УДК 517.929.4:519.21

В. Б. Говоруха, доктор фізико-математичних наук,
завідувач кафедри вищої математики
та інформатики Академії митної служби України
О. Ю. Лебідь, кандидат фізико-математичних
наук, доцент кафедри вищої математики
та інформатики Академії митної служби України

ЗАСТОСУВАННЯ ТЕОРІЇ НЕЧІТКИХ МНОЖИН ДО ІНФОРМАЦІЙНИХ СИСТЕМ

Наведено деякі особливості розв'язання прикладних задач, що виникають при побудові інформаційних систем. Досліджено можливість застосування методів та алгоритмів теорії нечітких множин до розв'язання таких задач.

Приведены некоторые особенности решения прикладных задач, которые возникают при построении информационных систем. Исследована возможность применения методов и алгоритмов теории нечетких множеств к решению таких задач.

The list of some characteristics of decision of applied tasks using at building of the information systems. Possibility of application of methods and algorithms of theory of fuzzy sets is investigational to the decision of such tasks.

Ключові слова. Інформаційна система, система захисту інформації, теорія нечітких множин.

Вступ. Сучасний етап розвитку соціуму характеризується підвищеною увагою до захисту національних інтересів держави у різних сферах життєдіяльності її суспільства.

Масштабне впровадження інформаційних систем, побудованих з використанням сучасних інформаційних технологій, до різних структур переважно на всіх рівнях стає визначальним фактором переходу економіки на інноваційний рівень.

Слід зазначити, що в Україні інформаційні системи діють під назвою "автоматизовані системи (АС)".

Нині актуально питання захисту електронної інформації, а також побудови систем захисту інформації (СЗІ), що постійно надходить до державних установ і є конфіденційною та засекреченою.

Будь-яка система захисту інформації має складну технічну систему і є складовою інформаційної системи. Розв'язування задач аналізу та синтезу СЗІ ускладнюється її основними властивостями [1, 2]:

- складний опосередкований взаємозв'язок показників якості СЗІ з показниками якості інформаційної системи;
- необхідність урахування великої кількості показників (вимог) СЗІ в оцінюванні та виборі її раціонального варіанта;
- переважно якісний характер показників (вимог), що враховуються під час аналізу та синтезу СЗІ;
- істотний взаємозв'язок та взаємозалежність цих показників (вимог), що мають суперечливий характер;
- труднощі, пов'язані з отриманням початкових даних, необхідних для розв'язування задач аналізу та синтезу СЗІ, особливо на ранніх етапах проектування.

Вищезазначені особливості роблять практично неможливим застосування традиційних математичних методів, у тому числі методів математичної статистики й теорії ймовірності, а також класичних методів оптимізації для розв'язування прикладних задач аналізу та синтезу СЗІ.

Постановка завдання. Складність прийняття рішень, відсутність математичного апарату для розв'язування задач, що виникають під час розробки СЗІ, приводять до того, що для оцінки й вибору альтернатив можливо (а найчастіше просто необхідно) використати й обробляти якісну експертну інформацію. Перспективним напрямком розробки методів прийняття рішень в експертній вихідній інформації є лінгвістичний підхід на базі теорії нечітких множин.

Дослідимо можливість застосування теорії нечітких множин для розв'язання деяких задач під час побудови інформаційних систем.

Результати дослідження. Теорія нечітких множин підтвердила істину: формальний апарат зі своїми потенційними можливостями та точністю має бути адекватним значеннєвому змісту та точності початкових даних. Математична статистика й теорія ймовірності використовують експериментальні дані, що мають чітко визначену точність та достовірність. Теорія нечітких множин має справу із "людськими знаннями", що прийнято називати експертною інформацією [3, 4, 5].

Згідно з [1, 2] оцінка параметрів системи захисту інформації з високим рівнем невизначеності умов її функціонування має визначатись із використанням не однієї математичної моделі, а узгодженої сім'ї моделей, що адаптивно конструюються одна на одній і, таким чином, неперервно удосконалюються на основі оптимального вибору початкових даних.

Під час синтезу оптимальних систем захисту опорними повинні стати такі два положення [1]:

- вибір математично продуктивного критерію оптимальності відповідно до архітектури системи захисту та технології обробки інформації на об'єкті;
- чітке математичне формулювання задачі, що враховує всі апріорні відомості й те, що дозволяє розв'язувати її за прийнятим критерієм.

Під методологією оптимізації систем захисту інформації розуміють розробку теорії, що зв'язує їх структуру, логічну організацію, методи та засоби діяльності для формування функції вибору та виокремлення підмножини найкращих стратегій.

Оптимальним називаємо розв'язок, який в заданих умовах за рахунок найраціональнішого розподілення ресурсів, що витрачаються на розв'язування проблеми захисту, найкраще задовольняє умови конкретної задачі.

