

еї і ої є, аоі і аеа оа аеаеої оаї леа

УДК 519.87:685.51

ЗАСТОСУВАННЯ ЕКСПЕРТНИХ СИСТЕМ ДЛЯ ВИРІШЕННЯ ЗАВДАНЬ МОНІТОРИНГУ БЕЗПЕКИ АВТОМАТИЗОВАНИХ СИСТЕМ НАФТОГАЗОВОГО КОМПЛЕКСУ

Р.І. Храбатур, О.В. Храбатур, Л.І. Григорчук, С.М. Никифорок, Л.В. Саманів

ІФНТУНГ, 76019, м. Івано-Франківськ, вул. Карпатська, 15, тел.(0342) 507796,
e-mail: redntv@nung.edu.ua

Розглядається можливість впровадження експертних систем для вирішення завдань моніторингу безпеки автоматизованих систем нафтогазового комплексу. Основою експертної системи є сукупність знань, структурованих з метою формалізації процесу ухвалення рішень. Було показано, що експертна система, яка заснована на правилах If – Then, є однією з найбільш ефективних і доцільних для застосування в автоматизованих системах. Заснована на правилах If – Then експертна система складається з: бази знань, бази даних, механізму логічного висновку, засобів пояснення результатів і інтерфейсу користувача. Мова, що використовується для розробки експертних систем, спроектованих на основі цих моделей, називається мовою подання знань. Використання експертних систем дає змогу у багатьох випадках відмовитися від послуг висококваліфікованих фахівців, але припускає необхідність залишити в системі місце експертів з нижчою кваліфікацією. Експертні системи є засобами для розширення і посилення професійних можливостей кінцевого користувача.

Ключові слова: нафтогазовий комплекс, експертна система, правило If – Then, знання, бази знань, автоматизовані системи.

Рассматривается возможность внедрения экспертных систем для решения задач мониторинга безопасности автоматизированных систем нефтегазового комплекса. Основой экспертной системы является совокупность знаний, структурированных с целью формализации процесса принятия решений. Было показано, что экспертная система, основанная на правилах If – Then, является одной из наиболее эффективных и целесообразных для применения в автоматизированных системах. Основанная на правилах If – Then экспертная система состоит из: базы знаний, базы данных, механизма логического вывода, средств объяснения результатов и интерфейса. Язык, используемый для разработки экспертных систем, спроектированных на основе этих моделей, называется языком представления знаний. Использование экспертных систем позволяет во многих случаях отказаться от услуг высококвалифицированных специалистов, но предполагает возможность оставить в системе место эксперту с низкой квалификацией. Экспертные системы являются средствами для расширения и усиления профессиональных возможностей конечного пользователя.

Ключевые слова: нефтегазовый комплекс, экспертная система, правило If – Then, знания, базы знаний, автоматизированные системы.

The article considers the possibility of introduction of expert systems to solve the problems of safety of oil and gas complex automation systems. The expert system based on If-Then rules has been proved to be one of the most effective and reasonable for use in oil and gas complex automation systems. The expert system based on If-Then rules consists of a knowledge base, a database, an inference engine, result explanation facility and user interface. The language used in such expert systems development is called a knowledge representation language. Such expert systems can be controlled by less qualified experts. They enhance professional possibilities of final users.

Keywords: oil and gas complex, expert system, If-Then rule, knowledge, data bases, automation systems.

ВСТУП

З метою ефективного впровадження автоматизованих систем в нафтогазову галузь та ефективного управління ними широко використовуються експертні системи. Але вони не зав-

жди адекватно реагують на різноманітні ситуації і впроваджені далеко не в усіх можливих випадках. З цією метою розглядається доцільність впровадження експертних систем для вирішення завдань моніторингу безпеки систем нафтогазового комплексу.

АНАЛІЗ ЛІТЕРАТУРНИХ ДЖЕРЕЛ

Проаналізувавши літературні джерела, можна зробити висновок, що в даний час відомий ряд методів застосування інтелектуальних засобів в інформаційних технологіях [1]. До найбільш популярних інтелектуальних засобів відносять експертні системи, які засновані на правилах If – Then [2].

