DOI 10.54398/20741707_2022_3_72
УДК 004.054

МНОГОКРИТЕРИАЛЬНАЯ ОЦЕНКА ЦЕЛОСТНОСТИ СУБЪЕКТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Статья поступила в редакцию 22.06.2022, в окончательном варианте – 22.08.2022.

Курчавов Павел Максимович, МИРЭА – Российский технологический университет, 119454, Российская Федерация, г. Москва, пр. Вернадского, 78,
аспирант, ORCID: 0000-0003-2589-6600, e-mail: aakvs@yandex.ru
Максимова Елена Александровна, МИРЭА – Российский технологический университет, 119454, Российская Федерация, г. Москва, пр. Вернадского, 78,
кандидат технических наук, доцент, ORCID: 0000-0001-8788-4256, e-mail: maksimova@ mirea.ru

Сегодня качество и уровень информационных технологий быстро растет, что приводит к эволюции угроз, заставляя разработчиков программно-аппаратных средств защиты информации работать на опережение. Один из новых классов угроз представлен угрозами, определяющими эффект инфраструктурного деструктивизма критической информационной инфраструктуры, т.е. саморазрушения информационной инфраструктуры. Данное явление может возникнуть на любом этапе жизненного цикла субъектов критической информационной инфраструктуры, в том числе в ходе эксплуатации системы, ввиду её качественных и количественных изменений. Для частичного решения данной проблемы предложена модель многокритериальной оценки инфраструктурной целостности субъекта критической информационной инфраструктуры, учитывающая его системные особенности, суть которой состоит в том, чтобы проанализировать по составленным с помощью экспертного мнения критериям возможных состояний объектов критической информационной инфраструктуры. С помощью этих результатов – возможно нахождение средней оценки целостности общего состояния инфраструктуры субъекта критической информационной инфраструктуры.

Ключевые слова: целостность, информационная безопасность, субъект, критическая информационная инфраструктура, многокритериальный анализ, инфраструктурный деструктивизм

USING MULTI-CRITERIA ANALYSIS TO ASSESS THE INTEGRITY OF THE SUBJECT OF CRITICAL INFORMATION INFRASTRUCTURE

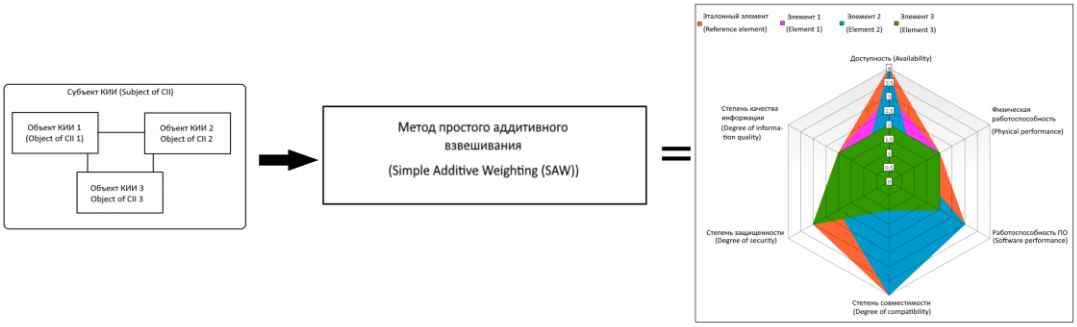
The article was received by the editorial board on 22.06.2022, in the final version – 22.08.2022.

Kurchavov Pavel M., MIREA – Russian Technological University, 78 Vernadsky Avenue, Moscow, 119454, Russian Federation,
postgraduate student, ORCID: 0000-0003-2589-6600, e-mail: aakvs@yandex.ru
Maximova Elena A., MIREA – Russian Technological University, 78 Vernadsky Avenue, Moscow, 119454, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, ORCID: 0000-0001-8788-4256, e-mail: maksimova@mirea.ru

Today, the quality and level of information technology is growing rapidly, which leads to a rapid evolution of threats, forcing developers to constantly improve their information security products, look for new approaches, and be one step ahead of intruders. One of the new classes of threats is represented by threats that determine the effect of infrastructural destruction of critical information infrastructure (CII), i.e. self-destruction of information infrastructure. This phenomenon can appear at any stage of the life cycle of critical information infrastructure subjects, due to its qualitative and quantitative changes, including the operation of the system. To partially solve this problem proposed a model of multi-criteria assessment of the infrastructural integrity of the critical information infrastructure subject, taking into account of the system features of the critical information infrastructure, the essence of which is to analyze according to the criteria of possible states of CII objects compiled with the help of expert opinion. With these results, it is possible to find an average assessment of the integrity of the overall state of the critical information infrastructure subject's infrastructure.

Keywords: infrastructure analysis, security of the CII subject, critical information infrastructure, information security, multi-criteria analysis

Graphical annotation (Графическая аннотация)



Введение. Критическая информационная инфраструктура (КИИ) РФ представлена объектами КИИ, количественный и качественный состав которых в процессе эксплуатации субъектов КИИ может изменяться. Объектами КИИ являются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления. Субъекты КИИ – совокупность объектов КИИ, а также сети электросвязи, используемые для организации взаимодействия таких объектов. Субъект КИИ представляет собой государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которые на каком-либо законном основании владеют объектами КИИ или же обеспечивают их взаимодействие. На рисунке 1 представлена схема, отображающая контекстное представление субъектов КИИ, а также объектов КИИ с точки зрения рассмотренного определения, а на рисунке 2 представлена типовая архитектура субъекта КИИ.

