УДК 004.056, 004.75

В. Дудикевич, Ю. Гарасим
Національний університет “Львівська політехніка”,
кафедра захисту інформації

ВИБІР ВАРІАНТА СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ЗА КРИТЕРІЄМ ЖИВУЧОСТІ В УМОВАХ НЕВИЗНАЧЕНОСТІ ВПЛИВУ ДЕСТАБІЛІЗУЮЧИХ ФАКТОРІВ

Розроблено метод вибору варіанта систем захисту інформації для корпоративних мереж зв’язку в умовах невизначеності впливу дестабілізуючих факторів за допомогою використання теорії підтримки прийняття рішень, який відрізняється від інших можливістю знайти рішення, яке буде оптимальним за критерієм живучості, що найкраще відповідатиме змісту та умовам задачі у випадку трьох інформаційних ситуацій про ймовірності появи дестабілізуючих факторів.

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

The method of information security system choosing for enterprise communication system under uncertainty destabilizing factors influences was developed using the decision support theory. This method gives an opportunity to find an optimal solution for the survivability criteria that corresponds to the problem contents and conditions of three information situations about destabilizing factors influences probability case because is different from others.

Keywords: survivability, survivability assessment, information security system.

Вступ

Системи захисту інформації (СЗІ) належать до такого класу систем, які є нестаціонарними, високодинамічними, з такою динамікою розвитку, яку важко прогнозувати [1–5]. Нестабільність дестабілізуючих факторів (ДФ) визначає високий динамізм зміни зовнішнього та внутрішнього середовищ (некерованих змінних системи), а часткові директивні впливи (атаки) роблять часові ряди короткими та неоднорідними, що переважно унеможливлює достовірне прогнозування зміни характеристик навколишнього середовища.

Загалом перераховані причини призводять до обмеження (неповноти) або неточності (неоднозначності), тобто до невизначеності інформації як про характеристики системи захисту, так і про ситуацію прийняття рішення, про вибір її модифікації для корпоративних мереж зв’язку (КМЗ) з використанням оцінки її живучості [6–10]. Ця невизначеність має принциповий характер і її неможливо подолати детермінізованими способами. У зв’язку з цим потрібно використовувати інші підходи до задачі прийняття рішень про використання системи захисту КМЗ за критерієм живучості.

1. Метод вибору варіанта системи захисту за критерієм живучості в умовах невизначеності впливу дестабілізуючих факторів

Вибір варіанта СЗІ за критерієм живучості ускладнений у зв’язку з тим, що в реальних умовах інформація про ймовірності появи дестабілізуючих факторів ($a_n = P(A_n)$) обмежена або відсутня повністю. Тому рішення доводиться приймати в умовах невизначеності. В цьому випадку скористаємося рекомендаціями теорії прийняття рішень [11, 12]. Задачу вибору СЗІ для КМЗ за критерієм живучості сформулюємо так [13].

Серед множини взаємовиключних варіантів систем $S=\{S_1,S_2,...,S_m\}$ в умовах впливу ДФ, що створюють повну групу подій $A=\{A_1,A_2,...,A_n\}$ за наявності множини оцінювальних функцій $F=\{l_{jk}\}, j=1,...,m, k=1,...,n$ необхідно знайти вирішення, яке буде оптимальним за критерієм живучості, що найкраще відповідатиме змісту та умовам задачі. В цьому випадку l_{jk} – значення детермінованого показника живучості S_j-го варіанта системи у разі впливу A_k-го ДФ. Формування критерію залежить від рівня інформованості та можливості виникнення тих або інших станів зовнішнього середовища, в окремому випадку від умовної ймовірності появи подій A_k. Можливі такі інформаційні ситуації:

1) задано розподіл ймовірностей a_k появи подій A_k, причому сума ймовірностей дорівнює одиниці;

2) задана система бажаних апріорних ймовірностей у вигляді нерівностей $a_1 \geq a_2 \geq ... \geq a_n$ або $a_1 > a_2 > ... > a_n$, причому сума ймовірностей дорівнює одиниці;

3) розподіл ймовірностей є невідомим.

Для першої інформаційної ситуації використовуватимемо критерії Байєса, максимуму ймовірності оцінкового функціонала модального критерію. Відповідно до критерію Байєса варіант системи виберемо із умови

$$L=\max_{(S_j)}\left(\sum_{k=1}^{n} a_k l_{jk}(S_j)\right).$$

Для другої інформаційної ситуації після ранжування подій A_k приймемо такі оцінки для ймовірностей a_k:

$$\overline{a_k}=2(n-k+1)/n(n+1), k=1,...,n,$$
$$\overline{a_k}=(n-k+2)/n2^k, k=1,...,n,$$

що дають змогу проектувальнику СЗІ КМЗ звести задачу до першої інформаційної ситуації.

