

УДК 004.056.57

И. В. Аникин, А. П. Кирпичников

ПРИМЕНЕНИЕ МЕТОДА АНАЛИЗА ИЕРАРХИЙ ДЛЯ РЕШЕНИЯ ЗАДАЧИ ВЫБОРА АНТИВИРУСНЫХ ПРОДУКТОВ

Ключевые слова: метод анализа иерархий, экспертные оценки, антивирусная защита.

В статье решается задача многокритериального выбора антивирусного продукта для предприятия. Предлагаются критерии отбора антивирусов. Для решения данной задачи используются экспертные оценки и метод анализа иерархий.

Keywords: analytic hierarchy process, expert judgments, antivirus.

We realize multi-criteria selection for antivirus products. Selection criteria for such products have been suggested. We use expert judgments and analytic hierarchy process to make multi-criteria selection.

Задачи многокритериального ранжирования и выбора альтернатив имеют широкое прикладное значение [1]. Для многих таких задач ведущими мотивами принятия решений являются предпочтения людей, а среди критериев принятия решений доминирующую роль играют качественные критерии, которые сложно оценивать в количественном виде. Примерами таких задач являются управление рисками информационной безопасности и выбор средств защиты для определенного объекта [2,3,4,5].

При решении подобных задач достаточную эффективность показал метод анализа иерархий (МАИ), предложенный Т. Саати [6,7,8]. Идея МАИ заключается в построении многоуровневой иерархии путем декомпозиции сложных событий на составные элементы, факторы, и разнесения их по различным уровням иерархии, одновременно идентифицируя величину связи между ними. Центральный вопрос, который исследуется в МАИ: насколько сильно влияют отдельные факторы самого низкого уровня иерархии на ее вершину – общую цель. Для получения ответа на данный вопрос на каждом уровне иерархии эксперт производит всевозможные парные сравнения объектов по отношению к элементам более высокого уровня иерархии на качественной шкале из 9 градаций, представленной в табл. 1.

Обозначим результат сравнения элементов i и j иерархии на качественной шкале через a_{ij} . В результате всевозможных парных сравнений формируется матрица парных сравнений A , обладающая следующими свойствами:

– Диагональными элементами являются единицы.

– Если $a_{ij} = \alpha$, то $a_{ji} = 1/\alpha$

Т.Саати показал, что для того, чтобы получить приоритеты исследуемых элементов по отношению к элементу более высокого уровня иерархии, необходимо найти собственный вектор матрицы парных сравнений, соответствующий ее максимальному собственному значению. Данный собственный вектор и будет являться вектором приоритетов. Су-

ществует численный метод определения собственного вектора матрицы парных сравнений [6,7].

Таблица 1 - Качественная шкала Т. Саати

Качественная оценка	Интенсивность важности	Объяснения
Одинаковая значимость	1	Элементы равны по значимости
Слабо значимее	3	Существуют показания о предпочтении одного элемента другому, но показания неубедительные
Существенно или сильно значимее	5	Существуют хорошие доказательства и логические критерии, которые могут показать, что элемент более важен
Очевидно значимее	7	Существует очевидное доказательство большей значимости одного элемента перед другим
Абсолютно значимее	9	Максимально подтверждается осознанность предпочтения одного элемента другому
Промежуточные оценки между соседними	2,4,6,8	

Пусть $A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1s} \\ a_{21} & a_{22} & \dots & a_{2s} \\ \dots & \dots & \dots & \dots \\ a_{s1} & a_{s2} & \dots & a_{ss} \end{pmatrix}$ – матрица

парных сравнений элементов $E_1, \dots, E_s$. Тогда для вычисления приоритетов важности элементов выполняют следующие действия.

