УДК 004.891.2

ЕКСПЕРТНА СИСТЕМА У ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Назарько А. І., Дюжаєв Л. П.

Розроблена консультаційна експертна система, що дозволяє оцінити ступінь відповідності системи менеджменту інформаційної безпеки підприємства вимогам міжнародного стандарту ISO 17799. Оцінювання ризиків проводиться за Байєсом. Програмний продукт реалізований в середовищі Borland C++ Builder 6.

Вступ

Центральна парадигма інтелектуальних технологій сьогодні — це обробка інформації, що має бути представлена у вигляді знань. Системи, ядром яких є база знань або модель предметної області, що описана мовою надвисокого наближеного до природного рівня, називають інтелектуальними. Найчастіше такі системи застосовуються для рішення складних завдань, де основна складність рішення пов'язана з використанням слабоформалізованих знань фахівців-практиків і де логічна (або значуща) обробка інформації превалює над обчислювальною. Прикладом можуть бути розуміння природної мови, підтримка ухвалення рішення в складних ситуаціях, постановка діагнозу й рекомендації з методів лікування, аналіз візуальної інформації та ін.

Постановка задачі

Сучасні експертні системи (ЕС) – це складні програмні комплекси, що акумулюють знання фахівців у конкретних предметних областях і передають цей емпіричний досвід для консультування менш кваліфікованих користувачів. Оцінювання інформаційної захищеності системи із залученням послуг кваліфікованого спеціаліста базується на якісних методах оцінки, на відміну від ЕС, які дозволяють на виході одержати не лише якісну оцінку, тобто відповідність системи певному класу або рівню захищеності, тому або іншому стандарту безпеки, а й кількісну.

Основна складність реалізації ЕС полягає у використанні мов логічного програмування *LISP* та *Prolog*, які не є загальновживаними і потребують значний час для ефективного їхнього оволодіння.

Натепер гостро стоїть питання управління інформаційною безпекою підприємств і тому виникає необхідність своєчасно отримувати ефективний експертний висновок у даній галузі. Тому виникає потреба створити ЕС на мові програмування, що знайома більшості людей і проектування якої не забере багато часу, при цьому розуміння програмної моделі ЕС дозволяє вдосконалювати і адаптувати її під інші потреби.

Аналіз досліджень і публікацій

Проблематиці ЕС на сьогодні приділено багато уваги, але в основному розглядаються можливості мов програмування, створених саме для ЕС. Фундаментальні знання про усі досягнення у сфері розробки ЕС можна знайти в [1], де описуються програмні алгоритми усіх ключових ланок ЕС,

не прив'язуючись конкретно до якихось мов програмування.

Для тестування та апробації існуючих на цей час закордонних комерційних ЕС авторами були вибрані програмні продукти Кондор 2005, Гриф 2005 (*Digital Security*, Росія) та *Cobra* (*C & A Systems Security Ltd*, Великобританія), як найкращі з сучасних ЕС в даній сфері, в результаті чого виявлені основні спільні риси в роботі цих програм, зокрема присутність аналізу ризиків та можливість власноруч змінювати вагові коефіцієнти. На основі досліджень була створена ЕС на мові програмування C^{++} в середовищі візуального проектування *Borland* C^{++} *Builder* 6. Вона дозволяє перевірити відповідність політики інформаційної безпеки компанії вимогам міжнародного стандарту безпеки *ISO* 17799 (*BS* 7799) "Управління інформаційною безпекою", в результаті чого виявляються основні погрози безпеки для бізнес-процесів, виробляються рекомендації з підвищення поточного рівня захищеності для захисту від виявлених погроз і по усуненню недоліків у системі безпеки й керування. В якості базового стандарту безпеки, за яким відбувається аудит, було використано стандарт *BS* 7799 [2], серед основних розділів якого можна відокремити: безпека персоналу; фізична безпека; контроль доступу; розробка й технічна підтримка обчислювальних систем; відповідність системи основним вимогам та ін.

Теоретичні викладки

В програмі використовується система оцінювання ризиків, в основі якої лежить теорема Байєса [3]:

$$P(H:E)=\frac{P(E:H)P(H)}{P(E:H)P(H)+P(E:\text{"не}H\text{"})P(\text{"не}H\text{"})}, \qquad (1)$$

де H - деяка гіпотеза; E - свідчення, що підтверджує або не підтверджує цю гіпотезу; $P(H)$ - апріорна ймовірність справедливості гіпотези H (це ймовірність того, що наступить H без врахування факту існування E); $P(H:E)$ або $P(H:\text{"не}E\text{"})$ - апостеріорна ймовірність гіпотези H, тобто ймовірність H при умові, що факт існування E відомий.

Формула (1) справедлива, для випадку, коли E відбулося. Якщо ж E не відбулося, у формулі (1) замість E слід вживати "неE". При цьому $P(H:E)$ часто є неочевидним, ймовірність же $P(E:H)$, навпаки, є величиною більш очевидною, якщо враховувати дані по предметній області. Для випадку двох и більше свідчень E_1 та E_2, за умови, що E_1 та E_2 незалежні - $P(E_1 \& E_2:H)=P(E_1:H)P(E_2:H)$. Якщо E є свідченням, яке говорить, що «всі E_i відбулися» і, крім того, всі вони незалежні один від одного, то можна визначити $P(E:H)$ як $P(E:H)=P(E_1:H)P(E_2:H)...P(E_i:H)$

Ствердження про незалежність свідчень дозволяє скоротити розміри предметної області та зменшити складність проблеми висновку.

