ЭФФЕКТИВНЫЙ МЕТОД МНОГОКРИТЕРИАЛЬНОГО АНАЛИЗА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

*Большаков А.С., Раковский Д.И.**

Ключевые слова: *информационная безопасность, защита информации, теория принятия решений, методы принятия решений, комплексный метод анализа иерархий, дискретные многокритериальные задачи, автоматизация принятия решений, программное обеспечение.*

Аннотация.

Цель работы: *совершенствование научно-методической и правовой базы принятия решений по обеспечению информационной безопасности.*

Метод исследования: *сравнительный анализ существующих методов принятия решений по двум критериям: количество операций сравнения и количество матриц парных сравнений.*

Результаты: *рассмотрен ряд методов принятия решений, из которых определен наиболее эффективный в контексте поставленной задачи — метод, обеспечивающий минимальное количество попарных операций сравнения. Проведенный анализ показал, что таким свойством обладает метод комплексного анализа иерархий. Данный метод является наименее сложным (по количеству проводимых операций сравнения) и может быть использован при решении дискретных многокритериальных задач. Применение выбранного метода демонстрируется авторами на примере выбора средства защиты информации. На основе выбранного метода с учетом контекста поставленной задачи разработано программное обеспечение для автоматизированного выбора наилучшего средства защиты информации, использующееся в учебном процессе в виде лабораторного практикума для студентов направления подготовки «Инфокоммуникационные технологии и системы связи».*

DOI: 10.21681/1994-1404-2020-4-55-66

Постановка задачи

Задача выбора средства защиты информации (СЗИ) из комплекса аналогичных средств, потенциально приемлемых для конкретной инфокоммуникационной системы правовой сферы [8], как правило, носит не простой характер, связанный с возможными значительными трудозатратами, которые желательно минимизировать путем автоматизации такого выбора. Применение специализированного *программного обеспечения* [1], созданного в соответствии с действующими нормативными правовыми актами, позволяет упростить процесс моделирования угроз информационной безопасности и является исходным материалом для дальнейшего принятия решений с целью нейтрализации сформированных угроз.

Проблему при автоматизации представляют задачи категории *принятия решений*, которые в области информационной безопасности широко распространены. Специалисты решают задачи данной категории, основываясь либо на собственном опыте, либо на основе экспертной оценки, либо на основе применения обоснованных численных функций конфиденциальности [4].

Для достижения оперативной объективной оценки принятия решений в области информационной безопасности экспертный подход представляется более предпочтительным[1]. Однако формирование компетентной экспертной группы, особенно в области мало-

[1] Методика моделирования угроз безопасности информации [Текст]: методический документ // Федеральная Служба по Техническому и Экспортному Контролю (ФСТЭК РОССИИ), 2020, 54 с. В документе (по сравнению с проектной методикой 2015 г., а также с принятой ранее методикой 2008 г.) наблюдается тенденция перехода к экспертной оценке параметров информационной системы вместо формализованной.

* ***Большаков Александр Сергеевич,*** *кандидат технических наук, доцент Московского технического университета связи и информатики, г. Москва, Российская Федерация.*

E-mail: alexbol57@mail.ru

Раковский Дмитрий Игоревич, *магистрант Московского технического университета связи и информатики, г. Москва, Российская Федерация.*

E-mail: dimitor1998@mail.ru

го бизнеса, часто бывает затруднительным делом — по этой причине многие решения принимаются специалистом в области информационной безопасности в одиночку. Это приводит к повышению рабочей нагрузки и времени, затрачиваемого на анализ и принятие решений в области информационной безопасности, а иногда и к не эффективному выбору самой меры защиты информации. То есть повышается вероятность принятия необъективного решения по причине человеческого фактора: нехватки времени, невнимательности, недостаточной компетенции и пр.

При принятии какого-либо решения может использоваться массив n атрибутов:

$$K = \{k_1, k_2, \dots, k_n\}, \quad (1)$$

где k_i — i-й атрибут в системе принятия решений, который задан некоторым текстовым описанием, включая, например:

- наличие действующих сертификатов соответствия СЗИ требованиям ФСТЭК России, ФСБ России, Госстандарта, МО РФ и других ведомств по определенным уровням и классам защищенности;
- совместимость СЗИ со смежными системами (информационными технологиями) и возможность работы программных СЗИ на технических средствах и общесистемном программном обеспечении инфосистем;
- соответствие СЗИ требованиям, определенным мерами защиты для выбранного класса защищенности инфосистем и сформированной модели угроз;
- простоту управления и внедрения СЗИ для различных конфигураций инфосистем;
- наличие у специалиста опыта работы с выбираемыми СЗИ конкретных производителей;
- наличие выявляемых качественных преимуществ между однотипными СЗИ;
- наличие выявляемых ценовых преимуществ между однотипными СЗИ;
- наличие сервисных центров и технической поддержки в Российской Федерации для СЗИ;
- наличие положительных отзывов на функционирование СЗИ и пр.

Однако с целью автоматизации процесса принятия решения о выборе СЗИ целесообразно перейти от текстовых индикаторов к их индексации:

$$J = \{j_1, j_2, \dots, j_n\}, j_i \in \mathbb{N}\ , \quad (2)$$

где j_i = 1, 2, . …n, т.е. может принимать, например, целые значения.

Поставим каждому индексу j_i в соответствие атрибут k_i, т.е. отобразим J в K:

$$f: J \to K. \quad (3)$$

Таким образом, массив K может быть представлен в виде массива индексов J, состоящего из оценок атрибутов n.

Пусть дана последовательность из n численных оценок по каждому атрибуту (1) для некоторого процесса, состоящего из последовательности событий «угроза — уязвимость — информационный ресурс — нарушаемое свойство информации — СЗИ», выставленная экспертом:

$$A = \{a_1, a_2, \dots, a_n\}, a_i \in \mathbb{N}\ . \quad (4)$$

Тогда m альтернатив (4), оцененных по каждому из n атрибутов (1), можно представить в виде таблицы:

$$Expert = \{(J, A_1), (J, A_2), \dots, (J, A_m)\ |(J, A_i) \in J \times A_{all}\}, \quad (5)$$

где $J \times A_{all}$ — декартово произведение двух множеств $J \times A_{all}$; причем элементами множества A_{all} являются наборы экспертных оценок, определенные в (4), а элементы множества J определены в (2) как индексы, соответствующие атрибутам (1), между которыми определено однозначное соответствие (3).

