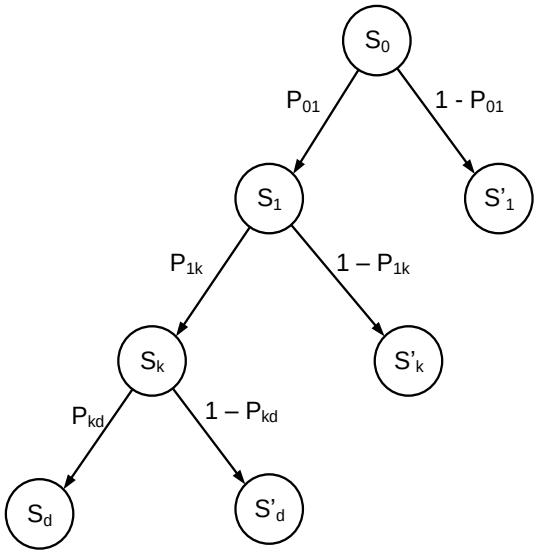

Рис. 4. Граф станів інформаційної системи при діях порушника

Моделювання комп'ютерних атак на основі марковських процесів є найбільш простим. Метод не потрібує запам'ятовування великих масивів даних про всі попередні стани, як у методах КА, когнітивних карт.

Марковський процес, що моделюється, кількісно характеризується лише матрицею перехідних ймовірностей вигляду

$$\left\| P_{i,j} \right\| = \begin{Vmatrix} P_{1,1} & \cdots & P_{1,j} & \cdots & P_{1,n} \\ & & \vdots & & \\ P_{i,1} & \cdots & P_{i,j} & \cdots & P_{i,n} \\ & & \vdots & & \\ P_{n,1} & \cdots & P_{n,j} & \cdots & P_{n,n} \end{Vmatrix}. \qquad (25)$$

Діагональні елементи матриці є ймовірностями знаходження системи у визначених станах. Імовірності $P_{i,j}$, $i = j = 1, \ldots, n$ є умовними ймовірностями переходу з *i*-го до *j*-го стану. Сума ймовірностей кожного рядка матриці дорівнює одиниці:

$$\forall i = 1, \ldots, n : \sum_{j=1}^{n} P_{i,j} = 1. \qquad (26)$$

Для *s*-го переходу ймовірності знаходження у станах обчислюються як:

$$P_j(s) = \sum_{k=1}^{n} P_k(s-1) \cdot P_{k,j}^{(s)}, \qquad (27)$$

де $P_{k,j}^{(s)} = \sum_{n=1}^{s} P_{k,n} \cdot P_{n,j}^{(s-1)}$ — ймовірність переходу з *k*-го до *j*-го стану в результаті здійснення *s* кроків.

Розв'язання (27) дозволяє визначити ймовірності знаходження системи у встановлених станах при заданому горизонті прогнозування, якщо встановлений початковий стан системи $P_1(0), \ldots, P_n(0)$ і задана матриця перехідних імовірностей (25).

Підхід (25)–(27) може бути розповсюджений на системи інформаційної безпеки будь-якої складності, де враховано не тільки дії порушника, але й застосування заходів безпеки.

Для виконання імітаційного моделювання для марковських і байесовських мереж використовуються програмні продукти на основі мереж Петрі. Для цього використовуються стохастичні мережі Петрі. Така мережа отримується, якщо дугам часової мережі Петрі присвоюються ймовірності переходів. Конфлікт за мітку (фішку) у попередній позиції розв'язується шляхом розіграшу результатів подій за допомогою генератора випадкових чисел.

2.6. Онтологічні моделі

Онтологія — це формальний опис релевантних понять та відношень у відповідній області, який спрощує та абстрагує представлення про реальність для розв'язання визначеної проблеми [69]. Онтологія, як технологія, забезпечує спосіб обміну семантичною інформацією між людиною і засобами обробки інформації.

Онтологія існує у вигляді графа, вузли якого представляють поняття або об'єкти предметної області, а ребра — відношення між поняттями. Звичайно цей граф структурований навколо ієрархічної «основи», яка аналогічна відношенням класу/підкласу в об'єктно-орієнтованому програмуванні. Завдяки формалізації онтології дозволяють здійснювати формальний аналіз предметної області та синтезувати і узагальнювати знання (здійснювати логічний вивід знань) за допомогою комп'ютерів [70].

Побудова онтології належить до групи методів формування доменних моделей. Це [71]:

— FODA (Feature-Oriented Domain Analysis): предметна область представляється у вигляді діаграми характеристик (елементарних властивостей). Сполучення цих характеристик відповідає різним об'єктам предметної області;

— RSEB (Reuse-driven Software Engineering Business): задаються правила об'єктно-орієнтованої декомпозиції предметної області з фіксацією результатів мовою UML;

— метод моделювання трансформацій Draco;

— Domain-Specific Modeling (DSM): предметно-орієнтоване моделювання;

— General-Purpose Modeling (GPM): моделювання загального призначення з фіксацією результатів мовами: UML, SysML, XML (представлення знань незалежно від їхньої природи);

— Model-Driven Engineering (MDE): інженерія, що виходить з моделей. Інструменти: CASE-системи. Результати у вигляді DSM-моделей.

Онтологічний метод ODB (Ontology Domain Business) відрізняється від згаданих методів тим, що використовується формалізоване зведення основних понять, відношень між ними і правил логічного виведення предметних знань. Переваги ODB — незалежність від особливостей конкретної предметної області.

Для побудови онтології, як правило, використовуються мови LINGO або OWL (Ontology Web Language), графічний редактор Protégé, система підтримки розподіленої роботи експертних груп — ONTOGRID.

Виділяють такі етапи онтологічного моделювання предметної області:

— побудова базової онтології, де ідентифікуються основні функції і задачі системи;

— базова онтологія деталізується за допомогою часткових онтологій, які входять до базової онтології понять;

— розширення базової онтології поняттями часткових онтологій.

Представлення результатів моделювання (проєктування) онтологій здійснюють, використовуючи такі способи (стилі представлення даних):

— стиль взаємодії. Представлення взаємодії у вигляді діаграм варіантів використання, обчислення, процесів тощо;

— алгоритмічний стиль. Представлення алгоритмів обчислення за допомогою різноманітних псевдокодів;

— інформаційно-орієнтований стиль. Опис моделі даних у вигляді діаграм «сутність – зв'язок»;

— потоковий стиль. Фіксація потокової структури в діаграмах потоків даних;

— аспектно-орієнтований стиль. Здійснення декомпозиції за аспектами, які враховуються.

В основу строгої формалізації онтологічного моделювання покладений аксіоматичний підхід, який почав застосовуватися в інформатиці з середини 70-х років (визначення абстрактних типів даних) [72]. Як фундаментальну основу онтологічного моделювання найчастіше використовують дискрипційні логіки та методологію аналізу формальних понять [73].

Головною задачею онтологічного моделювання в галузі інформаційної безпеки є побудова адекватних онтологій і онтологічних моделей загроз (небажаних ситуацій), а також суб'єктно-орієнтованих інтерфейсів до гетерогенних (різнорідних за складом) джерел інформації.

Онтологія предметної області щодо управління ризиками інформаційної безпеки має містити:

— експертні знання (стандарти, правові норми, концепти, процеси, відношення, вимоги, обмеження, вирішуючи правила, формули, алгоритми, прецеденти);

— правила логічного виводу, що враховують прецеденти.

За допомогою онтології можна отримувати явні та неявні знання, якщо задавати системі відповідні запитання. Запитання щодо отримання явних знань можуть бути описані за допомогою мови запитань SPARQL, а неявних (прихованих) знань — за допомогою правил логічного виводу, які фіксуються мовами SHACL, PIN, SWRL тощо.

Типові запитання до онтології мають наступні формулювання:

— «Дана подія є негативною?»;

— «Які негативні наслідки має дана подія?»;

— «Дані міри і засоби захисту є сумісними?»;

— «За якими параметрами слід оптимізувати сумісні міри та засоби захисту для даної загрози (списку загроз)?» тощо.

Переваги онтологічного підходу полягають у наступному:

— при формуванні онтології відбувається структуризація знань щодо інформаційної безпеки і, як наслідок, полегшується задача експертної оцінки;

— унаслідок структуризації предметної області стає можливим здійснити формалізацію задач прийняття рішень з управління ризиками для безпеки інформації;

— завдяки застосуванню процедур логічного виводу скорочується навантаження на аналітиків при встановленні причинно-наслідкових зв'язків факторів і параметрів системи захисту інформації.

2.7. Концептуальне проєктування

При побудові онтологій окремо можна виділити питання встановлення структури зв'язків і відношень між поняттями (об'єктами) предметної області, структуризації проблем досліджень. Головним чином, це стосується такого напрямку у сфері інформаційної безпеки як самоорганізація (концептуальне проєктування) систем захисту інформації.

Відомо кілька прикладів застосування методів концептуального проєктування для побудови інформаційних систем. Це:

— застосування конфайнмент-моделей (онтологічних універсалій) для побудови структури онтологій [74];

— автоматична адаптація алгоритмів обробки інформації до змін умов, задач і цілей системи захисту інформації на підставі трансформації зв'язаних онтологій (онтології алгоритмів залежно від онтології предметної області) [75];

— розгортання онтології предметної області на основі використання концептуальної схеми родів структури абстрактних відношень безпеки інформації [76, 77].

Конфайнмент-моделі (онтологічні універсалії)

Застосування конфайнмент-моделей для побудови онтологій дозволяє реалізувати системно-когнітивний підхід, який не залежить від особливостей формування когнітивних моделей окремими дослідниками. Тут онтології будуються, спираючись на онтологічні універсалії щодо моделювання системи відношень предметної області.

