Об'єкти, що досліджуються, можуть мати різну конфігурацію, тому деякі факти є необов'язковими для деяких з них. На цій підставі значно скорочується кількість питань, що ставляться. Цього можна домогтися шляхом реалізації в системі методів оптимізації логічних виразів, за якими будується виведення нових знань. У випадку, коли користувач не знає відповіді на поставлене питання, повинна бути виконана спроба деталізації питань, шляхом з'ясування значень пов'язаних з ним фактів. З іншого боку, якщо отримана відповідь на повне питання, додаткові запитання ставитися не повинні. Оскільки експертна система призначена для того, щоб замінити експерта у відповідній галузі, користувач, що працює з нею, може мати досить низький рівень кваліфікації. У зв'язку з цим у системі повинна бути передбачена можливість перефразування питання з використанням синонімічних тверджень. Користувача можуть не цікавити певні канали витоку інформації. Тому система повинна дозволяти користувачеві керувати процесом експертизи за допомогою відсікання гілок виведення, які його не цікавлять.

У системі має бути реалізована можливість працювати не тільки з логічними даними, а й з числовими, такими як імовірність витоку інформації або вартість методів захисту. Тому система має бути здатна розраховувати значення за арифметичними формулами. Арифметичні значення можуть залежати від результатів процесу виводу, тому має сенс ввести спеціальні функції, що дозволяють в арифметичних формулах використовувати логічні значення, а також робити обчислення над сукупністю фактів. Оскільки в арифметичних формулах можуть зустрічатися змінні, значення яких не були обчислені через те, що відповідні їм логічні значення пропущені в процесі оптимізації, арифметичні формули також необхідно оптимізувати. У процесі експертизи користувач повинен мати можливість контролювати одержані результати, тому бажано, щоб на екран постійно видавалися проміжні значення.

У експертній системі повинен бути реалізований ряд сервісних функцій, таких як служба відкату, система підказок, генератор звітів різного ступеня деталізації.

Всі згадані особливості були враховані при розробці експертної системи ExPro, створеної на кафедрі спеціалізованих комп'ютерних систем Національного Технічного Університету "Київський Політехнічний Інститут".

УДК 681.518.54

ОСОБЛИВОСТІ НАВЧАННЯ ЕКСПЕРТНИХ СИСТЕМ, ОРІЄНТОВАНИХ НА ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

Юрій Русаков, Євген Кудінов

Національний Технічний Університет України «КПІ»

Анотація: **Доповідь присвячено процедурі навчання експертних систем, орієнтованих на задачі інформаційної безпеки. Аналізується сутність навчання експертних систем та деякі проблеми, що при цьому виникають. Наведено узагальнену структуру подання знань в експертних системах, орієнтованих на захист інформації, й деякі складнощі їх формування. Розглянуто основні етапи створення бази знань для оцінки інформаційної захищеності об'єкта.**

Summary: **The report is devoted to the procedure of learning of consulting models for solution of the tasks of information safety. The essence of learning and some problems, which arise thus, are analyzed. The generalized structure of representation of knowledge and some complexities of their creation is given. The main stages of creation of a knowledge base for an estimation of information security of the object are considered.**

Останнім часом експертні ситеми широко використовуються в багатьох галузях діяльності людини, зокрема для вирішення задач інформацйної безпеки. Для їх ефективної роботи необхідно сформувати певний набір знань, якими оперує експертна система, та за допомогою яких робляться певні висновки й розрахунки. Процес навчання експертної системи зводиться до формування цієї сукупності знань (бази знань). Саме від конкретного наповнення бази знань значною мірою залежить працездатність експертної системи та якість й вірогідність висновків, що зроблено з її допомогою. Тому дуже велике значення має технологія наповнення бази знань та форма подання знань в експертній системі, що навчається. Врахування специфіки конкретної предметної галузі вимагає побудови бази знань за відповідними правилами. Формування бази знань, яка забезпечувала б ефективну роботу експертної системи в цілому та прийнятну вірогідність результатів, що отримані за її допомогою, є найбільш трудомісткою та сладною задачею серед тих, що вирішуються під час створення та навчання експертних систем.

Кафедрою спеціалізованих комп'ютерних систем НТУУ "КПІ" розроблена експертна система ExPro для оцінки інформаційної захищеності об'єкта. В рамках проекту для формування бази знань був створений інтелектуальний редактор інформаційної бази, що значно спрощує процес навчання системи і приховує деталі технічної реалізації.

Велике значення для вірогідності результатів, отриманих за допомогою експерної системи, має узгодженість оцінок незалежних експертів. Тому перед заповненням бази знань необхідно виконати попередню обробку експертних оцінок. Така обробка повинна мати на меті вибір найбільш достовірних оцінок й відсіювання оцінок з малим ступенем вірогідності. Для вирішення цієї проблеми в рамках програмного комплексу ExPro розроблена програма статистичної обробки експертних оцінок.

Всі знання в базі формують єдину складну деревоподібну систему і процес експертизи зводиться до обрахування відповідної гілки. Формування дерева відбувається на етапі заповнення бази знань. Постає проблема об'єднання декількох баз знань, що створені для вирішення одного кола задач. Таке поєднання баз може бути особливо корисним у випадку роботи над навчанням однієї системи декількох інженерів зі знань. Для поєднання декількох баз знань необхідно не тільки органічно поєднати окремі гілки знань, але й виявити окремі піддерева з різних баз, що мають однакове призначення. Таке виявлення синонімічних гілок пов'язане з семантичним аналізом вмісту баз, що об'єднуються. Цей аналіз є дуже складною та трудомісткою задачею, а в зв'язку з відсутністю загальноприйнятої термінології він великою мірою ускладнюється через застосування різними операторами різних термінів для позначення однакових понять. Вирішення цієї проблеми додатково ускладнюється у зв'язку з тим, що знання в базах експертних систем зберігаються в певній логічно–математичній формі. Тому знання можуть бути синонімічними не тільки за значеннями назв категорій, якими оперують інженери з знань, а й за змістом арифметичніх формул та логічних висновків, що об'єднують ці категорії. Велике значення має також усунення неодозначностей та протиріч, що виникають під час роботи декількох експертів над навчанням однієї системи. Тут мається на увазі, що окремі гілки бази, які можуть належати у загальному випадку до різних характеристик об'єкта, що оцінюється, можуть обчислювати однакові величини різним чином, й відповідно отримувати різні, а іноді й протилежні та взаємовиключні результати. Виявлення та усунення подібних проблем має ще більшу складність, тому що при цьому треба переробити великий обсяг інформації та визначити ступінь синонімічності величин, що обчислюються, та зробити висновки про протиріччя, які можуть виникнути між ними під час обчислення. В доповіді наведено декілька можливих шляхів усунення цих проблем.

Розроблено деякі рекомендації, щодо процесу заповнення бази знань стосовно галузі інформаційної безпеки. До них належать вимоги до змісту бази, перелік необхідних й необов'язкових розділів знань, та пропозиції щодо послідовності навчання системи для вирішення задач з оцінки інформаційної захищеності об'єкта.

Запропонована методика дозволяє систематизувати та формалізувати процес навчання експертних систем для вирішення задач оцінки інформаційної захищеності об'єкта, а також усуває труднощі щодо послідовності формування бази знань та деякі додаткові проблеми, що виникають під час навчання.