УДК 517.93.2

Хохлачова Ю.Є.

МОДЕЛЮВАННЯ КРИТЕРІЇВ ОПТИМАЛЬНОСТІ ТА ОБМЕЖЕНЬ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ

У даній статті розглянуто важливу та актуальну проблему побудови процедур формалізації критеріїв ефективності та обмежень. Запропоновано розробку та застосування аксіоматичної теорії для математичного моделювання критеріїв оптимальності та обмежень як певних функцій від керованих, так й некерованих змінних. Сформулювано та детально розглянуто систему правил (аксіоми) математичного моделювання критеріїв оптимальності та обмежень, яка будується на необхідних та достовірних умовах існування екстремумів функцій та функціоналів. Показаний ряд явних переваг, які мають математичні моделі критеріїв та обмежень.

Ключові слова: захист інформації, система захисту інформації, критерії оптимальності та обмежень.

Вступ. Процедура аналізу ефективності та оптимальності рішень для будь-якої системи, що створюється, в тому числі й системи захисту інформації, у загальному випадку повинна містити наступні необхідні етапи ітераційної процедури: визначення практичної потреби; вибір цілей та формування вимог до системи, яка повинна забезпечити досягнення поставлених цілей; визначення зовнішніх умов функціонування системи та систем, з якими буде взаємодіяти система, що розробляється; вибір критеріїв ефективності (оптимальності) системи та побудова їх математичних моделей; вибір та аналіз можливих способів вирішення поставлених задач; виявлення та дослідження необхідних ресурсів та обмежень на їх використання; розробка математичних моделей обмежень як функцій від керованих та некерованих змінних; порівняльний аналіз (порівнювання) ефекту та затрат ресурсів, можливих варіантів побудови системи; порівняння альтернатив, пошук та вибір оптимального рішення; аналіз адекватності та чуттєвості математичних моделей, критеріїв та обмежень до змін керованих змінних параметрів.

Ітераційна процедура циклу розробки – наукових досліджень, схемотехнічного, конструкторського та технологічного опрацювання – завершується створенням дослідного зразка системи, що проектується. Сучасні системи захисту інформації представляють собою складні ієрархічні багаторівневі системи [1]. Основними характеристиками таких систем є вертикальна та горизонтальна декомпозиція на самостійні підсистеми, які мають свої цілі, критерії та органи керування, пріоритет прийняття рішень, залежність рішень, що приймаються на кожному рівні та у кожній підсистемі від рішень, які приймаються на інших рівнях й в інших підсистемах, необхідність узгодження критеріїв та рішень, координації виконання рішень та дій. Процес керування критеріями та рішеннями підсистем здійснюється в умовах невизначеності, яка обумовлена неповною інформацією про поведінку інших підсистем, а також про їх зовнішнє оточення [2].

Основна частина. При виборі критеріїв та обмежень в ієрархічних системах можливі наступні проблемні ситуації: однорівневий вибір критеріїв при наявності однієї мети; однорівневий багатоцільовий вибір критеріїв; багаторівневий вибір критеріїв при умові, що кожний рівень керується однією метою; багаторівневий багатоцільовий процес формування критеріїв.

Відповідно, побудова математичних моделей критеріїв ефективності та обмежень є ключовою проблемою в усіх задачах аналізу, синтезу та оптимізації систем, що розробляються, тому побудова самих процедур формалізації критеріїв та обмежень само по собі є важливою та актуальною проблемою [3].

Тобто необхідні розробка та застосування аксіоматичної теорії для математичного моделювання критеріїв оптимальності та обмежень як певних функцій від керованих, так й некерованих змінних. Формалізація побудови математичних моделей дозволяє змістовно ставити та вирішувати задачі аналізу, синтезу та оптимізації систем за обраними критеріями та виявленим обмеженням. Некеровані змінні, як правило, відіграють роль параметрів родини рішень та визначають зазвичай ті чи інші умови функціонування та взаємодії систем, та/або області існування та єдності оптимальних рішень. Тому необхідно сформулювати системи правил (аксіоми).