Експертна система (ЕС) – це сукупність методів і засобів організації, накопичення і застосування знань для вирішення складних завдань в деякій наочній області. Експертна система досягає вищої ефективності за рахунок перебору великого числа альтернатив при виборі рішення, спираючись на високоякісний досвід групи фахівців, аналізує вплив великого об'єму нових чинників, оцінюючи їх при побудові стратегій, додаючи можливості прогнозу. Також ЕС – це клас комп'ютерних програм, які пропонують рекомендації, проводять аналіз, виконують класифікацію, дають консультації і ставлять діагноз. Вони орієнтовані на розв'язування задач, вирішення яких вимагає проведення експертизи людиною-спеціалістом. На відміну від програм, що використовують процедурний аналіз, експертні системи розв'язують проблеми у вузькій предметній площині (конкретній ділянці експертизи) на основі логічних міркувань. Такі системи часто можуть знайти розв'язок задач, які неструктуровані і неточно визначені. Вони через використання евристик компенсують відсутність структурованості, що корисно в ситуаціях, коли кількість необхідних даних або часу є недостатньою, виключає можливість проведення повного аналізу.

Однак *ЕС не завжди адекватно реагують на різноманітні ситуації і впроваджені далеко не у всіх можливих випадках, тому вони потребують постійного дослідження та вдосконалення.*

Метою дослідження даної статті є аналіз ефективності та обґрунтування доцільності впровадження ЕС для моніторингу безпеки автоматизованих систем нафтогазового комплексу.

Основою експертної системи є сукупність знань (бази знань), структурованих з метою формалізації процесу ухвалення рішень.

Експертна система може функціонувати у двох режимах: введення знань та консультації.

У першому режимі введення знань експерт за допомогою інженера по знаннях та редактора бази знань вводить відомі йому дані про предметну область у базу знань ЕС.

У другому режимі консультації користувач веде діалог з ЕС. Надає їй відомості про поточні завдання і отримує рекомендації ЕС. Наприклад, на основі відомостей про фізичний стан об'єкта, ЕС ставить діагноз у вигляді переліку можливих дефектів чи причин виникнення збою в роботі обладнання, які є найбільш ймовірними за наявних даних.

ЕС можна класифікувати за двома видами ознак:

Класифікація експертних систем за задачею, що розв'язується:

- Аналіз даних
- Діагностування
- Моніторинг
- Проектування
- Прогнозування
- Зведення
- Планування
- Навчання
- Управління
- Ремонт
- Налаштування

Класифікація експертних систем за зв'язком з реальним часом:

- Статичні ЕС
- Квазідинамічні ЕС
- Динамічні ЕС

ЕТАПИ РОЗРОБКИ ЕКСПЕРТНИХ СИСТЕМ

Етап ідентифікації проблем: визначаються завдання, які підлягають вирішенню; виявляється мета розробки; визначаються експерти і типи користувачів.

Етап здобуття знань: проводиться змістовний аналіз проблемної області; виявляються поняття, що використовуються, і їх взаємозв'язки; визначаються методи розв'язання задач.

Етап структурування знань: вибираються інформаційні системи (ІС) і визначаються способи подання всіх видів знань; формалізуються основні поняття; визначаються способи інтерпретації знань; моделюється робота системи; оцінюється адекватність цілям системи зафіксованих понять, методів рішень, засобів подання й маніпулювання знаннями.

Етап формалізації: здійснюється наповнення експертом бази знань, який є найбільш важливим і найбільш трудомістким етапом розробки ЕС.

Процес набуття знань поділяють на внесення знань експертом, організацію знань, що забезпечує ефективну роботу системи, і подання знань в програмному вигляді, зрозумілому ЕС. Процес здійснюється інженером по знаннях на основі аналізу діяльності експерта з розв'язання реальних завдань.

Реалізація ЕС: створюється один або декілька прототипів ЕС, що вирішують необхідні завдання.

Етап тестування: проводиться оцінка представлення знань в ЕС загалом.

Експертні системи розробляються з навчальною метою. Вони здатні обґрунтувати логіку вибору рішення, тобто володіють властивостями адаптивності і аргументації даного рішення. У більшості експертних систем є механізм пояснення, який використовує знання, необхідні для пояснення того, яким чином система дійшла даного рішення. Дуже важливим є визначення області застосування експертної системи, меж її використання і дії. Переваги експертних систем в порівнянні з використанням досвідчених фахівців полягають в наступному:

