Надежность, том 25, №4, 2025 / Dependability 4, 2025
Методы и системы защиты информации.
Информационная безопасность

УДК 519.81:004.056:007.51
Оригинальная статья
https://doi.org/10.21683/1729-2646-2025-25-4-52-60

Применимость метода ELECTRE I при многокритериальном выборе страхуемых автоматизированных систем и приоритете киберзащищенности и критерий трехзначной мажоритарной логики

The applicability of ELECTRE I as part of multi-criteria selection of insurable automated systems and the priority of cyber security and the criterion of three-valued majority logic

Шептунов М.В.
Sheptunov M.V.

Московский Государственный лингвистический университет (ФГБОУ ВО «МГЛУ»),
Московский Гуманитарный университет (АНО ВО «МосГУ»), Москва, Российская Федерация
Moscow State Linguistic University,
Moscow University for the Humanities, Moscow, Russia
triumf403@yandex.ru

Шептунов М.В.

Резюме. Цель. *Выяснить и показать применимость подхода разработки индексов попарного сравнения альтернатив (РИПСА) на примере одного из методов ELECTRE – для выбора автоматизированных информационных систем (АИС) с учетом критериев, относящихся к киберзащищенности АИС и страхованию киберрисков.* **Методы.** *Из группы методов ELECTRE в качестве ее представителя в статье использован метод ELECTRE I, подробно изложенный в известных книгах. Данная группа методов относится к подходу РИПСА, одним из отечественных первопроходцев которого, направленного на сопоставление многокритериальных альтернатив, был акад. РАН Ларичев О.И. В целях вводимого критерия, названного «трехзначный мажоритарный критерий киберзащищенности АИС с учетом страхования» применены элементы трехзначной мажоритарной логики.* **Результаты.** *Показана применимость подхода РИПСА в виде метода ELECTRE I для выбора АИС в ракурсе рассмотренных критериев, относящихся к киберзащищенности АИС, с учетом страхования киберрисков. Разработан модифицированный, новый в плане киберзащищенности при страховании киберрисков критерий, основанный на трехзначной мажоритарной логике – а именно позволивший выразить и учесть в логико-математическом виде: некоторые особенности страховой защиты АИС в связи с присущими им киберрисками, а также способность АИС противостоять собственными средствами классифицируемым по трем категориям кибератакам на подобные организационно-технические системы.* **Выводы.** *Критерий качества технико-экономического характера на основе трехзначной мажоритарной логики может использоваться не только в ракурсе технических и организационно-технических параметров либо характеристик киберзащищенности АИС, но и в ракурсе финансово-экономических параметров либо характеристик защищенности страхуемых АИС. Методы группы ELECTRE подхода разработки индексов попарного сравнения альтернатив применимы: как в ракурсе анализа и организационно-технических мер по снижению различных связанных с АИС киберрисков, так и в ракурсе страховой защиты от них. Как показано в статье, возможно обойтись в методах ELECTRE на две единицы меньшим количеством критериев за счет разработанного интегрального критерия, а именно трехзначной мажоритарной логики для многокритериальных альтернатив.*

Abstract. Aim. *To use the case of one of the ELECTRE methods to identify and demonstrate the applicability of the development of indexes for pairwise comparison of alternatives (RIPSA) for selecting automated information systems (AIS) taking into account criteria associated with AIS cybersecurity and cyber risk insurance.* **Methods.** *The paper uses the ELECTRE I method that is well-described in well-known publications. The ELECTRE group of methods belongs to the RIPSA approach that aims to compare multi-criteria alternatives. One of the Russian pioneers of this approach was the RAS member Larichev O.I. The introduced criterion called the "three-digit majority criterion of AIS cybersecurity taking into account insurance" uses elements of three-digit majority logic.* **Results.** *The paper shows the applicability of the RIPSA approach, ELECTRE I specifically, for selecting AIS as regards the examined criteria associated with AIS cybersecurity, taking into account cyber risk insurance. A modified criterion has been developed that is new as regards cyber security in the context of cyber liability insurance*

and is based on a three-digit majority logic. Specifically, it allows expressing and taking into account in a logical and mathematical form some features of AIS insurance protection given the inherent cyber risks, as well as the ability of AIS to independently withstand the three categories of cyber attacks. **Conclusion.** *The three-digit majority logic-based technical and economic quality criterion is applicable to not only technological and organisational parameters or characteristics of AIS cyber security, but the financial and economic parameters or security characteristics of insured AIS as well. The ELECTRE methods of developing pairwise alternative comparison indexes are applicable both in the analysis, organisational and technological measures to reduce various AIS-related cyber risks, and in associated insurance protection. The paper shows that the developed integral criterion, namely the three-digit majority logic for multi-criteria alternatives, allows using the ELECTRE methods with two criteria less.*

Ключевые слова: *принятие решений, сравнение альтернатив, управление доступом, показатель, многокритериальный выбор, франшиза, перестрахование.*
Keywords: *decision-making, comparison of alternatives, access control, indicator, multi-criteria choice, franchise, reinsurance.*

Для цитирования: *Шептунов М.В. Применимость метода ELECTRE I при многокритериальном выборе страхуемых автоматизированных систем и приоритете киберзащищенности и критерий трехзначной мажоритарной логики // Надежность. 2025. №4. С. 52-60. https://doi.org/10.21683/1729-2646-2025-25-4-52-60*
For citation: *Sheptunov M.V. The applicability of ELECTRE I as part of multi-criteria selection of insurable automated systems and the priority of cyber security and the criterion of three-valued majority logic. Dependability 2025;4: 52-60. https://doi.org/10.21683/1729-2646-2025-25-4-52-60*

Поступила: *16.05.2024* / **После доработки:** *25.05.2025* / **К печати:** *28.09.2025*
Received on: *16.05.2024* / **Revised on:** *25.05.2025* / **For printing:** *28.09.2025*

Введение

В настоящее время весьма актуален именно многокритериальный выбор автоматизированных информационных систем (АИС) гражданского назначения в ракурсе их киберзащищенности со страхованием киберрисков. Критерии для таких АИС нередко разнонаправлены, противоречивы и вполне могут представлять самостоятельный интерес. Все больший интерес вызывают и смежные вопросы о страховании киберрисков, для которых вследствие практической невозможности абсолютной комплексной защиты систем (даже при больших финансовых вложениях) – в условиях расширяющегося спектра киберугроз и из-за растущих возможностей компьютерных сетей – следует предусматривать страхование. Сказанное актуально для каждого предприятия – объекта экономики и одновременно информатизации, стремящегося защитить свои АИС и соответствующие электронные ресурсы.

