УДК 004.891.3 (043.2)

Д.В. Грінченко

*Національний авіаційний університет*

СТРУКТУРА ЕКСПЕРТНОЇ СИСТЕМИ ДЛЯ ВИЗНАЧЕННЯ ШЛЯХІВ ВИТОКУ ІНФОРМАЦІЇ

З метою автоматизації процесу визначення можливих шляхів витоку інформації з залученням експертних знань запропоновано створити експертну систему, що піддаватиме користувача опитуванню щодо значимих у даній галузі ознак.

З метою забезпечення таких можливостей база знань системи має наступну структуру:

1. База описів уразливостей (наприклад, «Зараження вірусами», «Злом системи», «Існування інсайдера»), організованих у вигляді класифікаційного дерева.

2. База описів ознак, за наявністю яких передбачається виносити судження про уразливості. Ці ознаки фігуруватимуть в питаннях, які система задає користувачеві при діагностиці.

3. Набір правил-продукцій, що дозволяють за зовнішніми ознаками судити про уразливості. Саме у них сконцентрована основна частина експертних знань. Антецеденти правил представляють нечітко-логічні вирази над показниками визначеності ознак. Кожне правило має свій показник потужності (від 0 до 1), тобто коефіцієнт, який вказує, наскільки сильно вираз в антецеденті впливає на показник визначеності тієї чи іншої уразливості.

З погляду кінцевого користувача процес діагностики виглядає таким чином: експертна система ставить користувачеві питання, що стосуються зовнішніх проявів, які можуть указувати на наявність прихованих уразливостей. Користувач відповідає, указуючи ступінь своєї упевненості за чисельною шкалою, наприклад від –100 (безумовне заперечення) до +100 (безумовне підтвердження). Далі у всіх правилах, в антецедентах яких фігурує дана ознака, відбувається перерахунок значень антецедентів і через показник потужності правила перераховуються коефіцієнти упевненості для відповідних уразливостей. Можливе додаткове управління викликом правил за допомогою передумов правил.