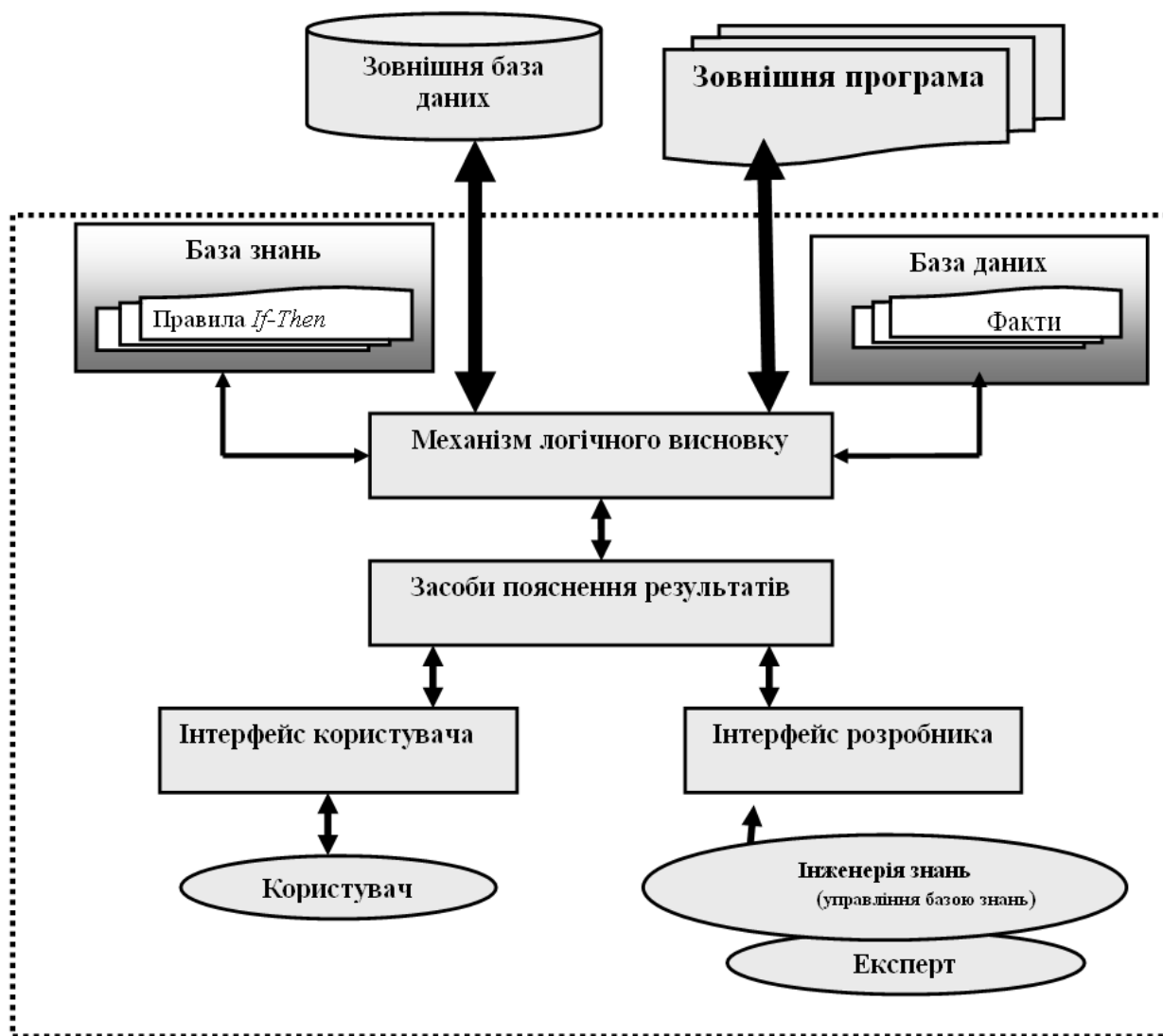


Рисунок 1 – Експертна система, яка заснована на правилах If - Then

- досягнута компетентність не втрачається, може документуватися, передаватися, відтворюватися і нарощуватися;
- мають місце стійкіші результати, відсутні емоційні і інші чинники людської ненадійності;
- висока вартість розробки урівноважується низькою вартістю експлуатації, можливістю копіювання, а загалом ЕС більш економічні за висококваліфікованих фахівців.

Подання знань в експертних системах

Першим і основним питанням, яке треба вирішити при поданні знань, є питання визначення складу знань, тобто визначення того, "ЩО ПОДАВАТИ" в експертній системі. Друге питання стосується того, "ЯК ПОДАВАТИ" знання. Необхідно відзначити, що ці дві проблеми не є незалежними. Дійсно, обраний спосіб подання може виявитися непридатним в принципі або неефективним для вираження деяких знань.