Відрізняють наступні конфайнмент-моделі:

— концептуальну конфайнмент-модель (ККМ) (рис. 5,*а*). Елементи зв'язані відношеннями: «викликає/залежить від». Частковий випадок — тріадна КМ (ТКМ);

— ієрархічну КМ (ІКМ), а саме: гіперонимічну (ГКМ) (рис. 5,*б*); міронимічну (МКМ) (рис. 5,*в*); атрибутивну (АКМ) (рис. 5,*г*). ГКМ призначена для класифікації видів понять, використовуються ієрархічні родовидові відношення «являється». МКМ призначена для здійснення системного аналізу — ідентифікації надсистеми. Використовуються відношення «являється частиною». АКМ — для класифікації властивостей. Використовується відношення «має властивість»;

— процесні КМ (ПКМ). Виділення процесів життєвого шляху. Використовуються відношення «являється входом/виходом для».

Створення практичних алгоритмів для трансформації онтології задач здійснюється у середовищі CLEPE (Conceptual level programming environment) з урахуванням положень концептуального моделювання [79].

У системі моделювання формалізоване представлення знань здійснюється таким чином.

Предметна область складається з множини об'єктів

$$A_1, A_2, ..., A_n,$$

де кожен із об'єктів класифікується як екземпляр відповідного поняття. Множина об'єктів і множина екземплярів, відповідна цьому об'єкту, утворюють множини-носії для n багатосортних алгебр.

На основі кожної множини A_i визначений абстрактний тип даних

$$E_i = (Name, \Sigma, Ex), \tag{28}$$

де $Name$ — назва типу (наприклад, коло); Σ — сигнатура багатосортної алгебри (параметри кола: координати центра та точок кола, радіус кола); Ex — визначальні співвідношення типу (рівняння кола).

З типів E_i формується множина алгебраїчних доменів:

$$E = \{E_1, ..., E_i, ..., E_n\}. \tag{29}$$

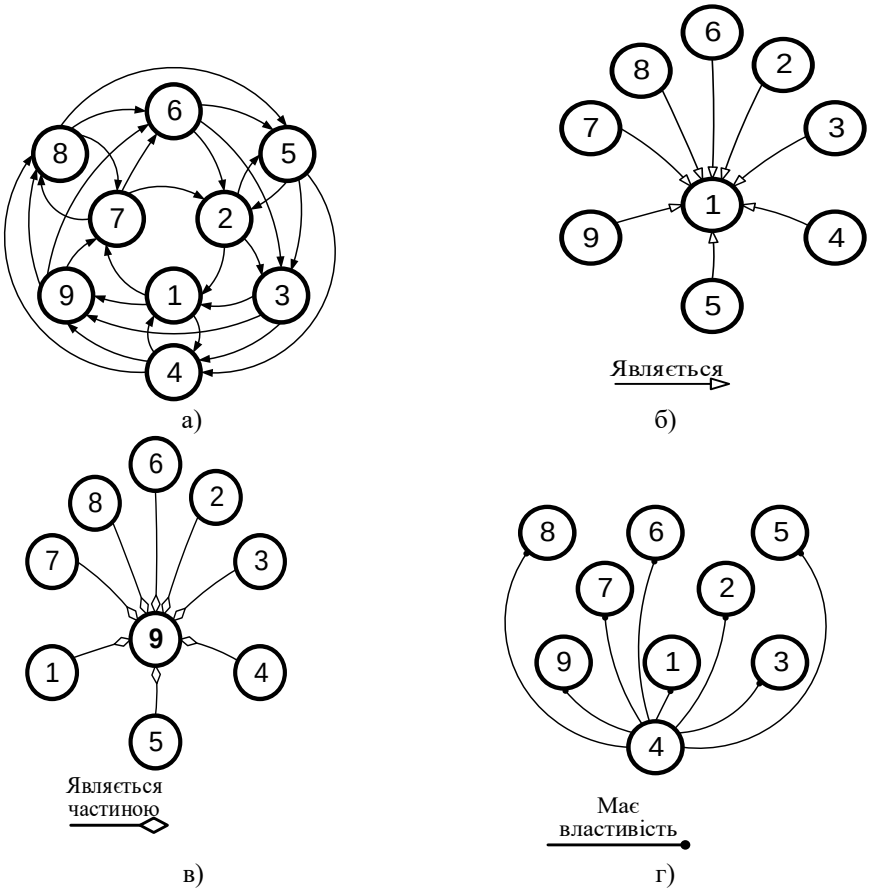

Рис. 5. Види конфайнмент-моделей: а) ККМ; б) ГКМ; в) МКМ; г) АКМ

Також, крім цього, вводяться:

— домен атрибутів, At, який визначений на списку значень атрибутів у вигляді пар:

$$(key, value\},$$

де key — ідентифікатор атрибута (наприклад, «ікс»); $value$ — його значення (дійсне число). Для цього домена визначено операції об'єднання, підстановки, видалення та інтерпретації. Крім цих операцій також визначено різноманітні функції, наприклад, функцію вибору значення домену:

$$F_{setval}(At, key) \to value;$$

— бульовий домен Cs, який містить вирази, за результатом взяття яких визначаються значення, що належать бульовій множині $\{true, false\}$. Операндами виразів є мінливі (ідентифікатори атрибутів), що належать іншим алгебраїчним доменам. Елементи Cs — це обмеження (умови). Операції для Cs — бульові операції: «І», «АБО», «В противному випадку»; операція інтерпретації (=) (необхідна для спрощення виразів). Екземпляр бульового домена — конкретна умова, обмеження;

— домен сутностей з атрибутами, T, який визначений на множині кортежів

$$\left\{\left(E_i, At_j, Cs_j^*\right)\right\},$$

де для кожного i існує тільки одне j, що утворює елемент домена T:

$$\forall i \; \exists^1 j : (E_i, At_j),$$

кожна умова (обмеження), що належить підмножині Cs_j^*, є виразом з операндами, які належать домену At_j. Операції над елементами цього домена — це об'єднання або поділ (merge, split) сутностей. Операція об'єднання інтерпретується як синтез нової сутності із сумісним набором властивостей і обмежень (умов) сутностей-операндів. Операція поділу сутностей — зворотна. Екземплярами домена сутностей з атрибутами є кортеж відповідних фактів;

— домен відношень, RI, який визначений на множині структур вигляду:

$$\left\{\left(T_{1,i} \times \ldots \times T_{k,i}, At_i^r, Cs_i^*\right)\right\},$$

де $T_{1,i} \times \ldots \times T_{k,i}$ — декартів добуток алгебраїчних типів даних з домена T (простір атрибутів, що відноситься до i-ї структури); At_i^r — типи атрибутів відношень; Cs_j^* — обмеження (умови), що визначають відношення. Над відношеннями виконуються операції: об'єднання; відокремлення; підстановки.

Онтологія є кортеж, який представлений доменами понять з атрибутами, відношеннями і обмеженнями (умовами), які стосуються доменів понять і відношень:

$$On = (T, RI, Cs^*). \tag{30}$$

Онтологічна модель задачі визначається наступним кортежем:

$$Md = \left\langle On_{Ts}, Ac_{Ts}^*, Cs_{Ts}^* \right\rangle, \tag{31}$$

де On_{Ts} — онтологія задачі за правилами побудови (30); Ac_{Ts}^* — множина дій задачі; Cs_{Ts}^* — множина додаткових обмежень (умов).

Дія є сутність з атрибутами (домен T), яка інтерпретується як команда деякому зовнішньому сервісу або команда на виконання іншої онтологічної моделі. Параметри команди є атрибутами елементів On_{Ts} або є константами.

Трансформація алгоритмів залежно від змін умов та обмежень здійснюється за допомогою функції ініціалізації параметрів (InstPar), яка подається як набір відображень між атрибутом дії і значеннями атрибутів сутностей і відношень зі складу онтологічної моделі:

$$InstPar : (Ac_{l,i}, pkey_{l,i}) \to SelVal(At_{l,j}, key_{l,k}),$$

$$Ac_{l,i} \in Md_l, \; At_{l,j} \in On_{Ts}^l \in Md_l, \tag{32}$$

де Md_l — онтологічна модель задачі, що розглядається; On_{Ts}^l — онтологія цієї задачі.

Програмна система на основі онтологічної моделі задач представлена на рис. 6 [75].

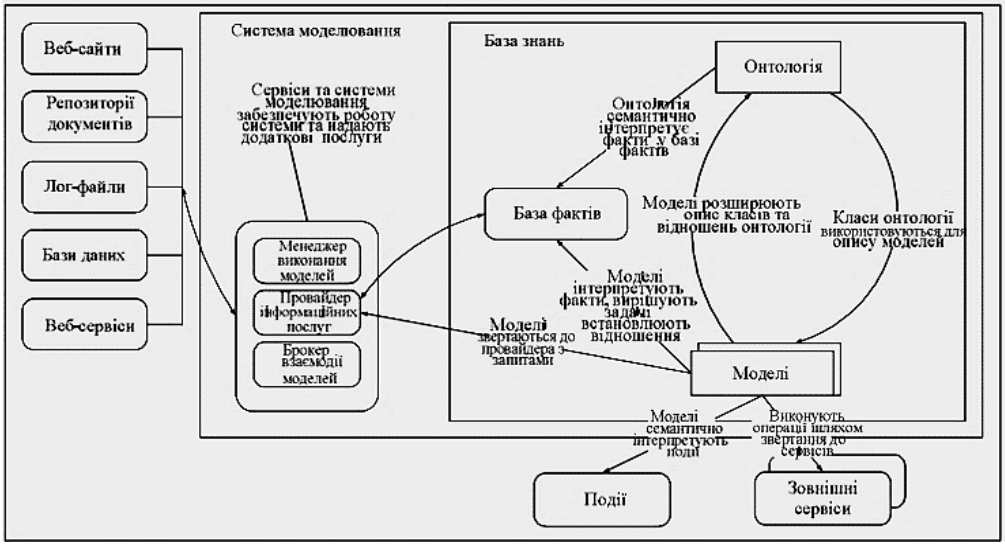

Рис. 6. Структура програмної системи на основі онтологічних моделей задач

Залежно від контексту подій, що відбуваються, активується та або інша онтологічна модель. Ініціатором активації є онтологічна модель, що виконується (рис. 7) [75].