1. Для каждой i -ой строки матрицы A вычисляются среднее геометрическое значение

$$A = \begin{pmatrix} a_{11} & \dots & a_{1j} & \dots & a_{1s} \\ \dots & \dots & \dots & \dots & \dots \\ a_{i1} & \dots & a_{ij} & \dots & a_{is} \\ \dots & \dots & \dots & \dots & \dots \\ a_{s1} & \dots & a_{sj} & \dots & a_{ss} \end{pmatrix} \quad \begin{aligned} a_1 &= \sqrt[s]{a_{11} \cdot \dots \cdot a_{1j} \cdot \dots \cdot a_{1s}} \\ \dots & \\ a_i &= \sqrt[s]{a_{i1} \cdot \dots \cdot a_{ij} \cdot \dots \cdot a_{is}} \\ \dots & \\ a_s &= \sqrt[s]{a_{s1} \cdot \dots \cdot a_{sj} \cdot \dots \cdot a_{ss}} \end{aligned}$$

2. Элементы вектора $a=(a_1, \dots, a_s)$ нормируют таким образом, чтобы $\sum_{i=1}^s a_i = 1$. Для этого формируют нормированный вектор $d=(d_1, \dots, d_i, \dots, d_s)$.

$$d_i = \frac{a_i}{\sum_i a_i} = \frac{\sqrt[s]{\prod_j a_{ij}}}{\sum_i \sqrt[s]{\prod_j a_{ij}}}$$

3. Для каждого столбца j матрицы A вычисляется сумма его элементов $b_j = a_{1j} + \dots + a_{sj} = \sum_{i=1}^s a_{ij}$.

4. Находится максимальное собственное число матрицы парных сравнений $\lambda_{\max}$ согласно выражению $\lambda_{\max} = b_1 \cdot d_1 + \dots + b_s \cdot d_s$.

5. Произвольно составленная матрица парных сравнений не может быть использована для вычисления вектора приоритетов. Метод анализа иерархий определяет способ определения согласованности оценок эксперта путем расчета индекса согласованности (IC) и отношения согласованности (OC) следующим образом:

$$\check{CN} = \frac{\lambda_{\max} - n}{n - 1} \quad OC = \frac{\check{CN}}{CC}$$

где CC – индекс случайной согласованности, зависящий от порядка матрицы.

6. Если $OC < 0.15$, то составленная матрица парных сравнений A приемлемо согласованна, а вектор $d=(d_1, \dots, d_i, \dots, d_s)$ является вектором приоритетов

В [6,7] определен также способ расчета приоритетов альтернатив в случае многокритериального выбора, а также для многоуровневых иерархий (число уровней больше 3).

Рассмотрим решение задачи многокритериального выбора антивирусных продуктов для некоего предприятия с помощью метода анализа иерархий. Задача сравнительного анализа антивирусных систем решалась в различных работах [9], однако исследований относительно перечня критериев производилось недостаточно. Будем осуществлять выбор среди следующих шести антивирусных продуктов:

- C_1 = Kaspersky Endpoint Security;
- C_2 = Dr.Web Enterprise Suite;
- C_3 = Symantec Protection Suite Small Business Edition;
- C_4 = ESET Endpoint Antivirus;
- C_5 = Panda Security for Business;
- C_6 = Avast! Endpoint Protection.

В качестве критериев выбора антивирусных продуктов будет использовать следующие:

- K_1 = «Полнота идентифицируемых видов угроз»;
- K_2 = «Качество обнаружения угроз»;
- K_3 = «Величина влияния на производительность системы»;
- K_4 = «Полнота необходимых средств управления и удобство их использования»;
- K_5 = «Качество построения отчетов»;
- K_6 = «Качество администрирования»;
- K_7 = «Контроль конфигурации»;
- K_8 = «Качество реализации механизма обновления»;
- K_9 = «Масштабируемость»;
- K_{10} = «Полнота поддержки средств архивирования»;
- K_{11} = «Приемлемость цены».

Для выбора наиболее предпочтительного антивирусного продукта на первом шаге строится трехуровневая иерархия, представленная на рис. 1.