Этим обусловлена уместность использования для ставящейся здесь проблемы данной теоретико-прикладной сферы т.н. (в основном в российской научной и образовательной литературе) подхода РИПСА (разработки индексов попарного сравнения альтернатив), направленного на сопоставление многокритериальных альтернатив. В СССР и РФ одним из первопроходцев этой проблематики был акад. РАН Ларичев О.И. [1]. Однако в переводе с французского заложенные профессором Руа Б. [2] методы группы ELECTRE (Elimination Et Choix Traduisantla Realite), относящиеся к упомянутому подходу, фигурируют как «исключение и выбор, отражающие реальность», однако нередко и как «исключение и выбор в условиях реальности».

Реальность такова, что для АИС, их выбора зачастую не только критериев более 2-х–3-х, но и альтернатив для ЛПР (лиц, принимающих решения) нередко не меньше трех или даже больше. Тем более, принимая в расчет страхование киберрисков, нуждающееся в предпочтительнее специализированном, обособленном критерии (и в то же время системно связанном с другими имеющимися и разработанными критериями для АИС, наиболее приоритетными здесь в ракурсе киберзащищенности). Среди таковых может быть, например (*в качестве лишь одного из множества возможных примеров для АИС в гражданской сфере*) [3]: среднее время проникновения нарушителя в автоматизированную систему защищенной обработки информации (далее АСЗОИ).

Известно, например, из [4], что при выборе между дорогостоящими проектами заказчику следует проводить собственные оценки технологий, обращаться к экспертам для осуществления независимого анализа проектов – сказанное относится и к проектируемым и модернизируемым АИС. Тем более, к альтернативам пока еще не апробированных технологий безопасности, предполагающих возможность доработки благодаря техническим решениям в процессе модификаций.

Исходя из известных книг[1], видятся вполне возможными для применения и такие критерии (показатели), здесь именно в рамках подхода РИПСА, причем по своей сущности относящиеся к киберзащищенности:

[1] Как, например: Хетагуров Я.А. Проектирование автоматизированных систем обработки информации и управления (АСОИУ): учебник. Москва: БИНОМ. Лаборатория знаний; 2015. 240 с.

I) коэффициент защиты системы обработки информации с N каналами

$$K_{\text{I}} \equiv K_{\text{з}} = \sum_{i=1}^{N_{\text{з}}} \frac{K_{\text{з}i}}{N}, \quad (1)$$

где $N_{\text{з}}$ – количество охваченных защитой каналов системы;

II) показатель сложности защиты системы

$$K_{\text{II}} \equiv \tilde{R} = \frac{\Delta R}{R} = \frac{\left[(R+\Delta R)-R\right]}{R}, \quad (2)$$

характеризующий относительные затраты дополнительных ресурсов ΔR на защиту основных ресурсов R (причем годовые эксплуатационные расходы из-за введения защиты увеличиваются не более чем на 13–60%);

III) величина остаточного (коммерчески ценного информационного) ресурса через время t при сокращении его хищения в процессе защиты

$$K_{\text{III}} \equiv S_{tx} = S_0(1+r)^t - (S_x - S_y)(1+r)^t = \\ = S_0(1+r)^t - \left(S_x - \frac{a_1 y_c}{1+b_1 y_c}\right)(1+r)^t, \quad (3)$$

где S_0 – величина (стоимость) исходного ресурса;

r – процентная банковская ставка;

t – анализируемый интервал времени;

S_x – величина похищенного ресурса;

$S_y = \frac{a_1 y_c}{1+b_1 y_c}$ – величина сокращения хищения, определяемая затратами y_c на средства защиты (обычно в виде подсистемы защиты);

$(S_x – S_y)$ – разность между величиной похищенного ресурса и величиной сокращения хищения;

a_1, b_1 – коэффициенты, определяемые методом экспертных оценок либо из выражений

$$a_1 = \frac{S_{y1}S_{y2}(y_{c1}-y_{c2})}{y_{c1}y_{c2}(S_{y1}-S_{y2})},\ b_1 = \frac{S_{y2}y_{c1}-S_{y1}y_{c2}}{y_{c1}y_{c2}(S_{y1}-S_{y2})},$$

вытекающих из уравнений для двух близких – к входящим во множество альтернатив – вариантов АИС, у которых определены соответствующие воздействия S_y и y_c:

$$S_{y1} = \frac{a_1 y_{c1}}{1+b_1 y_{c1}},\ S_{y2} = \frac{a_1 y_{c2}}{1+b_1 y_{c2}}.$$

Здесь и далее в статье под *киберзащищенностью* будем понимать, по аналогии, например, с [5], способность АИС успешно выполнять предусмотренные задачи при сохранении безопасного состояния в условиях кибератак, направленных на нанесение ущерба критически важным или потенциально опасным объектам, или объектам, представляющим повышенную опасность для жизни и здоровья граждан, имущества физических или юридических лиц, экономики, окружающей среды. Причем полагая, что первая зависит как от возможностей несанкционированного доступа к системе (НСД) вероятного нарушителя, так и от недекларированных возможностей (НДВ) программных и аппаратных средств АИС.