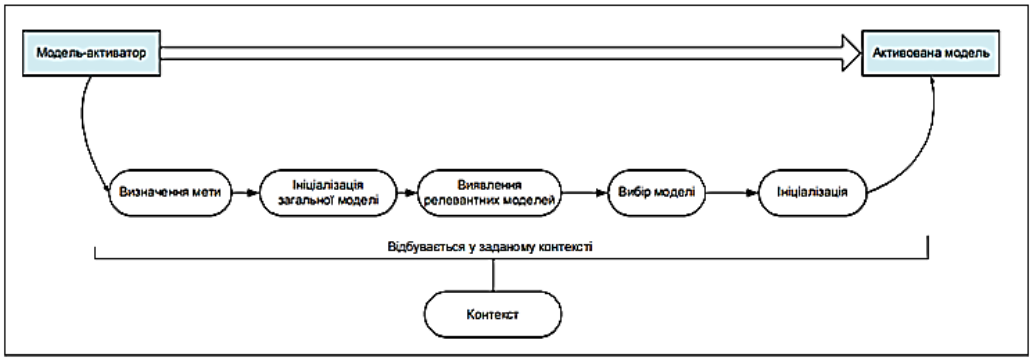

Рис. 7. Процес активації моделі задач

Також запропонований апарат забезпечує створення нових онтологій. При цьому виконуються наступні кроки:

— аналіз задачі та встановлення всіх сутностей, відношень, обмежень (умов) та операцій, які необхідні для її розв’язання;

— формування онтологічної моделі задачі із використанням установлених компонент із множини вже існуючих компонент;

— додавання до онтології компонент, яких немає серед існуючих;

— валідація оновленої онтології, усунення протиріч.

Інструментальний засіб щодо побудови програмних систем на базі онтології має такі основні функції:

— робота з онтологією: створення та модифікація класів і відношень, визначення обмежень для атрибутів;

— робота з фактами: створення та модифікація окремих фактів, які є екземплярами класів, перевірка обмежень і валідація фактів;

— створення та модифікація онтологічних моделей із використанням класів і фактів онтології, визначення додаткових обмежень; визначення елементів у контексті моделі, їхній пошук; визначення операцій, їхня прив'язка до сервісів; визначення операцій, що виконуються залежно від результатів виконання моделі;

— виконання моделей і мереж моделей: запуск і виконання моделей на тестовій базі фактів, перевірка відповідності результатам, що очікуються.

Для реалізації програмного продукту використана мова програмування Pyton і графічна бібліотека PyQt. Програмний продукт складається з наступних частин: редактора онтологій; редактора фактів; редактора моделей; програми моделювання.

Подальший розвиток апарату полягає у розширенні взаємодії моделей, реалізації механізмів логічного виводу, реалізації багатоваріантних обчислень і контекстної залежності.

Розгортання онтології предметної області на основі використання концептуальної схеми родів структури абстрактних відношень безпеки інформації

У [76] представлено підхід щодо моделювання предметної області «забезпечення безпеки» на основі оригінальної методології концептуального аналізу і проєктування.

Розглянуто концептуальну схему змішаного міжсуб'єктного і суб'єкт-об'єктного відношення безпеки, яка виведена на основі родоструктурної схеми абстрактного відношення безпеки.

Основні постулати відношення безпеки наступні: існує світ можливостей; можливість може актуалізуватися і тоді вона перестає бути можливістю; елементом світу можливого є можливість здійснення тієї або іншої події; можливості можуть бути зв'язані одна з одною «генетичним» відношенням (реалізація однієї або кількох можливостей — необхідна умова реалізації іншої можливості); можливості можуть бути зв'язані одна з одною відношенням блокування (якщо реалізується блокуюча можливість — не може бути реалізованою можливість, яку заблоковано); можливості являються атрибутами суб'єктів і об'єктів «дійсного світу», який реалізує ці можливості; існує світ суб'єктів; суб'єкти мають інтереси; інтереси різних суб'єктів можуть вступати у відношення; відношення між суб'єктами здійснюються тільки через їхні інтереси.

У світі можливостей можуть виникати складні мережеві структури з циклами.

Інтереси суб'єкта — номінально виділена підмножина його можливостей (суб'єкт зацікавлений у реалізації цих можливостей).

Будь-яка можливість, яка блокує можливості з області інтересів суб'єкта, представляє загрозу інтересам суб'єкта.

Можливість, яка блокує загрозу — є варіантом заходів безпеки по відношенню до даної загрози.

Захід щодо реалізації можливості — є можливостю, яка є утворюючою для даної можливості суб'єкта.

Оскільки для загрози та заходу щодо реалізації можливості також можна визначити загрозу та захід, то слід казати про загрози та заходи першого, другого, третього і т.д. порядків.

Для побудови онтології безпеки здійснюється послідовне визначення все більш спеціалізованого розбиття дерева фактор-структур, що визначені на множині можливостей. Розбиття здійснюється двома способами:

1) шляхом конкретизації (деталізації) вихідних понять;

2) шляхом утворення відношень між гілками (фрагментами) онтології з комбінуванням розбиття за ієрархічними рівнями та фактор-відношеннями.

Для побудови фактор-структури (онтології) запропоновано використовувати концептуальні схеми родів структури: абстрактних відношень безпеки; відношень безпеки ієрархічних суб'єктів, що трансформуються; полісуб'єктного управління безпекою; розповсюдження небезпеки, що симптоматично визначається. Фрагмент концептуальної схеми родів структури абстрактних відношень безпеки наведений у таблиці.

Концептуальна схема родів структури абстрактних відношень безпеки (фрагмент)

Позначення конституанти	Формальний вираз конституанти	Схемна інтерпретація конституанти
$X1$		Множина можливостей
$X2$		Множина суб'єктів
$D1.1$	$\text{B}(X1\times X1)$	Відношення генетичного зв'язку можливостей або множина пар: можливість – можливість, що виявляється необхідною умовою реалізації можливості, яка розглядається
$D1.2$	$\text{B}(X1\times X1)$	Відношення блокуючого зв'язку можливостей або множина пар: можливість – можливість, що блокує можливість, яка розглядається
$T1.0$	$\{\alpha \subset \text{B}(X1\times X1) \mid \text{Pr}_1\alpha = \text{Pr}_2\alpha\}$	Множина циклів можливостей
$A1.1$	$\{(\alpha \subset T1.0)\&(\alpha \subset \beta)\Rightarrow ((\alpha \subset D1.1)\vee(\alpha \subset D1.2))\}\Rightarrow:(\beta=\varnothing)$	Відношення генетичного, блокуючого, а також змішаного генетичного і блокуючого зв'язку можливостей не допускають циклів і петель
$A1.2$	$((\alpha \in B(X1\times X1))\&((d_1\in\alpha)\supset (d_1\subset D1.1))\&(x_1\in\text{Pr}_1\alpha)\&(x_2\in\text{Pr}_2\alpha)\&(\text{Pr}_1\alpha\setminus x_1=\text{Pr}_2\alpha\setminus x_2)\Rightarrow\neg((\beta\in B(X1\times X1)\&(d_2\in\beta))\Rightarrow (d_2\subset D1.2))\&(x_2\in\text{Pr}_2\beta)\&(x_3\in\text{Pr}_2\beta)\&(\text{Pr}_1\beta\setminus x_1=\text{Pr}_2\beta\setminus x_1)$	Можливості, які зв'язані генетичним відношенням, не можуть бути зв'язаними відношенням блокування і навпаки
…	…	…

Конституанти, що представлені в таблиці, є родами структури абстрактних відношень безпеки, які синтезуються за допомогою формальних правил перетворення тексту роду структури при застосуванні операцій утворення ступенів множин [80].

Даний підхід дозволяє реалізувати дедуктивний метод проєктування систем управління інформаційною безпекою, коли відбувається рух від абстрактного до конкретного, від загального до часткового. Проблемним питанням, яке вирішено не повною мірою, є питання інтерпретації конституант, відповідних вищим ступеням множин (а саме вони мають практичне значення). Колосальна розмірність не дозволяє здійснювати їхню інтерпретацію без розробки спеціальних засобів інтерпретації.

2.8. Матричний підхід

За допомогою матричного підходу реалізується універсальна формалізована методика, яка дозволяє здійснювати кількісну оцінку ризиків залежно від пара-метрів загроз і об’єктів (активів), на які спрямована загроза [81].

Система моделей і методів при цьому забезпечує: прогностичне моделювання (виявлення) загроз і стану об’єктів інформаційної системи; оцінку ризиків інформаційної безпеки; розв’язання задач вибору (синтезу) механізмів захисту інформації.

Усі ці методи та моделі вкладаються у наступну схему: онтологічна модель – матричні методи, що забезпечують кількісне визначення відношень між елементами онтології.

Вихідні матриці середовища безпеки, в загальному випадку, мають вигляд, що представлений на рис. 8.