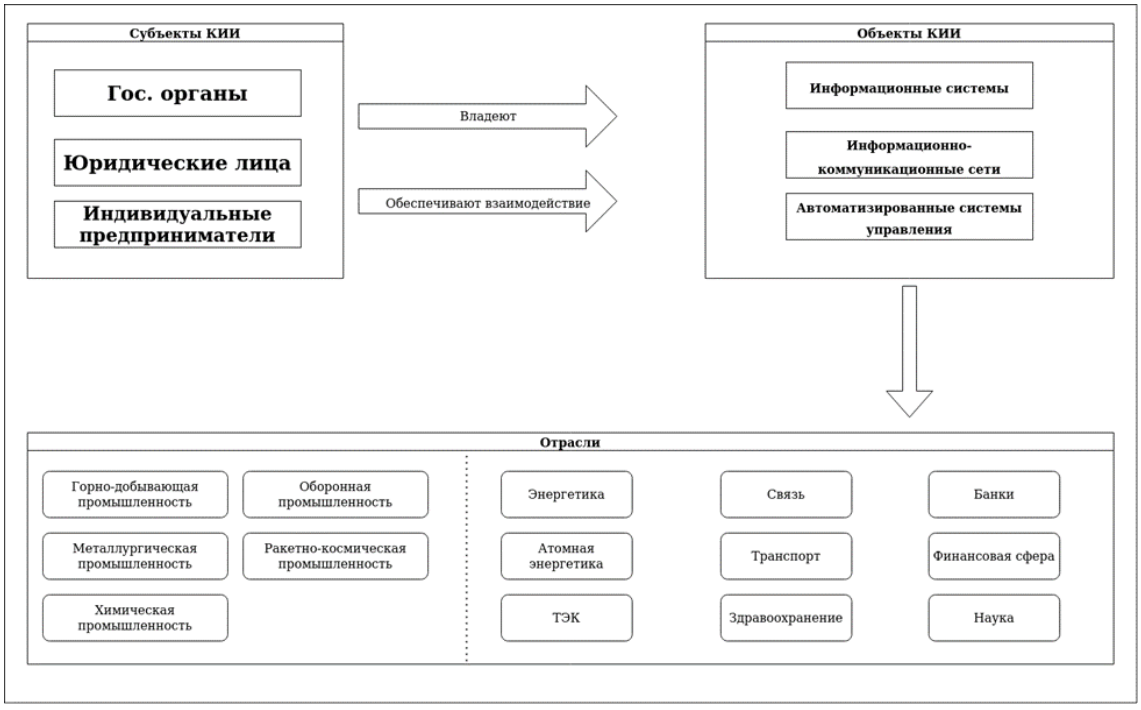


Рисунок 1 – Схема контекстного представления субъектов КИИ

Согласно [1], субъект КИИ обладает определенными правами и обязанностями, большинство из которых сводится к регулированию ситуации на объектах КИИ, обеспечению безопасности на объектах КИИ и своевременному информированию органов власти в случае нарушений функционирования объектов КИИ. Из этого следует, что субъект КИИ, в первую очередь, является юридическим лицом, которое обязано обеспечивать безопасное функционирование объектов, которыми оно владеет на законном основании. Т.е. субъекты КИИ являются элементами системы управления информационной безопасности (ИБ) КИИ. По данным ФСТЭК РФ, на сегодняшний день их более 50 000 [2].

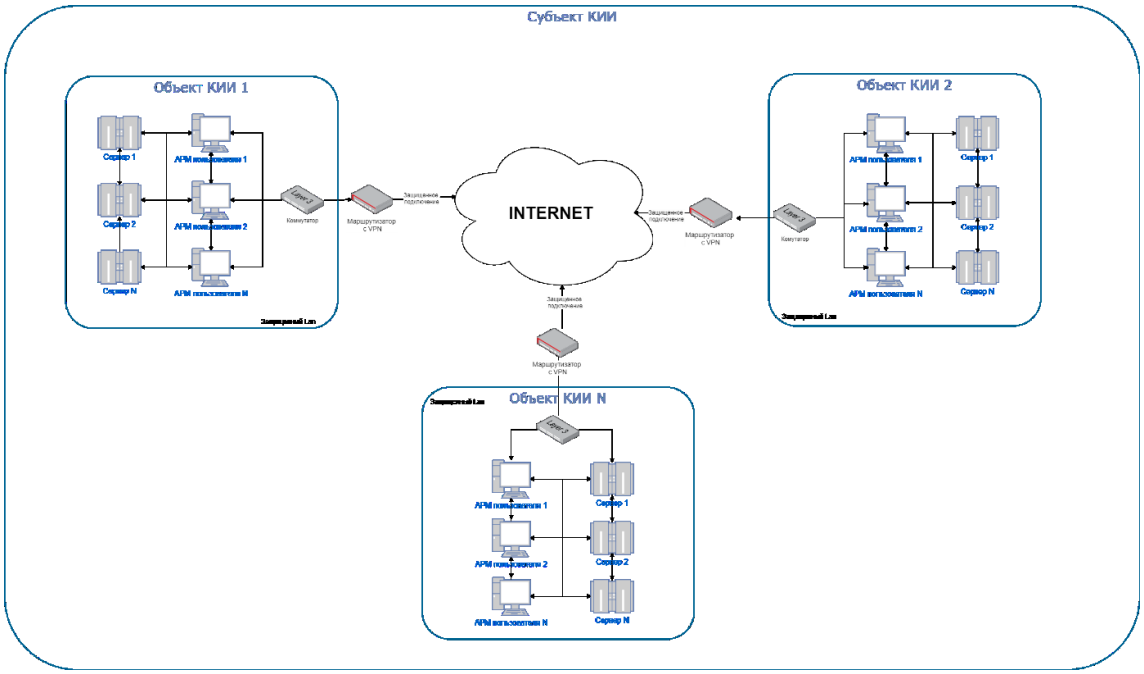


Рисунок 2 – Типовая архитектура субъекта КИИ

[1] регулирует отношения в области обеспечения безопасности КИИ РФ в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак. В [ст. 10, 1] детально описаны основные задачи и схема построения системы безопасности значимого объекта КИИ. В качестве ключевых задач определены:

1) предотвращение неправомерного доступа к информации, обрабатываемой значимым объектом критической информационной инфраструктуры, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;

2) недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта критической информационной инфраструктуры;

3) восстановление функционирования значимого объекта критической информационной инфраструктуры, обеспечиваемого в том числе за счет создания и хранения резервных копий необходимой для этого информации;

4) непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Особенностью КИИ в контексте ИБ является феномен инфраструктурного деструктивизма, проявляющийся в саморазрушении инфраструктуры при пролонгированном влиянии деструктивных воздействий инфраструктурного генеза (происхождения) [3]. Пролонгация в данном случае возникает за счет накопительного эффекта, которым обладает данный класс имманентных угроз.