Табличное представление записи (5), дополненное пояснительными строками и столбцами для упрощения визуального восприятия, представлено в табл. 1 (где a_{mn} — численные значения баллов, выставленные экспертами, отражающие степень соответствия m-й альтернативы n-му атрибуту — чем выше балл — тем больше соответствие).

Авторами предполагается наличие подобной таблицы экспертных оценок у специалиста в области информационной безопасности перед решением задачи о выборе методов принятия решений.

Таблица 1

Экспертная оценка соответствия m-альтернатив по каждому n-атрибуту

	Атрибуты			
Альтернативы	j_1	j_2	…	j_n
A_1	a_{11}	a_{12}	…	a_{1n}
A_2	a_{21}	a_{22}	…	a_{2n}
…	…	…	…	…
A_m	a_{m1}	a_{m2}	…	a_{mn}

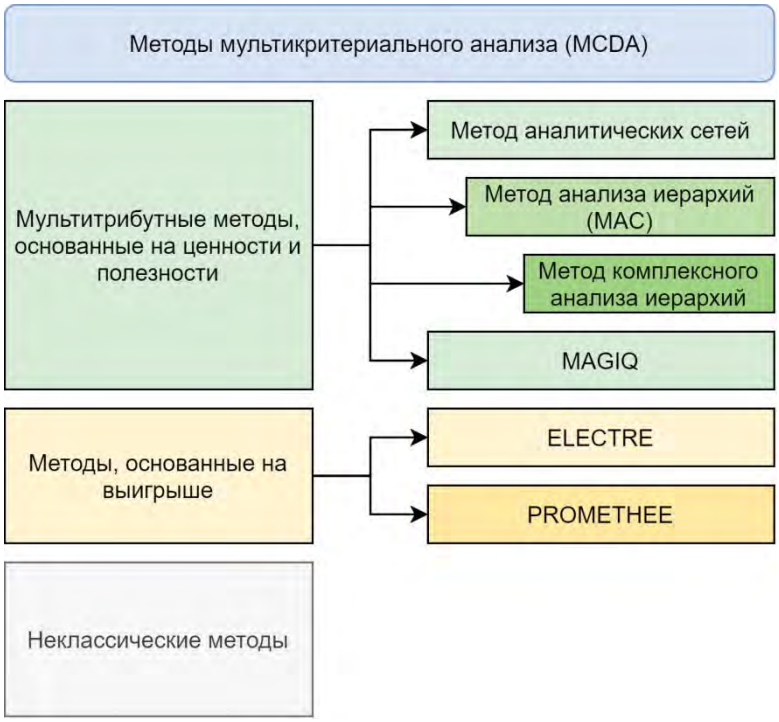

Рис. 1. Прагматическая классификация методов принятия решений и отобранные для анализа методы

Методы принятия решений можно разделить на три категории [14]: мультиатрибутные методы, основанные на ценности и полезности (*Multiattribute Utility and Value Theories*); методы, основанные на ценности (*Outranking Methods*); неклассические методы (рис. 1). Рассмотрение методов (за исключением неклассических) ведется с учетом наличия исходных данных в виде экспертной оценки, выраженной численно и представленной в виде описанной выше таблицы, или аналогичным по смыслу представлением.

Рассматриваемые методы и источники, на которые опираются авторы при рассмотрении методов, представлены в виде пронумерованного списка:

1. Метод аналитических сетей [3, 7];
2. Метод анализа иерархий (MAC)[2];
3. Метод комплексного анализа иерархий [10];
4. Мультиатрибутный глобальный вывод качества (*Magiq*)[3];
5. Метод исключений и выбора, отражающих реальность (*Electre*) [5, 6];
6. Метод организации ранжирования предпочтений для обогащения оценок (*Promethee*) [13]. Рассмотрены методы *Promethee-1, Promethee-2* в совокупности друг с другом.

Названные методы принятия решений рассматриваются в контексте следующих критериев:

– *количество матриц парных сравнений* — которые необходимо построить специалисту самостоятельно;
– *количество операций сравнения* — показывает суммарное количество операций сравнения, которые необходимо провести специалисту самостоятельно, определяемых из свойств, как конкретного метода принятия решений, так и из первого критерия.

На основании данных критериев выбирается метод, применимый в области защиты информации, позволяющий минимизировать участие специалиста в принятии решений.

Обзор методов принятия решений

Рассмотрены шесть методов принятия решений по указанным выше критериям путем выполнения подсчета количества матриц парных сравнений и операций сравнения, последующего заполнения специальной таблицы с формулированием вывода об эффективном методе принятия решений.

При рассмотрении методов принятия решений использованы следующие обозначения, определяемые из (5) и вышеприведенных критериев: M_i — количество матриц парных сравнений, присутствующих в i-м методе принятия решений; k — количество атрибутов в системе принятия решений; k_m — количество элементов в подмножествах атрибутов системы принятия решений; a — количество альтернатив в системе при-

[2] Саати Т. Принятие решений. Метод анализа иерархий. М. : Радио и связь, 1993.

[3] McCaffrey Jm. The Analytic Hierarchy Process // MSDN Magazine Issues. 2005. № 6. С. 139—144.

нятия решений; a_m — количество элементов в подмножествах альтернатив системы принятия решений.

Метод аналитических сетей. В данном методе количество матриц парных сравнений зависит от количества анализируемых альтернатив. Все матрицы, построенные таким образом, сводятся в единую суперматрицу парных сравнений. Количество матриц парных сравнений в суперматрице определяется как a^2 [11].

