

## **ЗАСТОСУВАННЯ FUZZY-ТЕХНОЛОГІЙ ПРИ ПОБУДОВІ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ**

Світова економічна криза призвела до загострення конкурентної боротьби на світових ринках. В умовах глобалізації та наростаючої конкурентної боротьби комплексні системи захисту інформації (КСЗІ) як в комерційних організаціях так і в державних підприємствах та корпораціях України є досить пріоритетним питанням інформаційної безпеки держави. Все частіше виникає потреба створення надійного захисту та збереження інформаційних ресурсів, як на рівні всієї організації взагалі так і на рівні окремих її підрозділів. І часто в тому наскільки ефективним є КСЗІ залежить загальна конкурентоздатність всієї організації. Підвищення вимог до ефективності захисту інформації (СЗІ) супроводжується підвищенням вимог щодо ефективності використання фінансових ресурсів, що виділяються на захист інформації (ЗІ). На теперішній час, найбільше розповсюдження отримали два підходи до визначення оптимального варіанту побудови КСЗІ організації. Перший з них ґрунтується на перевірці відповідності рівня захищеності інформації в організації вимогам одного зі стандартів (законодавчих актів) у галузі інформаційної безпеки. Основний недолік першого підходу полягає в тому, що коли рівень захищеності інформації чітко не визначений визначити найбільш ефективний варіант побудови КСЗІ організації достатньо складно. Другий підхід пов'язаний з використанням методів та моделей оптимізації складних систем для визначення оптимального варіанту побудови КСЗІ. У зв'язку з цим розробка відповідних методів та моделей оптимізації показників СЗІ отримує особливу актуальність. Кінцевою метою при оптимізації показників КСЗІ є забезпечення необхідного рівня інформаційної безпеки організації за різних умов конкурентної боротьби. Завдання ускладнюється тим, що пошук доводиться вести в умовах невизначеності, коли дії суперника нам не відомі і, в кращому разі, можуть бути оцінені з певною долею ймовірності. При відсутності статистичних даних, що характерно для комерційних структур, вибір параметрів розрахунку і функціональних залежностей, які входять в математичну модель, ведеться на основі експертних оцінок і вимагає розробки відповідних методів та методик. Рішення зазначених задач потребує включення до складу процедур спеціальних оптимізаційних моделей котрі встановлюють залежність між показниками кінцевого ефекту функціонування системи і сукупністю її параметрів. Саме такий підхід може бути покладено в основу оптимізації систем захисту інформації в умовах інформаційного протистояння. Таким чином, задача побудови оптимальної комплексної системи захисту інформації може бути вирішена на основі теоретичного (системного) підходу котрий використовує усесторонній розгляд та врахування основних факторів які впливають на ефективність системи. Під дослідженням операцій розуміють застосування математичних кількісних методів для обґрунтування рішень у всіх областях цілеспрямованої людської діяльності.

Реальною альтернативою та доповненням до базових методів оцінки рівня захисту інформації комплексних систем захисту інформації (КСЗІ) є застосування у дослідженнях Fuzzy-технологій, які дозволяють проводити оцінку за умов слабкої визначеності оціночних факторів та їх різноманітності. Вони уможливають аналіз значної кількості якісної інформації, отриманої від експертів та доповненої кількісними даними. Fuzzy-технології є сукупністю теоретичних основ, методів, алгоритмів, процедур і програмних засобів, що базуються на використанні теорії нечітких мір (ТНМ) і оцінок експертів для вирішення широкого класу задач з самих різних областей. Теорія нечітких мір, нечіткої логіки або Fuzzy Logic – новий підхід до опису процесів, в яких присутня невизначеність, що ускладнює і навіть виключає вживання точних кількісних методів і підходів. Основна відзнака методу – введення лінгвістичних змінних (суб'єктивних категорій) і методів їх обробки. Ця теорія може виступати як інструмент моделювання невизначеності, який базується на відомій розумовій здатності людини оперувати якісними категоріями і оформляти свої логічні висновки також в якісній формі.

Застосування даної технології підвищує достовірність і якість рішень, що приймаються, при суттєвому зниженні вимоги до вхідних даних (їх якості, кількості, достовірності), формалізація яких виконується настільки точно, наскільки дозволяє їх обсяг і якість. Розроблені моделі і методи вирішення задач нечіткого математичного програмування, які адекватні сучасним умовам функціонування спеціальних об'єктів інформаційної діяльності (СОІД), дозволяють підвищити наукову обґрунтованість, ефективність рішення, що формулюється та приймається при нечіткій вхідній інформації, збільшують аналітичну базу, надають можливість формалізації різних параметрів задачі та різноманітних цільових установок.

Необхідно відзначити, що нечіткі числа багато в чому аналогічні розподілам теорії імовірності, але вільні від властивих останнім недоліків, а нечіткі описи є моделлю згортки окремих імовірнісних розподілів подій з одночасним зважуванням цих сценаріїв за рівнем можливості (аналогічну функцію виконує і щільність імовірнісного розподілу).

Крім того, існує ще декілька причин використання ТНМ. По-перше, нечіткі множини ідеально описують суб'єктивну активність посадової особи, що приймає рішення щодо введення КСЗІ в експлуатацію. По-друге, нечіткі числа ідеально підходять для планування факторів у часі, коли їх майбутня оцінка ускладнена (розмита, не має достатніх імовірнісних умов). Таким чином, всі сценарії за тими чи іншими окремими факторами можуть бути зведені в один сценарій у формі трикутного числа, де відокремлюють три позиції: мінімально можливе, найбільш очікуване та максимально можливе значення фактору. Причому ваги окремих сценаріїв у структурі зведеного сценарію формалізуються як трикутна функція приналежності рівня фактора нечіткій множині “приблизного рівняння середньому”. По-третє, при використанні нечітких множин ми можемо в межах однієї моделі формалізувати особливості застосування СОІД.

*Науковий керівник – к.т.н., доц., В.О. Темніков*