УДК 621

І.В. Гордій
Національний університет “Львівська політехніка”,
кафедра захисту інформації

ЗАСТОСУВАННЯ ТЕОРІЇ НЕЧІТКИХ МНОЖИН ДЛЯ ВИЗНАЧЕННЯ РІВНЯ РИЗИКУ ВИТОКУ ІНФОРМАЦІЇ ТЕХНІЧНИМИ КАНАЛАМИ

Розглянуто проблему оцінки ризиків у сфері захисту інформації; описано підхід до визначення рівня ризику при побудові системи захисту інформації від витоку технічними каналами.

The article reviews problems of risk assessment in system of information protection from leakage on technical channels is considered; it shows method of risk level assessment herewith constructing system of information protection from leakage on technical channels.

Методики оцінки рівня ризику. З розвитком інформаційного суспільства проблема захисту інформації стала першочерговою для керівників фірм та організацій. Створюються підрозділи служби безпеки, розробляються політики безпеки та цілі системи захисту інформації з використанням низки технічних, програмних, організаційних методів захисту. Але ефективність системи захисту інформації (СЗІ) насамперед залежить від достовірного аналізу загроз. Важливим етапом створення системи захисту інформації є оцінка ризиків. Рівень ризику дає можливість застосувати адекватні заходи, методи, засоби захисту та підтримувати на належному рівні безпеку інформаційних ресурсів.

Нині відомі різні підходи в оцінці ризиків. За рекомендаціями Американського національного інституту стандартів і технологій *NIST* SP *800-30* рівень ризику визначається лише за двома параметрами – потенціальні збитки та ймовірність реалізації загрози. Проте істотним обмеженням такого підходу є недостатня гнучкість застосування до об’єктів різної категорії.

Відомі методики отримання оцінки ризику з попередньою оцінкою трьох параметрів (метод CRAMM). Крім потенційних збитків та ймовірності реалізації загрози, оцінюється ще ступінь вразливості. Методика оцінювання ризику CRAMM дає змогу аналізувати більшу кількість параметрів за точнішими шкалами. Поданий в CRAMM механізм виводу оцінок ризику за своєю суттю є табличним, тобто відображає тільки взаємозв’язки між рівнями, визначеними для шкал вхідних даних та величини ризику.

У статті [1] описано метод оцінки ризиків на основі застосування апарату нечіткої логіки як засобу підвищення точності оцінок у методах CRAMM і NIST. Поданий механізм, по суті, є експертною системою, в якій базу знань становлять правила, що відображають логіку взаємозв’язків вхідних величин та ризику.

Наведені методи здебільшого використовуються для оцінки ризиків у сфері безпеки інформаційних технологій. У цій статті описано підхід оцінки ризиків витоку інформації технічними каналами на основі нечіткої логіки. Розглянемо ситуацію, коли існує загроза порушення конфіденційності інформації за рахунок витоку по технічних каналах.

Обґрунтування параметрів оцінки ризиків. В умовах розвитку ринкової економіки та підвищення рівня конкуренції стало популярним використання технічних методів отримання

інформації. Методи технічної розвідки набувають популярності. При розгляді загрози витоку інформації по технічних каналах під час аналізу ризиків звертається увага на характеристики ймовірного порушника, ефективність захисту, рівень збитків [2, 3].

Основну категорію порушників, які для отримання інформації здатні та спроможні на використання технічних засобів розвідки, становлять конкуренти, а також іноді спецслужби. Ці зловмисники залежно від цінності інформації можуть застосувати різні за складністю методи отримання інформації через корисливі інтереси або виконуючи професійний обов'язок. Але загрозу можуть становити і працівники організації, які через безвідповідальність або прагнення до самоствердження можуть розголошувати цінну інформацію або порушити вимоги безпеки, позбавляючи інформацію належного захисту. Працівники, які не мають доступу до цінної інформації, але мають доступ до об'єкта інформаційної діяльності (ОІД), можуть в корисливих цілях допомагати конкурентам або спецслужбам, наприклад, встановити пристрої для зняття інформації. Отже, можна виділити такі категорії порушників:

- Внутрішні:
- працівники, що не мають доступу до цінної інформації;
- працівники, що безпосередньо працюють або ознайомлені з цінною інформацією;
- працівники служби безпеки організації;
- керівники різних рівнів посадової ієрархії.
- Зовнішні:
- партнери;
- відвідувачі;
- конкуренти;
- працівники спецслужб та особи, що діють за їхнім завданням.

Порушники можуть керуватися такими мотивами:

– безвідповідальність – працівник через свою халатність порушує вимоги політики безпеки, позбавляючи інформацію належного захисту;

– самоствердження ;

– корисливий інтерес – порушник в результаті злочинних дій для одержання інформації одержить винагороду або іншу користь від отриманої інформації;

– професійний обов'язок – порушник є працівником спецслужб і одержання інформації для нього є виконанням професійного обов'язку.