Суперматрица обладает такими же свойствами, как и матрица парных сравнений. Следовательно, суперматрица обладает свойством симметрии:

$$\boldsymbol{B} = \boldsymbol{B}^{\boldsymbol{T}} \quad (6)$$

Исходя из свойства симметрии: $\forall i,j: a_{ij} = a_{ji}$, количество матриц парных сравнений определяется с учетом вычета главной диагонали как:

$$M_1 = \frac{a^2 - a}{2} . \quad (7)$$

Каждая матрица парных сравнений, входящая в суперматрицу, строится на основе сравнения подмножества i-й альтернативы с подмножеством j-й альтернативы. Количество операций сравнений, учитывая вычет $a_{m\,ij}$ элементов главной диагонали, определяется как:

$$W_{ij} = \frac{a_{mij}{}^2 - a_{mij}}{2} . \quad (8)$$

Соответственно, общее количество операций сравнений может быть найдено как сумма количеств операций сравнений каждой подматрицы:

$$f_{AN} = \sum_{i=1}^{a} \sum_{j=1}^{a} W_{ij} \quad (9)$$

При отсутствии подмножеств альтернатив ($a_m = 0$) общее количество операций сводится к

$$f_{AN} = \frac{a^2 - a}{2} \quad (10)$$

Метод анализа иерархий. Данный метод является частным случаем метода построения аналитических сетей [11]. В методе анализа иерархий парные сравнения можно разделить на два шага.

Шаг 1. Выполняется парное сравнение атрибутов системы, т.е. количество операций сравнений для первого шага можно вычислить как:

$$f_{MAC\ 1} = \frac{k^2 - k}{2} \quad (11)$$

Шаг 2. На втором шаге выполняется парное всех атрибутов между собой по каждой альтернативе. В данном случае иерархическая зависимость альтернатив и подмножеств альтернатив не играет существенной роли. Для вычисления количества операций сравнения необходимо найти количество всех альтернатив вместе с подмножествами, т.е.:

$$U = a + a_m . \quad (12)$$

Следовательно, количество операций сравнения, которое необходимо провести, вычисляется как количество парных сравнений, умноженное на (12):

$$f_{\mathrm{MAC}\ 2} = U\ \frac{k^2 - k}{2} \quad (12)$$

Общее количество операций сравнения, проводимое экспертами в методе MAC, составляет:

$$f_{\mathrm{MAC}} = f_{\mathrm{MAC}\ 1} + f_{\mathrm{MAC}\ 2} . \quad (14)$$

Проведя операции подстановки и сокращения, получим:

$$f_{\mathrm{MAC}} = (U + 1)\ \frac{k^2 - k}{2} \quad (15)$$

Количество матриц парных сравнений зависит от количества альтернатив (12). Также необходимо учесть одно парное сравнение атрибутов между собой:

$$M_2 = 1 + U \quad (16)$$

Метод комплексного анализа иерархий. Метод является усовершенствованным методом анализа иерархий [3]. Сравнение альтернатив выполняется за два шага:

Шаг 1. Является аналогичным по отношению к методу анализа иерархий, однако парное сравнение альтернатив заменено таблицей экспертных оценок (5), что убирает необходимость строить матрицу парных сравнений.

Шаг 2. Выполняется одно парное сравнение атрибутов системы между собой. Следовательно, количество матриц парных сравнений равно единице:

$$M_3 = 1 \quad (18)$$

Количество операций сравнения для данного метода будет вычисляться как:

$$f_{\mathrm{CAN}} = \frac{k^2 - k}{2} \quad (18)$$

Сравнение альтернатив системы (средств защиты информации) между собой по атрибутам происходит без построения матрицы парных сравнений, на основе обобщенного показателя; проверка адекватности осуществляется на основе построения матрицы рисков.

Метод Electre. В методе *Electre* используется одно парное сравнение всех альтернатив по всем атрибутам. То есть количество матриц парных сравнений будет равно одной:

$$M_4 = 1 .$$

Сравнение альтернатив происходит без построения матрицы парных сравнений. Вместо этого альтернативы попарно сравниваются между собой с целью выявления превосходства одной альтернативы над другой.

Количество операций сравнения альтернатив сводится к операции размещения из a альтернатив по два, умноженное на количество атрибутов:

$$f_{Electre} = k \times A_a^2 . \quad (19)$$

Метод Magiq. В методе *Magiq* выполняется несколько операций парных сравнений. Сначала выполняется парное сравнение атрибутов системы. Общее количество таких операций сравнений равно:

$$f_{Magiq\ 1} = \frac{k^2 - k}{2} . \quad (20)$$

После парного сравнения атрибутов выполняются парные сравнения внутри каждого подмножества атрибутов: выполняется a парных сравнений, в каждом из которых количество операций сравнения зависит от количества элементов i-го подмножества:

$$q_i = \frac{k_{mi}{}^2 - k_{mi}}{2} . \quad (21)$$

Суммарное количество операций сравнения вычисляется как:

$$f_{Magiq\ 2} = \sum_{i=1}^{k} q_i . \quad (22)$$

На *третьем* этапе алгоритма выполняется парное сравнение альтернатив между собой по всем атрибутам вне зависимости от их иерархической зависимости (по аналогии с (12)). Сложив сумму всех подмножеств атрибутов и количество атрибутов:

$$U_{Magiq} = k + k_m . \quad (23)$$

Можно вычислить количество операций сравнения, которое на данном этапе зависит от количества альтернатив системы:

$$f_{Magiq\ 3} = U_{magiq} \frac{a^2 - a}{2} . \quad (24)$$

Соответственно, общее количество операций сравнения, проводимое экспертами в методе Magiq, составляет:

$$f(n) = f_{Magiq\ 1} + f_{Magiq\ 2} + f_{Magiq\ 3} \quad (25)$$

Количество матриц парных сравнений, на основании предыдущих трех шагов, определяется как:

$$M_5 = 1 + k + U_{magiq} . \quad (26)$$

Метод Promethee. В методах семейства *Promethee* входные данные обрабатываются в два этапа. *Первый* этап является общим для всех алгоритмом данного семейства, *второй* же этап зависит от конкретной реализации алгоритма (рассмотрены алгоритмы *Promethee*-1, *Promethee*-2).