Условием для возникновения данного феномена может стать качественное и (или) количественное изменение состава субъекта КИИ, так как при этом возникают импульсные явления на уровне систем взаимодействующих объектов КИИ [4]. В конечном итоге, это может привести к нарушению целостности инфраструктуры и разрушить ее.

Методы и подходы. Для оценки целостности системы сегодня, как правило, используются различные комплексы, связанные непосредственно с отслеживанием разных аспектов безопасности в системе. Как правило, в основе таких комплексов лежит метод мониторинга, суть которого заключается в контроле процессов и приложений, качества выполнения бизнес-процессов организации и т.д. Также, как правило, благодаря таким системам возможно предупредить инциденты ИБ. Например, это:

• ПО Zabbix, предназначенное для мониторинга параметров сети, таких как жизнеспособность и целостность серверов, виртуальных машин, приложений, сервисов и т.д. Оно предлагает механизм оповещений, который дает возможность пользователям настраивать уведомления практически на любое событие. Также Zabbix предлагает функции для отчетности и визуализации данных, которые основаны на данных истории [5];

• Форпост – это ПО, предназначенное для автоматического детектирования негативного влияния на анализируемую систему, которое может быть классифицировано как компьютерная атака [6]. Существует два вида исполнения этого ПО:

1) базовое – в нем все необходимые программные компоненты установлены в рамках одного устройства, и оно сразу готово к использованию;

2) модульное, состоящее из сетевых датчиков, центра управления и автоматизированного рабочего места администратора.

Однако рассмотренные системы представляют собой комплексы для сбора данных, которые могут быть проанализированы и предоставлены экспертам для конечного вердикта. Причем экспертные оценки могут разниться, так как может существовать множество показателей, по которым можно оценить информационную систему, в соответствии с параметрами внешней среды и поставленной задачей.

На основании вышеизложенного было решено ввести понятие инфраструктурной целостности (или целостности инфраструктуры) для четкого понимания предмета исследования.

Источником определения и исследования категории «целостность инфраструктуры» является интенсионал самого понятия «целостность». Существует несколько определений целостности. Например, целостность – это обобщённая характеристика объектов, обладающих сложной внутренней структурой [7]. Данное определение выражает интегрированность, самодостаточность, автономность этих объектов, их противопоставленность окружению, связанную с их внутренней активностью. Также «целостность» определяют как качество системы, которым она обладает, если корректно выполняет все свои функции, свободна от намеренных или случайных несанкционированных манипуляций [8].

Согласно [9], существует такое понятие, как «целостность ресурсов информационной системы». Оно описывается как некое состояние ресурсов информационной системы, в котором какие-либо изменения этих ресурсов намеренно производятся исключительно субъектами, имеющими на это право. Также сохраняются их состав, содержание и организация взаимодействия. Данное определение взято за основу в рамках исследования категории «инфраструктурная целостность».

Неоднозначным является подход и к определению понятия «инфраструктура». Но, как правило, «инфраструктура» определяется как совокупность связанных между собой структур, отраслей или объектов, служащих для нормального функционирования системы [10, 11]. При этом выделяют несколько видов инфраструктур: производственная, социальная, транспортная, инженерная, информационная инфраструктура, инфраструктура экономики и др.

Для данного исследования наибольший интерес представляет информационная инфраструктура, являющаяся системой организационных структур, подсистем, обеспечивающих работу и развитие информационного пространства [12]. Инфраструктурную целостность при этом определим как состояние системы, в котором компоненты её инфраструктуры (подсистемы, физические устройства, структуры и т.п.) функционируют в полном объеме и не оказывают деструктивного воздействия на взаимодействующие элементы.

Для оценки целостности системы сегодня используются следующие методы:

- дискретная модель – в рамках этого метода в качестве меры надежности оценивается среднее время между двумя ошибочным срабатываниями [13];
- метод соотношений – заключается в определении вероятности безотказной работы сложной вычислительной системы [13];
- экспоненциальная модель – основана на модели, подразумевающей установление связи между интенсивностью обнаружения ошибок при отладке с интенсивностью проявления ошибок при нормальном функционировании комплекса программ и определенном количестве первичных ошибок [13].

В данном исследовании решено использовать методы многокритериального анализа. Это обусловлено тем, что данный вид анализа представляет собой более гибкую и настраиваемую методику, которая может быть изменена, например, переосмыслением изучаемых критериев. Также, благодаря такому подходу, можно не ориентироваться на какую-то конкретную область качества функционирования системы, т.е. целостности, а производить комплексный анализ, который как раз и будет соответствовать введенному выше определению целостности.

В качестве наиболее распространенных методов многокритериального анализа используются:

- SAW – метод, необходимый для количественного измерения значимости критериев по каждому альтернативному варианту. При этом будет построена и нормализована матрица решений, определяющая вес каждого критерия. В конечном итоге выводится обобщённая оценка для представленных альтернатив [14];

- TOPSIS – метод, основанный на концепции того, что идеальный вариант должен иметь самое малое геометрическое расстояние от положительного идеального решения и наибольшее геометрическое расстояние от отрицательного идеального решения. В ходе этого метода создается матрица оценки, состоящая из m альтернатив и n критериев. Затем эта матрица нормализуется и вычисляется ее взвешенная. После этого определяются худшая и лучшая альтернативы и вычисляется расстояние между целевой альтернативой и лучшим и худшим состояниями. В итоге определяется соответствие с наихудшим состоянием и альтернативы ранжируются [15];
- ELECTRE – семейство методов многокритериального анализа, где каждый метод обладает индивидуальными особенностями, что делает их эффективными для разных типов задач принятия решений [16];
- метод анализа иерархий. В отличие от многих других методов многокритериального анализа, не заставляет лицо, принимающее решение (ЛПР), использовать конкретное «правильное» решение, однако дает возможность в интерактивном режиме выбрать именно то решение, которое наиболее подходит под ситуацию, понимание ЛПР сути проблемы и согласуется с требованиями к решению проблемы [17].

Важно отметить, что большинство общеизвестных методов многокритериального анализа используются для сравнения множества альтернатив по критериям, что, в свою очередь, сводится к поиску наилучшего варианта.