Разумеется, не только вышеуказанные критерии (1) и (2) могут быть использованы (и, как предполагается, определены наряду с их значениями и их весов, в т.ч., методом экспертных оценок) – в нашем случае в ракурсе подхода РИПСА, методов ELECTRE. Не считая страховой защиты АИС, не исключено, что можно было бы ограничиться иногда и этими двумя. Учитывая, что они достаточно универсальны в плане киберзащищённости АИС и информации (как хранящейся в АИС, так и обрабатываемой с их помощью) – что видится из известных книг – однако и ряд других реалистично и уместно использовать с вышеприведённым набором критериев в целях: настоящей статьи и большей объективности выбора. Далее ввиду того, что область их применения далеко не ограничивается каким-либо одним направлением, а подходит к выбору самых различных АИС в упомянутом разрезе, дополним (1), (2) и (3) таковыми:

IV) среднее время проникновения нарушителя в АИС $K_{\text{IV}} \equiv \bar{t}_{\text{пр}}$;

V) стоимость создания или модернизации подсистемы защиты информации $K_{\text{V}} \equiv S$.

Кроме того, при выборе АИС должен учитываться и функционал системы. Поэтому дополним предыдущие 5 критериев I) – V) еще и таким:

VI) интегральный показатель (функциональной) эффективности АИС

$$K_{\text{VI}} \equiv A = \sum_{i=1}^{N} A_i = \sum_{i=1}^{N} \frac{V_i}{T_i} = \sum_{i=1}^{N} \frac{\left(\sum_{j=1}^{m}\theta_j + \sum_{k=1}^{\xi}\delta_k\right)_i}{\left(\sum_{k=1}^{\xi} t_k - \sum_{j=1}^{m}\tau_j\right)_i}, \quad (4)$$

где V_i – суммарный объем информации, подготовленный i-м блоком АИС за определенный период времени и представленный в каких-либо универсальных единицах измерения информации;

T_i – интервал времени, характеризующий длительность подготовки i-м блоком АИС суммарного объема информации;

N – число блоков АИС, задействованных в реализуемом в АИС информационном процессе;

θ_j – объем информации, поступившей на i-й блок АИС от j-го источника информации;

m – число источников информации;

δ_k – случайного либо неслучайного характера объем выданной информации i-м блоком АИС на информационную шину, удовлетворяющей требованию k;

ξ – общее число требований k;

t_k – момент времени, соответствующий выдаче подготовленной информации (отвечающей требованию k) i-м блоком на информационную шину АИС;

τ_j – момент времени, соответствующий поступлению информации на i-й блок АИС от j-го источника информации,

причем на знаменатель формулы (4) накладывается ограничение в виде

$$T_i = \left(\sum_{k=1}^{\xi} t_k - \sum_{j=1}^{m}\tau_j\right) \le T_{0i} \quad (5)$$

на длительность каждого T_i по отношению к его предельно допустимому верхнему значению T_{0i}.

Примечание. Величина δ_k способна иметь случайный характер вследствие того, что часть поступившей информации может не удовлетворять отдельному требованию k среди ξ таких требований.

Добавление интегрального показателя V) – критерия (4)–(5) – сообразно еще и потому, что, в т.ч., от функциональной конкретной структуры зависит (функциональная) эффективность АИС. Данный показатель был предложен в статье [6], причем – как в ней утверждается – в качестве универсального показателя для оценки технико-эксплуатационных, технологических, прагматических, экономических и др. качеств АИС. Этот интегральный показатель эффективности A, как отмечается в [6], является функциональной характеристикой, которую можно повышать, совершенствуя техническую базу АИС и используя труд квалифицированных сотрудников. Приведенный показатель – указывающий и на то, что обесценение информации суть равнозначный результат недостаточно полного ее объема и ее запаздывания – отображает в равной мере временные и количественные (в разрезе количественных мер информации) факторы. Несмотря на невозможность учесть и этим одним показателем изменяющиеся (в самом процессе принятия решений) предпочтения ЛПР, как и все проблемы киберзащищенности, отметим следующее. При наличии в той или иной альтернативной АИС, например, всего N=6 функциональных блоков (подсистем) – отбора информации, преобразования информации, передачи информации, обработки информации, хранения информации, поиска информации – такого рода перечень структурных элементов системы является открытым. Он во многом зависит от круга задач, стоящих перед АИС и вполне способен повлечь изменение ее конфигурации и состава – в т.ч., при необходимости ее модернизации.

Практически значимы и затраты времени проникновения нарушителя в системы – пусть хотя бы в среднем, и затраты в абсолютном стоимостном выражении не только на создание, но и модернизацию соответствующей подсистемы АИС. Тем не менее, поскольку ни одна даже очень дорогостоящая АИС, АСОИУ (автоматизированная система обработки информации и управления), АСЗОИ не дает гарантии полной абсолютной защиты от НСД и НДВ – влекущих киберугрозы и кибератаки, в дополнение к организационно-техническим, программным и/или т.п. имеющимся мерам защиты следует учесть и страховую защиту.

Имеет смысл принять во внимание и следующее: например, из [4] известно, что для одинакового ущерба простой технической системе достаточно нанести меньше вреда, чем интеллектуальной – в силу наличия у последней запаса безопасности.

Страховая защита должна служить для АИС вспомогательным, но немаловажным рубежом, когда предшествующие уже пройдены нарушителем. Этот уровень защиты нередко игнорируется, что лишь отчасти связано с не очень большой распространенностью страхования подобных рисков. Хотя даже при наличии т.н. франшизы (как вариант, условной, т.е. когда по условиям страхового договора предусмотрено освобождение страховой компании от возмещения ее клиенту убытков, не превышающих определенного размера [7]), пренебрегать им вряд ли следует, полагаясь на идеальность прочих видов защиты.

Как справедливо отмечается в [8], сложность оценки количественных преимуществ киберстрахования может усугубляться: во-первых, широко распространенным отсутствием понимания того, какие события может покрывать киберстрахование и – как следствие – ошибочным мнением, что прочие виды страхования покроют убытки от киберинцидента; во-вторых – тем, что для многих юридических лиц характерна неосознанность того, насколько они уязвимы для кибератак, приводящая к принципиально неверному организационно-управленческому и т.п. решению о ненужности для них киберстрахования.