Критерій Байєса має недолік, який пов'язаний з тим, що вибрана система захисту, яка є найкращою у середньому, може мати низьку властивість живучості в окремих аварійних ситуаціях. Щоб не допустити ризику при виборі варіанта системи, оптимального за Байєсом, але який характеризуватимемо повною втратою якості функціонування СЗІ у деяких ситуаціях за впливу ДФ, доцільно використовувати критерій Ходжеса–Лемана. В цьому випадку оптимальну систему визначатимемо з умов

$$L\left(\{\overline{a_k}\}, S_{j0}\right)=\max_{(S_j)}\left(\sum_{k=1}^{n}\overline{a_k} l_{jk}(S_j,A_k)\right), l_{jk}\left(S_{j0},A_k\right)>\beta,$$
$$\min_{(S_j,A_k)} l_{jk}(S_j,A_k)<\beta<\max_{(S_j,A_k)} l_{jk}(S_j,A_k).$$

Для реалізації наведеного матеріалу необхідно уточнити тип показника живучості l в математичній моделі системи захисту. Але саме тут і виникають головні складності в оцінці живучості за такого підходу, оскільки для того, щоб визначити залежність l від стану елементів і зовнішнього середовища, треба глибоко проникнути в сутність фізичних процесів у системі. В багатьох випадках для отримання такої залежності необхідно досліджувати динамічну модель СЗІ.

2. Аналіз особливостей і постановка задачі вибору варіанта системи захисту інформації в умовах невизначеності

Проблему прийняття рішення про вибір варіанта системи захисту інформації в загальному випадку розділимо на три основні етапи:

- сформувати множину допустимих рішень X;
- визначити метрики, в яких порівнюватимуться допустимі рішення $x \in X$ (задача оцінювання);
- вибрати із допустимої множини ефективне (найкраще) рішення $x^0 \in X$ (задача оптимізації).

Множину допустимих рішень X задамо на основі змістового аналізу конкретної задачі, в неявному вигляді як підобласть області існування системи, яка обмежена співвідношеннями у вигляді нерівності

$$h_s(x, q_h) \le 0; s = \overline{1, S} \tag{1}$$

і рівності

$$g_l(x, q_g) = 0; l = \overline{1, L}, \tag{2}$$

де x – N-вимірна ($x \in X^N$) керована змінна; h_s, g_l – оператори, які визначають структуру математичної моделі відповідного обмеження; q_h, q_g – кількісні параметри відповідних обмежень.

Розв'язання задачі оптимізації, тобто визначення найкращого розв'язку $x^0 \in X$, пов'язане із формалізацією поняття «найкраще». Для цього знайдемо метрику, в якій порівняємо якість рішень $x \in X$. Нехай в загальному випадку кожне рішення $x \in X$ опишемо n різними кількісними характеристиками (окремими критеріями) $k_i(x), i = \overline{1, n}$. Вважатимемо, що на множині $k_i(x)$ існує модель оцінювання, яка дає змогу отримати скалярну, кількісну оцінку будь-якого рішення $x \in X$

$$P(x) = G[a_i, k_i(x)], \tag{3}$$

де G – оператор моделі, який визначає її структуру; a_i – кількісні параметри моделі, наприклад $a_n = P(A_n)$.

В загальному випадку (3) є функцією цілі системи. Враховуючи співвідношення (1)–(3), задачу умовної оптимізації (математичного програмування) запишемо у вигляді

$$\begin{gathered} x^0 = \arg extr_{x \in X} P(x); x \in R^N; \\ h_s(x, q_h) \le 0; s = \overline{1, S}, \\ g_l(x, q_g) = 0; l = \overline{1, L}. \end{gathered} \tag{4}$$

Системи захисту інформації корпоративних мереж зв'язку мають характерні особливості, які обмежують використання різних методів для вибору її структури за критерієм живучості [1–10]: структура об'єкта нестаціонарна (змінюється як у результаті внутрішнього розвитку, зокрема при вимірюванні кількісних значень параметрів, так і під впливом зовнішнього середовища, в окремих випадках в результаті дії зовнішніх директивних керуючих впливів (атак зловмисників)); велика кількість параметрів є нестаціонарними; наявність великої кількості нелінійних залежностей; для об'єкта характерна множина зворотних зв'язків; об'єкт не має кінцевого горизонту планування; часті зовнішні директивні керуючі впливи розбивають часові ряди вихідних змінних на короткі, статистично неоднорідні послідовності, що ускладнює коректне розв'язання задачі прогнозування, визначення статистичних параметрів процесів і оцінювання їхніх значень.

У цих умовах необхідно вибрати ефективну стратегію поведінки, тобто реалізувати задачу прийняття рішення. Проблема містить три задачі:

- синтез адекватної імітаційної математичної моделі системи;
- визначення цільового функціонала;
- вибір правила (алгоритму) прийняття рішення.