Этап 1. Входными данными являются: атрибуты и альтернативы. Необходимо задать относительный вес каждого атрибута, а также функцию предпочтения альтернативы $g_k(a)$ по каждому атрибуту. Для каждого атрибута функция предпочтения своя — она выбирается исходя из контекста решаемой задачи. Функция предпочтения показывает, насколько значима разница значений двух альтернатив (если альтернативы представлены метрическими величинами) по выбранному атрибуту, что роднит ее с методами, применяемыми в нечеткой логике [2].

На *этапе* 1 производится построение матриц парных сравнений альтернатив по каждому атрибуту. Сравнение происходит при помощи функции предпочтения. Количество операций сравнения определяется как:

$$f_{Promethee} = k \frac{a^2 - a}{2} . \quad (27)$$

После построения матриц парных сравнений строится матрица индексов предпочтения путем сложения всех матриц парных сравнений между собой. Предварительно каждую матрицу парных сравнений необходимо умножить на соответствующий ей относительный вес каждого атрибута.

Этап 2. Как было обозначено, в зависимости от выбранного алгоритма (*Promethee*-1, *Promethee*-2) количество операций парных сравнений различно.

Для *Promethee*-1 необходимо построить матрицу бинарных отношений альтернатив на основании матрицы индексов предпочтения. Соответственно, количество операций парных сравнений будет вычислено как:

$$f_{Promethee\ 1} = \frac{a^2 - a}{2} . \quad (28)$$

Promethee-2 опирается на коэффициенты, вычисленные из матрицы индексов предпочтения (называемые коэффициентами прямого и обратного восхождения). Дополнительных матриц парных сравнений строить не обязательно, однако авторы метода рекомендуют использовать *Promethee*-1 и *Promethee*-2 в совокупности друг с другом.

С учетом данных рекомендаций имеет смысл объединить (27) и (28). С учетом упрощения получим окончательное количество операций парных сравнений, определяемое как:

$$f_{Promethee\ 1+2} = (k+1) \frac{a^2 - a}{2} . \quad (29)$$

Количество матриц парных сравнений, определяемых для методов *Promethee*-1 + *Promethee*-2, определяется как:

$$M_6 = k + 1. \quad (30)$$

Итоговая таблица

Сведем полученные аналитические выражения в специальную таблицу (табл. 2). В *первом* столбце приведено название метода, во *втором* критерий «количество матриц парных сравнений», в *третьем* — критерий «количество операций сравнения».

Минимальным количеством парных сравнений обладают методы *Electre* и комплексного анализа иерархий. Метод комплексного анализа иерархий (адаптированная версия метода анализа иерархий) имеет меньшее количество операций сравнения, которые зависят только от количества атрибутов, по которым сравниваются альтернативы.

Следовательно, эффективным методом принятия решений с точки зрения минимизации количества операций парных сравнений можно признать метод комплексного анализа иерархий.

Пример использования метода комплексного принятия решений

Рассмотрим данный подход в контексте автоматизации процесса принятия решений. В качестве входных данных возьмем материалы публикации «Критерии выбора средств обеспечения информационной безопасности персональных данных» [9]. Анализируемые *критерии* (в нашем случае атрибуты) представлены в виде нумерованного списка:

Таблица 2

Сравнение методов по критериям «количество парных сравнений» и «количество операций сравнения»

Метод	Количество матриц M парных сравнений	Количество $f(n)$ операций сравнения
Аналитических сетей	$\frac{a^2-a}{2}$	$f(n)=\sum_{i=1}^{a}\sum_{j=1}^{a}W_{ij}$ $W_{ij}=\frac{{a_{mij}}^2-a_{mij}}{2}$
Анализа иерархий	$U+1$	$(U+1)\ \frac{k^2-k}{2}$ $U=a+a_m$
Комплексного анализа иерархий	1	$\frac{k^2-k}{2}$
Magiq	$U_{Magiq}+1+k$	$f_{Magiq\ 1}+f_{Magiq\ 2}+f_{Magiq\ 3}$
Electre	1	$k\times A_a^2$
Promethee 1 + Promethee 2	$k+1$	$(k+1)\frac{a^2-a}{2}$

1. Использование средств аппаратной поддержки.
2. Шифрование пользовательской информации.
3. Осуществление аудита событий.
4. Контроль целостности ресурсов.
5. Возможность настройки замкнутой программной среды.
6. Стоимость средств защиты.
7. Личные предпочтения администраторов безопасности.
8. Наличие механизма дискреционного контроля доступа к объектам файловой структуры и устройствам.
9. Затирание информации.
10. Поддержка аутентификации.

Средства защиты информации (альтернативы), рассмотренные в статье, приведены в виде нумерованного списка:

1. *Secret Net* (с платой *Secret net touch memory*).
2. *Secret Net* (без платы *Secret net touch memory*).
3. Secret Net (с платой Соболь).
4. ПАК Соболь.
5. АМДЗ Аккорд.
6. ПАК Аккорд.
7. *Dallas Lock* 8*K*.
8. *Dallas Lock* 8*C*.
9. Страж *NT*.

Сформируем таблицу экспертной оценки в соответствии с (5) и табл. 1. Экспертная оценка СЗИ по вышеприведенным атрибутам приведена в табл. 3. Стоит заметить, что при выборе метода комплексного анализа иерархий специалисту необходимо будет самостоятельно дополнительно построить матрицу парных сравнений анализируемых атрибутов.

Таблица 3

Экспертная оценка СЗИ по 10 атрибутам

СЗИ	Атрибуты									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	4	0	3	4	5	4	5	5	4	5
2	1	0	3	4	5	4	3	5	4	5
3	5	0	3	5	5	5	5	5	4	5
4	5	0	1	5	0	5	3	0	0	5
5	5	0	1	3	0	4	3	0	0	5
6	5	0	4	5	3	5	3	5	4	5
7	1	3	5	5	5	3	5	4	4	5
8	1	5	5	5	5	4	4	4	4	5
9	1	1	5	5	5	3	4	5	4	5

Решение задачи

Начнем решение задачи по методу комплексного анализа иерархий.