Чаще всего объектами киберстрахования по корпоративным программам, как известно, например, из [9], являются имущественные интересы клиента. Они могут быть связаны с такими рисками, как: наступления ответственности за причинение ущерба имуществу физических и (или) юридических лиц; несения непредвиденных расходов; наступления убытков от перерывов в производстве. В то время как отдельная страховка рисков кибератак в РФ является более редкой. Известные российские страховщики, в т.ч., этой разновидности: «АльфаСтрахование», «СбербанкСтрахование», «Согаз», «Альянс» и др. Для базовой программы страхования характерны охватываемые ею риски: утраты и искажения информации и обрабатывающего ее ПО, нарушения конфиденциальности, целостности и (или) доступности персональных данных, расследования и диагностики кибератак, хищения интеллектуальной собственности, вымогательства, ущерба деловой репутации и т.д.

Например, автор [10] выделяет как в отдельную группу риски, связанные с: реагированием на киберинциденты, ликвидацией последствий, финансовыми и иными расследованиями, аудитом безопасности и судебным урегулированием.

В любом случае, как отмечается, например, в [11], для большинства страховщиков киберрисков важнейшую роль играет сетевая компьютерная безопасность. Что вполне естественно, учитывая, что с бурным развитием вычислительных сетей существенно повышаются и шансы успешных кибератак через них.

Следует отметить, что стоимость программы страхования зависит не только от количества и набора покрываемых рисков, величин страхового покрытия и франшизы (при ее наличии), но и сфер(ы) деятельности клиента и др. факторов. Например [12], европейскими страховщиками принимаются во внимание при киберстраховании:

а) стоимость объекта страховой защиты (и чем она выше, тем страховая ставка ниже);

б) наличие средств (подсистемы) защиты информации, в т.ч., антивирусных программ (и чем более положительно себя зарекомендовали используемые средства

и подсистема защиты информации и чем большей они стойкости к атакам, тем ниже страховой тариф);

в) количество атак на страхователя, а также на др. компании той же либо схожей отрасли за тот же значимый период.

Для учета также страховой защиты видится уместным дополнительный разносторонний критерий, который, впрочем, может несложным и даже интуитивно понятным образом строиться на основе трехзначной мажоритарной логики – в ракурсе как нефинансовых особенностей, вариантов систем, так и финансовых, вводимых в следующем п. 1 операцией (6).

Однако даже в случае, если учитывать величины страховых взносов в самом критерии (показателе) I) в составе его величины ΔR, имело бы смысл такие нюансы, как наличие франшизы, наличие перестрахования (особенно для крупных информационных рисков больших, распределенных АИС) и т.п. учесть обособленным критерием (показателем).

Кроме того, отнюдь не следует «сбрасывать со счетов» и то обстоятельство, что процесс принятия решения (хотя и необязательно) одним ЛПР – пусть и в присутствии консультанта, усложняется и/или замедляется из-за изменений предпочтений ЛПР в самом процессе принятия решения. Эти изменения часто могут быть неоднократными, постепенными. Сказанным вновь подчеркнута уместность и востребованность в нашем случае именно методов группы ELECTRE: с учетом различных защитных мер и параметров при иных подходах весьма сложно в принципе принять решение в задачах многокритериального выбора АИС. В то время как проблемные вопросы, связанные с ацикличностью отношений между альтернативами – в случае появления такого цикла, включающего последние – как известно из [1] – несложным образом решаются при объявлении входящих в цикл альтернатив эквивалентными.

Цель исследования: выяснить и показать применимость подхода РИПСА на примере одного из методов ELECTRE – для выбора автоматизированных информационных систем при полагаемых приоритетными критериях, относящихся к киберзащищенности АИС с учетом страхования киберрисков.

Задачи исследования:

- выяснить и показать возможность применения метода ELECTRE I как одного из способов обоснования выбора наиболее защищенных АИС с учетом страхования киберрисков;

- разработать и/или модифицировать критерий, основанный на трехзначной мажоритарной логике, позволяющий выразить (учесть) в логико-математическом виде те или иные – хотя бы некоторые либо основные – особенности страховой защиты АИС в связи с присущими им киберрисками, а также способность АИС противостоять собственными средствами тем или иным кибератакам на подобные системы;

- посредством решения предыдущих задач исследования выяснить и показать более широкую применимость критерия (критериальной базы) на основе трехзначной мажоритарной логики, чем: а) только в ракурсе технических и/или организационно-технических параметров либо характеристик киберзащищенности АИС и б) только в ракурсе финансово-экономических или финансовых параметров либо характеристик киберзащищенности страхуемых АИС.

1. Методы

Вполне подходящим из известной и вышеупомянутой группы методов ELECTRE является метод ELECTRE I, подробно изложенный в известных книгах[1]. С учетом вышесказанного во Введении, опишем его на примере (с достаточной степенью детализации для решения поставленных задач), как и упомянутые для этого критерии. Прежде проясним формирование и смысловые особенности обоих логико-математических критериев а), б), указанных во Введении.