В многокритериальном анализе широко распространены системы поддержки принятия решений (СППР). Например:

- СППР «Выбор» [18]. Данная система поддержки принятия решений основана на методе анализа иерархий. Используется для оценки качества организационных и другого типа задач. Программа разработана компанией ДТК Софтр, работает на системах семейства Windows;
- ПО Super Decisions [19]. Обеспечивает поддержку принятия решений с помощью методов анализа иерархий и аналитического сетевого процесса. Является одними из самых мощных для объединения суждений и данных с целью более эффективного ранжирования вариантов и прогнозирования результатов;
- система Expert Choice – система, также использующая метод анализа иерархий [20]. Данная система является достаточно сложной и комплексной, направленной на решения разного спектра задач бизнеса [21].

В работе [22] выполнено сравнение популярных методов многокритериального анализа посредством реализации простых программ. Интерес в этой работе представляет тот факт, что у разработанного программного обеспечения выходными данными являются, помимо наилучшего варианта, в зависимости от заданных критериев, результативные значения всех анализируемых объектов.

Дискуссия. Нарушение инфраструктурной целостности может снизить уровень ИБ как отдельного элемента системы, так и системы в целом [23]. Таким образом можно определить следующий набор направлений мониторинговых процедур, реализация которых позволит этого не допустить:

1) оценка локальной целостности элементов инфраструктуры, т.е. оценка инфраструктурной целостности на уровне каждого объекта субъекта КИИ;
2) оценка целостности систем взаимодействующих объектов;
3) непосредственная оценка целостности субъекта КИИ.

Рассмотрим реализацию первого направления в качестве базового.

Для разработки модели анализа целостности инфраструктуры субъекта КИИ использовался метод многокритериального анализа, представляющий собой практическую реализацию структуры системного исследования в решении сложных, комплексных проблем. Согласно [24], многокритериальный анализ обеспечивает рациональный, систематизированный и прозрачный процесс принятия решений при анализе влияний и взаимосвязей в сложных системах. Для использования таких методов в первую очередь необходимо проработать перечень критериев, который сможет отвечать требованиям безопасности субъекта КИИ.

В данном исследовании предлагается использовать метод многокритериального анализа не для поиска лучшего варианта, а для вычислений, по заданным критериям, множества общих состояний объектов КИИ, на основании которых станет возможным нахождение средней оценки целостности общего состояния инфраструктуры субъекта КИИ.

Обозначенное возможно при формировании перечня критериев оценки целостности объектов КИИ, благодаря которым можно будет рассчитать показатель целостности каждого из объектов, функционирующих в системе данного субъекта КИИ. В дальнейшем эти показатели можно будет использовать для оценки инфраструктурной целостности непосредственно субъекта КИИ, а также производить более гибкую диагностику. Предложенные критерии для оценки целостности объектов КИИ представлены в таблице 1.

Таблица 1 – Критерии оценки инфраструктурной целостности элемента объекта КИИ

Наименование критерия	**Что характеризует критерий**	**Показатели для многокритериального анализа**	**Вес критерия**
Доступность	Доступность объектов КИИ, входящих в состав субъекта КИИ	1) недоступен ни одному из других объектов КИИ в составе субъекта КИИ (0 %); 2) доступен малой части объектов КИИ в составе субъекта КИИ (< 50 %); 3) доступен большей части объектов КИИ в составе субъекта КИИ (> 50 %); 4) доступен всем объектам КИИ в составе субъекта КИИ (100 %).	0,1
Физическая работоспособность	Общая оценка работоспособности физических составляющих всех объектов КИИ, входящих в состав субъекта КИИ	1) не работает одно или более физическое устройство, входящее в состав объекта КИИ; 2) работают все физические устройства, входящие в состав объекта КИИ.	0,19
Работоспособность ПО	Общая оценка работоспособности программного обеспечения в составе всех объектов КИИ, входящих в состав субъекта КИИ	1) нарушена работоспособность некоторых программных компонентов объекта КИИ, что полностью нарушает выполнение задач объекта КИИ; 2) нарушена работоспособность некоторых программных компонентов объекта КИИ, что не нарушает выполнение задач объекта КИИ; 3) работают все программные компонентов объекта КИИ.	0,19
Степень совместимости	Общий уровень совместимости между объекта КИИ с другими объектами КИИ, входящими в состав субъекта КИИ	1) отсутствие совместимости со всеми объектами КИИ в составе субъекта КИИ (0 %); 2) наличие совместимости с малой частью объектов КИИ в составе субъекта КИИ (< 50 %); 3) наличие совместимости с большей частью объектов КИИ в составе субъекта КИИ (> 50 %); 4) наличие совместимости со всеми объектами КИИ в составе субъекта КИИ (100 %).	0,17
Степень защищенности	Уровень обеспечения защиты каналов конкретного объекта КИИ, входящими в состав субъекта КИИ	1) уровень обеспечения защиты каналов связи не соответствует регламентам предприятия; 2) уровень обеспечения защиты каналов связи частично соответствует регламентам предприятия; 3) уровень обеспечения защиты каналов связи полностью соответствует регламентам предприятия.	0,2
Степень качества информации	Соответствие информации, передаваемой объектом КИИ, входящим в состав субъекта КИИ, общим стандартам качества.	1) информация не соответствует общим стандартам качества; 2) информация соответствует общим стандартам качества	0,15

В соответствии с представленными критериями предлагается производить общую оценку целостности объекта КИИ с использованием метода SAW по причине его простоты и прозрачности, что может быть полезным при работе с большим количеством данных.

Как видно из схемы, представленной на рисунке 3, многокритериальный анализ объектов КИИ рассматривается на уровне их элементов. В ходе работы выстраивается матрица элементов объектов КИИ, каждый элемент которой является значением того или иного критерия из представленных в таблице 1, для каждого элемента объекта КИИ.