Сравнение атрибутов. Сравним заданные атрибуты между собой, т.е. построим матрицу парных сравнений десяти анализируемых атрибутов. Матрица парных сравнений заполняется по шкале относительной важности Саати [13], которая приведена в табл. 4.

Таблица 4

Таблица интенсивности относительной важности

Интенсивность относительной важности	Определение
1	Равная важность
3	Умеренное превосходство
5	Существенное превосходство
7	Значительное превосходство
9	Очень сильное превосходство
2, 4, 6, 8	Промежуточные решения между соседними суждениями
Обратные величины	Обратные величины заполняются в соответствии со свойством обратной симметрии в матрице парных сравнений.

На основании табл. 4 и определения атрибутов [9] в соответствии с рекомендациями, данными в [10], авторами была составлена матрица парных сравнений (табл. 5).

Таблица 5

Авторская матрица парных сравнений анализируемых атрибутов

	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	G	q_i
K_1	1	0,33	3	3	3	5	5	1	1	3	1,98	0,16
K_2	3	1	3	1	0,33	5	5	1	3	1	1,78	0,14
K_3	0,33	0,33	1	0,33	0,33	3	5	0,33	0,33	0,33	0,61	0,05
K_4	0,33	1	3	1	1	5	5	1	3	1	1,54	0,13
K_5	0,33	3	3	1	1	5	5	1	3	1	1,72	0,14
K_6	0,20	0,20	0,33	0,20	0,20	1	5	0,20	0,33	0,14	0,36	0,03
K_7	0,14	0,14	0,20	0,20	0,14	0,14	1	0,20	0,33	0,20	0,22	0,02
K_8	1	1	3	1	1	5	5	1	3	1	1,72	0,14
K_9	1	0,33	3	0,33	0,33	3	3	0,33	1	0,33	0,80	0,07
K_{10}	0,33	1	3	1	1	5	5	1	3	1	1,59	0,13
Сумма											**12,32**	**1**

В табл. 5 использованы следующие обозначения: $K_1 \ldots K_{10}$ — номера атрибутов; G — среднее геометрическое n-й строки, являющееся оценкой компонента собственного вектора; q — нормализированная (к сумме G) оценка компонента собственного вектора.

Вычислим меру согласованности матрицы парных сравнений при помощи индекса согласованности (ИС):

$$\text{ИС} = \frac{\lambda_{max} - n}{n-1}, \quad (17)$$

где n — размер матрицы (в нашем случае $n = 10$); λ_{max} — максимальное собственное значение матрицы суждений.

Для определения адекватности оценки суждений вычислим отношение согласованности. Отношение согласованности (ОС) вычисляется как:

$$OC = h / ИС, \quad (18)$$

где h — индекс в таблице средних случайных индексов согласованности для матриц разного порядка [12] (табл. 6).

Таблица 6

Таблица средних случайных индексов согласованности для матриц разного порядка от 1 до 10

Размер матрицы	1	2	3	4	5	6	7	8	9	10
Случайная согласованность	0	0	0,58	0,90	1,12	1,24	1,32	1,41	1,45	1,49

ОС не должен превышать 10%, иначе суждения необходимо пересмотреть.

На основании вышеприведенных формул получим значения матрицы парных сравнений 5:

$\lambda_{max} = 11{,}19;$ ИС = 0,13; ОС = 0,09.

ОС не превышает 10 — 15%, что является адекватной величиной.

Преобразование экспертных оценок в относительные значения. Преобразуем экспертные оценки (см. табл. 3) в относительные значения. В соответствии с алгоритмом относительные значения (табл. 7) вычисляются построчно.

Таблица 7

Относительные значения экспертных оценок

СЗИ	Атрибуты									
	1	2	3	4	5	6	7	8	9	10
1	0,80	0	0,60	0,80	1	0,80	1	1	0,80	1
2	0,20	0	0,60	0,80	1	0,80	0,60	1	0,80	1
3	1	0	0,60	1	1	1	1	1	0,80	1
4	1	0	0,20	1	0	1	0,60	0	0	1
5	1	0	0,20	0,60	0	0,80	0,60	0	0	1
6	1	0	0,80	1	0,60	1	0,60	1	0,80	1
7	0,20	0,60	1	1	1	0,60	1	0,80	0,80	1
8	0,20	1	1	1	1	0,80	0,80	0,80	0,80	1
9	0,20	0,20	1	1	1	0,60	0,80	1	0,80	1

Выбор СЗИ на основании положений теории игр. Следующим шагом в данном подходе является выбор СЗИ на основании максимального обобщенного показателя и матрицы рисков.

Построим матрицу рисков. Для ее построения необходимо сформировать матрицу игры (табл. 8) на основании относительных значений в табл. 7.

Таблица 8

Матрица игры

Стратегии	СЗИ	Состояние природы K_j									
		1	2	3	4	5	6	7	8	9	10
	1	0,80	0	0,60	0,80	1	0,80	1	1	0,80	1
	2	0,20	0	0,60	0,80	1	0,80	0,60	1	0,80	1
	3	1	0	0,60	1	1	1	1	1	0,80	1
	4	1	0	0,20	1	0	1	0,60	0	0	1
	5	1	0	0,20	0,60	0	0,80	0,60	0	0	1
	6	1	0	0,80	1	0,60	1	0,60	1	0,80	1
	7	0,20	0,60	1	1	1	0,60	1	0,80	0,80	1
	8	0,20	1	1	1	1	0,80	0,80	0,80	0,80	1
	9	0,20	0,20	1	1	1	0,60	0,80	1	0,80	1
	β_i	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**0,80**	**1**

Численный показатель β вычисляется как:

$$\beta_j = \max(a_j), \quad (19)$$

где a — максимальное значение в столбце состояния природы K_j.

