умови відсутності обмеження у часі, то для ЕС реального часу це означатиме повну катастрофу, оскільки за умови таких перешкод ЕС може не встигнути розглянути правильну гілку та прийняти вірне рішення.

Отже запропонуємо структуру СБ ЕС, яка була б у змозі подолати описані проблеми.

Будь-які дії з ЕС, які проводяться через інтерфейс самої ЕС та викликають, як наслідок, оновлення БЗ або ЕС, повинні зберігатися у вигляді окремих операцій у спеціальному журналі транзакцій. Так, наприклад, якщо будь-яке знання змінювалося декілька разів, то повинна зберігатися вся історія змін. Це, безумовно, надлишково з точки зору компактності БД, але це єдина можливість у разі необхідності провести розслідування. Ведення журналу по зміні БЗ дозволить відключити певну групу знань та промоделювати процес без неї. У випадку встановлення хибності знань неважко буде знайти, хто їх ввів до БЗ. Щодо зберігання всіх сеансів з користувачем, тут інша ситуація. Сеанси роботи з користувачем необхідно зберігати, але який термін – це вже залежить від конкретної ЕС. Спеціальний евристичний аналізатор ЕС повинен з певною мірою вірогідності відрізняти серію атак від звичайної роботи.

Під евристичним аналізатором будемо розуміти підсистему, що має набір функцій аналізу, робота яких спрямована на виявлення порушень в роботі користувачів з ЕС. Так, наприклад, якщо атака направлена на ушкодження знань другого рівня, то для її подолання в евристичному аналізаторі передбачена спеціальна функція, яка порівнюється з максимальним допустимим рівнем навчання.

Описане вище є тільки внутрішньою СБ ЕС. Крім цього ЕС потребує ще й захисту від несанкційного доступу. Тобто треба забезпечити захист ЕС не тільки від ушкодження. Як не прикро, але це теж можна зробити з терміналу ЕС її ж засобами. Досвідчений користувач в змозі за n сеансів перебрати всі варіанти розвитку подій в ЕС – обійти все дерево знань та тим самим отримати знання ЕС. Завдяки тому, що всі сесії з користувачем зберігаються в журналі, евристичний аналізатор ЕС з певною мірою вірогідності повинен відрізнити перебір БЗ від звичайної роботи.

Таким чином, будь-яка робота/операція з ЕС, направлена на модифікацію БЗ або ЕС повинна реєструватися у журналі операцій. Ведення такого журналу дозволить уникнути не тільки спроби викрасти або пошкодити ЕС, але й суттєво збільшує шанс на локалізацію власних помилок та робить БЗ більш надійною і прозорою.

III Висновки щодо особливостей створення системи безпеки ЕС

ЕС, як будь-яке інше ПЗ, потребує наявності розвиненої специфічної СБ. Ведення протоколів роботи з ЕС дозволяє не тільки знайти та вірно відреагувати на хибні знання, введені експертом, а й не припустити зміни висновків системи внаслідок певної кількості сесій, спрямованих на агресію. Введення в СБ ЕС евристичного аналізатора дозволяє розв'язати питання, які не зачіпаються звичайною СБ. Будь-який розвинений захист можливий тільки за умов постійного аналізу самої ЕС та протоколів роботи з нею. Для того, щоб надійно захистити інтелектуальну систему, необхідна інтелектуальна система захисту. Питання безпеки ЕС потребує глибшого розгляду та розвитку порівняно із звичайним ПЗ.

УДК 681.518.54

МАТЕМАТИЧНИЙ АПАРАТ ДЛЯ ОБГРУНТУВАННЯ ЕКОНОМІЧНОЇ ДОЦІЛЬНОСТІ ВИКОРИСТАННЯ ЕКСПЕРТНИХ СИСТЕМ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ

Володимир Тарасенко, Антон Михайлюк, Андрій Петрашенко
Національний Технічний Університет України "КПІ"

Анотація: **Співвідношення між ефективністю та вартістю системи захисту інформації може бути розглянуто як критерій її оцінки. За цим методом математична модель аналізує ефективність застосування експертних систем прийняття рішень у галузі захисту інформації, порівнюючи її з традиційним підходом – залученням експертів.**
Summary: **Correlation between effectiveness and cost of information security systems can be served as a criterion for evaluation. Using this method mathematical model analyze effectiveness of expert systems application in branch of guarding, comparing it with traditional approach – attraction of experts.**
Ключові слова: **математична модель, експерт, експертна система.**

При проектуванні і реалізації систем захисту інформації вагоме значення приділяється економічним аспектам проблеми. Одним із критеріїв оцінки доцільності застосування подібної системи може служити співвідношення

«ефективність-вартість». Міру протидії інформаційній агресії вважають прийнятною, якщо її ефективність, виражена через зниження ймовірних збитків, перевищує витрати на її реалізацію:

$$C_{можл.зб.} > C_{витр.зах.} \quad (1)$$

Запропонований підхід враховує як збитки від порушення інформаційної безпеки $C_{можл.зб.}$, так і витрати на захист $C_{витр.зах.}$. Велика кількість каналів витоку інформації та невизначеність у діях порушника безпеки у значній мірі затруднює розрахунок економічної ефективності. Виходячи з того, що в реальній ситуації мають місце випадкові фактори, які призводять до порушення захищеності (наприклад, специфіка каналів витоку), можна розглядати $C_{можл..зб.}$ як математичне очікування суми збитків $C_{зб.}$ по всім каналам витоку інформації з урахуванням "вартості інформації". Під вартістю інформації будемо розуміти, наприклад, ймовірну суму збитків у разі порушення інформаційної безпеки. Таким чином,

$$C_{можл.зб.} = M(C_{зб.}) = \sum_{i=1}^{n} (C_{зб.\,i} * p_{піб.\,i}) \quad (2)$$

де $C_{зб.i}$ – сума збитків при порушенні інформаційної безпеки по *i*-му каналу витоку,
$p_{піб.i}$ – імовірність порушення інформаційної безпеки по *i*-му каналу витоку.

В загальному вигляді можна вважати, що $C_{зб.i}$ деяким чином залежить від статутного фонду підприємства, обороту коштів, вартості основних виробничих засобів, тощо.

Імовірність порушення інформаційної безпеки $p_{піб}$ визначається з урахуванням імовірності атаки $p_{інф.атаки}$ й ефективностей нападу ($E_{атаки}$) і захисту ($E_{захисту}$). Він дорівнює

$$p_{піб} = p_{інф.атаки} * f(E_{атаки} - E_{захисту}) \quad (3)$$

$$f(x) = \begin{cases} 0, при\ x <= 0 \\ x, при\ x > 0 \end{cases}$$

Під витратами на захист $C_{витр.зах.}$ розуміють вартість прийняття конкретного рішення про захисні заходи ($C_{оцінка}$) і безпосередньо витрати на захист $C_{зах.}$ (організаційні і технічні заходи).

$$C_{витр.зах.} = C_{оцінка} + C_{зах.} \quad (4)$$

Побудована модель орієнтується переважно на ефективність оцінки збитків і прийняття рішення щодо забезпечення захищеності. Згідно з нею, розглянуто два можливих методи вирішення цієї задачі: залучення експертів і використання експертних систем (ЕС). Початкова вартість експертних систем вища за послуги експертів, але надалі, вона залишається постійною, у той час як вартість послуг експертів фактично зростає лінійно. Тому з економічної точки зору, при одноразовому дослідженні об'єкту доцільніше використання першого методу. Застосовування експертних систем має сенс, якщо оцінка захищеності проводиться систематично.