

ОСОБЛИВОСТІ ТА МЕТОДИКА СТВОРЕННЯ ЕКСПЕРТНОЇ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕННЯ ЩОДО УПРАВЛІННЯ КОМПЛЕКСНОЮ БЕЗПЕКОЮ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ТА НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Розглядаються проблемні питання загальносистемного та специфічного характеру, пов'язані з управлінням комплексною безпекою інформації в інформаційно-телекомунікаційних системах (ІТС) та об'єктах інформаційної діяльності (ОІД) органів державного та військового управління. Обґрунтовано та запропоновано етапи методики створення експертної системи підтримки прийняття рішення (ЕС) з досліджених проблем управління комплексною безпекою інформації в ІТС та на ОІД.

Ключові слова: інформаційно-телекомунікаційна система (ІТС), технічний захист інформації (ТЗІ), експертна система (ЕС), об'єкт інформаційної діяльності (ОІД), об'єкти протидії загрозам інформації (ОПД), технічна розвідка (ТР), управління комплексною безпекою інформації (УКБІ), спеціальне програмне забезпечення (СПЗ), механізм прийняття рішень (МПР), конфіденційна інформація (КІ).

У сучасних умовах якість організації та впровадження на адміністративних та військово-промислових об'єктах України, інформаційно-телекомунікаційних системах, зразках та комплексах озброєння та військової техніки, обладнаних територіях (далі ОПД – об'єкти щодо яких можуть застосовуватися загрози інформації, об'єкти протидії загрозам інформації, об'єкти протидії технічним розвідкам) комплексу робіт з управління комплексною безпекою інформації (далі УКБІ) при здійсненні діяльності, пов'язаної з інформацією, що містить відомості, віднесені законодавством України до державної таємниці, службової інформації, а також конфіденційної інформації (далі - КІ) та іншої, вимоги щодо захисту якої встановлено законодавством, залежить від повноти і рівня автоматизації інформаційного, математичного та нормативно-методичного забезпечення цих заходів, від кількісного обґрунтування змісту й обсягу робіт із УКБІ.

Крім того, обґрунтований вибір відповідного рівня УКБІ є основною задачею проектування комплексу УКБІ для ОПД. При цьому необґрунтоване зниження або підвищення рівня захисту неминує веде до нераціонального розподілу ресурсів чи до втрати ресурсів, що виділяються для забезпечення УКБІ.

Метою статті є розгляд проблемних питань та методики розробки ЕС як взаємопов'язаної послідовності дій експертів і розробників з метою визначення її структури, особливостей і основних вимог до неї.

Загальні проблемні питання. Виконання завдань із створення комплексу технічного захисту інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах наявна достатня нормативна база, але її використання на практиці пов'язане зі значними труднощами. Ці труднощі обумовлені, перш за все, зі значним об'ємом вхідних даних для проведення оцінки можливих загроз із боку технічних розвідок та визначення переліку адекватних організаційних й інженерно-технічних заходів із протидії; з необхідністю створення розвинутих автоматизованих систем для обробки й аналізу цих даних, що потребує проведення відповідних наукових досліджень і розробки методик побудови цих систем.

Тому виникає гостра необхідність розробки інформаційних систем, що автоматизують процес оцінки можливостей технічних розвідок і надають кінцевому користувачеві конкретні рекомендації на основі всебічного аналізу ОПД та результатів розрахунку й оцінки можливих загроз. Формування і надання обґрунтованих та конкретних рекомендацій із УКБІ вимагає проведення науково-дослідних робіт щодо формалізації, автоматизованого накопичення й ефективного використання знань спеціалістів-експертів, в тому числі, знань, сконцентрованих у нормативно-методичному забезпеченні УКБІ. Виконання цих досліджень

можливо тільки шляхом розробки та впровадження в практику заходів із УКБІ нових інформаційних технологій, зокрема технології експертних систем.