На основании матрицы игры построим матрицу рисков (табл. 9). Риск определим следующим выражением:

$$\Delta r_y = \beta_j - W_j \ . \quad (20)$$

Таблица 9

Матрица рисков

Стратегии	СЗИ	Состояние природы K_j										R_i
		1	2	3	4	5	6	7	8	9	10	
	1	0,20	1	0,40	0,20	0	0,20	0	0	0	0	0,2271
	2	0,80	1	0,40	0,20	0	0,20	0,40	0	0	0	0,33076
	3	0	1	0,40	0	0	0	0	0	0	0	**0,16405**
	4	0	1	0,80	0	1	0	0,40	1	0,80	0	0,52202
	5	0	1	0,80	0,40	1	0,20	0,40	1	0,80	0	0,57786
	6	0	1	0,20	0	0,40	0	0,40	0	0	0	0,21702
	7	0,80	0,40	0	0	0	0,40	0	0,20	0	0	0,2262
	8	0,80	0	0	0	0	0,20	0,20	0,20	0	0	0,16611
	9	0,80	0,80	0	0	0	0,40	0,20	0	0	0	0,25948
	q_i	0,16	0,14	0,05	0,13	0,14	0,03	0,02	0,14	0,07	0,13	

Выигрышной будет стратегия, обладающая *минимальным* риском. Риск рассчитывается как:

$$R_i = \sum_{j=1}^{n} r_{ij} q_j. \quad (21)$$

Минимальный риск (см. табл. 9) — $R_3 = 0{,}16$. Соответственно, на основании данной таблицы делается вывод о том, что СЗИ № 3 является лучшим решением из представленных девяти, так как риск при его выборе и эксплуатации минимален.

Построение матрицы обобщенных показателей. Матрица обобщенных показателей (табл. 10) формируется на основании значений табл. 7 и весов (q оценок компонентов собственных векторов). Обобщенный показатель W_i рассчитывается следующим образом:

$$W_i = \sum_{j=1}^{n} a_{ij} q_j. \quad (22)$$

Таблица 10

Таблица обобщенных показателей СЗИ

СЗИ	Атрибуты										Wi
	К1	К2	К3	К4	К5	К6	К7	К8	К9	К10	
1	0,80	0	0,60	0,80	1	0,8	1	1	0,8	1	0,759866
2	0,20	0	0,60	0,80	1	0,8	0,6	1	0,8	1	0,656203
3	1	0	0,60	1	1	1	1	1	0,8	1	0,822916
4	1	0	0,20	1	0	1	0,6	0	0	1	0,464942
5	1	0	0,20	0,60	0	0,8	0,6	0	0	1	0,409103
6	1	0	0,80	1	0,60	1	0,6	1	0,8	1	0,769947
7	0,2	0,6	1	1	1	0,6	1	0,8	0,8	1	0,76081
8	0,2	1	1	1	1	0,8	0,8	0,8	0,8	1	0,820858
9	0,2	0,2	1	1	1	0,6	0,8	1	0,8	1	0,727483
qi	0,16	0,14	0,05	0,13	0,14	0,03	0,02	0,14	0,07	0,13	

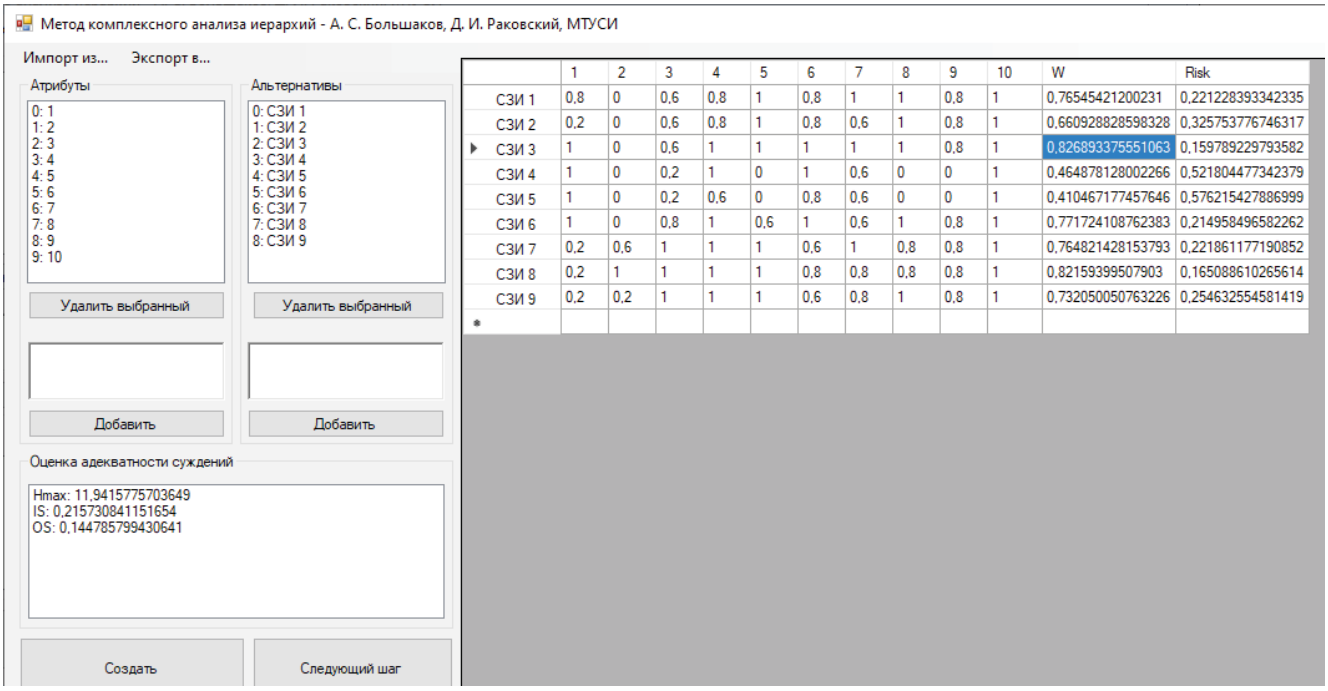

Рис. 2. Разработанное программное обеспечение, реализующее метод комплексного анализа иерархий

Необходимо выбрать максимальный обобщенный показатель — он будет соответствовать наилучшему СЗИ (по сумме оценок с учетом весов каждого атрибута).

