УДК 004.056, 656.6

НЕЧЕТКАЯ СИСТЕМА ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ ВОДНОГО ТРАНСПОРТА

БАРАНОВ Леонид Аврамович, д-р техн. наук, зав. кафедрой; e-mail: baranov.miit@gmail.com
ИВАНОВА Нина Дмитриевна, аспирант; e-mail: ivanovand.nina@yandex.ru
МИХАЛЕВИЧ Игорь Феодосьевич, канд. техн. наук, доцент, старший научный сотрудник; e-mail: mif-orelf@mail.ru

Российский университет транспорта (МИИТ), кафедра «Управление и защита информации», Москва

Интеллектуализация водного транспорта сопровождается расширением ландшафта угроз транспортной безопасности, обусловленных особенностями и слабостями внедряемых технологий, являющихся конвергенцией информационных и телекоммуникационных технологий, технологий автоматизированного и автоматического управления и искусственного интеллекта. Особенностями указанных технологий является работа с большими объемами информации. Нарушение безопасности информации, обрабатываемой в интеллектуальных системах водного транспорта (неправомерный доступ, модификация, удаление и тому подобное несанкционированное воздействие) вызывает нарушение транспортной безопасности и, как следствие, безопасности критической информационной инфраструктуры и критической инфраструктуры страны, национальной безопасности. Для конвергентных технологий, используемых в интеллектуальных транспортных системах, характерен множественный и слабо формализуемый характер проявления последствий реализации угроз. В статье представлена модель оценки рисков информационной безопасности интеллектуальных систем водного транспорта, основанная на методах теории нечетких множеств и нечеткой логики, применение которых позволяет учесть вышеизложенные особенности внедряемых технологий. Иерархическая структура модели и применение методов теории нечетких множеств и нечеткой логики позволяет адаптировать модель под различные критерии рисков, типы входных данных и уровень детализации анализа рисков. Для представленной модели разработана методика оценки рисков информационной безопасности и приведен пример расчета риска. Разработанные модель и методика предназначены для построения системы управления рисками информационной безопасности автономного судоходства, реализующей технологии гибридного (дополненного, расширенного) интеллекта, предусматривающих управляемое людьми применение искусственного интеллекта.

Ключевые слова: информационная безопасность, водный транспорт, транспортная безопасность, естественный интеллект, искусственный интеллект, интеллектуальные системы, лингвистические переменные, системы агрегирования информации.

DOI: 10.20295/2412-9186-2024-10-01-7-17

▼ Введение

Интеллектуализация водного транспорта сопровождается расширением ландшафта угроз транспортной безопасности, обусловленных особенностями и слабостями внедряемых технологий, являющихся конвергенцией информационных и телекоммуникационных технологий, технологий автоматизированного и автоматического управления и искусственного интеллекта[1]. Особенностями указанных технологий является работа с большими объемами информации. Нарушение безопасности информации, обрабатываемой в интеллектуальных системах водного транспорта (неправомерный доступ, модификация, удаление и тому подобное несанкционированное воздействие) вызывает нарушение транспортной безопасности и, как следствие, безопасности критической информационной инфраструктуры и критической инфраструктуры страны, национальной безопасности [1, 2].

Функционирование интеллектуальных систем водного транспорта (далее — ИСВТ) обеспечивается с использованием информации глобальных навигационных спутниковых систем, автоматических идентификационных

[1] Транспортная стратегия Российской Федерации до 2030 года с прогнозом на период до 2035 года (утверждена распоряжением Правительства Российской Федерации от 27 ноября 2021 года № 3363-р).

© Баранов Л. А., Иванова Н. Д., Михалевич И. Ф., 2024

систем, систем радиолокационного наблюдения и технического зрения, электронных навигационно-картографических систем, сайтов и множества других источников. Для указанных источников информации и конвергентных технологий, используемых в ИСВТ, характерен множественный [3–6] и слабо формализуемый характер проявления последствий реализации угроз, о чем свидетельствуют результаты исследований, опубликованных, в частности, в[2, 3].

Необходимым условием обеспечения транспортной безопасности и эффективности функционирования ИСВТ является управление рисками информационной безопасности (далее — ИБ) [7].