На даний час у сфері ТЗІ в Україні фактично відсутні єдині підходи і реальні розробки інформаційних систем з елементами штучного розуму, одним із класів яких є експертні системи. В основному існуючі експертні системи застосовуються для обґрунтування шляхів і методів ТЗІ на об'єкті [1], кінцевої експертної оцінки захищеності КІ та оцінки загроз (ризиків) в автоматизованих системах. Але більшість цих експертних систем носять загальний характер і слабо орієнтовані на практичне використання щодо оцінки захищеності інформації для конкретного об'єкта.

Також останнім часом у інших країнах активно ведуться науково-дослідні роботи із створення програмних систем для експертного оцінювання ризиків і обґрунтування комплексних систем безпеки [2], наприклад: система COBRA – у вигляді системного опитувача за міжнародним стандартом ISO 17799 (розробник фірма C&A System Security Ltd. COBRA); система RiskPac – перевіряє базовий рівень захищеності і представляє собою калькулятор середньорічних втрат, що очікуються у різних видах інформаційних ресурсів (розробник фірма CSCI, США); системи RiskWatch (США), MARION (розробник CLUSIF, Франція), CRAMM (розробник компанія Logica, Великобританія), які побудовані із використанням структурних методів системного аналізу і проектування.

Але вказані програмні системи стосуються тільки вирішення питань оцінки захищеності автоматизованих систем з урахуванням вимог міжнародних стандартів і фактично не використовують технологію експертних систем.

Одним із шляхів вирішення зазначених проблем у сфері ТЗІ є розробка й активне використання на практиці експертної системи підтримки прийняття рішень із управління комплексною безпекою інформації.

Із урахуванням положень [3], ЕС підтримки прийняття рішень – це діалогова система з елементами штучного розуму, яка на основі розвинутих баз даних і знань, математичних моделей формує (генерує) відповідні рекомендації і допомагає кінцевому користувачеві приймати оптимальні рішення щодо організації УКБІ на конкретному об'єкті.

Розробка ЕС може проводитися в рамках створення та впровадження у повсякденну діяльність органів і підрозділів відповідальних за захист інформації спеціального програмного забезпечення (СПЗ) для автоматизації процесів проведення розрахунків та оцінки ризиків та надання раціональних рекомендацій щодо адекватної протидії для ОПД як у разі конкретного виду загрози безпеки інформації, так і у разі комплексного їх застосування [4]. Створенню ЕС повинна передувати розробка сукупності функціонально закінчених програмних модулів для оцінки можливостей загроз з розвинутими базами даних щодо їх можливостей, умов застосування, які складуть інформаційну основу для функціонування ЕС. При цьому ЕС розглядається як “ядро” або інтелектуальна частина вказаної СПЗ. Розробка ЕС є однією із наукоємних і складних завдань, які доводиться вирішувати при створенні СПЗ, і тому потребує формування відповідної методики.

Методика розробки ЕС. Методика розробки ЕС, що пропонується, враховує властивості подібних інформаційних систем й спирається на існуючий досвід їх практичної розробки та застосування.

Методика являє собою технологічну послідовність від етапів дослідження і формалізації предметної області до розробки структури та основних вимог до ЕС. Методика має узагальнений характер і може використовуватися для побудови ЕС під час вирішення широкого кола завдань у сфері ТЗІ, а не тільки для підтримки прийняття рішень із управління комплексною безпекою інформації.

Методика передбачає послідовне вирішення наступних задач: проведення аналізу предметної області; обґрунтування доцільності розробки ЕС; визначення структури, рівня розробки й основних вимог до ЕС.

Етап 1. Аналіз предметної області.

1. Предметною областю, для якої створюється ЕС, є можливі загрози інформації для ОПД та організація відповідної роботи з протидії за результатами оцінки ризиків щодо конкретного об'єкта.