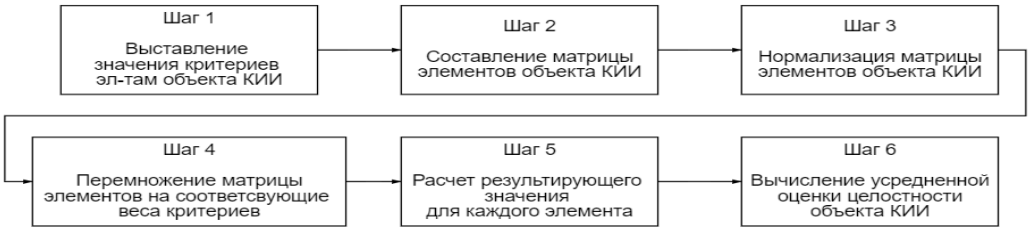


Рисунок 3 – Схема реализации метода SAWдля оценки инфраструктурной целостности объекта КИИ

После анализа и получения данных о состоянии элементов объекта КИИ становится возможным вычисление усредненного значения целостности объекта КИИ. Стоит отметить, что в рамках метода критерии являются максимизируемыми, т.е. мы заинтересованы в контексте работы системы, чтобы значения критериев были максимальными, а не минимальными. Данный факт обосновывает выбор формулы расчета нормированных значений матрицы. Формализация данного имеет вид:

$$P_{ij} = \frac{x_{ij} - x_j^{min}}{x_j^{max} - x_j^{min}}, \quad (1)$$

где xX_{ij} – значение из матрицы, соответствующее конкретному критерию; X_j^{min} – минимальное значение критерия; X_j^{max} – максимальное значение критерия.

$$\frac{\sum_{j=1}^{n} a_j \times 100\%}{X \times n}, \quad (2)$$

где n – это количество объектов КИИ; a_j – это показатель целостности j-го элемента объекта КИИ, а X – это показатель инфраструктурной целостности эталонного объекта КИИ. Для того чтобы вычислить значение X, необходимо с помощью метода SAW, просчитать результирующее значение инфраструктурной целостности для эталонного элемента объекта КИИ.

В ряде работ [8, 24–27] полагается расчет по критериям, для дальнейшего сравнения результатов между собой, для поиска самого удовлетворяющего значения. В данном исследовании для составления вывода об оценке инфраструктурной целостности изучаемого объекта необходимо оценить максимально возможные значения по данным критериям с обозначенными весами. Остро встает вопрос о необходимости эталонного значения, которое будет представлять собой некоторую абстракцию, с наивысшими значениями критериев, необходимую для проведения сравнения остальных результатов для выполнения шестого шага. В таблице 5 описаны значения критериев такого «эталонного» объекта, в соответствии со значениями критериев, представленными в таблице 2.

Таблица 2 – Значения критериев эталонного элемента объекта КИИ

Наименование критерия	**Значение критерия эталонного элемента объекта КИИ**	**Вес критерия**
Доступность	4	0,1
Физическая работоспособность	2	0,19
Работоспособность ПО	3	0,19
Степень совместимости	4	0,17
Степень защищенности	3	0,2
Степень качества информации	2	0,15

Для дальнейших расчетов нам необходим только один эталонный элемент объекта КИИ, в соответствии с чем для него будет существовать только один набор критериев. Поэтому далее получим:

$$\begin{pmatrix} 4 * 0{,}1 \\ 2 * 0{,}19 \\ 3 * 0{,}19 \\ 4 * 0{,}17 \\ 3 * 0{,}2 \\ 2 * 0{,}15 \end{pmatrix} = \begin{pmatrix} 0{,}4 \\ 0{,}38 \\ 0{,}57 \\ 0{,}68 \\ 0{,}6 \\ 0{,}3 \end{pmatrix}.$$

Результирующее значение инфраструктурной целостности для эталонного элемента объекта КИИ:

$$0{,}4 + 0{,}38 + 0{,}57 + 0{,}68 + 0{,}6 + 0{,}3 = 2{,}93.$$

Полученное значение является константой. Таким образом формула (2) примет вид:

$$\frac{\sum_{j=1}^{n} (a_j) \times 100\%}{2{,}93 * n}. \quad (3)$$

На основании предложенного метода выполнена программная реализация, на языке программирования Python, ввиду того, что данный язык достаточно часто используется для анализа данных,

а также в рамках этого языка реализовано большое количество библиотек для решения математических задач разного рода.

Экспериментальное исследование. Рассмотрим реализацию предложенного метода на примере субъекта КИИ, имеющего заданную структуру (рис. 4). Алгоритм реализации выполним в виде комплекса шагов. Более подробно остановимся на исследовании объекта КИИ № 1. Для остальных объектов в структуре субъекта КИИ пошаговое выполнение расчетов выполняется аналогично.

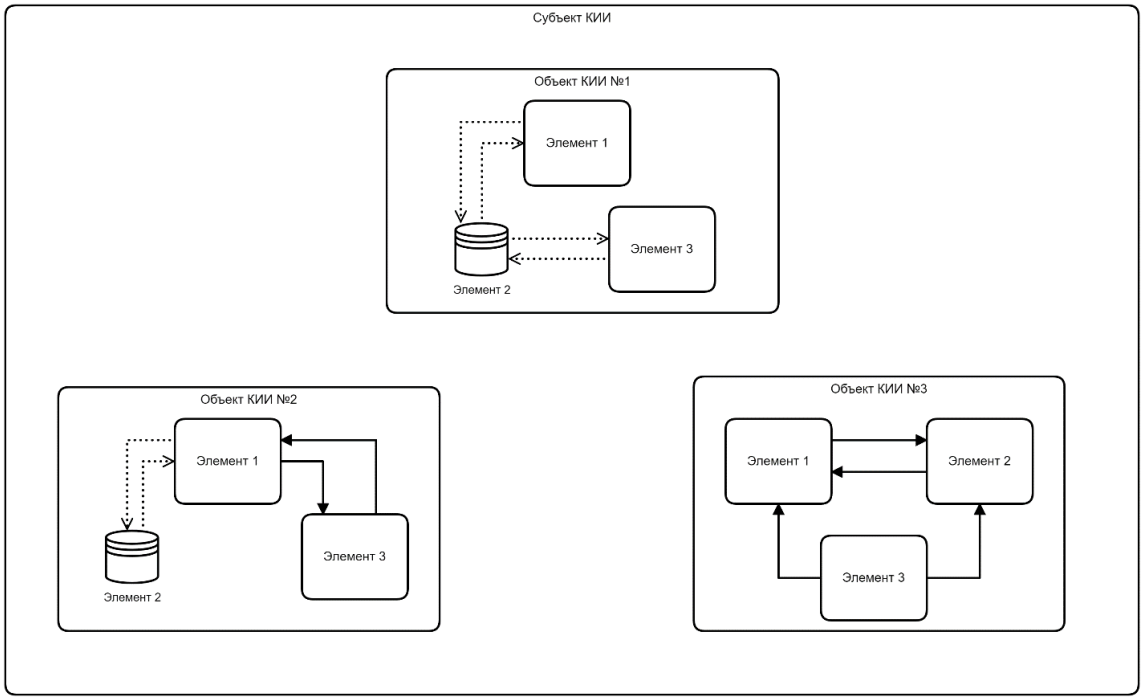


Рисунок 4 – Пример субъекта КИИ для тестового расчёта

Шаг 1: выставим значения критериев элементам тестового объекта КИИ № 1.
Шаг 2: составим матрицу элементов объекта КИИ № 1 (табл. 3).