Как известно из [13–14], может быть построен трехстабильный мажоритарный элемент с 3 входами и одним выходом, причем при значениях входных сигналов –1, 0 или 1 выходной сигнал такого элемента принимает одно из 3-х вышеуказанных значений -1, 0 или 1 в зависимости от алгебраической суммы входных сигналов. Имея выходным сигналом y, а входными x_1, x_2, x_3, получаем трехместную операцию (3-значную мажоритарную функцию):

$$y = sign_3\left(x_1 + x_2 + x_3\right) = \begin{cases} 1, \ если \ \ x_1 + x_2 + x_3 \geq 1, \\ 0, \ если \ \ x_1 + x_2 + x_3 = 0, \\ -1, если \ x_1 + x_2 + x_3 \leq -1. \end{cases} \quad (6)$$

Назовем обозначаемый через y логико-математический критерий VII) на основе операции (6), добавляемый к I)–VI): «*трехзначный мажоритарный критерий киберзащищенности АИС с учетом страхования*». Тогда пусть его смысловыми составляющими будут следующие, соответственно обозначенные: x_1=1 – «противостояние АИС всем известным кибератакам и киберугрозам»; x_1=0 – «противостояние АИС получившим известность кибератакам и киберугрозам, представляющим существенную опасность»; x_1=–1 – «противостояние АИС только самым известным кибератакам и киберугрозам»; x_2=1 – «сильная способность АИС самообучения при кибератаках»; x_2=0 – «слабая способность АИС самообучения при кибератаках»; x_2=–1 – «нет способности АИС самообучения при кибератаках»; x_3=1 – «нет франшизы при наличии перестрахования»; x_3=0 – «есть франшиза и/или нет перестрахования»; x_3=–1 – «страхования нет вовсе».

Естественно, что страховые компании обычно не страхуют риски, включая и такие, как киберриски, связанные с весьма вероятными или почти достовер-

[1] Как, например: Ларичев О.И. Теория и методы принятия решений, а также Хроника событий в Волшебных странах: Учебник (Гриф Министерства образования РФ). Изд. третье, перераб. и доп. Москва: Университетская книга, Логос; 2006. 392 с.

ными страховыми событиями – что и было принято здесь во внимание в ракурсе интегрального критерия *y* трехзначной мажоритарной логики. Т.е. позволившего (быть может, несколько своеобразно) объединить в рамках такового практически неизбежно соотносящиеся между собой показатели x_1, x_2, x_3, как и их значения. Тем более, т.к. видится важным учитывать нынешнюю распространенность искусственного интеллекта (ИИ) с самообучением систем. Здесь, например, значения x_2=1 и x_2=0 символизируют и характеризуют наличие соответственно «сильного» и «слабого» ИИ у более сложных «интеллектуальных» АИС, что может проявляться при защите от кибератак; нижнее значение x_2=–1 соответствует наиболее простым АИС вообще без ИИ.

Что же касается франшизы, которая, как ясно, например, из [6], может быть как безусловной, так и условной, то она не во всем выгодна клиенту-страхователю. Это связано с тем, что при безусловной франшизе при наступлении страхового случая страховое возмещение будет меньше, а при условной франшизе при малых ущербах (до определенного в договоре порогового уровня) у страховых компаний обычно нет обязательств по его выплате.

Относительно перестрахования рисков отметим, что оно – как видно, например, из [7] и [15] тем более актуально – и соответственно имеет место при тем большем количестве перестрахователей и перестраховщиков для повышения уровня страховых гарантий, чем более крупные риски страхуются прямым страховщиком (т.е. непосредственно связанной договором с клиентом страховой компанией). Ныне не вызывает сомнений важность обеспечения стабильной страховой защиты, которая для киберрисков при их страховании влечет если не обязательность, то предпочтительность перестрахования хотя бы одним перестраховщиком (по сравнению с его отсутствием).

На рис. 1 указан граф процесса многокритериального выбора АИС на основе метода ELECTRE I в достаточно общем случае с учетом, в т.ч., киберзащищенности и страхования, охватывающий и частный случай данного примера. Причем вершины (этапы, подпроцессы) с номерами 1–11 на этом графе означают следующее:

1 – формирование множества всего *N* критериев многокритериального выбора АИС, учитывающих, в т.ч., киберзащищенность и страхование АИС при использовании критерия на основе 3х-значной мажоритарной логики;

2 – формирование множества альтернатив для выбора наилучшей АИС;

3 – назначение весов критериям либо консультантом-экспертом, либо опросом нескольких экспертов, либо по числу голосов членов экспертного жюри, поданного за важность каждого критерия;

4 – разбиение множества критериев на 3 подмножества:

I^+ – подмножество критериев, по которым альтернатива A_i предпочтительнее, чем A_j;

$I^=$ – подмножество критериев, по которым альтернативы A_i и A_j равноценны;

I^- – подмножество критериев, по которым альтернатива A_j предпочтительнее, чем A_i;

5 – подсчет индексов согласия $C_{A_iA_j}$ о превосходстве гипотезы A_i над A_j;

6 – подсчет индексов несогласия $d_{A_iA_j}$ о превосходстве гипотезы A_i над A_j;

7 – задание уровней (коэффициентов) согласия α_q ЛПР с участием консультанта (где $q \geq 1$ – номер действующего уровня (коэффициента) по его хронологическому порядку);

8 – задание уровней (коэффициентов) несогласия γ_q ЛПР с участием консультанта (где $q \geq 1$ – номер действующего уровня (коэффициента) по его хронологическому порядку);

9 – проверка выполнения нестрогого неравенства для каждого из индексов согласия $C_{A_iA_j}$ по отношению к заданному уровню (коэффициенту) согласия α_q, т.е. $C_{A_iA_j} \geq \alpha_q$;

10 – проверка выполнения нестрогого неравенства для каждого из индексов несогласия $d_{A_iA_j}$ по отношению к заданному уровню (коэффициенту) несогласия γ_q, т.е. $d_{A_iA_j} \leq \gamma_q$;

11 – выбор наилучшей альтернативы (АИС) при соблюдении предъявляемых условий.

