УДК 004.056:007 (043.3) **В.Л. Бурячок, Я.В. Невойт**

МЕТОД ВИЗНАЧЕННЯ НАЙБІЛЬШ ЗНАЧИМИХ ЗАГРОЗ ІЗ “ГЕНЕРАЛЬНОЇ СУКУПНОСТІ” ЗАГРОЗ ІНФОРМАЦІЙНИМ РЕСУРСАМ НА ПІДСТАВІ ЇХ ЯКІСНИХ ТА КІЛЬКІСНИХ ПОКАЗНИКІВ

В статті розглянуто основні положення нового методу визначення найбільш значимих загроз із “генеральноїсукупності” загроз інформаційним ресурсам на підставі їх якісних та кількісних показників.Приведено підхід обчислення показників що характеризують рівень потенціальної небезпеки загроз з "еталонної вибірки". Геометрична інтерпретація формування комплексного показника рівня найбільш значимої загрози у двомірному просторі показника

***Ключові слова*:** загроза,інформаційний ресурс, генеральна сукупність, еталонна вибірка.

Вступ

Питання інформаційної безпеки особливо актуальні в даний час і для комерційних структур. Проте, не дивлячись на те, що для інформаційних систем існують визначені законодавством вимоги по захисту інформації, в подібних структурах особливу значущість мають підходи по створенню актуального переліку загроз інформаційній безпеці та дослідженню джерела походження.

Виходячи зі сформованої множини загроз доцільним стає завдання розроблення методу визначення найбільш значимої загрози , яка заподіє найбільшої шкоди інформаційним ресурсам (ІР).

Виклад основного матеріалу

Зважаючи на множину можливих загроз інформаційним ресурсам сучасного підприємства пропонується метод визначення найбільш значимих загроз із “генеральної сукупності” класів загроз на підставі їх якісних та кількісних показників[1,2].

Під "генеральною сукупністю" (N) розуміємо існуючу сукупність відомих загроз в рамках існуючих класів. Сукупність загроз, найбільш значимих для певного підприємства, є "еталонною вибіркою" (Q) з генеральної сукупності. Чим більшою буде величина (Q), тобто чим ближче вона наближатиметься до (N), тим більш обґрунтованим буде результат вибору.

На першому кроці визначення гіпотетичного напряму підвищення рівня небезпеки можливих загроз інформаційним ресурсам розташуємо існуючу сукупність відомих загроз ІР в ряд переваг по значимості можливого задіяного впливу.

Для цього:

а) сформуємо матриці парних порівнянь загроз за кожним *j*-м показником на підставі відповідних вагових коефіцієнтів α_k:

$$A_j = \left\lfloor a_{11},\ldots, a_{in},\ldots, a_{QQ} \right\rfloor,\ \ i,n = \overline{1,Q},\ \ \ j = \overline{1,L}. \qquad (1)$$

Умова: $A_j = \left| a_{in}^{(j)} \right|,\ \ i,n = \overline{1,Q}$. Якщо $a_{in}^{(j)} = \alpha_k,\ \ де\ \ \alpha_k \neq 0,\ \ \ k = \overline{1,5}$, то $a_{ni}^{(j)} = \dfrac{1}{a_{in}^{(j)}}$. Причому $a_{ii} = 1$;

б) обчислимо власні значення та притаманні їм вектори кожної з матриць A_j;

в) сформуємо узагальнену власну матрицю ($A_{Влij}$) з власних значень матриць A_j та проведемо нормування її елементів: $A_{Влij}^{нор} = A_{Влij} \Big/ \sum_{i=1}^{Q} A_{Влij}$, $i = \overline{1, Q};\ \ j = \overline{1, L}$;

г) сформуємо матриці важливості кожного показника для загрози одного класу на підставі надання їм H експертами відповідних вагових коефіцієнтів β_k:

$$B = \lfloor b_{11}, b_{jh}, ..., b_{LH} \rfloor \quad (2)$$

Умова: $b_{jh} = \beta_k,\ \beta_k \neq 0, k = \overline{1,5},\ j = \overline{1,L}\quad h = \overline{1,H};$

д) проведемо нормування елементів матриці B: $b_{jh}^{нор} = b_{jh} \Big/ \sum_{j=1}^{L} b_{jh}, h = \overline{1, H};$

ж) знайдемо середні значення вагових коефіцієнтів важливості кожного показника:

$$b_j^{середнє} = \sum_{h=1}^{H} b_{jh}^{нор} \Big/ \sum_{h=1}^{H} \sum_{j=1}^{L} b_{jh}^{нор},\ h = \overline{1, H};\ j = \overline{1, L};$$