Питання "ЯК ПОДАВАТИ" можна поділити на два значною мірою незалежні завдання: як організувати (структурувати) знання і як подати знання у вибраному формалізмі.

Прагнення виділити організацію знань в самостійну задачу викликано тим, що ця задача виникає для будь-якої мови подання знань. Способи вирішення цього завдання є однако-вими (або схожими) незалежно від формалізму, що використовується.

Отже, до кола питань, що вирішуються при поданні знань, будемо включати:

- визначення складу подання знань;
- організацію знань;
- подання знань, тобто визначення моделі подання.

Склад знань ЕС визначається такими чинниками:

- проблемним середовищем;
- архітектурою експертної системи;
- потребами та цілями користувачів;
- мовою спілкування.

Відповідно до загальної схеми статичної експертної системи (рис. 1). Для її функціонування потрібні такі знання:

- знання про процес розв'язання задачі (тобто керуючі знання), що використовуються інтерпретатором (користувачів);

- знання про мову спілкування і способи організації діалогу, використані лінгвістичним процесором (діалоговим компонентом);

- знання про способи подання та модифікації знань, які використовуються компонентом надбання знань;

- підтримання структурних та керуючих знань, використані пояснювальним компонентом.

Для динамічної ЕС, також, потрібні такі знання:

1) знання про методи взаємодії із зовнішнім оточенням;

2) знання про модель зовнішнього світу.

Залежність складу знань від вимог користувача проявляється в наступному:

- які завдання (із загального набору завдань) і з якими даними хоче вирішувати користувач;

- які бажані способи і методи вирішення;

- за яких обмежень на кількість результатів і способи їх отримання повинна бути вирішена задача;

- які вимоги до мови спілкування й організації діалогу;

- яка ступінь спільності (конкретності) знань про проблемну область, доступна користувачеві;

- які цілі користувачів.

Склад знань про мову спілкування залежить як від мови спілкування, так і від необхідного рівня розуміння.

З урахуванням архітектури експертної системи знання доцільно ділити на інтерпретуючі і неінтерпретуючі. До першого типу відносяться ті знання, які здатні інтерпретувати користувач (інтерпретатор). Всі інші знання відносяться до другого типу. Користувач не знає їх структури та змісту. Якщо ці знання використовуються компонентом системи, то він не "усвідомлює" цих знань. Неінтерпретуючі знання поділяються на допоміжні знання, що зберігають інформацію про лексику і граматику мови спілкування, інформацію про структуру діалогу, і підтримують знання. Допоміжні знання обробляються природно-мовною компонентою, але хід цієї обробки користувач не усвідомлює, тому що цей етап обробки вхідних повідомлень є допоміжним для проведення експертизи. Підтримуючі знання використовуються при створенні системи і при виконанні пояснень, виконують роль описів (обґрунтувань), як інтерпретуються знання, і дії системи. Підтримуючі знання поділяються на технологічні і семантичні:

- технологічні підтримують знання і містять відомості про час створення описуваних ними знань, про автора знань тощо;

- семантичні підтримують знання і містять смисловий опис цих знань. Вони містять інформацію про причини введення знань, про призначення знань, описують спосіб використання знань і одержуваний ефект.

Знання, що інтерпретуються, можна розділити на предметні знання, керуючі знання і знання про подання:

знання про подання містять інформацію про те, яким чином (в яких структурах) в системі подано знання, що інтерпретуються;

предметні знання містять дані про предметну область і способи перетворення даних у вирішенні поставлених завдань. Зауважимо, що стосовно предметних знань, знання про подання та знання про управління є метазнаннями. У предметних знаннях виділяють описувачі і власне предметні знання. Описувачі містять певну інформацію про предметні знання, зокрема коефіцієнт визначеності правил і даних, заходи важливості і складності. Власне предметні знання розбиваються на факти і виконуваний твердження. Факти визначають можливі значення сутностей і характеристик предметної області. Виконуваний твердження можуть містити інформацію про те, як можна змінювати опис предметної області в ході вирішення задачі. Інакше кажучи, виконуваний твердження – це знання, що задають процедури обробки. Під терміном "процедурні знання" ми розуміємо, що ці знання задаються не тільки в процедурній, але і в декларативній формі;

керуючі знання поділяють на фокусуючі і вирішальні. Фокусуючі знання описують знання, які слід використовувати в тій чи іншій ситуації. Зазвичай фокусуючі знання містять відомості про найбільш перспективні об'єкти або правила, які доцільно використовувати при перевірці відповідних гіпотез. У першому випадку увага фокусується на елементах робочої пам'яті, у другому – на правилах бази знань. Вирішальні знання містять інформацію, яка використовується для вибору способу інтерпретації знань, відповідно до поточної ситуації. Ці знання застосовуються для вибору стратегій або евристик, найбільш ефективних для вирішення даного завдання.