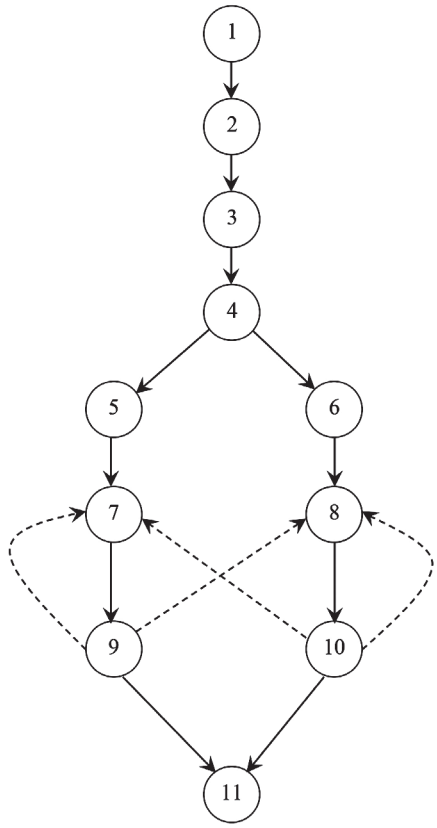

Рис. 1. Граф процесса многокритериального выбора АИС на основе метода ELECTRE I с учетом, в т.ч., киберзащищённости и страхования

Примечание. При успешном отыскании наилучшей альтернативы (АИС) указанные на рис. пунктиром переходы выполнять необязательно, хотя возможно в исследовательских, аналитических и т.п. целях.

Пример. Пусть дана группа из n=3 альтернатив A_i и N = 5 критериев, предназначенных для оценки этих A_i. При этом каждая из A_i характеризуется оценкой по каждому из 5-ти критериев, полученной от экспертов. Требуется в процессе выбора одной из АИС (A, B, D): выделить лучшую альтернативу A_i, построив для этого (на основе принципов конкорданса и дискорданса) один либо более таких индексов попарного сравнения альтернатив, что им отводится роль решающих правил.

Допустим, что альтернативы таковы: A(0,9; 0,15; 50 тыс.евро; 2 мес.; 3 тыс.евро; 90 Мбайт/час; –1); B(1; 0,3; 97 тыс.евро; 4 мес.; 5 тыс.евро; 450 Мбайт/час; 0); D(0,8; 0,4; 65 тыс.евро; 3 мес.; 4 тыс.евро; 120 Мбайт/час; +1), а (тоже экспертно оцененные) веса критериев соответственно: w_1=7, w_2=6, w_3=5, w_4=4, w_5=3, w_6=2, w_7=1, разброс оценок по критериям исчерпывается данными в табл. 1.

Табл.1. Разброс оценок вариантов АИС

Обозначения критериев	Наихудшее значение критерия	Наилучшее значение критерия
$K_{\text{I}} \equiv K_{\text{з}}$	0 (или 0 %)	1 (или 100 %)
$K_{\text{II}} \equiv \tilde{R}$	0,6 (или 60 %)	0 (или 0 %)
$K_{\text{III}} \equiv S_{\text{тх}}$	2 (тыс. евро)	98 (тыс. евро)
$K_{\text{IV}} \equiv \bar{t}_{\text{пр}}$	1 (мес.)	18 (мес.)
$K_{\text{V}} \equiv S$	6 (тыс. евро)	2 (тыс. евро)
$K_{\text{VI}} \equiv A$	80 (Мбайт/час)	560 (Мбайт/час)
$K_{\text{VII}} \equiv y$	-1	+1

Руководствуясь табл. 1, получаем такие длины шкал L_z (при $z = \overline{1,7}$):

L_1=1–0=1 или L_1=100–0=100 (%), L_2=0,6–0=0,6 или L_2=60–0=60 (%),

L_3=98–2=96 (тыс. евро), L_4=18–1=17 (мес.), L_5=6–3=3 (тыс. евро),

L_6=560–80=480 (Мбайт/час), L_7=1–(–1)=1+1=2.

Используя известные (общие для метода ELECTRE I) формулы, задействованные и в [3], определим сначала индексы согласия (конкорданса) – с гипотезой о превосходстве альтернативы A над альтернативой B и соответственно B над A. Т.к. A превосходит B по двум критериям K_{II} и K_{V}, в то время как B превосходит A по пяти K_{I}, K_{III}, K_{IV}, K_{VI} и K_{VII}, то получаем формулы примера:

$$C_{AB} = \frac{w_2 + w_5}{w_1 + w_2 + w_3 + w_4 + w_5 + w_6 + w_7},$$

$$C_{BA} = \frac{w_1 + w_3 + w_4 + w_6 + w_7}{w_1 + w_2 + w_3 + w_4 + w_5 + w_6 + w_7}.$$

Фигурирующие в тех же источниках (общие для метода ELECTREI) формулы позволяют определить соответствующие индексы несогласия (дискорданса), причем обычно для всех индексов: $0 \le C_{A_iA_j} \le 1, 0 \le d_{A_iA_j} \le 1$.

Результаты вычислений всех индексов согласия/несогласия сведены в табл. 2 в следующем п. 2, там же сделан обоснованный вывод о выбранной наилучшей альтернативе – при выдвинутых ЛПР уровнях согласия α_1=0,6 и несогласия γ_1=0,7 для данного примера (учитывая, что обычно $0<\alpha<1$, $0<\gamma<1$).

2. Результаты и обсуждение

Итак, как видно из результатов табл. 2, при выполнении характерных для метода ELECTRE I условий типа нестрогих неравенств $C_{A_iA_j} \ge \alpha_1$ и $d_{A_iA_j} \le \gamma_1$ (где выдвинутые ЛПР при помощи эксперта-консультанта значения α_1=0,6, γ_1=0,7), им обоим соответствует только альтернатива B. Две другие, а именно A и D, уступают ей; в ракурсе рассмотренного примера при заданных значениях единственная B превосходит эти остальные. Поэтому альтернатива B – наилучшая.

Табл. 2. Индексы согласия/несогласия для примера

Альтернатива	A		B		D	
A	*		0,321	0,75	0,571	1
B	***0,678***	***0,5***	*		***0,857***	***0,5***
D	0,428	0,417	0,143	0,688	*	

Особенно принимая во внимание, в т.ч., фигурирующее в ней наивысшее из возможных значение критерия $K_{\text{I}} \equiv K_{\text{з}} = 1$. Учитывая его наибольший среди всех вес w_1=7, такой результат видится естественным, хотя выбранная здесь АИС и дороже других. Однако вес стоимостного критерия $K_{\text{V}} \equiv S$ экспертно оценен ниже первых четырех большего приоритета, что также сыграло важную роль в пользу выбора альтернативы B.