Для побудова системи аксіом використовуються три основних принципи:

1. Критерії ефективності повинні дозволяти оптимальне керування, тобто готувати та приймати оптимальні рішення, у тому числі й при наявності обмежень.

2. Так як в двоїстих задачах оптимізації обмеження відіграють роль критеріїв, то математичні моделі обмежень конструюють також й моделі критеріїв.

3. Будь-яка задача з обмеженнями може бути перетворена у послідовність задач без обмежень, тому для вибору канонічних форм можна використовувати допоміжну функцію Лагранжа як узагальнений критерій оптимальності, який враховує обмеження.

Система аксіом математичного моделювання критеріїв оптимальності та обмежень будується на необхідних та достовірних умовах існування екстремумів функцій та функціоналів. Ця система аксіом дозволяє розробляти канонічні форми рівнянь оптимізації, як рівнянь балансу [4], критеріїв оптимізації та обмежень, як інтегральних перетворень цих канонічних форм.

Розглянемо послідовно та детально запропоновані аксіоми.

Аксіома 1. Будь-яка безперервна двічі диференційована функція $F(x_1, x_n)$ від n незалежних змінних (аргументів) може бути критерієм оптимальності (цільової функції), а самі аргументи відіграють роль керованих змінних, якщо для області існування функції дотримуються необхідні та достатні умови існування екстремумів.

Аксіома 2. Будь-яка безперервна двічі диференційована функція $G(x_1, x_n)$ від n незалежних змінних (аргументів) може бути обмеженням, а самі аргументи відігравати роль керованих змінних, якщо для області існування функції дотримуються необхідні та достатні умови існування екстремумів та задані значення обмежень у вигляді системи рівнянь

$$G_k(x_1, x_n) = G_k^*; k = 1, m, \tag{1}$$

де G_k^* - значення k-го обмеження, m - число обмежень.

Аксіома 3. Щоб оптимальне рішення існувало та було єдиним, необхідно щоб число керованих змінних та число обмежень задовольняли умові:

$$n - m > 0, n > m, m < n. \tag{2}$$

Аксіома 4. У випадках, коли обмеження (1) задані у вигляді нерівностей, задачі оптимізації зводяться до відомих способів введення фіктивних допоміжних змінних.

Аксіома 5. В двоїстих задачах оптимізації, коли цільові функції та обмеження можуть мінятися місцями, повинна виконуватися необхідна умова (2).

Аксіома 6. В задачах оптимізації з обмеженнями в ролі критерію оптимізації використовується допоміжна функція Лагранжа виду [5-7]:

$$L(x_1, x_n) = F(x_1, x_n) + \sum_{k=1}^{m} \lambda_k \left[G_k(x_1, x_n) - G_k^* \right], \tag{3}$$

де λ_k - допоміжні невизначені множники Лагранжа.

Аксіома 7. Система з $n + m$ рівнянь оптимізації

$$\begin{cases} \dfrac{\partial L(x_1, x_n; \lambda_1, \lambda_m)}{\partial x_i} = 0, i = 1, n; \\ \dfrac{\partial L(x_1, x_n; \lambda_1, \lambda_m)}{\partial \lambda_k} = 0, k = 1, m, \end{cases} \tag{4}$$

може бути представлена у канонічній формі виду

$$\begin{cases} \dfrac{\partial L_1(x_1, x_n; \lambda_1, \lambda_m)}{\partial x_i} = \dfrac{\partial L_2(x_1, x_n; \lambda_1, \lambda_m)}{\partial x_i}, i = 1, n; \\ G_k(x_1, x_n) = G_k^*. \end{cases} \tag{5}$$

Далі систему (5) будемо називати першою канонічною формою (ПКФ) представлення системи рівнянь оптимізації. Елементи лівої та правої частин рівнянь (5) будемо називати типовими елементами ПКФ (ТЕПКФ).