з) обчислимо вагові коефіцієнти та визначимо пріоритети (вектор значимості) загроз. З них сформуємо впорядковану "еталонну вибірку":

$$ZZ = A_{Вл_{ij}}^{нор} \cdot b_j^{середнє} = \begin{bmatrix} x_{11} & ... & x_{1j} & ... & x_{1L} \\ ... & ... & ... & ... & ... \\ x_{i1} & ... & x_{ij} & ... & x_{iL} \\ ... & ... & ... & ... & ... \\ x_{Q1} & ... & x_{Qj} & ... & x_{QL} \end{bmatrix} \cdot \begin{bmatrix} b_1^{середнє} \\ ... \\ b_j^{середнє} \\ ... \\ b_L^{середнє} \end{bmatrix} = \left(ZZ_{загр_1}, ..., ZZ_{загр_i}, ..., ZZ_{загр_Q} \right). \quad (3)$$

Умова: $\sum_{i=1}^{Q} Z_{загр_i} = 1$

В даному випадку загроза, яка має найнижчий пріоритет, обирається за "нульовий варіант", або інакше за так званий "найгірший еталон".

На другому кроці визначення гіпотетичного напряму підвищення рівня небезпеки можливих загроз ІР скористаємося відомим методом "прогресуючого еталону" й для впорядкованої "еталонної вибірки"обчислимо показники, що характеризують рівень їх потенціальної небезпеки. З цією метою:

а) представимо показники загроз ІР з "генеральної сукупності" в матричній формі:

$$C = \begin{bmatrix} c_{11} & ... & c_{1j} & ... & c_{1L} \\ ... & ... & ... & ... & ... \\ c_{i1} & ... & c_{ij} & ... & c_{iL} \\ ... & ... & ... & ... & ... \\ c_{Q1} & ... & c_{Qj} & ... & c_{QL} \\ ... & ... & ... & ... & ... \\ c_{N1} & ... & c_{Nj} & ... & c_{NL} \end{bmatrix}, \quad (4)$$

де c_{ij} - j-й показник i-го варіанта загрози ІР, $j = \overline{1, L},\ i = \overline{1, N}.$

б) проведемо нормування елементів сформованої матриці (C).

Правило: $\tilde{q}_{ij} = \left[c_{ij} - c_{ij}^{\min} \right] \cdot \left[c_{ij}^{\max} - c_{ij}^{\min} \right]^{-1},\ i = \overline{1, N},\ j = \overline{1, L};$

в) виділимо з нормованої матриці підматрицю, що відповідатиме "еталонній вибірці" та проведемо дослідження її кореляційних властивостей:

центруємо елементи виділеної підматриці $\tilde{q}_{ij}$**:**

$$\delta\tilde{q}_{ij} = \tilde{q}_{ij} - M_j, \textbf{ де } M_j = \frac{1}{Q} \sum_{i=1}^{Q} \tilde{q}_{ij} \text{ - МСП; } i = \overline{1, Q};\ j = \overline{1, L}; \quad (5)$$

сформуємо з відцентрованої підматриці матрицю розсіювання:

$$V = \left\lfloor v_{kj} \right\rfloor;\ k = \overline{1, L};\quad j = \overline{1, L},\quad v_{kj} = \sum_{p=1}^{Q} \delta^{T}_{\tilde{q}_{kp}} \delta_{\tilde{q}_{pj}} \tag{6}$$

обчислимо власні значення λ матриці $V = \left\lfloor v_{kj} \right\rfloor$ шляхом розкриття визначника $D(\lambda)$ та оберемо серед них максимальне:

$$D(\lambda) = \begin{vmatrix} v_{11} - \lambda & \dots & v_{1j} & \dots & v_{1L} \\ \dots & \dots & \dots & \dots & \dots \\ v_{k1} & \dots & v_{kj} - \lambda & \dots & v_{kL} \\ \dots & \dots & \dots & \dots & \dots \\ v_{L1} & \dots & v_{Lj} & \dots & v_{LL} - \lambda \end{vmatrix}, \tag{7}$$

де λ - множник Лагранжа (власне значення матриці V);

сформуємо вектор-стовпчик Ω^T власних значень матриці V: $\Omega^T = (\lambda_1, ..., \lambda_j, ..., \lambda_L)$, а також визначимо координати Ω^T з $D(\lambda)$ шляхом розкладання її першого рядка за алгебраїчними доповненнями D_{1j}, $j = \overline{1, L}$:

$$D(\lambda) = (v_{11} - \lambda) D_{11}(\lambda) + v_{12} D_{12}(\lambda) + ... + v_{1L} D_{1L}(\lambda); \tag{8}$$

сформуємо відносно $\lambda_{\max} = \max(\lambda_j)$, $j = \overline{1, L}$, – максимального власного значення матриці розсіювання, головний власний вектор $\Phi_{\max} = (W_1, ..., W_j, ..., W_L)$, який визначить напрямок підвищення рівня небезпеки можливих загроз ІР:

$$\Phi^T_{\max} = [D_{11}(\lambda_{\max}), D_{12}(\lambda_{\max}), ..., D_{1L}(\lambda_{\max})] = [W_1, W_2, ..., W_L],$$

Умова: уявні точки, що характеризують кожну з (N)загроз у $L-$ вимірному просторі показників групуються біля деякої гіперплощини (лінії) $\Phi_{\max}$, яка визначається МНК за критерієм:

$\sum_{i=1}^{N} s_i^2 \to \min$ відстаней s_i від $\Phi_{\max}$ до цих точок. При цьому $s_i = W^T \delta_{\tilde{q}_i}$,

де $\delta_{\tilde{q}_i} = \left\lfloor \delta_{\tilde{q}_{i1}}, \delta_{\tilde{q}_{i2}}, ..., \delta_{\tilde{q}_{ij}}, ..., \delta_{\tilde{q}_{iL}} \right\rfloor$ – вектор центрованих значень $\tilde{q}_{ij}$;

$W^T = \left\lfloor W_1, W_2, ..., W_j, ..., W_L \right\rfloor$ – коефіцієнти вагомості $j-$х показників ($j = \overline{1, L}$);

г) обчислимо показники, що характеризують рівень потенціальної небезпеки загроз з "еталонної вибірки":

$$Z_{загр_i} = \frac{\sum_{j=1}^{L} W_j (\tilde{q}_{ij} - \tilde{q}_{1j})}{\sum_{j=1}^{L} W_j (\tilde{q}^{\max}_{ij} - \tilde{q}_{1j})},\ i = \overline{1, N} \tag{9}$$

де $Z_{загр_i}$ – мінімальна відстань від уявної точки, що характеризує загрозу із "генеральної сукупності" класів загроз до гіперплощини, яка проходить через точку найменш значимої загрози вздовж $\Phi_{\max}$ і є ортогональною до неї;

W_j – вагові коефіцієнти небезпечності кожної загрози ІР;

$\tilde{q}_{1j}$ – значення першої нормованого показника в групі існуючих загроз;

$\tilde{q}^{\max}_{ij}$ – максимальне значення *j*-го нормованого показника для $i-$х загроз.

Геометрична інтерпретація формування комплексного показника рівня найбільш значимої загрози у двомірному просторі показників подона на рис.1.

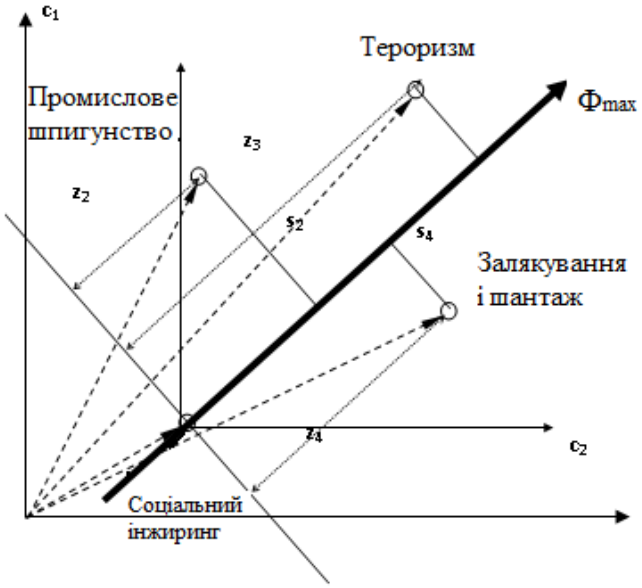

Рис.1. Геометрична інтерпретація формування комплексного показника рівня найбільш значимої загрози у двомірному просторі показника

Висновок

Таким чином, запропоновано метод визначення найбільш значимих загроз із «генеральної сукупності» загроз інформаційним ресурсам, який шляхом проведення попарних порівнянь та безпосередньої оцінки їх якісних і кількісних показників з всієї множини існуючих загроз дозволяє сформувати «еталонну вибірку» загроз інформаційним ресурсам, що забезпечує в подальшому можливість розрахунку показника найбільш небезпечної загрози.

Література

1. Невойт Я.В. Аналіз і оцінка ризиків інформаційної безпеки для банківських та комерційних систем / Невойт Я.В., Єрмошин В.В,// Сучасний захист інформації. – 2014.Частина 1. – №3, С. 26-29.

2. Невойт Я.В. Аналіз і оцінка ризиків інформаційної безпеки для банківських та комерційних систем / Невойт Я.В., Єрмошин В.В,// Сучасний захист інформації. – 2014.Частина 2. – №4, С. 12-22.

3. Jun M. Information inconsistencies detection using a rule-map technique / M. Jun, L. Jie, Z. Guangquan // Expert Systems with Applications: An International Journal. – 2009. – Vol. 36, issue 10. – P. 12510–12519.

4. Бурячок В.Л. Алгоритм порівняльного оцінювання програмних засобів однакового функціонального призначення для розв'язання завдань інформаційної діяльності. Збірник наукових праць в/ч А1906 МО України № 27, 2010, с. 124 - 139 Інв. 4590.

5. Ленков С. В. Методы и средства защиты информации : монография : [в 2-х т.] / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. – К. : Арий, 2008. – Т. 2 : Информационная безопасность. – 344 с.

Надійшла 10.08.2015 р. Рецензент: д.т.н., проф. Шелест М.Є.