Критериев могло быть больше на две единицы в случае попытки заменить предложенный критерий трехзначной логики, а именно тремя его раздельными критериальными составляющими без использования таковой. Однако с увеличением количества критериев на 2 ситуация с принятием решения стала бы гораздо более труднообозримой, тем самым только усложняя его процесс (в случае повышения изначального количества 7-ми критериев до 9-ти оно было бы более чем на 25%).

Видится также, что страхование киберрисков могло бы сыграть одну из ведущих ролей, но при куда более высоких экспертных оценках веса относящегося к нему критерия $K_{\text{VII}} \equiv y$. К этому следовало бы стремиться, в т.ч., всесторонне активизируя познавательную и просветительскую деятельность в сфере страхования, его возможностей и смежных вопросов. В перспективе развивая его сферу как таковую.

Заключение

Итак, цель статьи достигнута, а ее задачи выполнены. *Научная новизна* статьи заключается в следующем:

- выяснена применимость подхода РИПСА в виде метода ELECTRE I для выбора автоматизированных информационных систем в ракурсе рассмотренных – и небезосновательно полагаемых среди приоритетных –

критериев, относящихся к киберзащищенности АИС с учетом страхования киберрисков;

- разработан модифицированный, новый в плане киберзащищенности при страховании киберрисков критерий качества технико-экономического характера, основанный на 3-хзначной мажоритарной логике – а именно позволивший выразить и учесть в логико-математическом виде: некоторые особенности страховой защиты АИС в связи с присущими им киберрисками, а также способность АИС противостоять собственными средствами классифицируемым по трем категориям кибератакам на подобные организационно-технические системы.

Практическая ценность статьи состоит в:

- применимости критерия (критериальной базы) на основе трехзначной мажоритарной логики не только в ракурсе технических и организационно-технических параметров либо характеристик киберзащищенности АИС, но и в ракурсе финансово-экономических параметров либо характеристик защищенности страхуемых АИС;

- применимости метода группы ELECTRE подхода разработки индексов попарного сравнения альтернатив, причем как в ракурсе анализа и организационно-технических мер по снижению различных связанных с АИС киберрисков, так и в ракурсе страховой защиты от них – на случаи преодоления первичных иных рубежей защиты;

- возможности обойтись на 2 единицы меньшим количеством критериев (в рассмотренном на примере случае всего 7 критериев вместо 9 критериев) за счет разработанного (дополнительного) интегрального критерия трехзначной мажоритарной логики для многокритериальных альтернатив (по сравнению с неиспользованием такого критерия);

- при практическом применении результатов и материалов статьи – в улучшении условий управленческого труда лиц, принимающих организационно-управленческие, организационные и т.п. решения с многокритериальным выбором АИС путем его рационализации, а именно: повышении системности трудового процесса принятия решений и его обоснованности, объективности и достоверности наряду с его упрощением и адаптацией условий труда ЛПР, с учетом индивидуальных особенностей в виде предпочтений при участии консультанта.

Отметим, что для удобства расчетов и выбора – при нескольких критериях и числах, существенно превышающих рассмотренные в примере – имеет смысл использовать табличные, стандартные возможности MS Excel (чаще всего имеющегося практически на каждой ЭВМ).

Одно из возможных направлений дальнейших исследований – вопросы, связанные с применением предложенного критерия (критериальной базы) на основе трехзначной мажоритарной логики в ракурсе метода ELECTRE II и/или III.

Благодарности

Автор признателен своим прежним и нынешним вузам-работодателям: Финансовому университету при Правительстве РФ, где была начата данная работа после аттестации в должности доц., и продолжена в указанной должности в Российском Государственном гуманитарном университете, Московском Государственном лингвистическом университете и Московском гуманитарном университете за материальное стимулирование, периодическое премирование научной деятельности.

Список литературы

1. Анич И., Ларичев О.И. Метод ЭЛЕКТРА и проблема ацикличности отношений альтернатив // Автоматика и телемеханика. 1996. № 8. С. 108-118.

2. Roy B. Multicriteria Methodology for Decision Aiding. Dordrecht: Kluwer Academic Publisher, 1996. 303 p.

3. Шептунов М.В. Применимость метода ELECTRE I для оценки многокритериальных альтернатив в задачах выбора принципа управления доступом к музейным цифровым копиям // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2020. № 4. С. 62-71. DOI: 10.28995/2686-679X-2020-4-62-71

4. Лобач Д.И. О некоторых случаях количественной оценки ущерба технической системе // Надежность. 2024. Т. 24. № 4. С. 58-64. DOI: 10.21683/1729-2646-2024-24-4-58-64

5. Гапанович В.А., Розенберг Е.Н., Шубинский И.Б. Некоторые положения отказобезопасности и киберзащищенности систем управления // Надежность. 2014. № 2. С. 88-100. DOI: 10.21683/1729-2646-2014-0-2-88-100

6. Яшин В.Н. Оценка эффективности автоматизированных информационных систем // Вестник Самарского Государственного технического университета. Сер. Технические науки. 2017. № 3(55). С. 43–49.

7. Страхование от *А* до *Я* / Под ред. Л.И. Корчевской, К.Е. Турбиной. М.: ИНФРА-М, 1996. 624 с.

8. Бутакова Н.А. Стимулы обеспечения кибербезопасности и роль киберстрахования // Пермский юридический альманах. Научный журнал. М.: Статут, 2025. С. 211–221.

9. Просветова А.А., Дубкова Е.В. Кибер-страхование как способ обеспечения информационной безопасности // Международный журнал гуманитарных и естественных наук. 2020. № 4-3(43). С. 138–141. DOI: 10.24411/2500-1000-2020-10411

10. Крупенко Ю.В. Киберриски и теоретические основы киберстрахования // Проблемы современной экономики: глобальный, национальный и региональный контекст: сб. науч. ст. / ГрГУ им. Янки Купалы; редкол.: М.Е. Карпицкая (гл. ред.) [и др.]. Гродно: ГрГУ, 2022. С. 249-257.