Аксіома 8. Використання ПКФ (5) системи рівнянь оптимізації дозволяє створювати критерії оптимізації у вигляді сепарабельних адитивних критеріїв:

$$F(x_1, x_n) = \sum_{i=1}^{n} \int \frac{\partial L_1(x_1, x_n; \lambda_1, \lambda_m)}{\partial x_i} dx_i + C_{1i} - \sum_{i=1}^{n} \int \frac{\partial L_2(x_1, x_n; \lambda_1, \lambda_m)}{\partial x_i} dx_i + C_{2i}, \quad (6)$$

де C_{1i}, C_{2i} - постійні інтегрування.

Сепарабельність $F(x_1, x_n)$ означає, що всі недіагональні елементи матриці других приватних похідних цієї функції дорівнюють нулю.

Аксіома 9. Для обмежень виду (5) також зручно використовувати сепарабельну форму та адитивність

$$\sum_{i=1}^{n} G_{ik}(x_i) = G_k^*. \quad (7)$$

Задачу оптимізації, у якій критерій оптимізації представлений у вигляді (6), а обмеження у вигляді (7), будемо називати задачею сепарабельного програмування. Рішення прямих задач сепарабельного програмування існує, якщо $F(x_1, x_n)$ є випуклою, а $G_k(x_1, x_n)$ - вгнутою функцією. Для зворотних задач функції $F(x_1, x_n)$ та $G_k(x_1, x_n)$ повинні володіти протилежними властивостями. Властивості сепарабельності та адитивності широко використовують в математичному програмуванні, вони дозволяють створювати ефективні обчислювальні алгоритми пошуку оптимальних рішень.

Представлення критерію оптимізації у вигляді (6) називається другою канонічною формою (ДКФ) постановки задачі оптимізації. В двоїстих задачах оптимізації при побудові допоміжних функцій Лагранжа (3) критерій та одно з обмежень міняються місцями. При цьому змінюються і характер екстремуму, і вимоги випуклості та вгнутості цільових функцій та обмежень. Доданки суми (6) будемо називати типовими елементами ДКФ (ТЕДКФ).

Аксіома 10. Константи C_{1i}, C_{2i} у ДКФ (6) повинні обиратися зі змісту та логічного смислу критерію оптимізації та обмежень.

Запропонована система аксіом дозволяє створити загальну аксіоматичну теорію математичного моделювання сепарабельних критеріїв оптимізації та обмежень. Вона заснована на виборі типових елементів канонічних форм (5), (6) та методах сепарабельного програмування. Параметри канонічних форм грають роль параметрів сімейства оптимальних рішень, їх зручно використовувати як параметри середовища (зовнішнього оточення) або як параметри, які характеризують взаємодію системи, що розглядається з іншими системами.

Для класифікації типових елементів першої канонічної форми (5) корисно використовувати методи аналітичної та диференційної геометрії, які володіють високою наочністю. У ролі типових елементів форм можуть бути обрані алгебраїчні функції (поліноми) q-го порядку, показові, експоненціальні, тригонометричні, трансцендентні та інші.

Висновки. Аксіоматична теорія дозволяє ввести таку форму представлення системи рівнянь оптимізації, яка названа як "перша канонічна форма математичного моделювання критеріїв та обмежень", причому, за її допомогою інтегральне перетворення (друга канонічна форма математичного моделювання критеріїв та обмежень), дозволяє синтезувати морфологічним методом сепарабельних адитивних критеріїв та обмежень.

Такі математичні моделі критеріїв та обмежень мають ряд явних переваг: осмислений вибір керованих змінних та параметрів для пошуку оптимальних рішень, побудова таких критеріїв, які заздалегідь забезпечують виконання необхідних та достатніх умов оптимального управління; використання розвинутих методів сепарабельного програмування; застосування морфологічного метода синтезу можливих рішень; залучення такого мінімального числа вільних параметрів (некерованих змінних), які дозволяють адекватне відображення, в межах заданої точності моделювання, умов функціонування та взаємодії систем, що досліджуються.