В статье представлена модель оценки рисков ИБ ИСВТ, основанная на методах теории нечетких множеств и нечеткой логики, применение которых позволяет учесть вышеизложенные особенности внедряемых технологий.

1. Методика оценки рисков информационной безопасности на основе теории нечетких множеств и нечеткой логики

Система управления рисками ИБ ИСВТ предложена в [8]. Ее общая схема представлена на рис. 1. Схема отражает следующие сущности и процессы. Нарушители реализуют угрозы ИБ с использованием особенностей и слабостей (уязвимостей) ИСВТ, вследствие чего возникают риски нарушения свойств безопасности информации. Система оценки рисков ИБ ИСВТ формирует информационные свидетельства, достаточные для принятия решения о выборе мер обеспечения ИБ и снижения рисков. Используя результаты оценки рисков, система принятия мер обеспечения ИБ ИСВТ формирует и реализует меры, необходимые для поддержания требуемого уровня ИБ. Система мониторинга ИБ ИСВТ и базы данных уязвимостей и угроз безопасности информации (далее — УБИ) являются источниками входных данных для системы управления рисками ИБ.

Для автоматизации оценки рисков ИБ активно используются технологии искусственного интеллекта (далее — ИИ) [9, 10]. Однако их применение сдерживается, в частности, фактором недоверия, основанном на риске бесконтрольного функционирования ИИ. В связи с этим активно рассматривается вопрос применения технологий гибридного (дополненного, расширенного) интеллекта, основанных на сочетании возможностей человеческого (естественного) и искусственного интеллекта [11, 12], создания гибридных интеллектуальных систем [13]. Под гибридными интеллектуальными системами будем понимать системы, построенные с использованием технологий гибридного интеллекта. Гибридные интеллектуальные системы, для описания которых используется аппарат нечетких множеств и нечеткой логики, далее будем называть нечеткими системами.

Традиционно оценка рисков ИБ производится преимущественно с использованием методов экспертной оценки. Результат экспертной оценки представляет собой нечеткое знание, так как решение, принимаемое на основе мнений экспертов, почти всегда является компромиссом между противоречивыми требованиями, стремлением к широким возможностям создаваемой системы и низкой стоимостью. Для обоснования выбора лучшего решения используются следующие критерии качества результатов экспертной оценки (по методике, изложенной в [14]):

- коэффициент согласия (конкордации);
- коэффициент важности (предпочтительности) варианта решения.

Представим систему оценки рисков ИБ ИСВТ как иерархическую структуру, так как величина риска ИБ зависит от многих характеристик, таких как состояние защищенности системы от УБИ, возможности нарушителя ИБ, негативные последствия от успешной реализации УБИ и другие. Эти характеристики могут иметь как четкие, так и нечеткие оценки, выполненные экспертами с использованием различных шкал и критериев.

В [11, 12, 15, 16] заложена теоретическая основа для построения иерархических чело-

[2] Threat Landscape Transport Sector. ENISA, March 21, 2023. URL: https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape.

[3] Threat landscape for industrial automation systems. First half of 2023. URL: https://ics-cert.kaspersky.ru/publications/reports/2023/09/13/threat-landscape-for-industrial-automation-systems-statistics-for-h1-2023/.