Основною тематикою інформації, що повинна оброблятися в ЕС, є:

- можливості, тактико-технічні характеристики носіїв та засобів технічних розвідок для здійснення розвідувальної діяльності щодо України;
- характеристики конкретного адміністративного, військово-промислового об'єкта щодо якого створюється система управління комплексною безпекою інформації;
- експертні дані (факти) і знання спеціалістів-експертів у сфері технічного захисту інформації з питань УКБІ.

2. Визначення мети створення та основних завдань ЕС [5].

У нашому випадку, основною метою створення ЕС є забезпечення:

- науково-обґрунтованого вибору заходів із протидії в конкретних умовах функціонування ОПД;
- необхідного рівня оперативності прийняття рішень щодо реальних загроз КІ, яка циркулює на ОПД;
- обґрунтованості розробки керівних документів із УКБІ, в тому числі, перевірка діючих норм, методик тощо.

При цьому до основних завдань ЕС слід віднести:

- забезпечення підтримки користувачів у процесі підготовки і вибору раціональних рекомендацій (рішень) щодо достатнього рівня захисту КІ на основі отриманих оцінок можливостей загроз і формалізованих знань фахівців-експертів;
- проведення комплексної оцінки ризиків та прийняття обґрунтованих рекомендацій (рішень) щодо оптимізації організаційно-технічних заходів із захисту.

3. Вивчення та проведення аналізу існуючого математичного, інформаційного та нормативно-методичного забезпечення процесів прийняття рішень із УКБІ.

Аналіз діючої структури цих видів забезпечення (рис. 1), які дозволяють сформулювати обґрунтовані рекомендації із УКБІ, доводить необхідність автоматизації цього процесу в рамках розробки і впровадження відповідної ЕС.

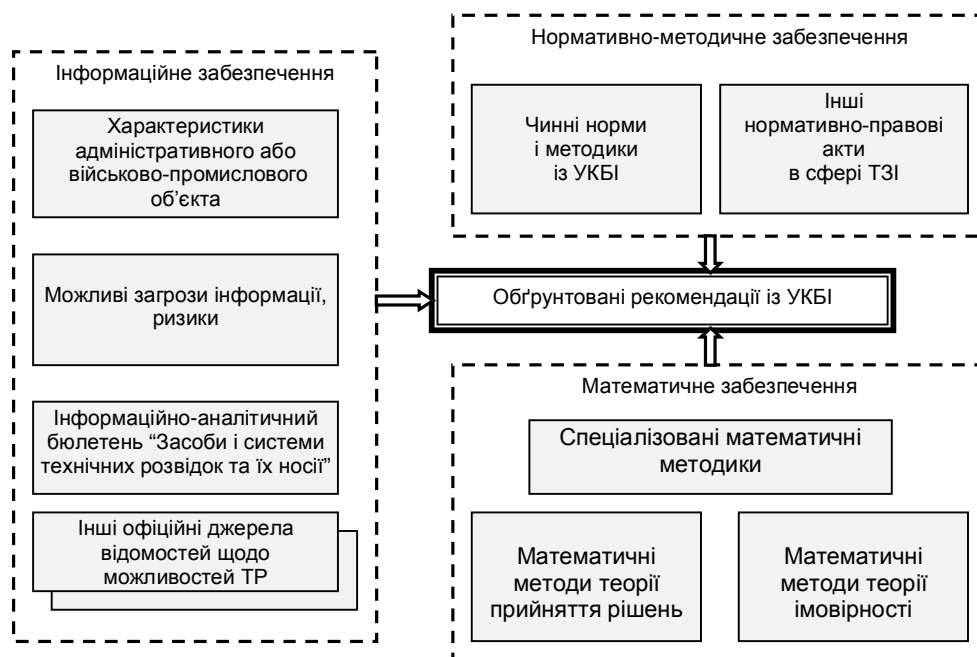


Рис. 1. Види забезпечення процесу прийняття рішень із УКБІ

4. Визначення основних критеріїв, які покладено у формування остаточних рекомендацій із УКБІ.