Якісні та кількісні показники експертної системи можуть бути значно покращені за рахунок використання метазнань, тобто знань про знання. Метазнання не мають певної єдиної сутності, вони можуть застосовуватися для досягнення різних цілей.

Перелічимо можливі застосування метазнань:

1) метазнання у вигляді стратегічних метаправил використовуються для вибору релевантних правил;

2) метазнання використовуються для обґрунтування доцільності застосування правил з області експертизи;

3) метаправила використовуються для виявлення синтаксичних і семантичних помилок в предметних правилах;

4) метаправила дозволяють системі адаптуватися до оточення шляхом перебудови предметних правил і функцій;

5) метаправила дозволяють явно вказати можливості і обмеження системи, тобто визначити, що система знає, а чого не знає.

Питання організації знань необхідно розглядати в будь-якому поданні, та їх вирішення здебільшого не залежить від обраного способу (моделі) уявлення.

Виділимо аспекти проблеми організації знань:

- організація знань за рівнями уявлення і за рівнями детальності;
- організація знань в робочій пам'яті;
- організація знань у базі знань;
- організація знань в базі даних.

Показником інтелектуальності системи з точки зору подання знань вважається здатність системи використовувати в потрібний момент необхідні (релевантні) знання. Системи, що не мають засобів для визначення релевантних знань, неминуче стикаються з проблемою "комбінаторного вибуху". Можна стверджувати, що ця проблема є однією з основних причин, що обмежують сферу застосування експертних систем.

У проблемі доступу до знань можна виділити три аспекти: зв'язність знань і даних, механізм доступу до знань і спосіб зіставлення.

Зв'язність (агрегація) знань є основним способом, що забезпечує прискорення пошуку релевантних знань. Більшість фахівців дійшли висновку, що знання слід організувати навколо найбільш важливих об'єктів (сутностей) предметної області. Всі знання, що характеризують деяку сутність, зв'язуються і подаються у вигляді окремого об'єкта. При подібній організації знань, якщо системі потрібна інформація про деяку сутність, то вона шукає об'єкт, що описує сутність, а вже потім всередині об'єкта знаходить інформацію про цю сутність. В об'єктах доцільно виділяти два типи зв'язків між елементами: зовнішні і внутрішні. Внутрішні зв'язки об'єднують елементи в єдиний об'єкт і призначені для вираження структури об'єкта. Зовнішні зв'язки відображають взаємозалежності, що існують між об'єктами в області експертизи. Багато дослідників поділяють зовнішні зв'язки на логічні і асоціативні. Логічні зв'язки виражають семантичні відносини між елементами знань, асоціативні зв'язки призначені для забезпечення взаємозв'язків, сприяють прискоренню процесу пошуку релевантних знань.

Моделі подання знань

Однією з найбільш важливих проблем, характерних для систем, заснованих на знаннях, є проблема подання знань. Це пояснюється тим, що форма подання знань здійснює суттєвий вплив на характеристики та властивості системи. Для того, щоб маніпулювати знаннями з реального світу за допомогою комп'ютера, необхідно здійснювати їх моделювання. У таких випадках необхідно відрізнити знання, призначені для обробки комп'ютером, від знань, що використовуються людиною. Крім того, при великому обсязі знань бажано спростити послідовне управління окремими елементами знань.

При проектуванні моделі подання знань слід враховувати такі фактори, як однорідність подання і простота розуміння. Однорідне подання призводить до спрощення механізму керування логічними висновками і спрощення управління знаннями. Спосіб подання знань має бути зрозумілим експертам і користувачам

системи. В протилежному випадку придбання знань та їх оцінка буде ускладнена. Проте виконати цю вимогу однаковою мірою як для простих, так і для складних завдань є досить важко. Зазвичай для нескладних завдань зупиняються на деякому середньому (компромісному) поданні, але для вирішення складних і об'ємних завдань необхідне структурування і модульне подання знань.

Типовими моделями подання знань є:

- логічна модель;
- модель, заснована на використанні правил (продукційна модель);
- модель, заснована на використанні фреймів;
- модель семантичної мережі.