11. Борисов Н.М., Адамчук Н.Г. Киберстрахование как инструмент обеспечения кибербезопасности // Страховое дело. 2020. № 4. С. 21–25.

12. Волкова Т.А., Суслякова О.Н. Страхование информационных рисков (киберстрахование) // Инновационная экономика: перспективы развития и совершенствования. 2018. № 7(33). Т.1. С. 117–122.

13. Варшавский В.И. Трехзначная мажоритарная логика // Автоматика и телемеханика. 1964. № 25(5). С. 673-684.

14. Овсиевич Б.Л. Некоторые свойства симметрических функций трехзначной логики // Проблемы передачи информации. 1965. № 1(1). С. 57-64.

15. Шептунов М.В. Страхование и новое научное направление: методы оперативного рационального перестрахования особо серьезного риска на базе эволюционных алгоритмов // Сборник работ победителей национального конкурса научных и инновационных работ по теоретической и прикладной экономике. СПб.: Первый класс, 2012. 156–167 с.

References

1. Anich I., Larichev O.I. [ELECTRA method and the problem of acyclicity of relations of alternatives]. *Automation and Remote Control*. 1996;57(8):1154–1162.

2. Roy B. Multicriteria Methodology for Decision Aiding. – Dordrecht: Kluwer Academic Publisher; 1996. 303 p.

3. Sheptunov M.V. [Applicability of the ELECTRE I method for evaluating multi-criterional alternatives in problems of choosing of a principle of access control to museum digital copies]. *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*. 2020;4:62–71. (in Russ.)

4. Lobach D.J. On some cases of quantitative estimation of damage to a technological system. *Dependability*. 2024;24(4):58–64. DOI: 10.21683/1729-2646-2024-24-4-58-64. (in Russ.)

5. Gapanovich V.A., Rozenberg E.N., Shubinsky I.B. Some concepts of fail-safety and cyber protection of control systems. *Dependability*. 2014;(2):88–100. DOI: 10.21683/1729-2646-2014-0-2-88-100. (in Russ.)

6. Yashin V.N. Evaluation of efficiency of automated information systems . *Vestnik of Samara State Technical University. Technical Sciences*. 2017;3(55):43–49. (in Russ.)

7. Insurance from *A* to *Z*. Korchevskaja L.I., Turbina K.E., ed. Moscow: INFRA-M, 1996. 624 p. (in Russ.)

8. Butakova N.A. Cybersecurity incentives and the role of cyber insurance. *Perm Legal Almanac*. – Moscow: Statute; 2025: 211–221. (in Russ.)

9. Prosvetova A.A., Dubkova E.V. Cyber insurance as method for ensuring information security. *International Journal of Humanities and Natural Sciences.* 2020; 4-3(43):138–141. DOI: 10.24411/2500-1000-2020-10411 (in Russ.)

10. Krupenko Y.N. Cyberrisks and theoretical foundations of cyberinsurance. *Problems of Modern Economy: Global, National and Regional Context: a collection of scientific articles / GrSU im. Janki Kupaly; ed. by M.E. Karpitskaya (chief ed.) et al. – Grodno: GrSU;* 2022; 249–257. (in Russ.)

11. Borisov N.M., Adamchuk N.G. The Ability of Insurers in the Cybersecurity Business. *Insurance business*. 2020; 4:21–25. (in Russ.)

12. Volkova T.A., Suslyakova O.N. Insurance of information risks (cyber insurance). *Innovative economy: prospects for development and improvement*. 2018;7(33):1:117–122. (in Russ.)

13. Varshavsky V.I. [Ternary majority logic]. *Automation and Remote Control*. 1964;25(5):673–684. (in Russ.)

14. Ovsievich B.L. [Certain properties of symmetric functions in three-valued logic]. *Problems of Information Transmission*. 1965;1(1):57–64. (in Russ.)

15. Sheptunov M.V. [Insurance and the new scientific direction: methods of operational rational reinsurance of extra-severe risks on the base of the evolutionary algorithms]. *Collection of works by the winners of the national competition of the scientific and innovative works in theoretical and applied economics*. Saint-Petersburg: Pervyi klass. Publ., 2012:156–167. (in Russ.)

Сведения об авторе

Шептунов Максим Валерьевич – кандидат технических наук, доцент; доцент кафедры Международной информационной безопасности и член Ученого совета Института информационных наук МГЛУ (ИИН ФГБОУ ВО «Московский Государственный лингвистический университет»); доцент кафедры Прикладной информатики и статистики факультета Экономики, управления и международных отношений МосГУ (Московского гуманитарного университета); Москва, Российская Федерация; e-mail: triumf403@yandex.ru.

About the author

Maxim V. Sheptunov, Candidate of Engineering, Associate Professor; Associate Professor, Department of International Information Security, Member of the Academic Council, Institute of Information Science, MSLU (Moscow State Linguistic University); Associate Professor, Department of Applied Computer Science and Statistics, Faculty of Economics, Management and International Relations, MosUH (Moscow University for the Humanities); Moscow, Russian Federation; e-mail: triumf403@yandex.ru.

Вклад автора в статью

Шептунов М.В. Выяснена применимость подхода РИПСА в виде метода ELECTRE I для выбора АИС в ракурсе рассмотренных критериев, относящихся к киберзащищенности АИС, с учетом страхования киберрисков. Разработан модифицированный, новый в плане киберзащищенности при страховании киберрисков критерий, основанный на трехзначной мажоритарной логике. Сделаны выводы относительно разработанного критерия качества технико-экономического характера, причем имеющего не только самостоятельное значение, но и при его применении в методах группы ELECTRE подхода разработки индексов попарного сравнения альтернатив.

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.