Вважатимемо, що імітаційна модель об'єкта задана. На відміну від детермінованих систем, для моделювання нестаціонарних, тобто змінних у часі систем, необхідно задати часовий сценарій поведінки навколишнього середовища $y(t)$. Кожному сценарію відповідатиме деяка оптимальна поведінка СЗІ, тобто траєкторія зміни структури, параметрів, керуючих змінних. Формально це означає, що оптимізаційна модель (4) матиме вигляд:

$$\begin{gathered} x^0 = \arg extr_{x \in X} P(x, y, t); x \in R^N; \\ h_s(x, q_h, y, t) \le 0; s = \overline{1, S}, \\ g_l(x, q_g, y, t) = 0; l = \overline{1, L}, \end{gathered} \tag{5}$$

Із моделі (5) видно, що кожній конкретній реалізації сценарію розвитку зовнішнього середовища $y(t)$ відповідає деяке конкретне ефективне рішення x^0. Зазначимо, що зовнішнє середовище не повністю кероване і контрольоване навіть із позиції метасистеми [14–17]. Це означає, що на рівні конкретної локальної системи точний сценарій зміни зовнішнього середовища невідомий і відповідно до вищесказаного його важко прогнозувати. Тому можна робити лише евристичні припущення про можливі значення $y(t)$. В таких умовах рішення x^0, вибране для конкретного сценарію $y(t)$, для іншого сценарію $y'(t)$ може виявитися недопустимим. Це зумовлено тим, що екстремальне розв'язання задачі умовного математичного програмування завжди міститься на межі допустимої області X. Оскільки для нестаціонарних систем, як видно із (5), обмеження, які визначають область допустимих рішень X, явно залежать від сценарію зміни зовнішнього середовища $y(t)$, то рішення x^0, вибране для конкретного $y(t)$ для іншого сценарію $y'(t)$, буде в кращому випадку неефективним, а в гіршому – недопустимим або катастрофічним. Останнє пов'язано з тим, що через нелінійність нестаціонарних систем і особливо через наявність в них булевих змінних, в деяких випадках система стає нестійкою, а її модель некоректною за Адамаром [18–21]. Звідси випливає, що невелика зміна $y(t)$ призводить до непропорційно великих змін вихідних змінних. Це може призвести до катастрофічних наслідків, які для СЗІ КМЗ можуть означати порушення конфіденційності, цілісності, доступності інформації, яка в ній функціонує.

Разом з тим, важливо зазначити, що для нестаціонарних систем необхідні спеціальні проблемно-орієнтовані методи прийняття рішень, бо такі методи, як оперативне регулювання та адаптивне управління, є неефективними.

Процедуру прийняття рішення в умовах невизначеності пропонуємо розділити на два етапи.

На першому етапі формуємо множину альтернативних виходів $x_k = \{x_{k_i}\}, i = \overline{1,n}$, що відповідають можливим сценаріям поведінки зовнішнього середовища $y_i(t), t \in [t_0, t_k], i = \overline{1,n}$, де t_0, t_k – відповідно початковий та кінцевий моменти інтервалу прийняття рішення. Для того, щоб розв'язати цю задачу, потрібна математична модель, яка повинна містити достатньо адекватну імітаційну (наприклад, задана мережею Петрі) модель, яка дасть змогу отримувати відповіді на питання типу «що буде, якщо…». Крім цього, вважатимемо, що цільова установка на момент прийняття рішення у момент t_0 є стабільною (незмінною). Це дає змогу сформулювати відповідну їй цільову функцію, яку можна оптимізувати, вибравши відповідні значення керованих змінних x. Отже, для кожного конкретного сценарію $y_i(t)$ на момент t_k буде визначено стан x_{k_i}, який екстремізує цільову функцію системи. В результаті отримаємо множину можливих станів системи $x_k = \{x_{k_i}\}, i = \overline{1,n}$.

Завдання другого етапу полягає у виборі стратегії поведінки системи $x(t_0)$, тобто в момент t_0, на основі аналізу множини станів X_k. Передбачимо, що на інтервалі часу $t \in [t_0, t_k]$ зміна початкового рішення $x(t_0)$ є неможливою [22].

3. Математична модель і алгоритми формування множини альтернатив

Для того, щоб сформувати множину допустимих альтернативних рішень (X_k), яку використовуватимемо як вихідну інформацію під час прийняття рішень в умовах ризику та невизначеності, необхідно: а) сформувати оптимальні опорні рішення; б) оцінити їхню чутливість і ефективність в умовах варіацій сценаріїв поведінки зовнішнього середовища.

3.1. Формування множини опорних рішень

Припускаємо, що для системи, яку вважаємо відомою, існує оптимізаційна модель виду (5), яку для зручності подальшого аналізу з урахуванням (3) подамо у вигляді

$$\begin{gathered} x^0 = \arg extr_x G(a_i, k_i(x), y, t); x \in R^N, y \in R^M; \\ h_s(x, q_h, y, t) \le 0; s = \overline{1,S}, \\ g_l(x, q_g, y, t) = 0; l = \overline{1,L}. \end{gathered} \tag{6}$$

Цільова установка на момент прийняття рішення t_0 є незмінною і не залежить від сценарію поведінки зовнішнього середовища $y(t)$. Це означає, що перелік керованих змінних x, структура цільової функції (оператор G) і склад окремих критеріїв $k_i(x), i=\overline{1,n}$ залишаються стабільними. В цьому випадку $y(t)$ впливає лише на кількісне значення параметрів a_i, структуру і параметри моделей обчислення окремих критеріїв $k_i(x)$, тобто

$$a_i(x) = f_a[y(t)],$$
$$k_i(x) = f_k(x, y, t).$$

Залежно від зовнішнього середовища може змінюватися структура обмежень, тобто вид операторів h_s, g_l, кількість обмежень, тобто S та L, значення параметрів q_h, q_g.