Однак у всіх розроблених системах з базами знань крім цих моделей використовувалися спеціальні (для конкретного випадку) моделі. Подання знань є складним, але класифікація моделей залишалася незмінною.

Мова, що використовується для розробки систем, спроектованих на основі цих моделей, називається мовою подання знань.

Основною проблемою при роботі з великою базою знань є проблема пошуку знань, релевантних до розв'язуваної задачі. У зв'язку з тим, що в даних може не міститися явних вказівок на значення, необхідних для їх обробки, необхідний більш загальний механізм доступу, ніж метод прямого доступу (метод явних посилань). Завдання цього механізму полягає в тому, щоб за деяким описом суті, наявним в робочій пам'яті, знайти у базі знань такі об'єкти, що задовольняють цьому опису. Очевидно, що впорядкування і структурування знань можуть значно прискорити процес пошуку.

Загалом знаходження бажаних об'єктів доречно розглядати як двоетапний процес. На першому етапі, що відповідає процесу вибору за асоціативними зв'язками, здійснюється попередній вибір у базі знань потенційних кандидатів на роль бажаних об'єктів. На другому етапі шляхом виконання операції зіставлення здійснюється остаточний вибір шуканих об'єктів. При організації такого механізму доступу виникають певні труднощі: «Як вибрати критерій придатності кандидата?»; «Як організувати роботу в конфліктних ситуаціях?» тощо.

Операція зіставлення може використовуватися не тільки як засіб вибору потрібного об'єкта з безлічі кандидатів, але й для класифікації, підтвердження, декомпозиції і корекції. Для ідентифікації невідомого об'єкта, він може бути зіставлений з деякими відомими зразками. Це дасть змогу класифікувати невідомий об'єкт як такий відомий зразок, при зіставленні з яким були отримані кращі результати. Якщо здійснюється зіставлення деякого відомого об'єкта з невідомим описом, то в разі успішного зіставлення буде здійснена часткова декомпозиція опису.

Існують різні операції зіставлення. Зазвичай виділяють такі їх форми: синтаксичне, параметричне, семантичне та примусове зіставлення. У випадку синтаксичного зіставлення

співвідносять форми (зразки). Успішним є зіставлення, в результаті якого зразки виявляються ідентичними. Зазвичай вважається, що змінна одного зразка може бути ідентична будь-якій константі (або виразу) іншого зразка. Іноді на змінні, що входять до зразка, накладають вимоги, що визначають тип констант, з якими вони можуть зіставлятися. Результат синтаксичного зіставлення є бінарним: зразки зіставляються або не зіставляються. В параметричному зіставленні вводиться параметр, що визначає ступінь зіставлення. У разі семантичного зіставлення співвідносяться не зразки об'єктів, а їх функції. У разі примусового зіставлення один зразок розглядається з точки зору іншого. На відміну від інших типів зіставлення, в цьому випадку буде отримано позитивний результат. Питання лише в силі примусу. Примус можуть виконувати спеціальні процедури, що пов'язуються з об'єктами. Якщо ці процедури не в змозі здійснити зіставлення, то система повідомляє, що успіх може бути досягнутий тільки в тому випадку, якщо певні частини аналізованих сутностей можна вважати частково зіставленими.

Методи пошуку рішень в експертних системах

Методи вирішення задач залежать від особливостей предметної області, в якій вирішується завдання, і від вимог, що висуваються користувачем до вирішення. Особливості предметної області, з точки зору методів розв'язання, можна характеризувати такими параметрами:

- розмір, що визначає обсяг простору, в якому належить шукати розв'язок;
- змінність області, характеризує ступінь змінності області в просторі і часі (виділяються статичні та динамічні області);
- повнота моделі, яка описує область, характеризує адекватність моделі, що використовується для опису даної області. Якщо модель не повна, то для опису області використовується декілька моделей, що доповнюють одна одну за рахунок відображення різних властивостей, предметної області;
- визначеність даних про розв'язок задачі, характеризується ступенем точності (хибності) та повноти (неповноти) даних. Точність (хибність) є показником того, що предметна область з точки зору розв'язуваних задач описана точними або неточними даними; під повнотою (неповнотою) даних розуміється достатність (недостатність) вхідних даних для однозначного вирішення завдання.