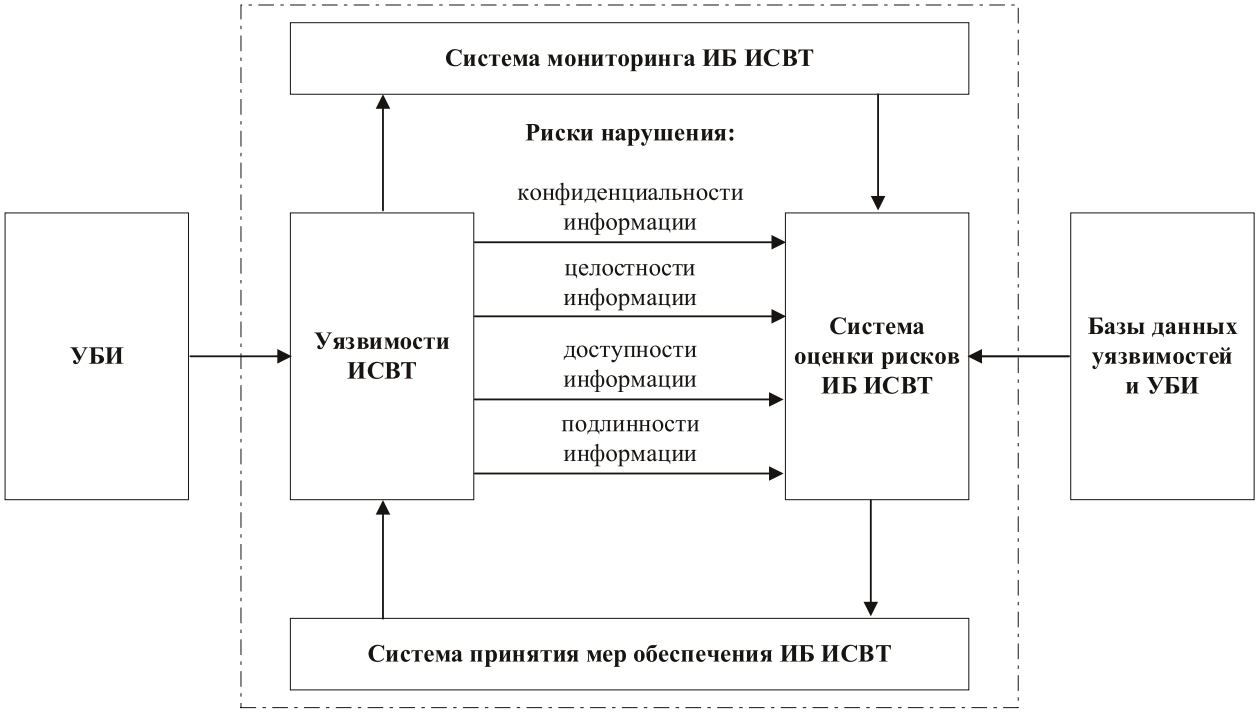

Рис. 1. Схема системы управления рисками ИБ ИСВТ

веко-компьютерных систем агрегирования информации, предлагаются соответствующие решения для объектов критической информационной инфраструктуры [11, 12] и социотехнических систем [16]. В [17] для оценки рисков ИБ технологий интернета вещей разработаны две нечеткие системы: оценки вероятности реализации УБИ и оценки вероятного ущерба.

В настоящей работе предлагается представить систему оценки рисков ИБ ИСВТ как нечеткую иерархическую систему агрегирования информации, входными данными для которой являются результаты экспертной оценки характеристик рисков, а в качестве инструмента для обработки и обобщения экспертных знаний использовать аппарат теории нечетких множеств и нечеткой логики.

Риск может быть определен лингвистической переменной (ЛП), представляющей кортеж вида (1):

$$< R, X, T^R >, \quad (1)$$

где R — «Риск» (имя ЛП);

X — множество действительных чисел из интервала [0;1];

T^R — нечеткое терм-множество, определенное на X.

T^R определяет множество всех возможных значений R. Согласно[4] риск ИБ может принимать одно из пяти лингвистических значений: «Очень низкий», «Низкий», «Средний», «Высокий», «Очень высокий». То есть: $T^R = \{t_i^R\}_{i=1}^5 = \{VL, L, M, H, VH\}$.

Каждый терм t_i^R нечеткого терм-множества T^R является нечетким множеством на множестве X и задается посредством функции принадлежности (ФП) $\mu^{t_i^R} : X \to [0;1]$. Значение $\mu^{t_i^R}(x)$ определяет степень принадлежности элемента x нечеткому множеству t_i^R на отрезке [0;1].

ФП может задаваться различными способами, одним из видов ФП является треугольная ФП, которая определяется в виде треугольника на графике, с возвышением в точке максимальной принадлежности. Треугольные ФП широко используются, особенно в приложениях реального времени, благодаря своей простоте, что обеспечивает высокую скорость вычислений [18]. Треугольная ФП задается

[4] ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection. Guidance on managing information security risks.