Максимальный обобщенный показатель (см. табл. 10) — $W_3 = 0{,}823$. Соответственно, на основании данной таблицы делается вывод о том, что СЗИ № 3 является лучшим решением из представленных.

Решения, полученные на основании матрицы рисков и матрицы обобщенных показателей, совпали. Таким образом, пользователю будет рекомендовано приобретать и использовать СЗИ № 3.

Программное обеспечение

На основе выбранного метода с учетом контекста решаемой задачи (информационная безопасность) было разработано программное обеспечение для автоматизации принятия решений специалистами в области информационной безопасности (рис. 2). Данное программное обеспечение используется в лабораторном практикуме для студентов направления подготовки 11.04.02 — «Инфокоммуникационные технологии и системы связи» по магистерской программе «Безопасность и программная защита инфокоммуникаций».

Программное обеспечение реализовано на языке программирования C# с применением сторонней библиотеки *ClosedXML*[4] и реализует рассмотренный в работе подход. Внутри программного обеспечения сформирован базовый набор функций по работе с таблицами; присутствует возможность работы с *CSV*[5] и *Excel*-таблицами (в режиме импорта и экспорта). Пользователь имеет возможность экспортировать основные параметры построенных матриц парных сравнений (оценки адекватности суждений; значения рисков и обобщенных показателей по каждому СЗИ) в отдельный текстовый файл. Разработанное программное обеспечение имеет интуитивно понятный, дружественный к пользователю интерфейс.

[4] ClosedXML. URL: https://github.com/ClosedXML/ClosedXML.

[5] CSV (Comma-Separated Values) — текстовый формат, предназначенный для представления табличных данных.

Заключение

В работе проведен сравнительный теоретико-экспериментальный анализ методов принятия решений, включая: метод аналитических сетей; метод анализа иерархий; метод комплексного анализа иерархий; метод исключения и выбора, отражающего реальность; мультиатрибутный глобальный вывод качества. Проведенный анализ показал, что минимальным количеством операций парных сравнений обладают методы *Electre* и комплексного анализа иерархий.

Метод комплексного анализа иерархий, являющийся адаптированной версией метода анализа иерархий с применением элементов теории игр, имеет меньшее количество операций сравнения, которые зависят только от количества атрибутов, по которым сравниваются альтернативы. Следовательно, эффективным методом принятия решений с точки зрения минимизации операций парных сравнений можно признать *метод комплексного анализа иерархий*. Данный метод является наименее сложным (по количеству проводимых операций сравнения) и может быть использован при решении дискретных многокритериальных задач.

Литература

1. Большаков А. С., Раковский Д. И. Программное обеспечение моделирования угроз безопасности информации в информационных системах // Правовая информатика. 2020. № 1. С. 26—39. DOI: 10.21681/1994-1404-2020-1-26-39.
2. Большаков А. С., Рогатнева Е. А. Применение нечеткой логики для управления информационным риском // Тр. XIII Междунар. отраслевой науч.-техн. конф. (20—21 марта 2019 г.) / МТУСИ. М. : Изд. дом «Медиа паблишер», 2019. С. 331—335.
3. Дорошенко В. А., Друк Л. В., Герасимов А. Э. Математическое описание взаимовлияния технических средств распределенных по уровням систем управления с обратными связями // Лесной вестник. 2017. Т. 21. № 1. С. 118—124. DOI: 10.18698/2542-1468-2017-1-118-124.
4. Князев В. В., Ловцов Д. А. Ситуационное планирование защищённой переработки информации в АСУ испытаниями сложных динамических объектов // Автоматика и телемеханика. 1998. № 9. С. 166—181.
5. Кравченко Т. К., Дружаев А. А. Адаптация методов семейства Electre для включения в экспертную систему поддержки принятия решений // Бизнес-информатика. 2015. № 2(32). С. 69—78.
6. Кузнецов М. А., Нгуен Т. У. Н. Использование методов Electre в задачах принятия решения // Прикаспийский журнал: управление и высокие технологии. 2010. № 2. С. 40—46.
7. Лабинский А. Ю., Козлов А. А. Принятие решений с помощью метода аналитических сетей // Вестник Санкт-Петербургского университета государственной противопожарной службы МЧС РФ. 2018. № 4. С. 24—33.
8. Ловцов Д. А. Проблема информационной безопасности ГАС РФ «Правосудие» // Российское правосудие. 2012. № 5. С. 103—109.
9. Ломазов В. А, Прокушев Я. Е. Критерии выбора средств обеспечения информационной безопасности персональных данных // Международный научно-исследовательский журнал. 2016. № 11. С. 84—86. DOI: 10.18454/IRJ.2016.53.015.
10. Петриченко Г. С., Нарыжная Н. Ю., Крицкая Л. М. Методика выбора средств защиты для корпоративной сети // Научный журнал КубГАУ. 2016. № 121. С. 121—130. DOI: 10.21515/1990-4665-121-130.
11. Саати Т. Относительное измерение и его обобщение в принятии решений. Почему парные сравнения являются ключевыми в математике для измерения неосязаемых факторов // Cloud of science. 2016. № 2. С. 171—262.
12. Харитонов С. В., Улитина Е. В., Дик В. В. Применение метода анализа иерархий при согласовании результатов оценки // Прикладная информатика. 2012. № 6 (42). С. 108—113.

13. Яковличев А. Ю., Мильман И. Е., Пилюгин В. В. Использование визуализации при решении дискретных многокритериальных задач методами семейства Promethee // Научная визуализация. 2016. № 3. С. 78—94.
14. H. R. Weistroffer, Y. Li, "Multiple criteria decision analysis software", Ch. 29, in: S. Greco, M. Ehrgott, J. Figueira (eds), "Multiple Criteria Decision Analysis: State of the Art Surveys Series", Springer: New York, 2016.