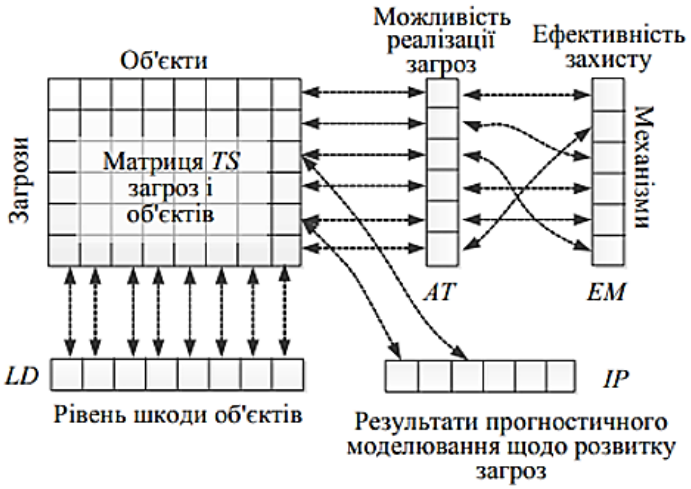

Рис. 8. Онтологія вихідних матриць середовища інформаційної безпеки

Матриця TS, по суті, є матрицею ризиків для інформаційної безпеки при заданих параметрах за станом об’єктів, можливостю реалізації загроз, прогнозом розвитку загроз, а також установленим механізмом захисту інформації.

Дослідження щодо безпеки зводяться до розв'язання різних пошукових задач на графі TS. Складність полягає у великій розмірності цього графа. Це можливо подолати шляхом розбиття загального графа на підграфи (підсистеми), які не зв'язані між собою.

Для виділених підграфів здійснюється оцінка ризиків для заданих сполучень: «механізм захисту – загроза» (рис. 9).

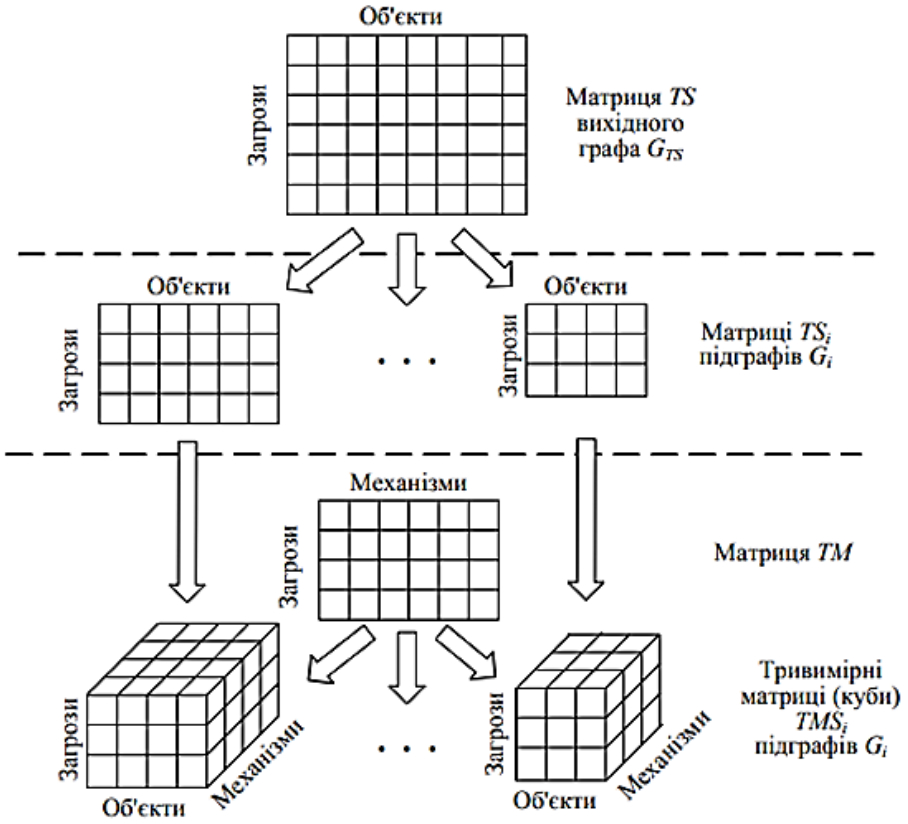

Рис. 9. Матричні трансформації на основі матричної моделі

Для отриманих тривимірних графів здійснюється подальша оцінка з урахуванням стану об'єкта і результатів прогнозу розвитку загрози.

Використовується метод експертної оцінки. Кожним експертом для кожної загрози заповнюється матриця оцінок можливості реалізації загрози при застосуванні визначеного механізму захисту.

Оцінка є вектор, де містяться ймовірнісні міри встановлених якісних апріорних оцінок: «реалізація загрози неможлива»; «ймовірність реалізації загрози низька» і т.д.

Здійснюється обробка і узагальнення результатів оцінки загроз експертами за допомогою використання апарату нечітких множин. Узагальнені дані згортаю-ться у комплексний показник перекриття загроз для безпеки інформації комплексом захисту інформації, що застосовується.

2.9. Методи Data mining: аналіз часових рядів

Data mining (добування даних, інтелектуальний аналіз даних, глибинний аналіз даних) — історична назва, яка використовується для позначення сукупності методів виявлення в даних раніш невідомих, нетривіальних, корисних і доступних для інтерпретації знань, що необхідні для прийняття рішень у різних сферах діяльності людини. Термін був уведений П'ятецьким-Шапіро в 1989 році .

Основу методів data mining складають різноманітні статистичні динамічні методи, які з'єднанні в групу методів аналізу часових рядів і доповнені моделями прогнозування, які, в свою чергу, включають застосування дерев рішень і графів. В основу статистичних методів покладено поняття кореляції [82], яке поєднує: вейвлет-аналіз; мультіфрактальний аналіз; ΔL метод; фрактальний аналіз; аналіз Фур'є; метод автокореляції.

Часовий ряд — це набір значень будь-якої характеристики, отриманих у результаті спостереження, які впорядковані за часом. Як правило, розглядаються дискретні часові ряди, значення яких фіксувалися через рівні (регулярні ряди) або нерівні (нерегулярні ряди) інтервали часу. Крім регулярності, часові ряди поді-ляють на детерміновані та недетерміновані.

Часові ряди використовують для аналітики та прогнозування, коли важливо визначити, що буде відбуватися з показниками на встановленому горизонті прогнозування. При розв'язанні задач інформаційної безпеки часові ряди розглядаються як реалізація стохастичних процесів.

Для аналізу часових рядів існують наступні програмні продукти:

1) ARMA (Autoregressive Moving Average) — авторегресійна модель ковзаючого середнього. Просте ковзаюче середнє є середньоарифметичною величиною за встановлений період часу;

2) ARIMA (Autoregressive Integrated Moving Average) — авторегресійна інтегрована модель ковзаючого середнього. Інтегрована модель ковзаючого середнього — це середнє арифметичне різниці між послідовними спостереженнями за встановлений період часу;

3) SARIMA — інтегроване ковзаюче середнє для сезонної авторегресії. Використовується для роботи з часовими рядами із сезонними компонентами. Це розширення моделі ARIMA;

4) Prophet — інструмент з відкритим кодом для бізнес-прогнозування. Модель Prophet заснована на чотирьох мінливих: $g(t)$ — тренд; $s(t)$ — сезонність (моделювання періодичних змін); $h(t)$ — свята та важливі події (врахування аномальних днів); $\varepsilon(t)$ — помилка (врахування решти впливів);

5) прогноз за методом експоненційного згладжування. Використовується зважена модель ковзаючого середнього, коли вага попередніх значень експоненційно зменшується. Забезпечує можливість здійснення прогнозу на великий період часу;

6) програмний комплекс SPSS [83].

Дані методи аналізу часових рядів будуються на припущенні про їхню стаціонарність — постійні статистичні властивості у часі.

Результати аналізу часових рядів застосовують з метою: прогнозування стану інформаційної системи; діагностики вразливостей і атак; навчання нейронних мереж у системах управління інформаційною безпекою.

2.10. Проблемно-орієнтовані методи та моделі

Проблемно-орієнтовані методи та моделі щодо дослідження проблем інформаційної безпеки розроблялися на підставі концепції, яку представлено у низці стандартів з інформаційних технологій [84–86]. Згідно цієї концепції основним елементом процесу управління інформаційною безпекою є оцінка рівня ризику та методи його зниження до встановленого рівня (рис. 10).