Первинними критеріями для прийняття рішень із УКБІ є критерії, що надані в діючих нормах із технічного захисту інформації та протидії технічним розвідкам.

Узагальненими критеріями (умовами) для обґрунтування комплексу заходів із УКБІ на ОПД можуть бути: вартість заходів із УКБІ не повинна перевищувати цінність КІ, яка захищається; адекватність заходів із УКБІ визначеним загрозам; мінімізація шкоди, що прогнозується, у разі реалізації можливих загроз і т.ін.

Для математичного опису та формування узагальненого критерію рекомендується використовувати способи, викладені у [6].

Етап 2. Обґрунтування доцільності розробки ЕС.

Для обґрунтування доцільності застосування ЕС пропонується використати методика наведену в [7]. Оцінка доцільності основана на результатах аналізу предметної області. Вважається, що застосування ЕС доцільно, як що її розробка можлива, виправдана та розумна. Під час оцінки можливості і розумності розробки ЕС необхідно брати до уваги стан знань про предметну область, характеристики задач прийняття рішень і поточний стан інженерії знань, включаючи розвиток програмних і технічних засобів проектування ЕС [8, 9].

Виправданість, у кінцевому рахунку, обумовлена економічними аспектами. В нашому випадку, виправданість обумовлена необхідністю проведення відповідних наукових досліджень під час розроблення експериментальної ЕС, основу яких повинні складати роботи щодо збору, опрацювання та формалізованому опису експертних даних і знань із УКБІ. При цьому за методикою [7] кінцева оцінка, а саме оцінка доцільності створення ЕС проводиться із використанням наступних правил:

<ЯКЩО існують експерти в даній предметній області й експерти можуть описати методи та моделі знань і прийняття рішень і експерти єдині у виборі цих моделей і методів

і задачі вимагають використання інтелектуальних навиків (застосування методів штучного інтелекту)

і задачі не є занадто складними

і задачі є цілком зрозумілими

і задачі не потребують загальнодоступних знань

ВИЗНАТИ розробку ЕС можливою>

<ЯКЩО задачі вимагають оперування символічними даними і задачі потребують евристичних рішень

і задачі не є занадто простими

і задачі представляють практичний інтерес

і розміри задач допускають їхню комп'ютерну реалізацію

ВИЗНАТИ розробку ЕС розумною>

<ЯКЩО одержання рішень задач рентабельне (високорентабельне)

або є гострий дефіцит експертів

або досвід експертів необхідний у багатьох місцях

або необхідно зафіксувати і накопичувати досвід експертів, щоб його не втратити

або досвід необхідно застосувати в шкідливих для людини умовах

ВИЗНАТИ розробку ЕС виправданою>

<ЯКЩО розробка ЕС можлива

і розробка ЕС розумна

і розробка ЕС виправдана

ВИЗНАТИ розробку ЕС доцільною>

Етап 3. Визначення структури ЕС.

На основі існуючого досвіду і досліджень з питань розробки ЕС [8-13] можливо запропонувати наступну структуру ЕС, яка наведена на рис. 2.