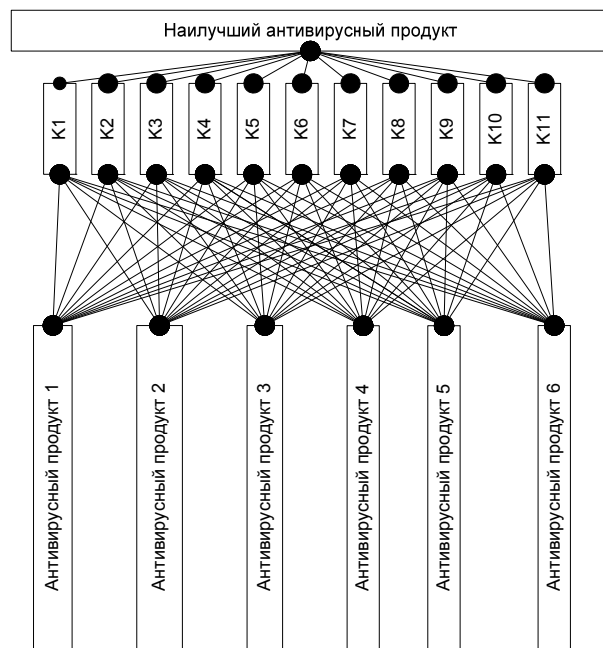


Рис. 1 - Иерархия выбора наилучшего антивирусного продукта

На первом уровне иерархии представлена цель – выбор наилучшего антивирусного продукта. На втором уровне иерархии представлены 11 критериев выбора антивирусных продуктов. Данные критерии являются неравнозначными, например, «Цена» может иметь меньший приоритет по сравнению с рядом функциональных критериев. На третьем уровне иерархии представлены 6 исследуемых антивирусных продуктов. Данные антивирусные продукты могут иметь различные приоритеты по отношению к различным критериям.

На втором шаге определяются веса важности $S_1, \dots, S_{11}$ критериев. Это осуществляется путем реализации всевозможных парных сравнений критериев на качественной шкале (таблица 1) и обработки

получившейся матрицы парных сравнений. В таблице 2 представлены веса важности критериев, полученные в результате выполнения шага 2.

Таблица 2 - Веса важности критериев

Критерий K_i	Вес важности S_i	Критерий K_i	Вес важности S_i
K_1	0.11	K_2	0.15
K_3	0.29	K_4	0.13
K_5	0.02	K_6	0.02
K_7	0.09	K_8	0.05
K_9	0.06	K_{10}	0.05
K_{11}	0.03		

На третьем шаге определяются приоритеты антивирусных продуктов $C_1 - C_6$ по отношению к каждому из 11 критериев. Для этого эксперт выполняет их всевозможные парные сравнения на качественной шкале. Для каждого из критериев K_i путем обработки матрицы парных сравнений формируется вектор весовых коэффициентов $S(K_i) = \{S_i(K_i)\}, i = \overline{1,6}$. Объединив векторы весовых коэффициентов по каждому из критериев, мы получим полную матрицу приоритетов антивирусных продуктов размерности 6×11 в следующем виде:

$$\begin{pmatrix} S_1(K_1) & \dots & S_i(K_1) & \dots & S_6(K_1) \\ \dots & \dots & \dots & \dots & \dots \\ S_1(K_j) & \dots & S_i(K_j) & \dots & S_6(K_j) \\ \dots & \dots & \dots & \dots & \dots \\ S_1(K_{11}) & \dots & S_i(K_{11}) & \dots & S_6(K_{11}) \end{pmatrix} \begin{matrix} E_1 \\ \dots \\ E_j \\ \dots \\ E_{11} \end{matrix}$$

Полученная на данном шаге матрица приоритетов представлена ниже:

$$\begin{pmatrix} 0.2 & 0.14 & 0.24 & 0.18 & 0.12 & 0.12 \\ 0.25 & 0.12 & 0.21 & 0.14 & 0.21 & 0.07 \\ 0.03 & 0.14 & 0.11 & 0.21 & 0.21 & 0.31 \\ 0.37 & 0.08 & 0.37 & 0.08 & 0.07 & 0.04 \\ 0.27 & 0.11 & 0.44 & 0.07 & 0.07 & 0.03 \\ 0.37 & 0.08 & 0.37 & 0.08 & 0.07 & 0.04 \\ 0.14 & 0.15 & 0.4 & 0.16 & 0.12 & 0.03 \\ 0.45 & 0.25 & 0.11 & 0.13 & 0.05 & 0.02 \\ 0.26 & 0.1 & 0.48 & 0.07 & 0.06 & 0.02 \\ 0.35 & 0.13 & 0.35 & 0.07 & 0.07 & 0.04 \\ 0.13 & 0.06 & 0.13 & 0.05 & 0.03 & 0.6 \end{pmatrix}$$