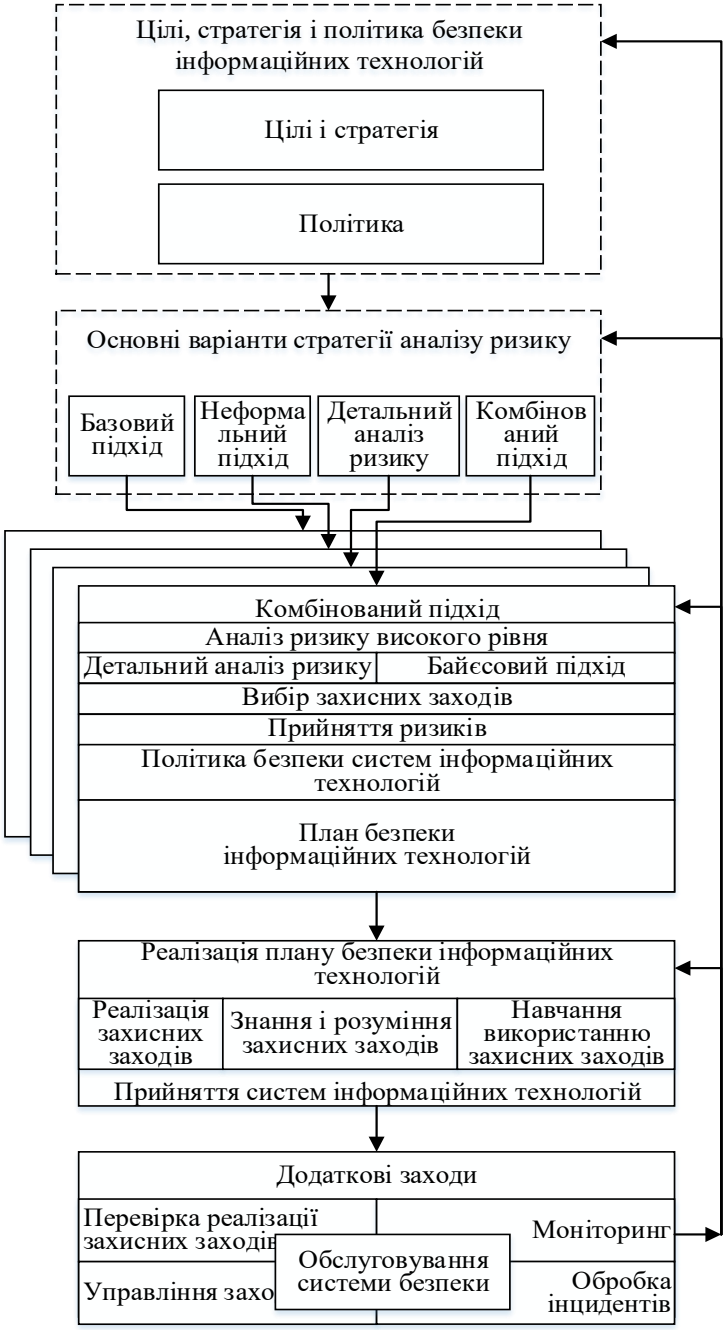

Рис. 10. Схема застосування різних підходів у процесі аналізу ризику інформаційної безпеки

Існують чотири варіанти стратегії аналізу ризику інформаційної безпеки: 1) базовий підхід (для низького ступеня ризику). Рівень забезпечення безпеки іноді може виявитися недостатнім; 2) неформалізований підхід до аналізу ризику. Звертається увага на системи з найбільшим ризиком; 3) детальний аналіз усіх систем; 4) комбінований підхід. Проведення спочатку аналізу високого рівня з метою класифікації систем за рівнем ризику. Потім проведення детального аналізу систем з високим рівнем ризику або тих систем, що мають критичні показники. Для решти — базовий підхід.

Базовий підхід передбачає використання стандартного набору захисних заходів, що наведено в [87].

Неформальний підхід передбачає використання знань і досвіду спеціалістів, без використання формальних методів.

Детальний аналіз ризику передбачає детальну ідентифікацію і оцінку активів, оцінку можливих загроз активам, оцінку рівня їхньої вразливості, наступну оцінку ризиків та обґрунтування захисних заходів.

Комбінований підхід — це поєднання базового і детального підходів на основі попереднього аналізу високого рівня.

3. Засоби моделювання загроз інформаційній безпеці

Для визначення та моделювання загроз, як важливої складової у загальній задачі забезпечення інформаційної безпеки системи, існує велика кількість різноманітних моделей та методів, які подаються як засоби моделювання загроз [88]. Методичне наповнення цих засобів залежить від типу об’єкта захисту та функціонального наповнення (повноти) блоку оцінки (класифікації) ризиків інформаційній безпеці.

Згідно [88] виділяють наступні типи об’єктів захисту:

— розумна мережа енергопостачання. Особливості опису об’єкта пов’язані з його ієрархічністю, один об’єкт вкладається в інший;

— процесно-орієнтовані системи. Особливості опису пов’язані з декомпозицією моделей і цільових критеріїв;

— комп’ютерні мережі. Особливості опису пов’язані з уразливістю системи до невірних результатів машинного навчання, несанкціонованого доступу до баз даних;

— виконувані файли. Особливості опису пов’язані з уразливістю системи до мережевих вторгнень, спаму, несанкціонованого використання;

— бездротові сенсорні мережі. Особливості опису пов’язані з можливостями здійснення паралельного управління;

— інтернет речей. Особливості опису пов’язані з уразливістю системи до невірних результатів машинного навчання;

— корпоративні додатки. Особливості опису пов’язані з необхідністю виявлення прихованої структури програмних додатків;

— хмарне сховище. Особливості опису пов’язані з можливістю несанкціонованого доступу до даних, що зберігаються;

— розподілені системи. Особливості опису пов’язані з трансформацією об’єкта у часі протягом його життєвого шляху, необхідністю врахування параметрів розгалуженої структури.

Для оцінки та моделювання загроз застосовують такі методичні підходи:

— Microsoft STRIDE (Spoofing, Tampering, Repudiation, Information, Disclosure, Denial of Service, Elevation of Privilege) [89]. Методологія визначення актуальних загроз інформаційних систем, яка включає оцінку ризиків за наступними категоріями: спуфінг, модифікація, відмова від авторства, розголошення, відмова в обслуговуванні та підвищення привілеїв. Виявляється найбільш зрілим методом, що має розвинуту бібліотеку вхідних даних. Простий у використанні. Але метод потребує тривалого часу для введення вхідних даних, мають місце хибні спрацьовування;

— PASTA (Process for Attack Simulation and Threat Analysis) [90]. Реалізований повний цикл детального аналізу ризиків для інформаційної безпеки за такими етапами: 1) визначення цілей; 2) визначення технічного контексту; 3) декомпозиція системи; 4) аналіз загроз; 5) аналіз уразливостей; 6) моделювання атак; 7) аналіз ризиків. Недоліки: великий обсяг вхідних даних стосовно операційного рівня, управління, архітектури та розвитку інформаційної системи; велика трудомісткість;

— LINDDUN (Linkability, Identifiability, Non Repudiation, Detectability, Disclosure of Information, Unawareness, Non-Compliance) [91]. Методологія для аналізу загроз за наступними категоріями: зв'язаність загроз; забезпечення конфіденційності в процесах ідентифікації і автентифікації. Недоліки: швидке зростання кількості загроз унаслідок розвитку інформаційної системи; недостатня ефективність при виявленні загроз загального характеру; велика трудомісткість;

— CVSS (Common Vulnerability Scoring System) [92]. Загальна методика оцінки уразливості за визначеними системами критеріїв. На цей час використовують базові вектори критеріальних показників CVSS v2.0 і CVSS v3.0. Вектор CVSS v2.0 має більшу повноту порівняно із CVSS v3.0. CVSS v2.0 складається з трьох груп метрик оцінки уразливості: базових; часових і контекстних. CVSS v3.0 має тільки базові метрики. Недоліки: непрозора методика обчислення показників; великий обсяг вхідних даних, який треба задавати;

— Attack trees [93]. Моделювання атак за допомогою мережевих деревоподібних моделей. Недоліки: потребує детальної проробки та структуризації проблеми безпеки інформації; не враховує динаміку розвитку атак;

— Persona non Grata [94]. Моделювання дій і цілей потенційно зловмисних небажаних користувачів. Недоліки: не здійснюється синтез нових зловмисних дій;

— Security Cards та hTMM [95]. Моделювання складних багатопараметричних загроз. Недоліки: нестабільність оцінок, багато хибних спрацьовувань;

— Quantitative TMM (Threat Modeling Method) [96]. Кількісне моделювання та класифікація загроз. Недоліки: велика трудомісткість;

— Trike [97]. Моделювання загроз з відкритим кодом, що спрямоване на забезпечення процесу аудиту безпеки з точки зору управління ризиками інформаційній безпеці. Недоліки: система вагових коефіцієнтів є недостатньо адекватною реальним проблемним ситуаціям інформаційної безпеки;

— OCTAVE [98]. Операційна оцінка загроз, активів і уразливостей, яка підтримує профілювання виконання коду на рівні функцій. Методологія орієнтована на оцінку організаційних (нетехнічних) ризиків. За цією методологію моделювання загроз інформаційні ресурси організації ідентифікуються, а набори даних, які вони

містять, отримують атрибути залежно від типу даних, що зберігаються. Недоліки: великий рівень складності;

— VAST modeling [99]. Спрямована на масштабування процесу моделювання загроз по всій інфраструктурі і SDLC (Secure Development Lifecycle), а також досягнення плавної інтеграції до методології гнучкої розробки програмного забезпечення. Забезпечує цілісне уявлення всієї поверхні атаки, дозволяючи мінімізувати загальний ризик. Недоліки: підвищені вимоги до рівня кваліфікації фахівців з інформаційної безпеки.

Перелічені методи та моделі використовуються за різними напрямками управління інформаційної безпекою. Головним завданням, яке при цьому вирішується, є оцінка рівня ризику для інформаційної безпеки організації (системи) за результатами відслідковування інформаційних потоків, проведення функціонального контролю та аудиту діяльності за встановлений період часу. Велике різноманіття моделей і методів, які використовуються, викликане різноманіттям об'єктів охорони та особливостями їхнього функціонування.

4. Аналіз методів та моделей, що використовуються в галузі інформаційної безпеки

Вище розглянуто лише деякі методи та моделі, що можуть застосовуватись у такій глобальній сфері як інформаційна безпека, що обумовлено обмеженням обсягу представлення матеріалів у форматі статті. У поле розгляду не потрапили методи теорії ігор; розподілу обмежених ресурсів при формуванні рішень з організаційного управління інформаційною безпекою; розпізнавання багатопараметричних об'єктів та інші.