Наявність моделі системи (6) дає змогу визначити для кожного конкретного сценарію поведінку зовнішнього середовища $y_j(t), j=\overline{1,m}$, відповідне йому оптимальне рішення x_j^0, яке надалі називатимемо опорним. Зазначимо, що в окремому випадку $y(t)$ може не залежати від часу на інтервалі $t\in[t_0,t_k]$, а бути постійним, наприклад, $y(t)=y(t_0)$ [22].

Отже, визначення множини опорних рішень $x_j, j=\overline{1,m}$ пов'язане із формуванням вихідних сценаріїв поведінки зовнішнього середовища $y_j(t)$. Існують два підходи до розв'язання цієї задачі – евристичний та формальний.

У першому випадку можливі конкретні сценарії поведінки зовнішнього середовища, їхню кількість і параметри формують експерти-аналітики на інтуїтивному рівні, що не виключає використання на різних етапах попереднього аналізу формальних процедур [23, 24]. Другий підхід орієнтований на створення деяких більше або менше формалізованих процедур формування сценаріїв $y_j(t)$.

3.2. Формування альтернативних рішень і оцінка їхньої якості

Метою цього етапу є оцінювання ефективності (стійкості) опорних рішень в умовах зміни сценарію поведінки зовнішнього середовища $y(t)$.

У результаті реалізації попереднього етапу визначено декілька опорних рішень x^0. Кожне з них є оптимальним в межах коректності моделей (4.6) і конкретного сценарію $y(t)$. Щоб спростити подальший аналіз, але без втрати узагальненості, розглянемо одне опорне рішення x^0. Його отримаємо для конкретної реалізації зовнішнього середовища $y_0(t)$ і опишемо значеннями керованих змінних $x^0=\{x_v\}, v=\overline{1,N}$, які на інтервалі прийняття рішення $t\in[t_0,t_k]$ за визначенням є незмінними. Через нестабільність зовнішнього середовища реальний сценарій його змінюється, тобто $y_k(t)$ є неоптимальним. Необхідно визначити якісні та кількісні наслідки (необов'язково негативні) цієї неоптимальності. Для цього синтезуємо математичну модель оцінки цих наслідків:

- зміна цільового функціонала, без зміни обмежень, які визначають область допустимих значень керованих змінних;
- трансформація обмежень за незмінного цільового функціонала;
- одночасна зміна цільового функціонала і обмежень.

Розглянемо математичні моделі оцінки наслідків варіацій $y(t)$ у кожному із виділених випадків [22].

Оцінка наслідків зміни цільової функції. В загальному випадку, що випливає із (6), цільову функцію можна подати у вигляді

$$P=[a_i, k_i(x), y, t], c\in R^N, y\in R^M, \qquad (7)$$

де a_i – кількісні параметри функції; $k_i(x)=f_i(x)$ – окремі критерії, $i=\overline{1,n}$.

Цільова установка на момент прийняття рішення є незмінною, тому вважатимемо, що оператор G не залежить від $y(t)$, а зовнішнє середовище може частково або повністю змінювати кількісні характеристики $a_i, i=\overline{1,n}$ і вид операторів формування окремих критеріїв $f_i(x)$. Значення керованих змінних залишимо у всіх випадках незмінними $x=x^0$, тобто такими, що відповідають сценарію $y(t)$.

Функцію цілі запишемо у вигляді

$$P=\sum_{i=1}^{n} a_i(y)x_i, \tag{8}$$

де y – зовнішні некеровані змінні.

Нехай x^0 – оптимальне (опорне) рішення, яке отримане з урахуванням обмежень за моделлю (6) для конкретного сценарію зовнішніх умов $y_0(t)$. Значення цільової функції (8) в цьому випадку дорівнюватиме

$$P^0=\sum_{i=1}^{n} a_i(y)x^0,$$

а для будь-якої іншої конкретної реалізації сценарію зміни параметрів зовнішнього середовища $y_j(t), j=\overline{1,m}$.

$$P_j=\sum_{i=1}^{n} a_i(y_j)x^0.$$

Оцінка наслідків зміни параметрів зовнішнього середовища у цьому випадку дорівнюватиме

$$\Delta P_j=\sum_{i=1}^{n} a_i(y_0)x^0-\sum_{i=1}^{n} a_i(y_j)x^0.$$

У загальному випадку можна записати, що цільова функція дорівнює

$$P=G(x,y),$$

її оптимальне значення для $y(t)$

$$P=G[x^0,y_0(t)],$$

а оцінка наслідків зміни сценарію розвитку зовнішнього середовища щодо опорного рішення x^0

$$\Delta P=P^0-G[x^0,y_j(t)], j=\overline{1,m}. \tag{9}$$

Розглянемо визначення наслідків зміни обмежень. Нехай цільова функція (7) є стабільною, тобто не залежить від варіацій вектора зовнішніх умов $y(t)$, але останній визначає зміни обмежень в моделі (6). Такі зміни можуть стосуватися видів операторів нерівностей $h_s, s=\overline{1,S}$ і рівностей $g_l, l=\overline{1,L}$, їхніх кількісних параметрів q_h, q_g і навіть кількості обмежень S та L. Отже,

$$h_s=f_s(y); g_l=f_l(y); \tag{10}$$

$$q_h=f_h(y); q_g=f_g(y); \tag{11}$$

$$S=f_1(y); L=f_2(y). \tag{12}$$

Параметр Y призводить до деформації області допустимих рішень X. Вважаємо, що математичні моделі (10)–(12) відомі. Загалом моделі (10)–(12) означають, що зміна вектора зовнішніх умов

$$X=\Theta[y],$$

в той час як опорне рішення x^0 за визначенням є незмінним. У результаті можуть виникнути дві ситуації

$$x^0 \in X(y); x^0 \notin X(y).$$

В першому випадку опорне рішення x^0 задовольняє усі нові обмеження і система не зазнає прямих втрат (залишається живучою). Можна вести мову лише про упущені можливості, оскільки опорне рішення в загальному випадку не є оптимальним в нових умовах.

