Метод вибору варіанту системи захисту інформації за критерієм живучості в умовах невизначеності впливу дестабілізуючих факторів

Ю. Р. Гарасим

В роботі розроблено метод вибору варіанту системи захисту інформації для корпоративних мереж зв'язку за критерієм живучості в умовах невизначеності впливу дестабілізуючих факторів.

Вступ

Системи захисту інформації (СЗІ), зокрема, корпоративних мереж зв'язку (КМЗ) відносять до такого класу систем, які є нестаціонарними, високо динамічними, з такою динамікою розвитку, що погано піддається прогнозу. Нестабільність впливу дестабілізуючих факторів (ДФ) визначає високий динамізм зміни зовнішнього та внутрішнього середовища (некерованих змінних системи), а часткові директивні впливи (атаки) роблять часові ряди короткими та неоднорідними, що переважно виключає можливість достовірного прогнозування зміни характеристик оточуючого 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. Ця невизначеність має принциповий характер і її неможливо подолати детермінізованими способами. У зв'язку з цим виникає необхідність використовувати інші підходи до вирішення задачі прийняття рішень про використання системи захисту КМЗ за критерієм живучості, що зумовлює актуальність даної роботи [1].

Аналіз особливостей систем захисту інформації як складної системи

Особливостями СЗІ КМЗ, які дозволяють віднести їх до класу складних систем та виокремити їх з множини інших складних систем є: структура СЗІ є нестаціонарна, її зміна відбувається як в результаті внутрішнього розвитку, в тому числі 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 СЗІ є нестаціонарними; наявність великої кількості нелінійних залежностей; для СЗІ характерною є 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 рішення задачі прогнозування, визначення статистичних параметрів процесів і оцінку їх значень [2].

Вищенаведені особливості СЗІ КМЗ дозволяють вирішити проблему вибору варіанту системи захисту КМЗ за критерієм живучості в умовах невизначеності впливу ДФ наступним чином.

Постановка задачі вибору варіанту системи захисту інформації в умовах невизначеності впливу дестабілізуючих факторів

Проблему прийняття рішення про вибір варіанту СЗІ в загальному випадку розділимо на наступні три основні етапи:

- сформувати множину допустимих рішень X;
- визначити метрики, в якій здійснювати порівняння допустимих рішень $x \in X$(задача оцінювання);

- вибрати із допустимої множини ефективне (найкраще) рішення $x^0 \in X$ (задача оптимізації).

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

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

і рівності

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

де x - N-мірна ($x^0 \in R^N$) керована змінна; h_s, g_l - оператори, які визначають структуру математичної моделі відповідного обмеження; q_h, q_g - кількісні параметри відповідних обмежень. Рішення задачі оптимізації, тобто визначення найкращого рішення $x^0 \in X$ пов'язане із формалізацією поняття "найкраще". Для цього визначимо метрику, в якій здійснювати порівняння якості рішень $x \in X$. В загальному випадку кожне рішення $x \in X$ опишемо n різними кількісними характеристиками (окремими критеріями) $k_i(x), i = \overline{1, n}$. Будемо вважати, що на множині $k_i(x)$ існує модель оцінювання, яка дозволяє 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. З врахуванням співвідношень (1)-(3) задачу умовної оптимізації (математичного програмування) запишемо у вигляді

$$x^0 = argextr_{x \in X} P(x); x \in R^N; h_s(x, q_h) \leq 0; s = \overline{1, S}; g_l(x, q_g) \leq 0; l = \overline{1, L}. \tag{4}$$

Прийняття рішень про структуру системи захисту інформації 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 визначення компромісу між ефективністю і стійкістю рішення. Правило реалізації компромісу визначають критерієм вибору рішення. Більшість відомих критеріїв прийняття рішень в умовах невизначеності є окремими випадками адитивної схеми компромісу. Нехай задано допустиму множину рішень X. На цій множині визначені два критерії $k_1(x)$ та $k_2(x)$, перший з яких характеризує ефект, а другий стійкість рішення. Для простоти будемо вважати, що ці два критерії мають однакову розмірність. Тоді загальна схема вибору компромісного рішення матиме вигляд

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

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

Критерій оптиміста. Цьому критерію відповідає наступне значення вагових коефіцієнтів: $a_1 = 1$, $a_2 = 0$. Це означає, що при виборі рішення враховуватимемо лише його ефективність. Позначимо через $P_{ij}(x)$ ефективність рішення $P_{ij}(x) = P_{ij} + \Delta P_{ij}, i = \overline{1, m}, j = \overline{1, m}$. Тоді схема прийняття рішення буде мати вигляд $x^0 = arg \max_i \max_j P_{ij}(x)$. Тобто вибиратимемо рішення, яке матиме максимальне значення цільової функції при найбільш бажаному сценарію розвитку зовнішнього середовища $y_j(t)$.

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

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

Це рішення вибиратимемо при умові самого негативного сценарію розвитку зовнішнього середовища $y_j(t)$, що забезпечує в цих умовах гарантований результат.

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

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

а правило вибору ефективності рішення

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

Таким чином критерій Гурвіца є універсальним, оскільки дозволяє реалізувати як розглянуті вище окремі критерії, так і будь-які інші вподобання ЛПР. Принциповим є те, що величину параметру b задає ЛПР на основі евристичних положень і не існує формальних методів визначення b [3].

Висновки

Розроблено метод вибору варіанту системи захисту для КМЗ в умовах невизначеності впливу дестабілізуючих факторів за допомогою використання теорії підтримки прийняття рішень, що дає змогу знайти вирішення, яке буде оптимальним за критерієм живучості, що найкраще відповідає змісту та умовам задачі у випадку трьох інформаційних ситуацій про ймовірності появи ДФ. Здійснено аналіз особливостей і постановку задачі вибору варіанту СЗІ в КМЗ за критерієм живучості в умовах невизначеності впливу ДФ у вигляді задачі умовної оптимізації вибору конкретного ефективного рішення (більш живучої системи захисту) для кожної конкретної реалізації сценарію розвитку зовнішнього середовища. Вдосконалено та досліджено математичну модель і алгоритми формування множини альтернатив для задачі вибору варіанту СЗІ в КМЗ за критерієм живучості в умовах невизначеності впливу ДФ, яку доцільно на практиці використовувати в якості вихідної інформації при прийнятті рішень про структуру СЗІ, яка має властивість живучості в умовах ризику та невизначеності.

Список літератури

[1] 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.

[2] Гарасим Ю. Р. Модель захищеної корпоративної мережі зв'язку, яка має властивість живучості / Ю. Р. Гарасим, В. Б. Дудикевич // Збірник тез VI Міжнародної науково-технічної конференції "Сучасні інформаційно-комунікаційні технології". - АР Крим, Ялта-Лівадія, 2010. - С. 196-197.

[3] 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 : ОЛДІ-плюс, 2003. - 380 с.

Автори

Юрій Романович Гарасим — аспірант 1-го року навчання, кафедра захисту інформації, Національний університет "Львівська політехніка", Львів, Україна; E-mail: *garasym_yr@polynet.lviv.ua*