Наведені методи та моделі можна умовно поділити, за напрямками науково-практичної спрямованості, на три групи.

Перша група — це методи та моделі, що використовуються для контролю поточного стану системи і прийняття рішень з оперативного управління інформаційною безпекою. Для цього доцільно застосовувати нейромережеві моделі, методи data mining, матричний метод і проблемно-орієнтовані методи та моделі.

Нейромережеві моделі та методи data mining у сукупності з матричним методом дозволяють суттєво знизити участь людини у процесі управління інформаційною безпекою за рахунок кількісної оцінки рівня безпеки. Однак, автоматизовані системи, що побудовані на базі даного науково-методичного апарату, суттєво залежні від особливостей об'єктів (процесів), для яких створюється система захисту. Розвиток (еволюція) об'єкта захисту потребує суттєвих змін у програмному забезпеченні системи захисту інформації. Треба донавчати нейромережі та (або) змінювати їхню структуру, доповнювати або корегувати систему гіпотез для алгоритмів статистичної обробки даних.

Це також стосується і проблемно-орієнтованих методів і моделей. Вони потребують попереднього налаштування вхідних даних та алгоритмів оцінювання загроз. При цьому ця функція тут покладена на експертів, що обумовлює збільшення трудомісткості та тривалості виконання задач модернізації програмного забезпечення. До того ж ці методи та моделі, на цей час, не дозволяють здійснювати оцінку системних загроз, коли спостерігається синергетичні та каскадні ефекти від небажаних дій. Необхідно розробити більш повну абстрактну модель об'єкта, що за-

хищається, і спрямованих на нього загроз, щоб ця модель була адекватною для будь-якої організації і формувала для неї засоби захисту від більшості загроз.

Друга група — методи та моделі, що застосовуються для підтримки прийняття рішень щодо організаційного управління та проєктування систем інформаційної безпеки. Тут можна використовувати когнітивні карти, кінцеві автомати, марковські та байесовські мережі, онтологічні моделі та матричний метод. За їхньою допомогою зручно розв'язувати як пряму задачу (прогнозна оцінка рівня безпеки при заданих умовах), так і зворотну (визначення раціонального обрису системи захисту, параметрів заходів захисту і порядку їхнього виконання). Причому математичний апарат дозволяє розв'язувати ці задачі як у стаціонарній, так і нестаціонарній постановці. Також, для розв'язання прямої задачі, додатково можуть бути використані моделі на основі мережі Петрі (для здійснення імітаційного моделювання динаміки дискретно-подійних систем).

Марковські та байесовські мережі дозволяють суттєво знизити обчислювальну складність задач моделювання за рахунок лінеаризації систем рівнянь. Але при цьому не враховується фактор передісторії подій. Це накладає суттєві обмеження на область досліджень. Особливо це стосується напрямку оцінки системних загроз.

Когнітивні карти, кінцеві автомати, онтологічні моделі та матричний метод надають значно більше можливостей щодо побудови моделей загроз, атак і поведінки системи та об'єкта захисту. Але при цьому швидко зростає обчислювальна складність задач за рахунок збільшення їхньої розмірності. Розмірність моделей, які мають практичний інтерес, суттєво перебільшує можливості обчислювальних засобів за їхньою швидкодією та обсягом пам'яті.

Для другої групи методів та моделей головною науковою проблемою є проблема обґрунтування декомпозиції і лінеаризації задач при проведені досліджень. Це суттєво залежить від характеру предметної області, де ведуться дослідження.

Третя група — це методи та моделі, що призначені для розв'язання задач адаптації і самоорганізації системи. За цим напрямком слід звернути увагу на такі методи як концептуальне проєктування онтологій і їхня трансформація.

У статті проаналізовано приклади розробки адаптаційних моделей на основі застосування: конфайнмент-моделей для онтологічних мереж; апарату алгебри систем (бульова алгебра і алгебра геометричних об'єктів: кола, решета) [78]; апарату теорії ступенів множин Н. Бурбакі [100]. Принципова можливість синтезу структур об'єктів (систем) із визначеними властивостями, яка продемонстрована у згаданих прикладах, не знімає проблему розмірності. Логічні вирази, шляхом інтерпретації яких здійснюється фіксація результатів, мають дуже велику розмірність. Без розробки спеціальної мови, інших засобів інтерпретації (представлення) результатів концептуального проектування, не можна говорити про подальший розвиток систем адаптивного управління інформаційною безпекою.

5. Висновки

Інструментарій моделювання щодо інформаційної безпеки представлений такими трьома основними напрямками:

— розроблення методів і моделей контролю поточного стану системи та прийняття рішень з оперативного управління інформаційною безпекою;

— розроблення методів і моделей підтримки прийняття рішень щодо організаційного управління та проєктування систем інформаційної безпеки;

— розроблення методів і моделей самоорганізації системи.

На основі першої групи методів і моделей (нейромережі, методи data mining, матричний метод і проблемно-орієнтовані методи та моделі) створено велике різноманіття корпоративних автоматизованих систем, комерційних програмних платформ управління інформаційною безпекою. При цьому має місце сильна залежність програмного забезпечення від особливостей об'єкта захисту та предметної області, в якій здійснюється моделювання і оцінка процесів захисту інформації. Завдання модернізації та адаптації засобів захисту інформації пов'язані з великими трудовитратами (в основному за рахунок широкого застосування експертних методів оцінки).

Друга група методів (когнітивні карти, кінцеві автомати, марковські та байєсовські мережі, онтологічні моделі, мережі Петрі та матричний метод) представлена більшою мірою в галузі проведення системних досліджень щодо розвитку систем захисту інформації і обґрунтування вимог до них. Особливістю цих методів є наявність проблеми обґрунтування раціональної декомпозиції і лінеаризації задач при проведені досліджень.

Напрямок досліджень інформаційних систем, що адаптуються, змінюють свою структуру та параметри залежно від зовнішніх умов і трансформації предметної області, представлений методами концептуального проєктування. На підставі цих методів можна розв'язувати задачі синтезу структур об'єктів (систем) із визначеними властивостями. Для побудови систем адаптивного управління зі складністю, що відповідає реальним процесам, треба вирішити проблему створення спеціальної мови, інших засобів інтерпретації (представлення) результатів концептуального проєктування (логічних виразів великої розмірності).

Окремо виділено засоби моделювання загроз інформаційній безпеці. Велике різноманіття моделей і методів, які для цього використовуються, викликане наявністю різних типів систем як об'єктів захисту та особливостями їхнього функціонування. Методичне наповнення цих засобів залежить від типу об'єкта захисту та функціонального наповнення (повноти) блоку оцінки (класифікації) ризиків інформаційної безпеки. На вибір конкретного засобу впливає, крім цього, рівень складності його використання та, відповідно, наявний рівень кваліфікації фахівців з інформаційної безпеки.

1. Ситник В.Ф., Краснюк М.Т. Інтелектуальний аналіз даних (дейтамайнінг): навч. посіб. — Київ: КНЕУ, 2007. 376 с.

2. Introduction to Time Series Analysis and Forecasting, 2nd Edition, Wiley Series in Probability and Statistics, by Douglas C.Montgomery, Cheryl L.Jennings and MuratKulahci (eds). Published by John Wiley and Sons, Hoboken, NJ, USA, 2015. Total number of pag: INTRODUCTION TO TIME SERIES ANALYSIS AND FORECASTING, 2ND EDITION, WILEY SERIES IN PROBABILITY AND STATISTICS, by Douglas C. Montgomery, Cheryl L. Jen

3. Alice Brown. Концептуальне проектування: методи, засоби, цілі та завдання. URL: https://uk.cmcollections.com.ng/kontseptualnoe-proektirovanie-738

4. Гайна Г.А. Основи проектування баз даних: навч. посіб. — Київ: Київський національний університет будівництва і архітектури. 2005. 204 с. ISBN 966-627-117-6.

5. Petri Nets World. URL: http://www.informatik.uni-hamburg.de/TGI/PetriNets/

6. Судачевскі В.М., Абабій В.В., Гуцуляк Е.Н., Подубний М. Проектування систем управління на основі мереж Петрі. *Вісник Вінницького політехнічного інституту*. 2011. № 3. С. 98–102. ISSN 1997- 9266.

7. Онищенко Б.О., Супруненко О.О. Управляючі мережі Петрі, як засіб моделювання та автоматизованого аналізу алгоритмічних конструкцій. *Вісник Запорізького національного університету*. 2009. № 1. С. 163–169.

8. Sawaragi T., Iwai S., Katai O. An integration of qualitative causal knowledge for user-oriented decision support. *Control Theory and Advanced Technology*. 1986. Vol. 2. P. 451–482.

9. Baranovska L.V., Bukovskiy O.M. Mixed strategy Nash equilibrium in one game and rationality [Архівовано 27 листопада 2020 у Wayback Machine]. International Scientific and Practical Conference «WORLD SCIENCE». Proceedings of the III International Scientific and Practical Conference «Scientific Issues of the Modernity» (April 27, 2017, Dubai, UAE). 2017. No. 5(21), Vol. 1, May. P. 4–8.

10. Бартіш М.Я., Роман Л.Л. Теорія ігор. Львів: Видавничий центр ЛНУ, 2005. 120 с.

11. Dantu R., Kolan P. Risk management using behavior based Bayesian networks. *Intelligence and Security Informatics*. 2005. P. 165–184.

12. Bielza C., Li G., Larrañaga P. Multi-dimensional classification with Bayesian networks. Int. *J. Approx. Reason*. 2011.**52**. P. 705–727.

13. GAO Jian-bo, ZHANG Bao-wen, CHEN Xiao-hua, LUO Zheng Ontology-Based Model of Network and Computer Attacks for Security Assessment. *J. Shanghai Jiaotong Univ. (Sci.)*. 2013. **18**(5): 554–562.