Друга ситуація означає, що опорне рішення не належить новій допустимій області, тобто не задовольняє усі або окремі обмеження. Це призводить до прямих втрат системи. Величина сумарних втрат за рахунок зміни обмежень-рівностей дорівнюватиме

$$\Delta P_g = \sum_{i=1}^{L(y)} H_l \left| g_l(x^0, y) \right|, \tag{13}$$

де H_l – оператор (лінійний або нелінійний), який визначає величину втрат за порушення i-го обмеження, $L(y)$ – кількість обмежень-рівностей залежно від конкретної реалізації y.

Модуль в (13) беремо для того, щоб вказати, що будь-яке порушення обмеження рівності незалежно від його знака призводить до негативних наслідків.

На відміну від (13), сумарні втрати за рахунок порушення обмежень нерівностей дорівнюватимуть

$$\Delta P_h = \sum_{s=1}^{S(y)} \delta_s \left| H_s h_s(x^0, y) \right|, \tag{14}$$

де H_s – оператор штрафу за порушення S-го обмеження; $S(y)$ – кількість обмежень-нерівностей залежно від Y

$$\delta_s = \begin{cases} 0, \textit{ якщо нерівність задовольняється}, \\ 1, \textit{ в іншому випадку}. \end{cases} \tag{15}$$

Загальні втрати у разі порушення обмеження при зміні поведінки зовнішнього середовища $y(t)$ дорівнюватимуть

$$\Delta P_y = \sum_{i=1}^{L(y)} H_l \left| g_l(x^0, y) \right| + \sum_{s=1}^{S(y)} \delta_s \left| H_s h_s(x^0, y) \right|, \tag{16}$$

з урахуванням (15). Зазначимо, що ці втрати завжди недодатні, тобто

$$\Delta P_y \le 0.$$

Розглянемо оцінку комплексних наслідків зміни вектора Y. У багатьох випадках зміна вектора Y або деяких його компонент призводять до комплексних наслідків, тобто до одночасних змін функцій цілі та обмежень. З урахуванням (9), (14) та (16) математична модель оцінки комплексних наслідків зміни сценарію поведінки зовнішнього середовища $y_j(t)$ матиме вигляд:

$$\Delta P_{kj} = F[x^0, y_0(t)] - F[x^0, y_j(t)] + \sum_{i=1}^{L(y)} H_l \left| g_l, (x^0, y_j(t)) \right| + \sum_{s=1}^{S(y)} \delta_s \left| H_s h_s(x^0, y_j(t)) \right|; \tag{17}$$

$$\delta_s = \begin{cases} 0, \textit{ якщо } s - \textit{та нерівність задовольняється}, \\ 1, \textit{ в іншому випадку}. \end{cases}$$

Значення ΔP_{kj} може бути як від'ємним, так і додатним.

Припустимо, що математична модель (17) визначена, на її основі для кожного опорного рішення $x_j{}^0$ обчислимо оцінку наслідків зміни поведінки зовнішнього середовища для кожної конкретної реалізації сценарію $y_j(t)$. Для того, щоб різні опорні рішення можна було порівнювати між собою за ефективністю та рівнем стійкості до зміни характеристик зовнішнього середовища, проаналізуємо усі $x_j{}^0$ для однакового складу зовнішніх змінних $y_j(t)$. Результати такого аналізу наведемо у вигляді таблиці.

Матриця оцінок наслідків варіацій сценаріїв поведінки зовнішнього середовища

Реалізація $y_j(t)$ / Опорні рішення x_j^0	$y_1(t)$	$y_2(t)$	…	$y_m(t)$
$x_1^0[y_1(t)]$	$P_{11}^0[x_1^0, y_1(t)]$	$\Delta P_{12}[x_1^0, y_2(t)]$	…	$\Delta P_{1m}[x_1^0, y_m(t)]$
$x_2^0[y_2(t)]$	$\Delta P_{21}[x_2^0, y_1(t)]$	$P_{22}^0[x_2^0, y_2(t)]$	…	$\Delta P_{2m}[x_2^0, y_m(t)]$
…	…	…	…	
$x_m^0[y_m(t)]$	$\Delta P_{m1}[x_m^0, y_1(t)]$	$\Delta P_{m2}[x_m^0, y_2(t)]$	…	$P_{mm}^0[x_m^0, y_m(t)]$

У цій таблиці по діагоналі запишемо значення функції цілі для кожного із опорних рішень x_j^0, що відповідають реалізації зовнішніх умов $y_j(t)$, а всі інші елементи кожного рядка будуть оцінками наслідків варіацій $y_j(t), j=\overline{1,m}$. Таблиця містить вихідну інформацію для прийняття ефективного рішення про структуру СЗІ КМЗ за критерієм живучості.

