УДК 665.9

Л.В. МЕЛЬНИЧУК, О.В. ШМАТКО доцент

Дослідження рівня безпеки інформаційної системи підприємства

У сучасному світі інформація активно впливає на всі сфери життєдіяльності, у тому числі на ринкову економіку. Виникає загроза витоку інформації, в результаті чого стає неможливим нормальне функціонування підприємства [1]. Процес захисту інформації в інформаційній системі відбувається за рахунок функціонування DLP-системи (Data loss prevention), яка забезпечує повну або часткову компенсацію загроз витоку даних.

Однією з проблем при виборі систем захисту інформації є задача багатокритеріального вибору DLP-системи для максимального захисту інформаційної системи підприємства від витоків даних.

Під час рішення задачі вибору найкращої системи від витоків даних, неможливо зібрати статистичні дані по всім існуючим DLP-системам для певного підприємства. У цьому випадку зручно використовувати експертне оцінювання, яке використовує лінгвістичний підхід на базі теорії нечітких множин.

Для рішення задачі вибору оптимальної DLP-системи в роботі розглянуті методи, які належать до теорії нечітких множин [2]: метод головного показника, метод результуючого показника, лексикографічні методи. У роботі використовується метод результуючого показника. Вибір варіанту DLP-системи проводиться при адитивності критеріїв. Спочатку формуються та оцінюються ризики підприємства, на основі них формуються критерії вибору та альтернативні варіанти DLP-систем. Відносна важливість більшості критеріїв визначається на основі експертних оцінок. При цьому враховується компетентність експертів. Для визначення критерію надійності використовується метод статистичного моделювання. Експериментальні дані отримуються шляхом проведення тестування на проникнення та хисту вразливих даних. Далі, використовуючи експертне оцінювання, визначається оцінка кожної DLP-системи по визначеним критеріям, як представлено на рис.1.

Для визначення оптимальної DLP-системи, проводиться ранжування альтернативних варіантів із використанням отриманих зважених оцінок на основі нечіткої композиції [3]:

$$\mu_J(j) = \sup_{r_1, r_2, \ldots, r_m : r_i \geq r_j} \min_{j=1,\ldots,m} \mu_{R_j}(r_j)$$

де $\mu_J(j)$ – нечітка множина альтернатив, які відповідають значенню «найкраща альтернатива». Найкращою вважається альтернатива, яка має найбільше значення $\mu_J(j)$.

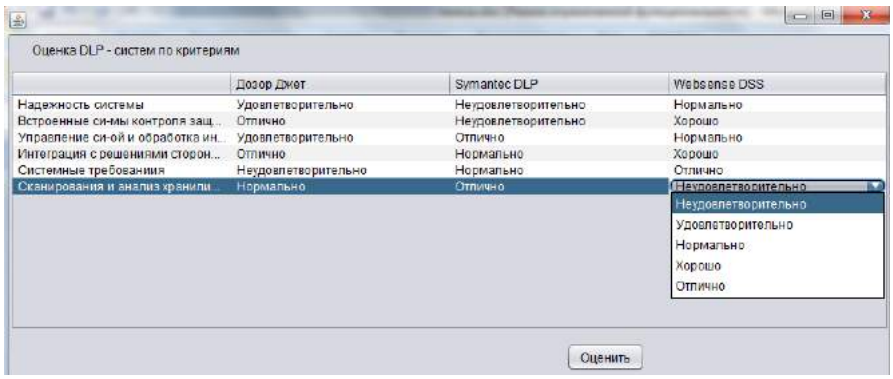

Рис. 1 – Виставлення лінгвістичних оцінок кожній DLP-системі по заданим критеріям

Пріоритет кожної альтернативи визначається вибором мінімуму серед точок перетину правої межі відповідного їй нечіткого числа R_j з межами нечітких чисел, що представляють зважені оцінки альтернатив, розташованих правіше на числовій осі, які задовольняють умову $r_k > r_j$. Результати дослідження визначення оптимальної DLP-системи наведені на рис. 2.

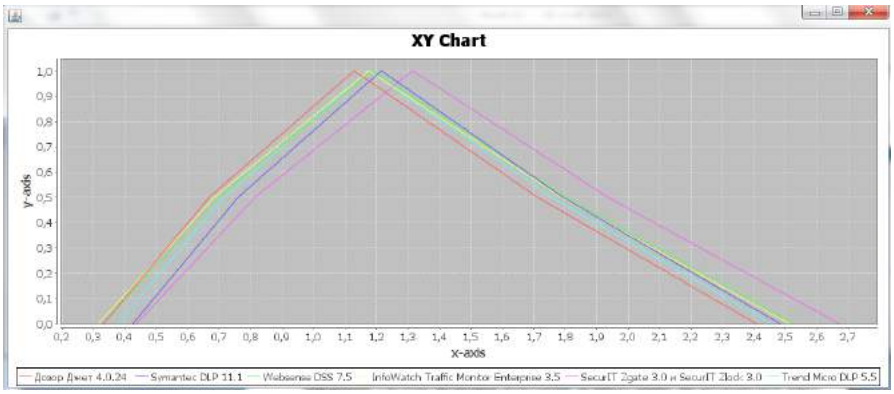

Рис. 2 – Порівняння DLP-систем на основі зважених оцінок

В результаті виконання роботи було визначено рівень безпеки інформаційної системи підприємства та обрано найкращу, відповідно до заданих умов, DLP-систему. Запропонований метод дозволяє обрати оптимальну DLP-систему індивідуально для кожного підприємства із розумінням того, які задачі вона має вирішувати. Таким чином, процес вибору системи захисту інформації від витоків даних дає змогу застосовувати індивідуальний підхід для кожного підприємства та зменшує рівень суб'єктивного підходу під час оцінки запропонованих DLP-систем.

Список літератури:

1. *Домарев В.В.* Безопасность ИТ: Системный подход / *В.В. Домарев* – К.:ООО ТИД «Диасофт», 2004. – 992 с.

2. *Бармен С.* Разработка правил информационной безопасности / *С. Бармен* – М.: ИД "Вильямс", 2002. – 208с.

3. *Андрейченков А.В.* Анализ, синтес, планирование решений в экономике / *А.В. Андрейченков, О. Н. Андрейченкова* – М.: «Финансы и статистика», 2000. – 205с.