14. Кононюк А.Е. Общая теория распознавания. Книга 1. Начала. Київ: Освіта України, 2012. 586 с.

15. Dharamkar B., Singh R. A review of cyber-attack classification technique based on data mining and neural network approach. *Int. J. Comput. Trends Technol. (IJCTT)*. 2014. **7**. P. 100–105.

16. Hodo E., Bellekens X., Hamilton A., Tachtatzis C., Atkinson R. Shallow and Deep Networks Intrusion Detection System: A Taxonomy and Survey. Available online: https://www.researchgate.net/publication/312170608_Shallow_and_Deep_Networks_Intrusion_Detection_System_A_Taxonomy_and_Survey.

17. Khristolyubova A.A., Konev A.A., Shelupanov A.A., Solovev M.L. Modeling threats to information security using IDEF0 methodology. In Proceedings of the IOP Conference Series Materials Science and Engineering. Tomsk, Russia. 23–26 April 2019. P. 1–6.

18. Лахно В.А., Гусєв Б.С., Смолій В.В., Блозва А.І., Касаткін Д.Ю., Осипова Т.Ю. Методи системного аналізу при формуванні політики інформаційної безпеки на транспорті. *Кібербезпека: освіта, наука, техніка*. 2021. № 4(12). С. 51–60. ISSN 2663-4023.

19. Khan R., McLaughlin K., Laverty D., Sezer S. STRIDE-based Threat Modeling for Cyber-Physical Systems. In Proceedings of the IEEE PES Innovative Smart Grid Technologies Conference Europe. Turin, Italy, 26–29 September 2017.

20. Scandariato R., Wuyts K., Joosen W. A descriptive study of Microsoft's threat modeling technique. Requir. Eng. 2015. **20**. P. 163–180.

21. Sion L., Yskout K., van Landuyt D., Joosen W. Solution-aware data flow diagrams for security threat modeling. In Proceedings of the 33rd Annual ACM Symposium on Applied Computing. Pau, France, 9–13 April 2018. P. 1425–1432.

22. Honkaranta, A.; Leppanen, T.; Costin, A. Towards Practical Cybersecurity Mapping of STRIDE and CWE — A Multi-Perspective Approach. In Proceedings of the 29th Conference of Open Innovations Association (FRUCT). Tampere, Finland. 12–14 May 2021.

23. Karahasanovic A., Kleberger P., Almgren M. Adapting Threat Modeling Methods for the Automotive Industry. In Proceedings of the 15th ESCAR Conference. Berlin, Germany. 7–8 November 2017.

24. Pell R., Moschoyiannis S., Panaousis E. Multi-Stage Threat Modelling and Security Monitoring in 5GCN. In Cybersecurity Issues in Emerging Technologies; CRC Press: Boca Raton. FL, USA. 2021. P. 59–76.

25. Lee C.C., Tan T.G., Sharma V., Zhou J. Quantum Computing Threat Modelling on a Generic CPS Setup. In International Conference on Applied Cryptography and Network Security. Springer: Cham, Switzerland, 2021. P. 171–190.

26. Van Landuyt D., Joosen W. A descriptive study of assumptions made in LINDDUN privacy threat elicitation. In Proceedings of the 35th Annual ACM Symposium on Applied Computing. Brno, Czech Republic. 30 March–3 April 2020. P. 1–8.

27. Deng M., Wuyts K., Scandariato R., Preneel B., Joosen W. A Privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements. *Requir. Eng*. 2011. **16**. P. 3–32.

28. Li E., Kang C., Huang D., Hu M., Chang F., He L., Li X. Quantitative Model of Attacks on Distribution Automation Systems Based on CVSS and Attack Trees. *Information*. 2019. **10**. 251.

29. Johnson P., Lagerstrom R., Ekstedt M., Franke U. Can the Common Vulnerability Scoring System Be Trusted? A Bayesian Analysis. IEEE Trans. Dependable Secur. Comput. 2016. **15**, P. 1002–1015.

30. Mantha B.. Jung Y.. Garcia B. Implementation of the Common Vulnerability Scoring System to Assess the Cyber Vulnerability in Construction Projects. In Proceedings of the Creative Construction Conference. Opatija, Croatia. 28 June – 1 July 2020. P. 117–124.

31. Czekster R.M., Morisset C. BDMPathfinder: A tool for exploring attack paths in models defined by Boolean Logic Driven Markov Processes. In Proceedings of the European Dependable Computing Conference. Munich, Germany, 13–16 September 2021. P. 83–86.

32. Falco G., Viswanathan A., Santangelo A. CubeSat Security Attack Tree Analysis. In Proceedings of the 8th IEEE International Conference on Space Mission Challenges for Information Technology. Pasadena, CA, USA. 26–30 July 2021. P. 1–9.

33. Mead N., Shull F., Spears J., Heibl S., Weber S., Cleland-Huang J. Crowd Sourcing the Creation of Personae Non Gratae for Requirements-Phase Threat Modeling. In Proceedings of the IEEE 25th International Requirements Engineering Conference. Lisbon, Portugal, 4–8 September, 2017. P. 404–409.

34. Omotunde H.. Ibrahim R. A Hybrid Threat Model for Software Security Requirement Specification. In Proceedings of the International Conference on Information Science and Security. Pattaya, Thailand. 19–22 December 2016. P. 1–4.

35. Luna J., Suri N., Krontiris I. Privacy-by-design based on quantitative threat modeling. In Proceedings of the Risk and Security of Internet and Systems. Cork, Ireland. 10–12 October 2012. P. 1–8.

36. Alberts C., Dorofee A., Stevens J., Woody C. Introduction to the OCTAVE Approach. In Introduction to the OCTAVE Approach; Software Engineering Institute, Carnegie Mellon University: Pittsburgh, PA, USA. 2003.

37. Saitta P., Larcom B., Eddingto M. Trike v.1 Methodology Document. 2005. Available online: https://www.octotrike.org/papers/ Trike_v1_Methodology_Document-draft.pdf (Last accessed 4 January 2022).

38. Nhlabatsi A., Hussein A., Fetais N., Khan K.M. Design and Implementation of a Threat-Specific Security Risk Assessment Tool. In Proceedings of the IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT). Doha, Qatar. 2–5 February 2020.

39. Shevchenko N., Chick T. A., O'Riordan P., Scanlon T. P., Woody C. Threat modelling: A summary of available methods. Carnegie Mellon University Software Engineering Institute. 2018. P. 1–24.

40. Yue Li, Teng Zhang, Xue Li, Ting Li. A Model of APT attack Defense Based On Cyber Threat Detection // Communications in Computer and Information Science, Cyber Security,15th International Annual Conference, CNCERT 2018. P. 122–134.

41. Верес Ю.О. Розподіл обмежених ресурсів в управлінні проектами. URL: https://science.lpnu.ua/ sites/default/files/journal-paper/2018/aug/14107/05.pdf.

42. Ferraiolo D., Kuhn D. Introduced formal model for role based access control. 15th national computer security conference. Oct 13–16, 1992. P. 554–563. URL: http://csrc.nist.gov/groups/sns/rbac/documents/role_based_access_control-1992.html

43. LaPadula L., Elliott J. Secure Computer Systems: A Mathematical Model. URL: http://www.albany.edu/acc/courses/ia/classics/bellla-padula1.pdf

44. McLean John. Security models. Encyclopedia of software engineering. URL: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.34.8561.

45. Кутковецький В. Я. Розпізнавання образів: навч. посіб. — Миколаїв: Вид-во ЧНУ ім. Петра Могили, 2017. 420 с. ISBN 978-966-336-384-4.

46. Сілагін О.В., Денисюк В.О. Онтологічне моделювання бази знань з організації подорожей *Український журнал інформаційних технологій*. 2022. Т. 4, № 1. С. 44–52.

47. Кирилюк Є.М., Дуб Б.С. Матричні методи оцінювання економічної безпеки підприємства. В: Актуальні проблеми економіки та управління в епоху глобальних викликів і загроз. Всеукр.

наук.-практ. конф., Дніпро, 26–27 квіт.У 2-х томах. Т. 1. Нац. метал. академія України. 2018. С. 270–272.

48. Cichocki A., Zdunek R., Phan A.-H., and Amari S. Nonnegative Matrix and Tensor Factorizations: Applications to Exploratory Multi-way Data Analysis and Blind Source Separation. Chichester. U.K.: John Wiley&Sons Ltd, 2009. 407 p.

49. Tensor Toolbox version 2.6 by Brett W. Bader, Tamara G. Kolda, Jimeng Sun, Evrim Acar, Daniel M. Dunlavy, Eric C. Chi, Jackson Mayo, et al. Copyright 2015, Sandia National Laboratories. Released February 6, 2015.

50. Никифоров О.В. Путятін В.Г**.** Нейромережеві моделі управління процесом функціонування систем захисту інформації. *Математичні машини і системи*. 2023. № 2. С. 34–43. ISSN 1028-9763.

51. Brain Maker Professional, Neural Network Simulation Software. User Guide and Reference Manual. California Scientific Software, 1993. 496 p.

52. Кононюк А.Ю. Нейронні мережі і генетичні алгоритми. Київ: «Корнійчук», 2008. 446 с.

53. Rostyslav Kryvyy, Serhii Tkachenko, Volodymyr Karkuljovskyy. Analysis of Frameworks for Developing Genetic Algorithms. Proc.of the VII-th International Conference MEMSTECH'2011. Lviv – Polyana, 2011. P. 209–210.