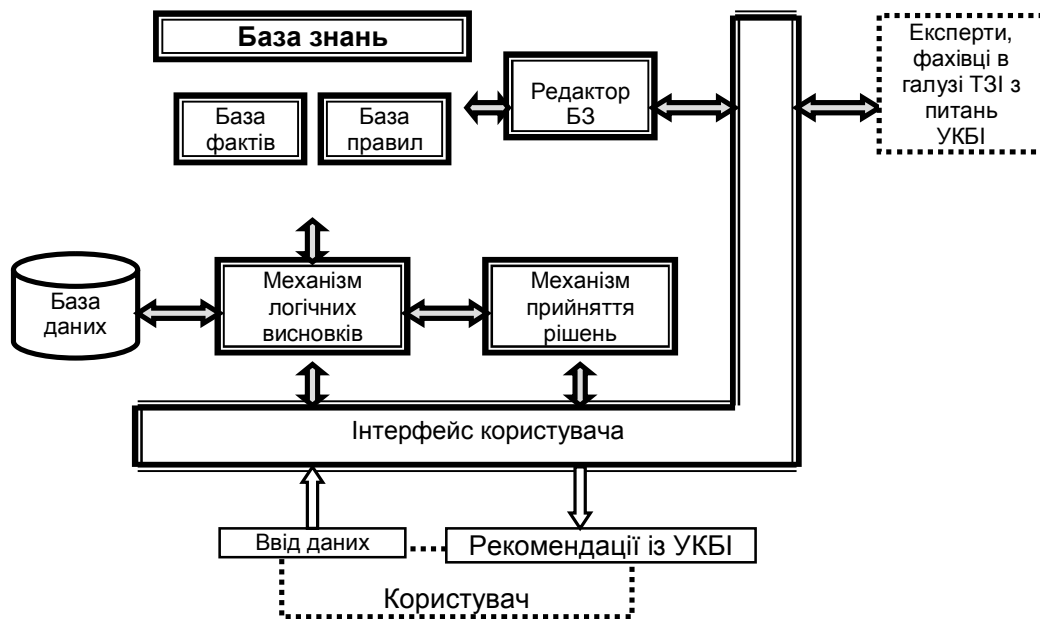


Рис.2. Структура експертної системи підтримки прийняття рішень із УКБІ

Для наочності розглянемо основне призначення елементів ЕС. Перш за все, основою ЕС є база знань (БЗ), яка представляє сукупність відредагованих формалізованих знань з питань УКБІ і забезпечує керування ними. БЗ складається із бази фактів і бази правил. База фактів це формалізоване представлення відомих (фактично незмінних) в даній предметній області знань типу $\langle A \in A \rangle$, наприклад, ті знання, що викладені у спеціальній літературі (підручниках, довідниках тощо). База правил – змінна частина БЗ і звичайно відображає власний досвід спеціалістів-експертів, в тому числі, викладений у нормативно-методичних документах із УКБІ. Враховуючи кількість видів ТР, норм і методик із УКБІ за кожним видом можливо передбачити, що обсяг бази правил на початковому етапі створення ЕС буде складати близько 50÷100 правил. Це необхідно врахувати під час вибору способу опису (формалізації) знань. На даний час основними способами опису знань є: система продукцій типу $\langle \text{Якщо} - \text{то} \rangle$ (явище – реакція); фреймова форма [15]; семантичні мережі [11, 13]; за допомогою логіки предикатів 1-го і 2-го порядків [11]; за допомогою нечіткої логіки [16]. Враховуючи невелику кількість правил (50÷100) доцільно для моделювання БЗ ЕС обрати систему продукцій. При цьому треба пам'ятати, що зі збільшенням множини продукційних правил в БЗ швидкодія ЕС значно знижується.

Механізм логічного висновку (МЛВ) забезпечує надання ЕС відповідного висновку після аналізу поточних вхідних фактів шляхом пошуку і проведення їх порівняльного аналізу з правилами в базі правил БЗ. Для систем продукції на даний час існує прямий, зворотній або комбінований логічний висновок [11-13]. Вибір типу МЛВ проводиться розробником ЕС як правило після формування БЗ.

Механізм, що забезпечує функції отримання знань від експертів, підтримку БЗ (її верифікацію, модифікацію тощо) і доповнення її за необхідністю, має назву редактору БЗ.

Механізм прийняття рішень (МПР) використовує отримані від МЛВ дані та з урахування визначених критеріїв формує обґрунтовані рекомендації (рішення) із УКБІ. Крім того, МПР може надавати коментарі та необхідні пояснення до сформованих рекомендацій. Для розробки МПР можуть бути використані як формальні та й неформальні методи прийняття рішення [17]. Вибір методу проводиться тільки після побудови БЗ і МЛВ ЕС.