4. Методика та критерії вибору ефективного рішення про структуру системи захисту інформації

Таблиця містить декілька опорних рішень, оцінки їхньої якості в оптимальних умовах P_j^0, а також оцінки наслідків можливих змін сценаріїв поведінки зовнішнього середовища $y_j(t)$. На підставі цієї інформації проектувальнику СЗІ КМЗ необхідно вибрати єдине рішення.

Розв'язання цієї задачі прийняття рішення пов'язане із визначенням деякого показника якості. В детермінованих системах і за повної поінформованості людина, яка приймає рішення (ЛПР), критерієм вибирає комплексну цільову функцію, що враховує властивості системи і витрати на її досягнення, які приводять до скалярного виду. Правило прийняття рішення в цьому випадку полягає у пошуку такого рішення x^0, яке екстремізує цільову функцію [22].

Прикладом такого підходу є математична модель (6). Реалізувавши її, отримаємо для кожної j-ї конкретної ситуації опорне рішення x_j^0 і відповідне йому значення цільової функції (діагональні елементи таблиці). Відповідно єдиним вибираємо опорне рішення, якому відповідає максимальне значення цільової функції.

Реалізація такого алгоритму в умовах невизначеності може призвести до негативних наслідків. В умовах невизначеності необхідно враховувати не лише ефективність рішення, але і його стійкість до зміни умов. Кількісну інформацію про стійкість опорних рішень x_j^0 до варіацій сценаріїв зміни зовнішнього середовища $y_j(t)$ дають відповідні значення ΔP_{ij}^0 (див. таблицю). Доцільно використовувати цю інформацію для прийняття рішення. Для цього виберемо відповідні критерії і сформуємо правило прийняття рішення.

Розв'язання цієї задачі суттєво залежить від рівня неповноти вихідної інформації і форми її подання. Залежно від цього розрізнятимемо дві групи задач прийняття рішення:

- в умовах ризику;
- в умовах невизначеності.

Незважаючи на принципову відмінність детермінованих систем від систем з різним рівнем невизначеності параметрів, нескладно простежити методологічну аналогію процедур прийняття рішення в обох випадках. Так, множину можливих рішень, яку визначено у таблиці, можна інтерпретувати як аналог наближеної області компромісів. Якість кожного із цих рішень характеризуємо двома локальними числовими критеріями ефективності і можливих втрат. Багато-

критерійні задачі прийняття рішення є некоректними за Адамаром [18–20] і для їх регулювання необхідно сформувати узагальнену скалярну багатофакторну (у цьому випадку двокритерійну) оцінку якості. Можливі варіанти таких критеріїв розглянемо нижче.

4.1. Прийняття рішень про структуру системи захисту інформації в умовах ризику

Методи прийняття рішень про структуру системи захисту інформації в умовах ризику базуються на припущенні, що ЛПР відомі ймовірності реалізації різних ситуацій, тобто розглядаємо випадок, коли ймовірна реалізація різних сценаріїв поведінки зовнішнього середовища $y_j(t)$. В цьому випадку як критерій оцінки різних рішень використаємо математичне сподівання цільової функції

$$M(P_i^0) = \sum_{j=1}^{m} V_j (P_{ij} + \Delta P_{ij}) \tag{18}$$

де V_j – ймовірнісна реалізація j-ї ситуації (сценарію).

Правило прийняття рішення в цій ситуації матиме вигляд:

$$x^0 = \arg\max_i \sum_{j=1}^{m} V_j (P_{ij} + \Delta P_{ij}), i = \overline{1,m}, \tag{19}$$

передбачимо, що розглянуті $y_j(t), j = \overline{1,m}$ сценарії утворюють повну групу несумісних випадкових подій і відповідно $\sum_{j=1}^{m} V_j = 1$.

У цьому випадку ймовірності V_j невідомі (прийняття рішень в умовах невизначеності), пропонуємо вважати усі можливі ситуації $j = \overline{1,m}$ рівноймовірними, тобто

$$V_j = 1/m.$$

У цьому випадку критерій (18) перетворюється на критерій Лапласа, а правило прийняття рішень (19) матиме вигляд

$$x^0 = \arg\max_i \sum_{j=1}^{m} (P_{ij} + \Delta P_{ij}), i = \overline{1,m},$$

оскільки V_j перетворюється на масштабний коефіцієнт, що не впливає на розміщення екстремуму та ним можна знехтувати.

Розглянуті ймовірнісні критерії є узагальненою двокритерійною скалярною оцінкою якості можливих альтернатив (рішень), оскільки враховуємо сумарну ймовірнісну оцінку як додатного ефекту (доданки P_{ij}), так і можливих втрат (доданки ΔP_{ij}). За формою ця оцінка є типовою для адитивної багатофакторної оцінки з однією відмінністю, яка полягає в тому, що всі доданки мають однакову розмірність. У зв'язку з цим не потрібно приводити їх до ізоморфного вигляду (нормалізації), а роль коефіцієнтів міри a_i виконують ймовірності V_j.