Таблица 3 – Значения критериев элементов объекта КИИ № 1 для тестового расчёта

Наименование критерия	**Значение критериев элемента 1**	**Значение критериев элемента 2**	**Значение критериев элемента 3**
Доступность	3	4	2
Физическая работоспособность	2	1	2
Работоспособность ПО	2	3	2
Степень совместимости	4	4	1
Степень защищенности	1	2	3
Степень качества информации	2	1	2

Шаг 3: выполним поиск нормированных оценок по данным таблицы 2. Для этого выполним поиск максимальных и минимальных оценок критериев путем отбора максимальных значений в строке (для каждого из критериев):

$$X_{max} = (4; 2; 3; 4; 3; 2),$$
$$X_{min} = (2; 1; 2; 1; 1; 1).$$

Далее следует расчет нормированных значений матрицы по формуле (1). Результат нормирования представлен в таблице 4.

Таблица 4 – Нормированные значения критериев элементов объекта КИИ № 1 для тестового расчёта

Наименование критерия	Нормализованный результат критериев элемента 1	Нормализованный результат критериев элемента 2	Нормализованный результат критериев элемента 3
Доступность	0,5	1	0
Физическая работоспособность	1	0	1
Работоспособность ПО	0	1	0
Степень совместимости	1	1	0
Степень защищенности	0	0,5	1
Степень качества информации	1	0	1

Шаг 4: выполним произведение полученных нормированных значений на веса критериев.

Шаг 5: выполним расчет результирующих значений инфраструктурной целостности элементов объекта КИИ № 1 для тестового расчёта (табл. 5).

Таблица 5 – Итоговые значения критериев элементов объекта КИИ № 1 для тестового расчёта

Наименование критерия	Нормализованный результат критериев элемента 1	Нормализованный результат критериев элемента 2	Нормализованный результат критериев элемента 3
Доступность	0,05	0,1	0
Физическая работоспособность	0,19	0	0,19
Работоспособность ПО	0	0,19	0
Степень совместимости	0,17	0,17	0
Степень защищенности	0	0,1	0,2
Степень качества информации	0,15	0	0,15
Результирующее значение инфраструктурной целостности элементов объекта КИИ № 1	0,56	0,56	0,54

Таким образом, в ходе исследования получен условный рейтинг показателей инфраструктурной целостности элементов объекта КИИ.

На рисунке 5 представлена лепестковая диаграмма, построенная на основе значений критериев (табл. 1) элементов, взятых в рамках тестового расчета. В реальной ситуации такими элементами могут выступать: базы данных, сервера, сервисы, используемые внутри объекта КИИ и т.д.

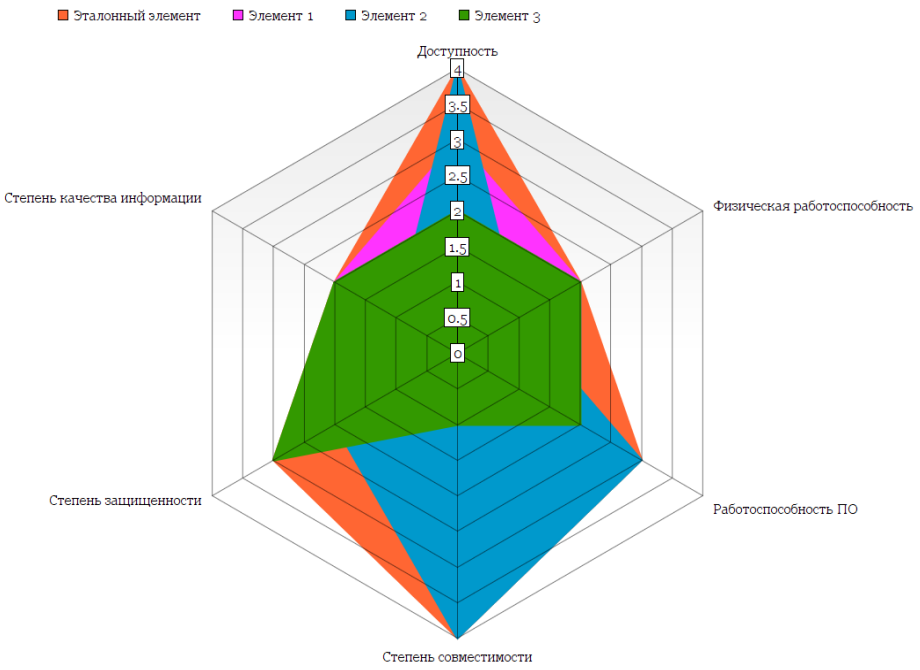


Рисунок 5 – Лепестковая диаграмма сравнения значений критериев элементов объекта КИИ № 1 для тестового расчёта

Шаг 6: в соответствии с формулой (3), завершим тестовый расчет для объекта КИИ № 1:

$$\frac{(0{,}56+0{,}56+0{,}54)\cdot 100\%}{2{,}93\cdot 3}=\frac{165}{8{,}79}=18{,}8\%.$$

Следовательно, значение результирующей оценки инфраструктурной целостности объекта КИИ № 1 для тестового расчета, в сравнении с эталонными значениями, составляет 18,8 %, что на самом деле будем считать весьма низким уровнем инфраструктурной целостности на объекте. Полученное говорит о серьезных нарушениях, функциональной нестабильности и росте инфраструктурного деструктивизма как на объекте КИИ № 1, так и на исследуемом субъекте КИИ в целом.