Для реалізації певної загрози порушник повинен мати деякий рівень кваліфікації та рівень оснащеності, що впливають на рівень ризику. Потенціал загрози порушника з урахуванням ефективності захисту визначає ймовірність реалізації загрози. Цінність інформації визначається розміром збитків, які можуть бути завдані в результаті порушення конфіденційності інформації. Рівень збитків при реалізації загрози та ймовірність реалізації загрози визначають рівень ризику для інформації для конкретної загрозі. Сукупність ризиків за кожною із загроз визначають загальний рівень ризику для інформації.

Особливості оцінки рівня ризику в галузі захисту інформації від витоку технічними каналами. Для визначення рівня ризику доцільно використати апарат теорії нечітких множин, що дає змогу описувати нечіткі поняття і знання, оперувати ними і робити нечіткі висновки. Теорія нечітких множин використовується саме для розв'язання задач, в яких вхідні дані є ненадійними та слабкоформалізованими, як у нашому випадку. Для оцінки ризику застосуємо механізм нечіткого логічного висновку (одержання висновку у вигляді нечіткої множини, що відповідає поточним значенням вхідних змінних, з використанням нечіткої бази знань і нечітких операцій). Існують розроблені моделі нечіткого висновку Мамдані, Сугено, Ларсена, Цукамото [4].

Найчастіше на практиці застосовують алгоритми Мамдані та Сугено. Основна відмінність між ними полягає в способі задання значень вихідної змінної в правилах, що становлять базу знань. В системах типу Мамдані значення вхідних змінних задаються нечіткими термами, в системах типу Сугено – як лінійна комбінація вхідних змінних.

Для задач, в яких важливіша ідентифікація, доцільно використовувати алгоритм Сугено, а для задач, в яких важливішим є пояснення і обґрунтування прийнятого рішення, алгоритм Мамдані буде мати перевагу. Тому для оцінки ризику використаємо алгоритм Мамдані.

На підготовчому етапі необхідно визначити лінгвістичні змінні та задати їх шкалами, на яких визначені нечіткі терми, що відповідають значенням змінних, розробити базу правил.

Вхідними величинами для нечіткого логічного висновку є:

– рівень проникнення порушника;

– можливості порушника;

– рівень збитків;

– ефективність захисту.

Для визначення цих параметрів розробнику необхідно прискіпливо ознайомитись з ОІД, з'ясувати у керівника організації (або керівника служби безпеки організації) вимоги до системи захисту інформації, створення моделі ймовірного зловмисника. За результатами відповідей за допомогою експертної системи визначають параметри, які є вхідними для нечіткого логічного висновку.

Основою для нечіткого логічного висновку є нечітка система, яка складається з лінгвістичних правил. Нехай x і y – вхідна та вихідна лінгвістична змінна; A і B – деякі нечіткі множини (функції приналежності), взяті із терм-множин змінних x і y відповідно. Лінгвістичним правилом нечіткого логічного висновку «якщо-то» називається конструкція типу:

$$R = якщо\ x \in A,\ то\ y \in B,$$

де «$x \in A$» – нечітке висловлювання, що називають умовою правила; «$y \in B$» – нечітке висловлювання, що називають висновком правила.

Розроблення необхідної бази знань та системи правил потребує значних трудових та часових затрат. Вона призначена для формального подання емпіричних знань або знань експертів в тій чи іншій предметній галузі. Необхідно вдало систематизувати інформацію в предметній сфері; визначити множину термів для кожної лінгвістичної змінної.

Основними етапами нечіткого логічного висновку є: формування бази правил, фазифікація вхідних змінних, агрегація, активізація, акумулювання. Для реалізації нечіткого логічного висновку можна скористатись пакетом Fuzzy Logic Toolbox редактора Matlab [5, 6].

Фазифікація – це визначення значень функції приналежності нечітких множин (термів). В результаті для всіх вхідних змінних повинні бути визначені конкретні значення функції приналежності для кожної з лінгвістичних змінних.

Агрегація – процедура визначення рівня істинності умов правил системи нечіткого висновку.

Активація – процедура визначення рівня істинності висновків продукційних правил.

Акумулювання – процедура пошуку функції приналежності для кожної з вихідних лінгвістичних змінних, заданих сукупністю правил.

Дефазифікація – перетворення отриманих лінгвістичних змінних до чітких значень.