Рецензент: ***Алексеев Владимир Витальевич,*** *доктор технических наук, профессор, член-корреспондент РАЕН, почетный радист РФ, заведующий кафедрой информационных систем и защиты информации Тамбовского государственного технического университета, Российская Федерация, г. Тамбов.*
E-mail: vvalex1961@mail.ru

AN EFFICIENT MULTIPLE-CRITERIA DECISION ANALYSIS METHOD IN THE FIELD OF INFORMATION SECURITY

Aleksandr Bol'shakov, *Ph.D. (Technology), Associate Professor at the Moscow Technical University of Communication and Informatics, Moscow, Russian Federation.*
E-mail: *alexbol57@mail.ru*

Dmitrii Rakovskii, *master's student of the Moscow Technical University of Communication and Informatics, Moscow, Russian Federation.*
E-mail: *dimitor1998@mail.ru*

Keywords: *information security, information protection, decision theory, decision-making methods, complex analytic hierarchy process method, discrete multiple-criteria problems, decision making automation, software.*

Abstract.
Purpose of work: *improving the methodological and legal basis for making decisions aimed at ensuring information security.*
Method of study: *comparative analysis of existing decision-making methods according to two criteria: number of comparison operations and number of matrices of paired comparisons.*
Results obtained: *a number of decision-making methods were considered among which the most efficient one in the context of the problem at hand was selected, i. e. the method ensuring the minimum number of pairwise comparison operations. The analysis given showed that the complex analytic hierarchy process method is the one possessing this property. This method has the least complexity (in terms of the number of comparison operations performed) and can be used for solving discrete multiple-criteria problems. The use of the chosen method is demonstrated by the authors using the case of selecting an information protection tool. Based on the chosen method and considering the context of the problem at hand, software for automated selection of the best information protection tool has been developed which is used in the teaching process in the form of a laboratory practicum for students whose field of study is "Information & Communications Technology and Communication Systems".*

References

1. Bol'shakov A. S., Rakovskii D. I. Programmnoe obespechenie modelirovaniia ugroz bezopasnosti informatsii v informatsionnykh sistemakh. Pravovaia informatika, 2020, No. 1, pp. 26-39. DOI: 10.21681/1994-1404-2020-1-26-39.
2. Bol'shakov A. S., Rogatneva E. A. Primenenie nechetkoi logiki dlia upravleniia informatsionnym riskom. Tr. XIII Mezhdunar. otraslevoi nauch.-tekhn. konf. (20-21 marta 2019 g.) / MTUSI. M. : Izd. dom "Media pablisher", 2019, pp. 331-335.
3. Doroshenko V. A., Druk L. V., Gerasimov A. E. Matematicheskoe opisanie vzaimovliianiia tekhnicheskikh sredstv raspredelennykh po urovniam sistem upravleniia s obratnymi sviaziami. Lesnoi vestnik, 2017, t. 21, No. 1, pp. 118-124. DOI: 10.18698/2542-1468-2017-1-118-124.
4. Kniazev V. V., Lovtsov D. A. Situatsionnoe planirovanie zashchishchennoi pererabotki informatsii v ASU ispytaniiami slozhnykh dinamicheskikh ob"ektov. Avtomatika i telemekhanika, 1998, No. 9, pp. 166-181.
5. Kravchenko T. K., Druzhaev A. A. Adaptatsiia metodov semeistva Electre dlia vkliucheniia v ekspertnuiu sistemu podderzhki priniatiia reshenii. Biznes-informatika, 2015, No. 2(32), pp. 69-78.
6. Kuznetsov M. A., Nguen T. U. N. Ispol'zovanie metodov Electre v zadachakh priniatiia resheniia. Prikaspiiskii zhurnal: upravlenie i vysokie tekhnologii, 2010, No. 2, pp. 40-46.

7. Labinskii A. Iu., Kozlov A. A. Priniatie reshenii s pomoshch'iu metoda analiticheskikh setei. Vestnik Sankt-Peterburgskogo universiteta gosudarstvennoi protivopozharnoi sluzhby MChS RF, 2018, No. 4, pp. 24-33.
8. Lovtsov D. A. Problema informatsionnoi bezopasnosti GAS RF "Pravosudie". Rossiiskoe pravosudie, 2012, No. 5, pp. 103-109.
9. Lomazov V. A, Prokushev Ia. E. Kriterii vybora sredstv obespecheniia informatsionnoi bezopasnosti personal'nykh dannykh. Mezhdunarodnyi nauchno-issledovatel'skii zhurnal, 2016, No. 11, pp. 84-86. DOI: 10.18454/IRJ.2016.53.015.
10. Petrichenko G. S., Naryzhnaia N. Iu., Kritskaia L. M. Metodika vybora sredstv zashchity dlia korporativnoi seti. Nauchnyi zhurnal KubGAU, 2016, No. 121, pp. 121-130. DOI: 10.21515/1990-4665-121-130.
11. Saati T. Otnositel'noe izmerenie i ego obobshchenie v priniatii reshenii. Pochemu parnye sravneniia iavliaiutsia kliuchevymi v matematike dlia izmereniia neosiazaemykh faktorov. Cloud of science, 2016, No. 2, pp. 171-262.
12. Kharitonov S. V., Ulitina E. V., Dik V. V. Primenenie metoda analiza ierarkhii pri soglasovanii rezul'tatov otsenki. Prikladnaia informatika, 2012, No. 6 (42), pp. 108-113.
13. Iakovlichev A. Iu., Mil'man I. E., Piliugin V. V. Ispol'zovanie vizualizatsii pri reshenii diskretnykh mnogokriterial'nykh zadach metodami semeistva Promethee. Nauchnaia vizualizatsiia, 2016, No. 3, pp. 78-94.
14. H. R. Weistroffer, Y. Li, "Multiple criteria decision analysis software", Ch. 29, in: S. Greco, M. Ehrgott, J. Figueira (eds), "Multiple Criteria Decision Analysis: State of the Art Surveys Series", Springer: New York, 2016.