Заключение. Вышеописанный метод является первым шагом для оценки уровня инфраструктурной целостности субъекта КИИ. Важно отметить, что на основе методик многокритериального анализа возможно добиться получения множества состояний анализируемых объектов для дальнейшего расчета общего состояния субъекта КИИ на более высоких уровнях в соответствии с описанными ранее мониторинговыми процедурами.

Библиографический список

1. О безопасности критической информационной инфраструктуры Российской Федерации // Федеральный закон от 26.07.2017. – № 187-ФЗ.

2. Рекомендации по оценке показателей критериев экономической значимости объектов КИИ от ФСТЭК // SecurityLab.ru. – Режим доступа: https://www.securitylab.ru/blog/personal/valerykomarov /350276.php, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 25.04.2022).

3. Максимова, Е. А. Инфраструктурный деструктивизм субъектов критической информационной инфраструктуры : монография / Е. А. Максимова. – Москва ; Волгоград : Издательство Волгоградского государственного университета, 2021.

4. Максимова, Е. А. Аксиоматика инфраструктурного деструктивизма субъекта критической информационной инфраструктуры / Е. А. Максимова // Информатизация и связь. – 2022. – № 1 (68–74). – Режим доступа: https://www.elibrary.ru/item.asp?id=48316441, свободный. – Заглавие с экрана. – Яз. рус.

5. Что такое Zabbix // Zabbix Documentation. – Режим доступа: https://www.zabbix.com /documentation/5.0/ru/manual/introduction/about, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 28.05.2022).

6. Программно-аппаратный комплекс «Форпост» // Российские наукоемкие технологии. – Режим доступа: http://www.rnt.ru/ru/production/detail.php?ID=20, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 05.06.2022);

7. Ильичёв, Л. Ф. Философский энциклопедический словарь / Л. Ф. Ильичёв, П. Н. Федосеев, С. М. Ковалёв, В. Г. Панов. – Москва : Советская энциклопедия, 1983.

8. Домарев, В. В. Безопасность информационных технологий. Системный подход / В. В. Домарев. – 2004.

9. ГОСТ Р 50.1.053-2005. Основные термины и определения в области технической защиты информации. – 2005.

10. Инфраструктура // Академик. – Режим доступа: https://investments.academic.ru/1013/Инфраструктура, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 07.06.2022);

11. Инфраструктура // Глоссарий.ru. – Режим доступа: http://www.glossary.ru/cgi-bin/gl_sch2. cgi?RIt(wgxywzqyzwg, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 20.08.2022).

12. Информационная инфраструктура // Глоссарий.ru. – Режим доступа: http://www.glossary.ru/cgi-bin /gl_sch2.cgi?RIt(uwsg.outtg9!ot(wgxywzqyzwg, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 20.08.2022).

13. Оценка надежности информационных систем // StudRef. – Режим доступа: https://studref.com /521413 /menedzhment/otsenka_nadezhnosti_informatsionnyh_sistem, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 08.06.2022).

14. Кочкина, М. В. Анализ многокритериальных методов принятия управленческих решений. (на примере задачи выбора поставщиков материально-технических ресурсов) : учеб. пособие / М. В. Кочкина, А. Н. Карамышева, И. И. Махмутова, А. Г. Исавнина, А. К. Розенцвайга. – 2017. – С. 4–8.

15. Hwang, C. L. Multiple Attribute Decision Making: Methods and Applications / C. L. Hwang, K. Yoon. – New York : Springer-Verlag, 1981.

16. Методы семейства ELECTRE // Studme.org. – Режим доступа: https://studme.org/212185/informatika /metody_semeystva_electre, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 11.05.2022).

17. Saaty, Thomas L. On the measurement of intengibles: a principal Eigenvector approach to relative measurement derived from paired comparisons / Thomas L. Saaty // Notices of the American Mathematical Society 60. – 2013. – P. 192–208.

18. СППР Выбор // Monobit. – Режим доступа: https://monobit.ru/sppr-vybor.html#:~:text=Система %20поддержки%20принятия%20решений%20“Выбор”,альтернативы%20по%20каждому%20из%20факторов, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 15.05.2022).

19. About SuperDecisions // Super Decisions. – Режим доступа: https://www.superdecisions.com/about/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 19.05.2022).

20. Система поддержки принятия решений Expert Choice // Studme.org. – Режим доступа: https://studme.org/212182/informatika/sistema_podderzhki_prinyatiya_resheniy_expert_choice, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 10.06.2022).

21. Expert Choice. – Режим доступа: https://www.expertchoice.com, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 10.06.2022).

22. Клоков, С. А. Сравнение и разработка методов многокритериального анализа принятия решений / С. А. Клоков // Молодой ученый. – 2021. – № 18 (360). – С. 30–33. – Режим доступа: https://moluch.ru /archive/360/80477/, свободный. – Заглавие с экрана. – Яз. рус.

23. Основы информационной безопасности. Часть 1: Виды угроз // Хабр. – Режим доступа: https://habr.com/ru/company/vps_house/blog/343110/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 14.06.2022).

24. Методы форсайт-исследования. Методы форсайта // Bstudy.net. – Режим доступа: https://bstudy.net /880551/ekonomika/metody_forsayt_issledovaniya, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 16.06.2022).

25. Ярошевич, Н. Ю. Методологические подходы к формированию аэропортов-хабов на территории страны / Н. Ю. Ярошевич, Т. С. Орлова // Journal of new economy. – 2014. – № 3. – С. 53. – Режим доступа: https://cyberleninka.ru/article/n/metodologicheskie-podhody-k-formirovaniyu-aeroportov-habov-na-territorii-strany, свободный. – Заглавие с экрана. – Яз. рус.

26. Родригес, В. С. Многокритериальная оценка альтернатив территориального планирования при строительстве плотин с использованием технологий географических информационных систем / В. С. Родригес, Н. В. Мокрова // Отходы и ресурсы : интернетжурнал. – 2020. – № 1. – DOI: 10.15862/11INOR120. – Режим доступа: https://resources.today/PDF/11INOR120.pdf, свободный. – Заглавие с экрана. – Яз. рус.

27. Подиновский, В. В. Идеи и методы теории важности критериев в многокритериальных задачах принятия решений / В. В. Подиновский. – 2019.

