вигляд логічного дерева, і яка може бути зручно приведена до системи логічних формул, які мають механізм оптимізації та скорочення. Схема побудови формул має практично універсальний набір функцій та констант, за допомогою яких можливий опис формули довільної складності з довільною кількістю аргументів. Тим самим за допомогою схем побудови предикатів та формул можливий опис предикатів та формул для довільного факту з довільної галузі знань. Отже експертна система оцінки інформаційної захищенності об’єкту має високий ступінь унівенсальності і може бути з успіхом застосована для вирішеня класу задач діагностики та покращення стану захищеності об’єкту дослідження від загроз в доволі великій кількості сфер діяльності людини, таких як медицина, захист інформації, спорт, психологія та інших.

УДК 681.518.54

АЛГОРИТМІЧНІ ОСОБЛИВОСТІ ЕКСПЕРТНИХ СИСТЕМ, ОРІЄНТОВАНИХ НА ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Денис Замятін, Михайло Прокофьєв

Національний Технічний Університет України “КПІ”

Анотація: **Доклад присвячено проблемам та особливості реалізації і використання експертних систем в області захисту інформації. Розглянуті методи забезпечення конфіденційності даних щодо конфігурації об’єкту, який досліджується. Особлива увага приділена питанням розробки блоку виведення нових знань.**

Summary: **The report is devoted to problems and features of realization and using of expert systems in branch of guard. Is examined methods of guarantee confidentiality of data about investigated object and peculiarities of development of block derivation of new knowledge.**

В сучасних умовах інформація є одним із найважливіших та найдорожчих ресурсів. У такій ситуації особливо актуального значення набуває задача оцінки імовірності витоку інформації для певного об’єкта і пошуку методів підвищення інформаційної захищенноті цього об’єкта. Розв’язання цієї задачі традиційними методами пов’язане з цілим рядом труднощів, як економічного, так і психологічного характеру. Одним із шляхів підвищення ефективності процесу оцінки захищеності об'єкта є створення відповідних комп'ютерних систем. В зв’язку з тим, що при аналізі інформаційної захищеності об'єкта необхідно брати до уваги велику кількість непов'язаних між собою чинників, реалізація такого аналізу є нетривіальною задачею, що складно формалізується. Для розв’язання такого роду задач найбільш продуктивним виявляється використання систем із штучним інтелектом, зокрема експертних систем.

Експертна система збирає інформацію про об'єкт, що досліджується, задаючи питання користувачеві. Відповіді користувача перетворюються в логічні константи, що відповідають певним фактам. На підставі цієї інформації виводяться нові знання про об'єкт, такі як імовірність витоку інформації і т.п.

Досвід розробки і застосування подібних систем дозволив визначити ряд специфічних проблем і алгоритмічних особливостей, характерних для галузі захисту інформації.

Інформація про об'єкт, що досліджується, представляється у вигляді сукупності логічних фактів. Оскільки ситуація на об'єкті звичайно динамічно змінюється, користувач може бути зацікавлений у можливості модифікувати значення вже зібраних фактів або додавати нові. Для реалізації такої можливості система має бути здатна зберігати базу даних на магнітних носіях. База даних сама по собі може бути об'єктом нападу зловмисників, оскільки вона містить практично всю інформацію про засоби і заходи захисту, використані на об'єкті, що досліджується. Тому сама база має бути надійно захищена від несанкціонованого доступу шляхом шифрування. Система має бути здатна идентифікувати користувача, що працює з нею, і дозволяти йому працювати тільки зі своїми базами.

Як зазначалося вище, вся інформація про об'єкт подана як сукупність фактів, слабо пов'язаних між собою. Тому, крім звичайних методів виведення, система повинна мати механізм послідовного встановлення ряду фактів. Цей механізм може бути реалізований у вигляді ряду ключових точок, що відображують певні стадії процесу виведення.

Для повноцінної роботи системи недостатньо двох стандартних логічних значень фактів. Крім того, що значення факту може бути істинним або хибним, мають бути додаткові варіанти для відображення ситуації, коли користувач не знає відповіді або система не здатна встановити факт. У зв'язку з цим необхідно розробити спеціальний розширений логічний тип даних. Для такого типу повинні бути спеціально модифіковані стандартні булеві функції, які коректно працюють зі значеннями, що були додані.

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.