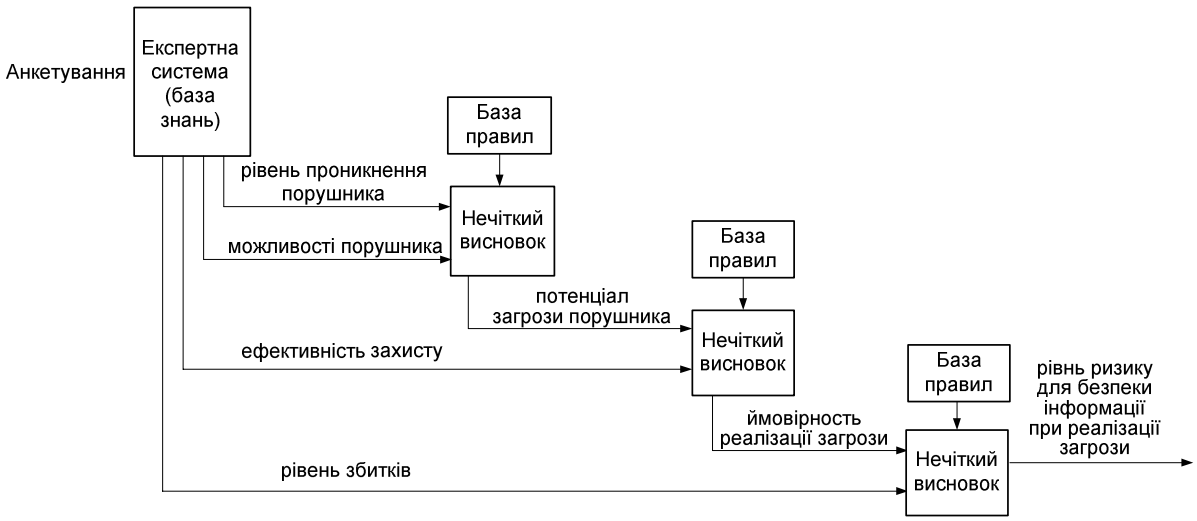

Рис. 1. Схема визначення рівня ризику для безпеки інформації при реалізації загрози

На рис. 1 зображений процес оцінки ризику для безпеки інформації при реалізації загрози. Визначивши рівень ризику для кожної із загроз, можна оцінити загальний рівень ризику. Описаний у статті метод оцінки ризиків дає змогу оцінити рівень ризику для кожної загрози. Причому під загрозою розуміємо не виникнення деякого технічного каналу витоку інформації, а конкретний метод реалізації. Це дасть змогу під час розроблення СЗІ детальніше визначити необхідний рівень захисту. Отже, СЗІ стане оптимізованішою.

Висновок. У сфері захисту інформації оцінка рівня ризику є важливим етапом для побудови ефективної СЗІ. Описаний у статті метод дає змогу виконати оцінку ризиків у разі небезпеки порушення конфіденційності інформації через її виток по технічних каналах. Однією з відмінностей розглянутого методу від відомих є визначення рівня ризику окремо для кожної загрози. Оцінка рівня ризику з використанням теорії нечітких множин уможливлює підвищення ефективності та оптимальності системи захисту інформації на ОІД від витоку інформації технічними каналами.

1. Балашов П.А., Кислов Р.И., Безгузиков В.П. Оценка рисков информационной безопасности на основе нечеткой логики // Защита информации. – Конфидент. – № 5'2003. 2. Бузов Г.А., Калинин С.В., Кодратьев А.В. Защита от утечки информации по техническим каналам. – М.: Горячая линия – Телеком, 2005. – 416 с. 3. Домарьов В.В.Безопасность информационных технологий. Методология создания систем защиты. – М.: DiaSoft, 2002. – 671 с. 4. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практика. – К.: ЭМК-Прес, 2006. – 302 с. 5. Леоненков А.В. Нечеткое моделирование в среде MATLAB и fuzzyTECH. – СПб.: БХВ-Петербург, 2005. – 736 с. 7. Штовба С.Д. Проектирование нечетких систем средствами MATLAB. – М.: Горячая линия – Телеком, 2007. – 288 с.

УДК 536. 532

Е.Й. Адамюк
Національний університет "Львівська політехніка"

ПРОБЛЕМИ ПРЕЦИЗІЙНОГО ВИМІРЮВАННЯ ТЕМПЕРАТУРИ В АГРЕСИВНИХ СЕРЕДОВИЩАХ

Здійснено огляд сучасних термоперетворювачів для вимірювання температури в агресивних середовищах. Проаналізовано вплив агресивного середовища на матеріал чутливого елемента термоперетворювача і відповідно на точність вимірювання температури. Запропоновано використання як матеріалу чутливого елемента термоперетворювачів металевих аморфних стопів.

The overview of modern thermal converter for temperature measuring in aggressive medium performed. The influence of aggressive medium to material of sensitive element of thermal converter and to precision of temperature measuring respective are considered. The metallic amorphous glass are offered to use as material of sensitive element of thermal converter.

Вступ. У багатьох галузях народного господарства необхідно вимірювати температуру в агресивних середовищах. Це текстильна, харчова, хімічна промисловості, нафтопереробна, фармакологія. Наприклад, в текстильній промисловості у агресивному середовищі відбілюють волокна. В хімічній промисловості більшість технологічних процесів або їх окремі стадії проходять в газовому