Інтерфейс користувача забезпечує взаємодію всіх елементів ЕС і, як правило, містить сукупність діалогових процедур для прийому-передачі повідомлень ЕС від користувача або експерта. Основними властивостями сучасного інтерфейсу користувача ЕС є: дружній багатовіконний діалоговий характер; використання стандартної термінології з питань інформаційних технологій і УКБІ; розподіл прав доступу до ресурсів ЕС за пріоритетами між простими користувачами й експертами.

База даних ЕС складається із значень кількісних показників, отриманих за результатами роботи програмних модулів оцінки можливостей технічних розвідок СПЗ, кількісних й якісних характеристик ІС та навколишнього середовища. Користувач системи має можливість уточнювати дані щодо ІС, можливостей ТР або ввести нові дані.

Етап 4. Визначення рівня розробки ЕС.

Для досягнення повноти і високої якості рішення завдань, покладених на ЕС, необхідне проведення комплексу досліджень й експериментів, тому розвиток даної ЕС відбувається еволюційно. Необхідний рівень розробки ЕС з урахуванням кількості продукційних правил в базі знань БЗ ЕС, її гібридності можливо визначити за результатами обґрунтування [3].

ЕС підтримки прийняття рішень із УКБІ відноситься до першого типу за кількістю продукційних правил та завдань, що вирішуються, а її демонстраційний прототип розробляється в рамках відповідної науково-дослідної роботи.

Етап 5. Визначення особливостей та основних вимог до ЕС

1. Визначення класифікаційних ознак ЕС.

Визначення класифікаційних ознак ЕС можливо провести за прийнятою сучасною класифікацією інтелектуальних систем [5, 9, 10], наведеною на рис. 3.



Рис. 3. Класифікація інтелектуальних інформаційних систем

За результатами аналізу предметної області, структурних елементів ЕС можна стверджувати, що ЕС підтримки прийняття рішень із УКБІ відноситься до експертно-аналітичних систем вибору рішень і повинна надавати рекомендації користувачеві щодо протидії, а також є багатофункціональною та гібридною.

Крім того, для формування повного переліку класифікаційних ознак ЕС можна додатково використати класифікацію, наведену в [8]. За даною класифікацією запропонована ЕС відноситься до статичних ЕС, тому що її вихідні дані не змінюються під час рішення конкретної задачі із УКБІ, а за ступенем складності структури (рис. 2) - до поверхневих ЕС.

2. Визначення переліку основних вимог до ЕС

Аналіз предметної області із протидії технічним розвідкам, яка підлягає формалізації в рамках створення ЕС дозволяє висунути до неї наступні вимоги.

Загальні вимоги до ЕС:

1) Розробка ЕС має провадитися у відповідності до загальних принципів теорії програмування, інженерії знань, теорії ймовірностей, теорії захисту інформації та її практичних застосувань і нормативно оформлених положень.

2) В основу механізму прийняття рішень в ЕС можуть бути покладені наряду з формальними (класичними) методами [5] й неформальні методи пошуку оптимальних рішень [17].

3) Рекомендації (рішення) в ЕС мають формуватися на основі отриманих імовірнісних характеристик ризиків за допомогою відповідних програмних модулів та наданих користувачем або наявних у базі даних ЕС описів конкретного об'єкта в Україні.

4) ЕС має надавати можливість аналізу загрози конкретному ІС та вибору адекватної протидії як по відношенню до окремих видів загроз, так і їх сукупності.

5) В ЕС має бути забезпечена функція розмежування прав користувачів у відповідності до наданих їм повноважень.

Окремі вимоги щодо оболонки ЕС та бази знань:

1. Оболонка ЕС має бути універсальною щодо відсутності жорсткої структурно-алгоритмічної орієнтації на конкретні види загроз, типи ОПД та форми КІ.

2. В ЕС мають бути засоби настроювання її оболонки на випадок появи нових методик оцінки можливостей ТР та норм протидії ТР за видами в якості нормативно-методичних документів системи ТЗІ.