Разом із цим ймовірнісний підхід не є універсальним, що зумовлено двома причинами [22]:

- складністю визначення ймовірності V_j реалізації різних ситуацій, особливо для нестаціонарних систем (зокрема системи захисту інформації) з короткими інтервалами статичної однорідності;
- неможливістю коректної інтерпретації багатьох класів систем як стохастичних.

Це означає, що існують системи, для яких ймовірнісний підхід до прийняття рішення є некоректним.

4.2. Прийняття рішень в умовах невизначеності

Особливістю цієї групи задач прийняття рішень є відсутність апріорної інформації (навіть ймовірнісної) про можливості реалізації різних станів системи (різних сценаріїв). Загальною основою для визначення ефективного рішення в цих умовах є компроміс між його ефективністю і

стійкістю. Правило реалізації компромісу визначатимемо критерієм вибору рішення. Більшість відомих критеріїв прийняття рішень [12] в умовах невизначеності є окремими випадками адитивної схеми компромісу.

Задамо допустиму множину рішень X. На цій множині визначено два критерії $k_1(x)$ та $k_2(x)$, перший з яких характеризує ефект, а другий стійкість рішення. Для простоти вважатимемо, що ці два критерії мають однакову розмірність. Тоді загальна схема вибору компромісного рішення набуде вигляду

$$x^0 = \arg\max_{x\in X} \sum_{i=1}^{2} a_i k_i(x); \sum_{i=1}^{2} a_i = 1.$$

Вибір рішень a_i визначає конкретний вид критерію прийняття рішень і відповідну йому схему компромісу. Розглянемо деякі окремі випадки.

Критерій оптиміста. Цьому критерію відповідає таке значення вагових коефіцієнтів: $a_1 = 1, a_2 = 0$. Це означає, що під час вибору рішення враховуємо лише його ефективність. Позначимо через $P_{ij}(x)$ ефективність рішення

$$P_{ij}(x) = P_{ij} + \Delta P_{ij}, i = \overline{1,m}, j = \overline{1,m},$$

де $P_{ij}, \Delta P_{ij}$ – відповідні елементи таблиці 1.

Тоді схема прийняття рішення матиме вигляд

$$x^0 = \arg\max_i \max_j P_{ij}(x),$$

Тобто вибираємо рішення, яке має максимальне значення цільової функції за найбажанішого сценарію розвитку зовнішнього середовища $y_j(t)$.

Критерій Вальда (песиміста). В цьому випадку $a_1 = 0, a_2 = 1$, а відповідно рішення приймаємо лише з урахуванням його стійкості. Найстійкішим є максимальне рішення

$$x^0 = \arg\max_i \min_j P_{ij}(x).$$

Це рішення вибираємо у випадку найнегативнішого сценарію розвитку зовнішнього середовища $y_j(t)$, що і забезпечує в цих умовах гарантований результат.

Критерій Гурвіца. В цьому випадку $a_1 = b, 0 \le b \le 1; a_2 = (1-b)$. Відповідно оцінка якості x_i^0 опорного рішення має вигляд

$$P_i^0 = \left\lfloor \max_j P_{ij}(x) \right\rfloor b + \left\lfloor \min_j P_{ij}(x) \right\rfloor (1-b),$$

а правило вибору ефективності рішення

$$x^0 = \max_i P_i^0 = \max_i \left\{ \left\lfloor \max_j P_{ij}(x) \right\rfloor b + \left\lfloor \min_j P_{ij}(x) \right\rfloor (1-b) \right\}.$$

Як бачимо, критерій Гурвіца є універсальним, оскільки дає змогу реалізувати як розглянуті вище окремі критерії, так і будь-які інші вподобання ЛПР. Принциповим є те, що величину параметра b задає ЛПР на основі евристичних положень і не існує формальних методів визначення b [22].

Висновки

1. Розроблено метод вибору варіанта системи захисту для КМЗ за критерієм живучості в умовах невизначеності впливу ДФ. Для цього використано теорії підтримки прийняття рішень, що дає змогу знайти оптимальне вирішення, що найкраще відповідатиме змісту та умовам задачі у випадку трьох інформаційних ситуацій про ймовірності появи подій A_k.

2. Проаналізовано особливості і сформульовано задачі вибору варіанта системи захисту інформації в КМЗ за критерієм живучості в умовах невизначеності впливу ДФ у вигляді задачі

умовної оптимізації вибору конкретного ефективного рішення (живучішої системи захисту) для кожної конкретної реалізації сценарію розвитку зовнішнього середовища.

3. Вдосконалено та досліджено математичну модель і алгоритми формування множини альтернатив для задачі вибору варіанта системи захисту інформації в КМЗ за критерієм живучості в умовах невизначеності впливу ДФ, яку доцільно на практиці використовувати як вихідну інформацію для прийняття рішень про структуру СЗІ, яка має властивість живучості в умовах ризику та невизначеності.