Принципи побудови розробленої ЕС

Алгоритм роботи програми базується на алгоритмі, наведеному в [3], де розглянута можливість створення ЕС на мові програмування *BASIC*. Створена ЕС для встановлення відповідностей так само використовує масиви і структури, при цьому використовуються переваги мови програмування C^{++} в порівнянні з *BASIC*ом.

Створена база знань підключається до експертної системи у вигляді динамічної бібліотеки, що дозволяє для подальшого доопрацювання системи без внесення змін у модуль роботи з користувачем (інтерфейс опитування) проводити роботи лише над файлом бази знань, а також використовувати інші бази знань, що будуть базуватись на інші стандарти безпеки. Кожен розділ бази знань представлений у вигляді правил і запитів, що стосуються лише його і аналізується окремо. Це дозволяє використовувати паралельну процедуру аналізу інформації, в результаті чого весь розрахунок базується на використанні всієї сприйнятої інформації і проводиться після завершення опитування користувача системи. На даному етапі користувач повинен відповісти на всі запити експертної системи в межах одного розділу, після чого формується відповідна картина інформаційної безпеки. Надалі можливе проведення аналізу безпеки не по всім запитам, тобто за відсутності якоїсь частини інформації (невпевненість користувача у відповіді, відсутність відповіді на запитання). Незадіяні запити зберігаються системою, як не використані, і в подальшому сеансі роботи, відповівши на них, їх можна буде долучити до аналізу. Така гнучкість дозволяє користувачеві відповідати на запитання не лише в жорстко заданих межах (як це реалізовано в існуючих системах), а мати вибір порядку відповіді. Кожне запитання має певний діапазон можливих відповідей, що дозволяє створити шкалу впевненості, яка містить максимальні і мінімальні значення для всіх змінних.

Для оцінювання ступеня впливу розглядається сума квадратів відхилень для кожної змінної. Спочатку розраховується середнє значення оцінок, отриманих в результаті застосування правил для кожної змінної: $m = \sum_{j=1}^{n} \frac{x_{i,j}}{n}$, де m - середнє значення оцінок; n - кількість можливих виходів (результатів) системи; $x_{i,j}$ - значення масиву правил. Потім розраховується квадратичне відхилення цих оцінок від отриманих середніх значень: $v_i = \sum_{j=1}^{n} (x_{i,j} - m)^2 \cdot \left|\mathrm{MINI}(i) - \mathrm{MAXI}(i)\right|$, де MINI - масив мінімальних значень змінних; MAXI - масив максимальних значень змінних. Остання формула визначає значення v_i як суми квадратів відхилень відносно $x_{i,j}$ для змінної i за кожним можливим виходом системи.

Розглянутий метод вибирає змінну як найбільш важливу ту, оцінки якої більше відрізняються від середнього значення. В кінці аудиту генерується звіт, в якому структурно міститься інформація про заходи, що вже прийняті в інформаційній системі компанії, а також про ті, що відсутні, але мають бути застосовані для усунення ризиків, що присутні в системі менеджменту інформаційної безпеки компанії.

Висновки

Створена ЕС зручна у користуванні, увібрала у себе найкращі якості існуючих аналогів та позбавлена тих недоліків, що були виявлені при тестуванні подібних ЕС. Хоча на сьогоднішній день дана ЕС не може в повній мірі конкурувати зі своїми аналогами, перш за все за відсутності вибору різних методів обробки інформації та неможливості роботи в умовах невизначеності, але виявлені напрямки подальшого її доопрацювання. Отримані експериментальні результати свідчать про можливість створення ефективної ЕС на мові програмування високого рівня. Незначна доробка розробленої ЕС дозволить використовувати її для аудиту не лише в сфері інформаційної безпеки, а й у інших галузях науки й техніки, де традиційні математичні методи моделювання малопридатні.

Література

1. Стюарт Рассел, Питер Норвиг Искусственный интеллект: современный подход, 2-е изд.: Пер. с англ.- М.: Издательский дом “Вильямс”, 2006.- 1408 с.
2. Стандарт безопасности BS 7799 “Управление информационной безопасностью. Практические правила”, 2000.
3. Нейлор К. Как построить свою экспертную систему. М.: Энергоатомиздат, 1991.286с.

Дюжаев Л. П., Назарько А. И.

Экспертная система в области защиты информации.

Разработана консультационная экспертная система, позволяющая оценить степень соответствия системы менеджмента информационной безопасности предприятия требованиям международного стандарта ISO 17799 “Управление информационной безопасностью. Практические правила”. Оценивание рисков производится по Байесу. Программный продукт реализован в среде Borland C++ Builder 6.

Dyuzhaev L. P., Nazar’ko A. I.

Expert system in the field of the information security.

Consultative expert system for estimation of the level of conformance of the information security management system of the enterprise to the requirements of the standard ISO 17799 “Code of Practice for Information Security Management” has been developed. Bayes’s estimation of risks is performed. Appropriate software has been realized in the environment of Borland C++ Builder 6.