На четвертом шаге определяется итоговый вектор $w = (w_1, \dots, w_{11})$ приоритетов антивирусных продуктов в следующем виде:

$$w = (w_1, \dots, w_{11}) = (S_1, \dots, S_{11}) \cdot \begin{pmatrix} S_1(K_1) & \dots & S_i(K_1) & \dots & S_6(K_1) \\ \dots & \dots & \dots & \dots & \dots \\ S_1(K_j) & \dots & S_i(K_j) & \dots & S_6(K_j) \\ \dots & \dots & \dots & \dots & \dots \\ S_1(K_{11}) & \dots & S_i(K_{11}) & \dots & S_6(K_{11}) \end{pmatrix}$$

В нашем случае

$$w = (w_1, \dots, w_{11}) = (0.2, 0.13, 0.25, 0.15, 0.14, 0.14)$$

Ранжирование антивирусных продуктов и выбор наиболее предпочтительного из них осуществляется в соответствии с их приоритетами w_i . Наилучший антивирусный продукт C_k выбирается в соответствии с правилом: $C_k | w_k = \max_{i=1,6} w_i$. В нашем

случае наилучшим антивирусным продуктом для предприятия является продукт Symantec.

Литература

1. В. И. Глова, И. В. Аникин, М. Р. Шагиахметов. Методы многокритериального принятия решений в условиях неопределенности в задачах нефтедобычи. Казань: Изд-во Казан. гос. техн. ун-та, 2004. 31 с.
2. Аникин И.В. Управление внутренними рисками информационной безопасности корпоративных информационных сетей // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. -2009, Т.3, № 80. - С.35-50.
3. Аникин И.В. Метод оценки внутренних рисков информационной безопасности корпоративных информационных сетей // Информация и безопасность. - 2014, Т.17, № 2. - С. 320-323.
4. Аникин И.В. Метод количественной оценки уровня ущерба от реализации угроз на корпоративную информационную сеть // Информационные технологии. - 2010, № 1. - С. 2-6.
5. Аникин И.В., Кирпичников А.П., Назаров А.О. Практическое применение метода концептуальной кластеризации объектов, характеризуемых нечеткими параметрами // Вестник Казанского государственного технического университета. - 2014, Т.17, № 11. - С. 203-206.
6. Саати Т. Принятие решений. Метод анализа иерархий. М.: Радио и связь, 1993.
7. Саати Т., Кернс К. Аналитическое планирование. Организация систем. М.: Радио и связь, 1991.
8. Аникин И.В. Метод анализа иерархий в задачах оценки и анализа рисков информационной безопасности // Вестник Казанского государственного технического университета им. А.Н. Туполева. - 2006, № 3. - С.11-18.
9. Бегалин А.Ш., Бегалина М.Ш. Антивирусы: Анализ производительности и эффективности // Наука и мир. - 2014, Т. 1, № 2. - С. 153-155.

© **И. В. Аникин** – канд. техн. наук, зав. каф. систем информационной безопасности КНИТУ-КАИ, anikinigor777@mail.ru; **А. П. Кирпичников** – д-р физ.-мат. наук, зав. каф. интеллектуальных систем и управления информационными ресурсами КНИТУ, kirpichnikov@kstu.ru.

© **I. V. Anikin** - PhD, Head of the Department of Information Security Systems, KNRTU-KAI, anikinigor777@mail.ru; **A. P. Kirpichnikov** - Dr. Sci, Head of the Department of Intelligent Systems and Information Systems Control, KNRTU, kirpichnikov@kstu.ru.