нечетким треугольным числом, представляющим собой тройку действительных чисел $< a, b, c >$ $(a \le b \le c)$ (2):

$$\mu^{t_i^R}(x) = \begin{cases} \dfrac{x-a}{b-a}, x \in [a,b] \\ \dfrac{x-c}{b-c}, x \in [b,c] \\ 0, x \notin [a,c] \end{cases} \quad (2)$$

При $b - a = c - b$ такая ФП называется симметричной треугольной ФП. Для ЛП «Риск», представимой терм-множеством $T^R = \{t_i^R\}_{i=1}^5 = \{VL, L, M, H, VH\}$ на $X = [0,1]$, термы могут характеризоваться следующими симметричными треугольными ФП (рис. 2): $\mu_{VL}^{T^R}(x)$, $\mu_L^{T^R}(x)$, $\mu_M^{T^R}(x)$, $\mu_H^{T^R}(x)$, $\mu_{VH}^{T^R}(x)$.

Если *A, B* — нечеткие множества, то операции пересечения (логическое И) и объединения (логическое ИЛИ) задаются для них следующим образом (3):

$$\begin{aligned} \mu^{A \cap B}(x) &= \min(\mu^A(x), \mu^B(x)) \\ \mu^{A \cup B}(x) &= \max(\mu^A(x), \mu^B(x)) \end{aligned} \quad (3)$$

Существуют множество методов и средств нечеткого логического вывода [19], которые используются для обработки нечеткой информации и принятия решений на основе нечетких данных. Для нечетких систем, в качестве входных данных использующих экспертное знание, наиболее распространенным методом нечеткого логического вывода являются продукционные правила. Примером таких правил в сфере обеспечения ИБ и оценки рисков ИБ являются матрицы риска[5].

Основными компонентами нечеткой системы являются [18, 20, 21]:

- фаззификатор, реализующий процедуру фаззификации исходных данных (четких или нечетких), то есть нахождения значений ФП нечеткому терм-множеству;
- машина вывода, которая с использованием операторов агрегирования информации генерирует нечеткие выходные данные на основе нечетких входных данных;
- дефаззификатор, реализующий процедуру, обратную фаззификации, для нахождения четкого значения величины риска.

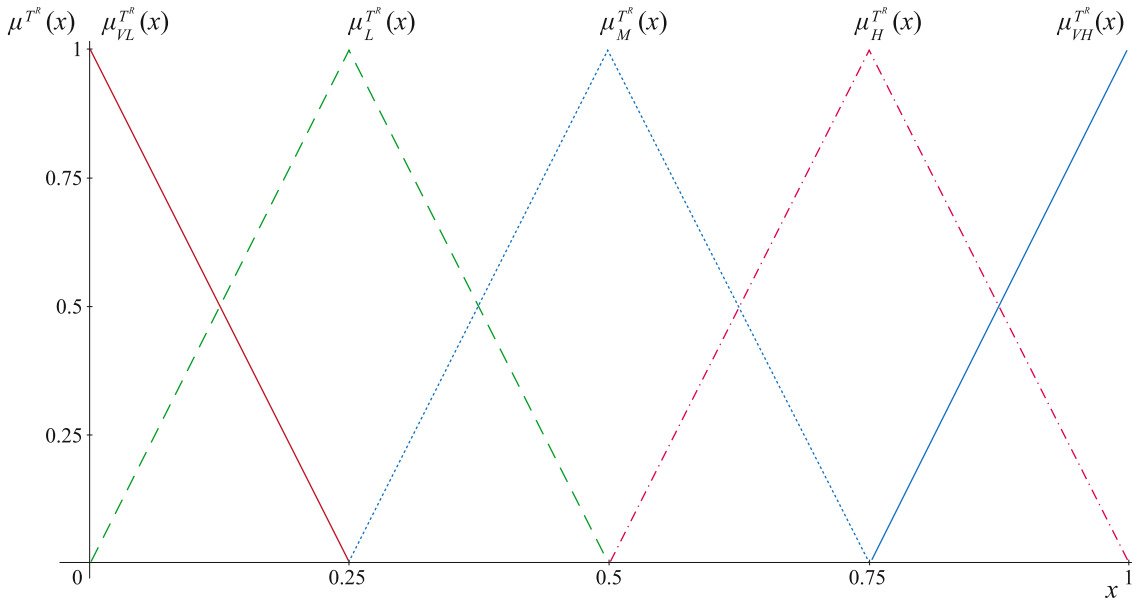

Рис. 2. Треугольные ФП термов ЛП «Риск»

[5] ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection. Guidance on managing information security risks.