Окремі вимоги щодо бази знань та її редактора:

1) Предметна спрямованість ЕС має повністю визначатись наповненням бази знань.

2) При створенні ЕС має бути розроблений редактор з інтелектуальними ознаками, призначений для поповнення, верифікації та редагування (модифікації) БЗ ЕС.

3) При розробці редактора БЗ має бути передбачено засоби контролю цілісності бази у ході її наповнення і редагування.

4) В редакторі БЗ мають бути присутні засоби контекстного пошуку окремих елементів знань та семантично споріднених їх груп.

Окремі вимоги щодо інтерфейсу користувача ЕС:

1) Присутність засобів оптимізації діалогу як по семантичній спорідненості суміжних запитань, так і по його тривалості.

2) Наявність засобів аргументації (пояснення) рекомендацій, що пропонуються користувачеві.

3) Присутність можливості динамічної деталізації (роз'яснення) запитань, які ставляться користувачеві у діалозу до рівня, що мінімізує імовірність неоднозначного тлумачення. При цьому слід передбачити як текстову, так і графічну форму подання інформації.

4) Наявність засобів компенсації можливої невизначеності у відповідях користувача. При цьому автоматично повинен актуалізуватись найбільш песимістичний варіант відповіді.

5) Можливість оперативного і без втрати інформації переривання діалогу, котре може бути викликане необхідністю уточнення відповіді, або підбором конкретних даних, або сторонніми факторами.

Додаткові вимоги до ЕС:

1) Можливість надання прогностичної оцінки згенерованих рекомендацій, у тому числі

за трудомісткістю, вартістю та тривалістю впровадження відповідних організаційно-технічних заходів та засобів на ІОД.

2) Наявність механізму ітераційної оптимізації заходів з УКБІ на конкретному ІС за критерієм відповідності очікуваного ефекту від їх впровадження.

3) Процес розробки ЕС повинен передбачити можливість доробки, уточнення визначених вимог та формування додаткових вимог.

Етап 6. Розробка алгоритмів і програмних засобів елементів ЕС.

На даний час фахівці в галузі технології ЕС відрізняють чотири основних типу програмної реалізації цих систем, а саме: загальноцільові мови програмування (Паскаль, Си тощо); типові засоби для розробки ЕС (мови, орієнтовані на розроблення БЗ ЕС: Лисп, Пролог, Делфі (на основі CASE-технологій [15]) тощо); генератори або засоби автоматизованого проектування ЕС [8]; узагальнені ЕС (оболонки ЕС, які потребують настроювання на конкретну предметну область) [5, 8].

Для розробки ЕС підтримки прийняття рішень із УКБІ доцільно використовувати загальноцільові мови програмування, враховуючи їх доступність для використання та економічність (в смислі використання пам'яті ПЕОМ).

Етап 7. Налаштування програмного забезпечення ЕС та оцінка її ефективності.

На жаль на сьогодні не існує єдиної, уніфікованої та науково-обґрунтованої методики оцінки ефективності ЕС. Але основними методами оцінки ефективності ЕС, які найбільш широко використовуються на практиці є:

- проведення порівняльного аналізу характеристик розробленої ЕС з подібними діючими автоматизованими системами в галузі ТЗІ;
- розрахунок очікуваного економічного ефекту від впровадження ЕС з урахуванням витрат на її створення;
- визначення якості ЕС за такими показниками діалогових програмних систем як, складність, відкритість, здатність до адаптації і т.ін.

Висновки.

1. Запропонована методика визначає послідовність та зміст основних етапів створення експертної системи і дозволяє її розробникам спрямувати зусилля на вирішення першочергових завдань щодо проектування ЕС.

2. Кожен етап запропонованої методики передбачає фактично проведення окремих наукових досліджень й експериментів.