Вимоги користувача до результату завдання, що вирішується за допомогою пошуку, можна характеризувати кількістю рішень і властивостями досягнутого результату і (або) способом його одержання. Параметр "кількість рішень" може набувати таких основних значень: одне рішення, декілька рішень, всі рішення. Параметр "властивості" задає обмеження, яким повинен задовольняти отриманий результат або спосіб його одержання. Параметр "властивості" може, визначати і такі особливості, як: час ви-

рішення ("не більш ніж", "діапазон часу" і т.п.); обсяг пам'яті, що використовується для отримання результату; вказівку про обов'язковість (неможливість) використання будь-яких знань (даних) і т.д.

Отже, складність завдання, що визначається вищенаведеним набором параметрів, варіюється від простих задач малої розмірності з незмінними певними даними і відсутністю обмежень на результат і спосіб його отримання до складних задач. Вони визначаються великою розмірністю змінних, помилковими і неповними даними і довільними обмеженнями на результат і спосіб його отримання. Із загальних міркувань випливає, що будь-яким одним методом не можна вирішити всі завдання.

Відмінності експертних систем від звичайних комп'ютерних програм:

- експертні системи маніпулюють знаннями, тоді як будь-які інші системи – даними;
- експертні системи, як правило, дають ефективні оптимальні рішення і здатні іноді помилитися, але, на відміну від традиційних комп'ютерних систем, вони мають потенційну здатність вчитися на своїх помилках.

Ефективність експертних систем полягає в можливості опису досвіду спеціалістів інформаційної безпеки у вигляді доступної для аналізу форми системи правил If (Умова) – Then (Наслідок) або дерева рішень, а процес логічного висновку подібний за характером до людських міркувань.

Процес опису послідовності міркувань за правилами If (Умова) – Then (Наслідок) реалізований в ланцюжках прямих і зворотних міркувань [3, 4].

У першому випадку в основу покладено принцип готовності даних. Для частини If (Умова) правил справедливі всі значення, то правило активується і формується висновок, що міститься в частині Then (Наслідок). Перевагою даного підходу є потенційна можливість розпаралелювання пошуку готових правил по всій базі знань експертної системи, а недоліком - витрати обчислювальних потужностей автоматизованих систем на обробку всіх готових правил без урахування їх необхідності для вирішення конкретних завдань.

У другому випадку спочатку обмежується зона пошуку готових до обробки правил If (Умова) - Then (Наслідок) шляхом розповсюдження запитів, а потім здійснюється обробка відібраної підмножини правил If (Умова) – Then (Наслідок).

Заснована на правилах If – Then експертна система (рис. 1) складається з: бази знань, бази даних, механізму логічного висновку, засобів пояснення результатів і інтерфейсу користувача. Знання в експертній системі організовані у вигляді ієрархічної системи правил If (Умова) – Then (Наслідок).

Система логічного висновку здійснює підстановку значень з бази даних у поля посилки частини If (Умова) правил бази знань. У випадку заповнення полів всіх посилки активізує готові до обробки правила, формуючи висновки

відповідно до частини Then (Наслідок) правил. Результати роботи експертної системи доступні користувачеві через діалоговий інтерфейс. Він за необхідності дозволяє ознайомитися з ходом логічних міркувань системи що призводить до отримання даного результату.

Експертні системи можуть успішно застосовуватися для виявлення несанкціонованих дій порушників в автоматизованих системах обробки інформації [5]. Схеми виявлення несанкціонованих дій можна поділити на дві категорії: виявлення зловживань і виявлення аномалій [6].

До виявлення зловживань можна віднести несанкціоновані дії, які використовуються відомими вразливими місцями автоматизованих систем.

Для виявлення аномалій виявляється діяльність, яка відрізняється від шаблонів, встановлених для користувачів або груп користувачів автоматизованої системи.

Виявлення аномалій пов'язане зі створенням бази даних, що містить профілі контролюваної діяльності. Виявлення зловживань пов'язане з порівнянням діяльності користувача з відомими шаблонами поведінки порушника, використовуючи методи, засновані на правилах, що описують сценарії атак. Механізм виявлення несанкціонованих дій ідентифікує потенційні атаки в тому випадку, якщо дії користувача не збігаються з встановленими правилами.

Більшість систем виявлення зловживань та аномалій засновані на моделі [7], яка підтримує набір профілів легальних користувачів; погоджує запис підсистеми аудиту з відповідним профілем; оновлює і повідомляє про виявлені аномалії. Поведінка користувача може бути подана моделлю на основі правил або аналізом зміни стану. Для виявлення факту атаки використовують методи зіставлення із зразком.