У процесі створення оптимальної СЗІ обов'язково виникає задача корекції вимог до системи захисту. Важкість її розв'язання полягає у тому, що з'являються неточності нестохастичного характеру, які визначаються:

- наявністю цілеспрямованої протидії з боку протиборчої системи, засоби дій якої невідомі досліднику;
- недостатньою вивченістю деяких явищ, що супроводжують процес функціонування систем захисту;
- нечітким формулюванням мети операції, що призводить до неоднозначного трактування відповідності реального результату операції необхідному.

Труднощі дослідження питань забезпечення захисту інформаційних технологій погіршуються через значну невизначеність умов функціонування інформаційної системи.

Таким чином, постановка задачі забезпечення захисту інформації, як правило, виявляється некоректною, оскільки найчастіше формулюється в умовах непередбачуваної дії системи у нестандартних і, особливо, в екстремальних ситуаціях. Вплив невизначеності дуже помітний в інформаційних системах, що трансформуються. Вони нестабільні, низько організовані через неповноту, несвоєчасність, ненормованість і малоймовірність інформації.

У зв'язку з цим задача забезпечення захисту інформаційних технологій, як правило, не має єдиного розв'язку, ефективність і оптимальність якого визначаються ступенем

урахування обмежень, характерних для конкретної ситуації. Для підвищення коректності постановки задачі забезпечення захисту інформаційних технологій необхідно підвищувати знання про інформаційну систему в умовах її функціонування, що постійно змінюються.

Таким чином, отримання й використання знань має здійснюватися безпосередньо під час функціонування системи шляхом поступового накопичення необхідної інформації, аналізу й використання її для ефективного виконання заданої цільової функції в умовах змінних внутрішнього й зовнішнього середовищ.

Відомі математичні моделі, що використовуються для опису структури, поведінки й управління СЗІ, особливо нестабільні в умовах некоректної постановки задачі й не дають бажаного результату [1, 2]. Тому необхідна розробка нових, орієнтованих на специфіку процесів захисту інформації, методів і засобів моделювання.

Перевірка й аналіз значень названих параметрів, необхідних для підвищення знань про систему, повинні здійснюватися таким чином, щоб забезпечити можливість прийняття своєчасних і достовірних рішень та коректування поведінки системи під час функціонування. Отже, у СЗІ обов'язково слід передбачити виконання процедур контролю її працездатності й діагностування станів.

Прийняття рішень базується переважно на експертних оцінках. Однак за невизначеності початкових даних і некоректності постановки задачі управління ці оцінки можуть спричинити додаткову некоректність прийнятого рішення, збільшивши початкову невизначеність.

Принциповими особливостями розв'язування задачі вибору раціонального варіанта СЗІ, що визначають метод її розв'язування, є:

- багатокритеріальність задачі вибору;
- не тільки кількісне, а також і якісне (нечітке) описання показників якості СЗІ, що задаються у вигляді вимог;
- за нечіткої постановки задачі вплив на вибір методу її розв'язування експертної інформації, що визначає перевагу того чи іншого показника.

Загальна постановка задачі багатокритеріальної оптимізації має такий вигляд. Нехай $\overline{X} = (x_1,...,x_i,...,x_n)$ – вектор параметрів деякої системи *S*, що необхідно оптимізувати. Певна *j*-та властивість системи *S* характеризується величиною *j*-го показника $q_j(\overline{X}),\ j=\overline{1,m}$. Тоді система в цілому характеризується вектором показників $\overline{Q} = (q_1,...,q_j,...,q_m)$. Задача багатокритеріальної оптимізації зводиться до того, щоб із множини M_S варіантів системи *S* обрати такий варіант (систему S_0), що має найкраще значення вектора $\overline{Q}$. При цьому припускається, що поняття "найкращий вектор $\overline{Q}$" попередньо сформульовано математично, тобто обраний (обгрунтований) відповідний критерій переваги (відношення переваги). Розв'язування даної задачі може базуватися на алгоритмах та методах теорії нечітких множин [1].

Висновки. Таким чином, на основі аналізу та використання відомої літератури з теорії нечітких множин [3, 4, 5] можна стверджувати про можливість застосування даного сучасного математичного апарату для розв'язування прикладних задач, що пов'язані з оцінкою та вибором варіантів побудови інформаційних систем, у тому числі й систем захисту інформації. Надалі автори планують розробку на основі теорії нечітких множин методів та алгоритмів розв'язання задач, що виникають під час побудови інформаційних систем, та подальшу їх реалізацію.

Література

1. Домарев В. В. Безопасность информационных технологий. Системный подход / Домарев В. В. – К. : ДиаСофт , 2006. – 904 с.

2. Домарев В. В. Защита информации и безопасность компьютерных систем / Домарев В. В. – К. : ДиаСофт, 1999. – 480 с.

3. Борисов А. Н. Принятие решения на основе нечетких моделей: примеры использования / Борисов А. Н., Крумберг О. А., Федоров И. П. – Рига : Знание, 1990. – 184 с.

4. Поспелов Д. А. Нечеткие множества в моделях управления и искусственного интеллекта / Поспелов Д. А. – М. : Наука, 1986. – 312 с.

5. Ротштейн А. П. Интеллектуальные технологии идентификации / Ротштейн А. П. – Винница : Универсум-Винница, 1999. – 320 с.