References

1. On the security of the critical information infrastructure of the Russian Federation. Federal Law No. 187-FZ of July 26, 2017.

2. Recommendations on the evaluation of indicators of criteria for the economic significance of CII objects from the FSTEC. *SecurityLab.ru*. Available at: https://www.securitylab.ru/blog/personal/valerykomarov/350276.php (accessed 25.04.2022).

3. Maksimova, E. A. *Infrastrukturnyy destruktivizm subektov kriticheskoy informatsionnoy infrastruktury : monografiya* [Infrastructural destructivism of subjects of critical information infrastructure : monograph]. Volgograd : Volgograd State University Publishing House, 2021.

4. Maksimova, E. A. Aksiomatika infrastrukturnogo destruktivisma subekta kriticheskoy informatsionnoy infrastruktury [Axiomatics of infrastructural destructivism of the subject of critical information infrastructure]. *Informatizatsiya i svyaz* [Informatization and communication], 2022, no. 1, pp. 68–74 (accessed 25.04.2022).

5. What is Zabbix. *Zabbix Documentation*. Available at: https://www.zabbix.com/documentation /current/ru/manual/introduction/about (accessed 28.05.2022).

6. Hardware-software complex "Forpost". *Russian high-tech technologies*. Available at: http://www.rnt.ru/ru /production/detail.php?ID=20 (accessed 05.06.2022).

7. Ilichev, L. F., Fedoseev, P. N. Kovalev, S. M., Panov, V. G. *Filosofskiy entsiklopedicheskiy slovar* [Philosophical Encyclopedic Dictionary]. Moscow, Sovetskaya entsiklopediya, 1983.

8. Domarev, V. V. *Bezopasnost informatsionnykh tekhnologiy. Sistemnyy podkhod* [Information technology security. A systematic approach], 2004.

9. *GOST R 50.1.053-2005. Osnovnyye terminy i opredeleniya v oblasti tekhnicheskoy zashchity informatsii* [State Standard 50.1.053-2005. Basic terms and definitions in scope of technical protection of information], 2006.

10. Infrastructure. *Academician*. Available at: https://investments.academic.ru/1013/Infrastruktura (accessed 07.06.2022).

11. Infrastructure. *Glossary.ru*. Available at: http://www.glossary.ru/cgi-bin/gl_sch2.cgi?RIt(wgxywzqyzwg.

12. Information infrastructure. *Glossary.ru.* Available at: http://www.glossary.ru/cgi-bin/gl_sch2. cgi?RIt(uwsg.outtg9!ot(wgxywzqyzwg (accessed 20.08.2022).

13. Assessment of the reliability of information systems. *StudRef.* Available at: https://studref.com/521413/menedzhment/otsenka_nadezhnosti_informatsionnyh_sistem.

14. Kochkina, M. V., Karamysheva, A. N., Makhmutova, I. I., Isavnina, A. G., Rozentsvayga, A. K. Analiz mnogokriterialnykh metodov prinyatiya upravlencheskikh resheniy (na primere zadachi vybora postavshhikov materialno-tekhnicheskikh resursov) [Analysis of multi-criteria methods of managerial decision-making. (using the example of the task of selecting suppliers of material and technical resources)], 2017. – P. 4–8.

15. Hwang, C. L., Yoon, K. *Multiple Attribute Decision Making: Methods and Applications*. New York : Springer-Verlag, 1981.

16. Methods of the ELECTRE family. *Studme.org*. Available at: https://studme.org/212185 /informatika/metody_semeystva_electre (accessed 11.05.2022).

17. Saaty, Thomas L. On the measurement of intengibles: a principal Eigenvector approach to relative measurement derived from paired comparisons. *Notices of the American Mathematical Society 60*, 2013, pp. 192–208.

18. DSS choice. *Monobit.* Available at: https://monobit.ru/sppr-vybor.html#:~:text=Система%20поддержки%20принятия%20решений%20“Выбор”,альтернативы%20по%20каждому%20из%20факторов (accessed 15.05.2022).

19. About SuperDecisions. *Super Decisions.* Available at: https://www.superdecisions.com/ (accessed 15.05.2022).

20. Decision Support System – Expert Choice. *Studme.org*. Available at: https://studme.org/212182/informatika/sistema_podderzhki_prinyatiya_resheniy_expert_choice (accessed 10.06.2022).

21. *Expertchoice*. Available at: https://www.expertchoice.com (accessed 15.05.2022).

22. Klokov, S. A. Sravnenie i razrabotka metodov mnogokriterial'nogo analiza prinjatija reshenij [Comparison and development of methods of multi-criteria analysis of decision-making]. *Molodoy uchenyy*. [Young Scientist], 2021, no. 18, pp. 30–33. Available at: https://moluch.ru/archive/360/80477/.

23. Fundamentals of information security. Part 1: Types of Threats. *Habr.* Available at: https://habr.com/ru/company/vps_house/blog/343110/ (accessed 14.06.2022).

24. Methods of foresight research. Foresight methods. Bstudy.net. Available at: https://bstudy.net/880551/ekonomika/metody_forsayt_issledovaniya (accessed 16.06.2022).

25. Yaroshevich N. Yu., Orlova, T. S. Metodologicheskie podkhody k formirovaniyu aeroportov-khabov na territorii strany [Methodological approaches to the formation of hub airports in the country]. *Journal of new economy*, 2014, no. 3, p. 53. Available at: https://cyberleninka.ru/article/n/metodologicheskie-podhody-k-formirovaniyu-aeroportov-habov-na-territorii-strany.

26. Rodriges, V. S., Mokrova, N. V. Mnogokriterialnaya otsenka alternativ territorialnogo planirovaniya pri stroitelstve plotin s ispolzovaniem tekhnologiy geograficheskikh informatsionnykh sistem [Multi-criteria assessment of alternatives to territorial planning in the construction of dams using geographic information system technologies]. *Otkhody i resursy* [Waste and resources], 2020, no. 1. DOI: 10.15862/11INOR120. Available at: https://resources.today/PDF/11INOR120.pdf.

27. Podinovskiy, V. V. *Idei i metody teorii vazhnosti kriteriev v mnogokriterialnykh zadachah prinyatiya resheniy* [Ideas and methods of the theory of the importance of criteria in multi-criteria decision-making tasks.], 2019.