В результате методика оценки рисков ИБ ИСВТ на основе теории нечетких множеств и нечеткой логики включает в себя следующую совокупность последовательных действий:

– построение модели системы оценки рисков ИБ ИСВТ как нечеткой иерархической системы агрегирования информации, в том числе определение характеристик рисков, оцениваемых экспертами;
– получение экспертных оценок характеристик рисков;
– фаззификация экспертных оценок характеристик рисков;
– применение операторов агрегирования информации (продукционных таблиц и операций (3) и получение нечетких выходных данных;
– дефаззификация полученного нечеткого значения величины риска.

2. Модель нечеткой системы оценки рисков информационной безопасности интеллектуальных систем водного транспорта

Модель нечеткой системы оценки рисков ИБ ИСВТ (рис. 3) представляет собой дерево, где каждая некорневая вершина — ЛП характеристики рисков ИБ ИСВТ, которой поставлено в соответствие некоторое терм-множество ее всевозможных значений. Назовем индикаторами концевые вершины дерева, для которых эксперты задают значения (на рис. 3 обозначены пунктирной линией). Каждой неконцевой вершине приписан некоторый оператор агрегирования информации, позволяющий на основе оценок состояния подчиненных вершин вычислять ее состояние.

В табл. 1 приведен перечень обозначений для рис. 3.

Основываясь на определениях международных и государственных стандартов в области менеджмента риска ИБ[6, 7] в предлагаемой модели в качестве основных характеристик

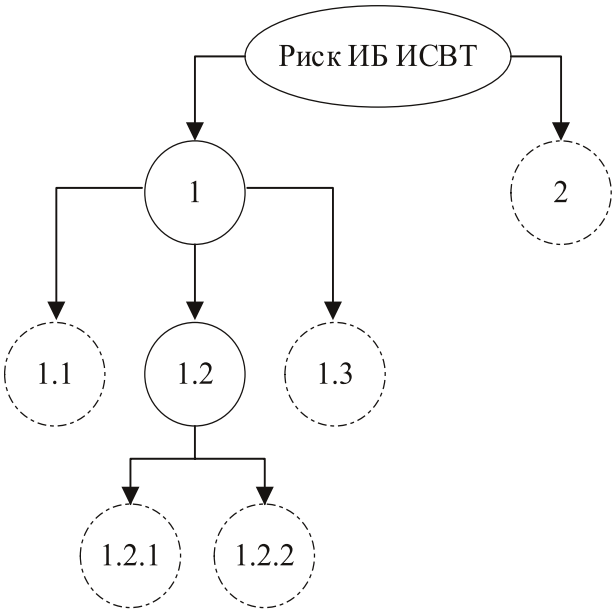

Рис. 3. Модель нечеткой системы оценки рисков ИБ ИСВТ

Таблица 1. Перечень характеристик рисков ИБ ИСВТ

Код показателя	Наименование показателя
1	Вероятность реализации УБИ
1.1	Возможности нарушителя, достаточные для использования уязвимости
1.2	Серьезность используемой уязвимости
1.2.1	Оценка уязвимости CVSS (Common Vulnerability Scoring System)
1.2.2	Статистика использования уязвимости
1.3	Защищенность системы
2	Негативные последствия реализации УБИ

для расчета рисков ИБ ИСВТ выбраны следующие два показателя:

– вероятность реализации УБИ;
– негативные последствия реализации УБИ.

Показатель характеризуется субпоказателями (подчиненными вершинами), которые вносят вклад в значение соответствующего показателя. Для показателя «Возможность реализации УБИ» применимы следующие субпоказатели:

– возможности нарушителя, достаточные для использования уязвимости;
– серьезность используемой уязвимости;
– защищенность системы.