1. Гарасим Ю. Р. Концепція організації системи захисту інформації на відомчих цифрових системах комутації / Ю. Р. Гарасим, В. В. Хома // Зб. наук. статей «Управління розвитком» МНПК «Сучасні засоби та технології розроблення інформаційних систем». – Харків: ХНЕУ, 2008. – № 15. – С. 41–42. 2. Гарасим Ю. Р. Технології функціонування захищених корпоративних мереж зв'язку / Ю. Р. Гарасим // Современные информационные и электронные технологии : Мат. науч. трудов десятой МРПК. – Одесса, 2009. – С. 63. 3. Гарасим Ю. Р. Деякі аспекти інформаційної безпеки корпоративних мереж зв'язку / Ю. Р. Гарасим // II тур Всеукраїнського конкурсу студентських наукових робіт з технічних наук, напрям «Телекомунікації», спеціальності «Телекомунікаційні системи та мережі», «Інформаційні мережі зв'язку» : Тез. доп. – Одеса, 2009. – С. 19. 4. Гарасим Ю. Р. Інформаційна безпека захищених корпоративних мереж зв'язку / Ю. Р. Гарасим, В. Б. Дудикевич // Вісник Національного університету «Львівська політехніка» «Автоматика, вимірювання та керування». – Львів, 2009. – № (639). – С. 124–132. 5. Гарасим Ю. Р. Структура технологій функціонування систем захисту інформації корпоративних мереж зв'язку / Ю. Р. Гарасим, В. Б. Дудикевич // Матеріали IV МНПК «Спеціальна техніка у правоохоронній діяльності». – К., 2009. – С. 226–228. 6. Гарасим Ю. Р. Поняття живучості системи захисту інформації захищених корпоративних мереж зв'язку / Ю. Р. Гарасим, В. Б. Дудикевич // Тези доп. III МНПК «Інформаційна та економічна безпека (INFECO-2010)». – Харків, 2010. – Вип. 3 (84). – С. 107–109. 7. Гарасим Ю. Р. Живучість розподіленої системи управління системою захисту інформації в захищених корпоративних мережах зв'язку та її моделі / Ю. Р. Гарасим, В. Б. Дудикевич // Труди XI МНПК «Сучасні інформаційні та електронні технології». – Одеса, 2010. – Т.1. – С. 96. 8. Dudykevych V. Survivable security Systems Analysis / V. Dudykevych, I. Garasym // Computer science and information technologies: Materials of the VIth International scientific and technical conference CSIT, 2010. – Lviv: Publishing House Vezha&Co, 2010. – pp. 108–110. 9. Дудикевич В. Б. Системи захисту інформації, що мають властивість живучості. Основні поняття / В. Б. Дудикевич, Ю. Р. Гарасим // Науково-технічний журнал «Сучасний захист інформації», спеціальний випуск. – 2010. – № 4. – С. 6–13. 10. Гарасим Ю. Р. Модель захищеної корпоративної мережі зв'язку, яка має властивість живучості / Ю. Р. Гарасим, В. Б. Дудикевич // Зб. тез VI МНТК «Сучасні інформаційно-комунікаційні технології». – АР Крим, Ялта-Лівадія, 2010. – С. 196–197. 11. Ларичев О. И. Теория и методы принятия решений / О. И. Ларичев. – М. : Логос, 2000. – 296 с. 12. Катренко А. В. Теорія прийняття рішень / А. В. Катренко, В. В. Пасічник, В. П. Пасько. – К.: Видавнича група BHV, 2009. – 448 с. 13. Черкесов Г. Н. Методы и модели оценки живучести сложных систем / Г. Н. Черкесов. – М., 1987. – 38 с. 14. Гиг Дж. Прикладная общая теория систем: пер. с англ. / Дж. ван Гиг. – М.: Мир, 1981. – 336 с. 15. Гайдес М. А. Общая теория систем. (Системы и системный анализ) / М. А. Гайдес. – Глобус-пресс, 2005. – 202 с. 16. Цофнас А. Ю. Теория систем и теория познания / А. Ю. Цофнас. – Одесса : АстроПринт, 1999. – 308 с. 17. Згуровський М. З. Основи системного аналізу / М. З. Згуровський, Н. Д. Панкратова. – К.: Видавнича група BHV, 2007. – 544 с. 18. Верлань А. Ф., Сизиков В. С. Интегральные уравнения: методы, алгоритмы, программы. — К.: Наук. думка, 1986. — 544 с. 19. Манжиров А. В., Полянин А. Д. Справочник по интегральным уравнениям. Методы решения. — М.: Физматлит, 2003. — 608 с. 20. Тихонов А. Н., Арсенин В. Я. Методы решения некорректных задач. — М.: Наука, 1986. — 288 с. 21. Катренко А. В. Теорія прийняття рішень / А. В. Катренко, В. В. Пасічник, В. П. Пасько. – К. : Видавнича група BHV, 2009. – 448 с. 22. Петров Э. Г. Методы и средства принятия решений в социально-экономических и технических системах / Э. Г. Петров, М. В. Новожилова, И. В. Гребенник, Н. А. Соколова. – Херсон: ОЛДИ-плюс, 2003. – 380 с. 23. Литвак Б. Г. Экспертные оценки и принятие решений / Б. Г. Литвак. – М.: Патент, 1996. – 271 с. 24. Тинякова В. И. Математические методы обработки экспертной информации / В. И. Тинякова. – Воронеж, 2006. – 68 с.