54. Дубровін В.І., Субботін С.О. Методи оптимізації та їх застосування в задачах навчання нейронних мереж: навч. посібн. — Запоріжжя: ЗНТУ, 2003. 136 с.

55. Руденко О.Г., Бодянський Є.В. Штучні нейронні мережі: навч. посібн. — Харків: ТОВ «Компанія СМІТ», 2006. 404 с.

56. Plett G.L. Adaptive inverse control of linear/nonlinear systems usingdynamic neural networks. *IEEE Trans. Neural Networks*. 2003. Vol. 5, N 2. P. 360–376.

57. Субботін С.О. Подання й обробка знань у системах штучного інтелекту та підтримки прийняття рішень. Запоріжжя: ЗНТУ, 2008. 341 с.

58. Глибовець М.М., Олецький О.В. Системи штучного інтелекту. Київ: КМ Академія, 2002. 366 с.

59. Axelrod R. The Structure of Decision: Cognitive Maps of Political Elites. Princeton University Press, 1976

60. Roberts F.S. Discrete Mathematical Models, with Applications to Social, Biological and Environmental Problems. Prentice-Hall, Englewood Cliffs, NJ, 1976. 559 p. ISBN-13: 978-0132141710.

61. Kosko B., Fuzzy Cognitive Maps. *International Journal of Man-Machine Studies* 1986. **24**. P. 65–75.

62. Kosko B. Fuzzy Thinking. Hyperion, 1993.

63. Carvalho J.P. and Tom J.A.B., Rule Based Fuzzy Cognitive Maps - Fuzzy Causal Relations // Computational Intelligence for Modelling, Control and Automation: Evolutionary Computation & Fuzzy Logic for Intelligent Control, Knowledge Acquisition & Information Retrieval, edited by M. Mohammadian, IOS Press, 1999

64. Bourke M.M., Fisher D.G.. Solution algorithms for fuzzy relation equations with max-product composition. *Fuzzy Sets and Systems.* 1998. Vol. 94. P. 61–69/

65. Глушков В.М. Теория алгоритмов. Киев: Изд-во КВИРТУ, 1961. 167 с.

66. Peterson James Lyle. (1981). Petri Net Theory and the Modeling of Systems. February 1981. Prentice Hall, Englewood Cliffs. 302 p. ISBN-10: 1080591176.

67. Дифучин А.Ю. Веб-сервіс моделювання дискретно-подійних систем // Магістерська дисертація з додатками. Київ: НТУУ «КПІ ім. Ігоря Сікорського», 2018. 95 с.

68. Herbert G. Markov models of social dynamics: Theory and applications. *ACMTrans. Intell. Syst. Technol*. 2013. Vol. 4, No. 3. Article 53. P. 1–19.

69. Ванд Ю., Стори В.С., Вебер Р. Онтологический анализ построения отношений в концептуальном моделировании. *Транзакции АСМ в системах баз данных (TODS*). 1999. Т. 24. Вып. 4. С. 494–528.

70. Грубер Т.Р. Подход к переводу спецификаций переносимых онтологий. *Приобретение знаний*. 1993. Т. 5.Вып. 2, С. 199–220.

71. Межуев В.И. Особенности компьютерного моделирования предметных областей и систем. *Штучний інтелект.* 2010. № 3. С. 665–663.

72. Gougen J.A., Thatcher J.W., Wagner E. An initial algebra approach to the specification, correctness and implementation of abstract data types. Current Trends in Programming Methodology (R. Yen ed.). Englewood Cliffs, NJ: Prentice Hall, 1978. P. 80–149.

73. Ganter B., Wille R. Formal Concept Analysis. Mathematical foundations. Berlin-Heidelberg: Springer-Verlag, 1999.

74. Mukhacheva N.N., Popov D.V. (2011). Ontologicheskie modeli i metody dlya upravleniya informatsionnointellektualnymi resursami organizatsii [Ontological models and methods for managing information and intellectual resources of an organizatio]. Vestnik UGATU – Bulletin of USATU, 14, 1(36), 123–135. URL: https://cyberleninka.ru/article/n/ontologicheskie-modeli-i-metody-dlya-upravleniya-informatsionno-intellektualnymi-resursami-organizatsii.pd

75. Буров Є.В., Пасічник В.В. Програмні системи на базі онтологічних моделей задач. *Вісник Національного університету «Львівська політехніка»*. Серія: Інформаційні системи та мережі: зб. наук. праць. 2015. № 829. С. 36–57.

76. Nikanorov S.P., Vybornov S.V., Ivanov A.Yu., Korshikov S.E., Kostyuk A.V., Kuchkarov Z.A., Mikheev V.V., Shalyapina S.K. Safety research. Ed. S.P. Nikanorova. Concept, 2006. 624 p. https://vestnik. socio.msu.ru › issue › download

77. Ivanov A.Yu., Nikanorov S.P., Garayeva Yu.R. Handbook of system-theoretic constructs. Series «Conceptual Analysis and Design». Methodology and technology. Concept, 2008. 314 p.

78. Koo B., Simmons W. Algebra of systems: a metalanguage for model synthesis and evaluation. *IEEE Transactions on systems, man and cybernetics*. 2009. Vol. 39, No. 3. P. 501–513.

79. Буров Є. В. Концептуальне моделювання інтелектуальних програмних систем/монографія. Львів: Вид-во Львівської політехніки, 2012. 432 с.

80. Nikitina N.K., Postnikov V.V. Development of a language for gender-structural explication of subject areas. Development and conceptual design of intelligent systems: Sat. abstracts of reports and messages. 1990. Part 1. P. 70–73.

81. Нестеренко О.В., Нетесін І.Є., Поліщук В.Б. Метод обчислень у задачах підтримки прийняття рішень щодо забезпечення безпеки. *Математичні машини і системи*. 2021, № 3. С. 47–59.

82. Додонов А.Г., Ландэ Д.В., Прищепа В.В., Путятин В.Г. Компьютерная конкурентная разведка. Киев: ТОВ «Інжиніринг», 2021. 357 с.

83. Büül Achim, Zöfel Peter. SPSS: Die Kunst der Informationsverarbeitung. Analyse statistischer Daten und Wiederherstellung verborgener Muster. München 2005. - 608 p.

84. ISO/IEC 13335-1: 2004 «Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management».

85. ISO/IEC TR 13335-3:1998 «Information technology — Guidelines for the management of information technology security — Part 3: Techniques for the management of information technology security».

86. ISO/IEC 15408-1-99 «Methods and means of ensuring security. Criteria for assessing information technology security. — Part 1. Introduction and general model».

87. ISO/IEC TR 13335-4:2000 «Information technology Guidelines for the management of information technology security — Part 3: Selection of safeguards».

88. Konev, A.; Shelupanov, A.; Kataev, M.; Ageeva, V.; Nabieva, A. A Survey on Threat-Modeling Techniques: Protected Objects and Classification of Threats. *Symmetry*. 2022. **14**, 549. https://doi.org/ 10.3390/ sym14030549.

89. STRIDE Treat Modeling: What You Need to Know. Available online: https://www.softwaresecued.com/stridemodeling (станом на 4 червня 2022).

90. Real World Threat Modeling Using the PASTA Methodology. Available online: https://owasp.org/www-pdf-archive/AppSecEU2012_PASTA.pdf (станом на 4 червня 2022).

91. LINDDUN Privacy Engineering. Available online: https://linddun.org (станом на 4 червня 2022).

92. Johnson P., Lagerstrom R., Ekstedt M., Franke U. Can the Common Vulnerability Scoring System Be Thrusted? A Bayesian Analysis. *IEEE Trans. Dependable Secur. Comput*. 2016. 15. P. 1002–1015.

93. Czekster R.M., Morisset C. BDMPathfinder: A tool for exploring attack path in models defined by Boolean Logic Driven Markov Processes, In Proceedings of the European Dependable Computing Conference. Munich, Germany 13–16 September 2021. P. 83–86.

94. Mead N., Shull F., Spears J., Heibl S., Weber S., Cleland-Huang J. Crowd Sourcing the Creation of Personae Non Grate for Requirements-Phase Threat Modeling. In Proceeding of the IEEE 25th International Requirements Engineering Conference. Lisbon, Portugal. 4–8 September 2017. P. 404–409.

95. Omotunde H., Ibrahim R. A Hybrid Threat Model for Software Security Requirement Specification. In Proceedings of the International Conference on Information Science and Security. Pattaya, Thailand, 19–22 December 2016. P. 1–4.

96. Luna J., Suri N., Krontiris I. Privacy-by-design based on quantitative threat modeling. In Proceedings of the Risk and Security of Internet and System. Cork, Ireland. 10–12 October 2012. P. 1–8.

97. Saitta P., Larcom B., Eddington M. Trike v.1 Methodology Document. 2005. Available online: https://www.octotrike.org/papers/Trike_v1_Methodology_Document-draft.pdf (станом на 4 червня 2022).

98. Alberts C., Dorofee A., Stevens J., Woody C. Introduction to the OCTAVE Approach. Software Engineering Institute, Carnegie Mellon University: Pittsburgy, PA, USA, 2003. 27 p.

99. Nhlabatsi A., Hussein A., Fetais N., Khan K.M. Design and Implementation of a Threat-Specific Security Risk Assessment Tool. In Proceedings of the IEEE International Conference on Informatics, IoT, and Enabling Thechnologies (ICIoT). Doha, Qatar. 2–5 February 2020.

100. Bourbaki Nicolas. Eléments de Mathématique. XX. Première partie. Les structures fondamentales de l'Analyse. Livre I Théorie des Ensembles. Hermann et Cie, Paris, 1956. Première édition. 118 p.

Надійшла до редакції 03.11.2023