Недоліком експертних систем, характерним для їх сучасного стану, є менша пристосованість до навчання новим правилам і концепціям, до творчості і винахідництва. Використання експертних систем дозволяє у багатьох випадках відмовитися від висококваліфікованих фахівців, але припускає залишити в системі місце експертів з нижчою кваліфікацією. Експертні системи є засобами для розширення і посилення професійних можливостей кінцевого користувача.

Експертна система повинна демонструвати компетентність, тобто досягати в конкретній наочній області того ж рівня, що і фахівці-експерти. Недостатньо знаходити правильні рішення, але треба робити це швидко. Системи повинні мати не тільки глибоке, але і достатньо широке розуміння об'єкту. Методи знаходження рішення проблем досягаються на основі знаходження вирішень задач, які впливають з фундаментальних принципів у разі некоректних даних або неповних наборів правил. Такі властивості найменш розроблені в комп'ютерних експертних системах, але саме вони притаманні фахівцям високого рівня.

Крім того, до недоліків експертних систем слід віднести трудомісткість формування та підтримки актуальної бази знань у вигляді несуперечливої системи правил логічного висновку, заснованої на особистому досвіді експертів. Орієнтована на чіткі достовірні дані, ієрархія правил експертної системи не є достатньо гнучкою.

Тому з метою застосування експертних систем для вирішення завдань моніторингу безпеки автоматизованих систем нафтогазового комплексу необхідно створити програмні продукти, що відрізняються від традиційних програм. Їхні основні властивості:

- застосування для вирішення проблем великого досвіду, що є рівнем мислення найбільш кваліфікованих експертів у даній області, і веде до прийняття творчих рішень – точних і ефективних;
- наявність прогностичних можливостей, за яких ЕС видає відповіді не тільки для конкретної ситуації, але і показує, як змінюються ці відповіді в нових ситуаціях, з можливістю докладного пояснення, яким чином нова ситуація призвела до змін;
- можливість використання ЕС для навчання і тренування керівників, забезпечуючи нових спеціалістів великим багажем досвіду і стратегій.

ВИСНОВКИ

Отже, проблема впровадження експертних систем для вирішення завдань моніторингу безпеки автоматизованих систем нафтогазового комплексу є актуальною і потребує подальшого вивчення та вдосконалення. Методи знаходження рішень проблем досягаються на основі знаходження розв'язків задач, що виникли, чи впливають з фундаментальних принципів у разі некоректних даних або неповних наборів правил. Одним із шляхів для цього є впровадження запропонованої ЕС, яка заснована на правилах If – Then.

Але ЕС не завжди адекватно реагують на різноманітні ситуації і впроваджені далеко не у всіх можливих випадках. Тому ЕС потребують постійного подальшого дослідження та вдосконалення.

Література

- 1 Суханов А.В. Организация средств защиты на основе аналогии с биосистемами / А.В. Суханов // Журнал научных публикаций аспирантов и докторантов. – 2008. – № 6. – С. 114-119.
- 2 Суханов А.В. Оценки информационных ресурсов и безопасности глобальных информационных систем / А.В. Суханов // V Санкт-Петербургская региональная конференция «Информационная безопасность регионов России-2007 (ИБРР-2007)». – 2007. – С. 85-92.

3 Суханов А.В. Моделирование средств оценки защищенности информационных систем / А.В. Суханов // V Санкт-Петербургская региональная конференция «Информационная безопасность регионов России-2007 (ИБРР-2007)». – 2007. – С. 102-104.

4 Нестерук Г.Ф. Адаптивные средства обеспечения безопасности информационных систем / Нестерук Г.Ф., Суханов А.В.; под ред. Л.Г. Осовецкого. – СПб.: Изд-во Политехнического университета, 2008.

5 Суханов А.В. Автоматизированные средства анализа защищенности информационных систем / А.В. Суханов // Журнал научных публикаций аспирантов и докторантов. – 2008. – № 5. – С. 137-141.

6 Суханов А.В. Адаптивная защита информационных систем / Суханов А.В. Крылов А.И. // Изв. вузов. Приборостроение. – 2008. – № 12. – С. 17 – 22.

7 Суханов А.В. Подход к построению защищенных информационных систем / А.В. Суханов // Информационные технологии. – 2009. – № 6. – С. 57 – 61.

*Стаття надійшла до редакційної колегії
07.02.12
Рекомендована до друку професором
Д.Ф. Тимківим*