ЛІТЕРАТУРА

1. Ленков С.В. Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов Д.А., Хорошко В.А. – К.: Арий, 2008.
2. Горелик В.А. Исследование операций / Горелик В.А., Ушаков И.А. – М.: Машиностроение, 1986. – 288 с.
3. Вунш Г. Теория систем / Вунш Г. – М.: Сов. радио, 1978. – 288 с.
4. Тиснина Е.О. Абсолютная устойчивость положения равновесия системы поддержки принятия решений в системе защиты информации / Тиснина Е.О., Хорошко В.А. // Сучасний захист інформації, №4, 2010. – С. 74-79.
5. Мину М. Математическое программирование. Теория и алгоритмы / Мину М. – М.: Наука, 1990. – 488 с.
6. Хоменюк В.В. Элементы теории многоцелевой оптимизации / Хоменюк В.В. – М.: Наука, 1983. – 343 с.
7. Игнатов В.А. Аксиоматическая теория математического моделирования критериев оптимальности и ограничений / Игнатов В.А., Минаев Ю.Н., Гузий Н.Н. // Захист інформації, №4, 2005. – С. 46-56.

Надійшла: 22.10.2012 р.

Рецензент: д.т.н., професор Щербак Л.М.

УДК 004.056.53(045)

Корченко А.А.

МОДЕЛЬ ЭВРИСТИЧЕСКИХ ПРАВИЛ НА ЛОГИКО-ЛИНГВИСТИЧЕСКИХ СВЯЗКАХ ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛИЙ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Недостатком современных систем обнаружения вторжений, построенных на принципе идентификации аномального состояния является то, что они в основном ориентированы на использование таких математических моделей, которые требуют много времени на подготовку статистических данных. Математические модели, основанные на экспертных подходах в этом отношении являются более эффективными, но для выполнения своих функций необходимо использование соответствующих решающих правил. Для решения этой задачи в работе предложена модель эвристических правил на нечеткой логике, которая за счет использования множества пар "атака $\rightarrow$ параметры" и "атака $\rightarrow$ набор логико-лингвистических связок", а также универсальной модели эталонов параметров позволяет отображать аномальное состояние, порождаемое определенным типом кибератак в компьютерной сети. На основе этой модели были разработаны примеры правил для обнаружения сканирования, спуфинга и Dos-атак, которые могут практически использоваться для усовершенствования реальных систем выявления аномалий порожденных атакующими действиями в компьютерных системах.

Ключевые слова: кибератака, системы обнаружения вторжений, атака в компьютерных системах, аномалия в сетевом трафике, обнаружение аномалий в компьютерных системах, логико-лингвистическая связка, эвристические правила, экспертная оценка.

Стремительное развитие информационных технологий (ИТ) в свою очередь породило большое количество угроз ресурсам информационных систем (РИС). Одним из решений обеспечения безопасности РИС, являются системы обнаружения вторжений (СОВ) представляющие собой программные или аппаратные средства, ориентированные прежде всего на выявление фактов неавторизованного доступа. Следует отметить, что современные СОВ основываются на сигнатурном (шаблонном) и аномальном принципах.

Первый базируется на представлении каждой атаки в виде определенного шаблона (модели, сценария, правила, сигнатуры) отражающего характеристики и сценарии возможных вторжений. Поэтому такие системы с достаточно высокой точностью выявляют тип кибератак и практически функционируют без ложных срабатываний. Анализ сетевого трафика с использованием сигнатурного принципа характерен тем, что распознавание возможно только при известных кибератаках, а для этого необходимо постоянно обновлять и расширять наборы шаблонов. Кроме неустойчивости к новейшим типам вторжений, такие системы сильно зависят от скорости разработки и обновления сигнатур. Также известно, что для сложных распределенных атак проверка известных шаблонов является достаточно сложной задачей.

Второй принцип основан на выявлении аномального состояния системы порожденного кибератакой и ориентирован на контроль активности в среде окружения, например, наблюдение за параметрами сетевого трафика. Преимущества систем,