3. ЕС є уніфікованою частиною СПЗ для оцінки можливих загроз для інформації на ОПД. При цьому реалізація концепції ЕС на практиці дозволить звичайним користувачам, що не мають спеціальної підготовки в питаннях автоматизованого опрацювання, самостійно, без участі посередників-програмістів та спеціалістів-експертів в сфері ТЗІ з питань УКБІ готувати та вводити в ПЕОМ вхідні дані для опису задач УКБІ, і при зміні умов цих задач вчасно коректувати їх опис, отримати відповідні рекомендації від ЕС та оперативно приймати рішення щодо організації робіт з УКБІ на об'єкті.

ЛІТЕРАТУРА

1. Интеллектуальные системы поддержки принятия решений / Герасимов Б.М., Локазюк В.М., Окслюк О.Г., Поморова О.В. – К.: Вид-во Європ.ун-ту, 2007. - 335 с.
2. Современное состояние, методологии анализа рисков при обеспечении информационной безопасности компьютерной системы // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - НТУУ „КПІ”. – Випуск 4. – 2002. – С. 34-49.
3. Герасимов Б.М. Человеко-машинные системы принятия решений с элементами искусственного интеллекта / Б.М. Герасимов. – К.: Наукова думка, -1993.-184 с.
4. Довбня С.Я. Методологічні та організаційно-технічні основи створення систем та методів захисту інформації від витоку технічними каналами / С.Я. Довбня, Д.А. Алексеев // Зб. наук. праць СТСЗІ. - 2011. - №1(19). - С.58-77.
5. Информационно-вычислительные системы принятия решений / Хаджинов В.В., Быков В.А., Храмов И.А., Усачев В.Г. - К.: Наукова думка, 1992. - 140 с.

6. Довбня С.Я. Нормативні вимоги та техніка апаратного захисту інформації з обмеженим доступом / С.Я. Довбня, С.В. Биков, В.В. Зайкін // Матеріали Міжнародної науково-практичної конференції «Безпекотворення: питання теорії і практики та правові аспекти». Київ, Європейський університет, 16 лютого 2007 р. - К.: 2007. - С. 48-51.
7. Петрушин В.А. Экспертно-обучающие системы / Петрушин В.А.; Отв. ред. А.М. Довгяло; АН УССР. Ин-т кибернетики. – К.: Наукова думка, 1992. - 78 с.
8. Искусственный интеллект: В 3 кн. Кн. 1. Системы общения и экспертные системы: Справочник / Под ред. Э.В. Попова. - М.: Радио и связь, 1990. - 464 с.
9. Кокарева Л.В. Диалоговые системы и представление знаний: Справочное пособие / Л.В. Кокарева и др. - К.: Наукова думка, 1993. - 448 с.
10. Курілін Б.І. Експертні системи для військового користування / Б.І. Курілін, О.О. Глущенко, І.Я. Загоруйко // Праці КВІУЗ. - 1998. - Вып.2. - С.89-106.
11. Представление и использование знаний. – М.: «Мир», 1989. – 216 с.
12. Приобретение знаний. – М.: «Мир», 1989. – 384 с.
13. Лорьер Ж.-Л. Системы искусственного интеллекта / Лорьер Ж.-Л. - М.: «Мир», 1989. – 432с.
14. Ажмухамедов И.М. Анализ и управление комплексной безопасностью на основе когнитивного моделирования / Ажмухамедов И.М. // Управление большими системами / сборник трудов ИПУ РАН. - 2010. - Вып. 29. - С. 5-16.
15. Шорошев В.В. Базова модель експертної системи оцінки безпеки інформації в комп'ютерних системах / В.В. Шорошев // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К.: НТУУ „КПІ”, 2001. - Вип.. 3. - С. 79-86.
16. Прикладные нечеткие системы. - М.: «Мир», 1993. – 368 с.
17. Борисов А.Н. Теория принятия решений / А.Н. Борисов – Рига: Зинатне, 1986. – 191 с.

Надійшла: 15.01.2013

Рецензент: д.т.н., проф. Єрохін В.Ф.