[6] ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection. Guidance on managing information security risks.

[7] ГОСТ Р 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

Таблица 2. Индикаторы модели нечеткой системы оценки рисков ИБ ИСВТ

Наименование индикатора	Используемые для оценки данные или соответствующий методический документ	Методика определения числового значения индикатора
Возможности нарушителя, достаточные для использования уязвимости	Оценка возможностей нарушителя (ВН) в соответствии с методикой[8]	$x^{ВН} = \begin{cases} 0,0 - \textit{если базовые возможности}; \\ 0,33 - \textit{если базовые повышенные возможности}; \\ 0,66 - \textit{если средние возможности}; \\ 1,0 - \textit{если высокие возможности}. \end{cases}$
Оценка уязвимости CVSS	Оценка CVSS в соответствии с методикой[9]	$x^{CVSS} = \frac{CVSS}{10}$, где $CVSS \in [0;10]$ — оценка CVSS
Статистика использования уязвимости	Оценка на основе данных годовых отчетов и рейтингов уязвимостей	$x^{стат} = \begin{cases} 0,0 - \textit{если очень редко}; \\ 0,25 - \textit{если редко}; \\ 0,5, - \textit{если достаточно часто}; \\ 0,75 - \textit{если часто}; \\ 1,0 - \textit{если очень часто}. \end{cases}$
Защищенность системы	Оценка реализованных мер защиты (МЗ) согласно требованиям ФСТЭК России[10]	$x^{МЗ} = \begin{cases} 0,0 - \textit{если очень низкий уровень защищенности}; \\ 0,25 - \textit{если низкий уровень защищенности}; \\ 0,5 - \textit{если средний уровень защищенности}; \\ 0,75 - \textit{если высокий уровень защищенности}; \\ 1,0 - \textit{если очень высокий уровень защищенности}. \end{cases}$
Негативные последствия реализации УБИ	Оценка негативных последствий (НП) в соответствии с методикой[11]	$x^{НП} = \begin{cases} 0,0 - \textit{если незначительные негативные последствия}; \\ 0,25 - \textit{если значительные негативные последствия}; \\ 0,5 - \textit{если серьезные негативные последствия}; \\ 0,75 - \textit{если критические негативные последствия}; \\ 1,0 - \textit{если катастрофические негативные последствия}. \end{cases}$

В свою очередь, серьезность используемой уязвимости характеризуется оценкой уязвимости CVSS и статистикой использования уязвимости.

Индикаторы нечеткой модели системы оценки рисков ИБ ИСВТ и способы их оценки представлены в табл. 2.

Значения индикаторов определяются методом экспертной оценки. Для обоснования оценок экспертов могут быть приняты критерии качества, оговоренные ранее.

[8] Методический документ. Методика оценки угроз безопасности информации: утверждена ФСТЭК России 05.02.2021.

[9] Common Vulnerability Scoring System version 4.0: Specification Document / Forum of Incident Response and Security Teams (FIRST).

[10] Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (утверждены Приказом ФСТЭК России от 25.12.2017. № 239).

[11] Проект национального стандарта ГОСТ Р ИСО/МЭК 27005. Информационная безопасность, кибербезопасность и защита частной жизни. Руководство по управлению рисками информационной безопасности. Требования и руководства. URL: https://fstec.ru/tk-362/standarty/proekty/proekt-natsionalnogo-standarta-gost-r-iso-mek-27005?ysclid=lsakd3b9i41408646.

3. Пример оценки риска информационной безопасности

Пусть на вход нечеткой системы поступают следующие утверждения (значения индикаторов):

- возможности нарушителя: базовые повышенные;
- оценка уязвимости CVSS: 6;
- статистика использования уязвимости: часто;
- защищенность системы: средняя;
- негативные последствия реализации УБИ: значительные.

Операция агрегирования информации реализуется с использованием продукционных таблиц, составленных экспертами, и операций логического И и логического ИЛИ (3). Исходные данные оцениваются и нормализуются согласно табл. 2 при $X = [0;1]$. В качестве ФП выбраны симметричные треугольные ФП (см. рис. 2), $T = \{VL; L; M; H; VH\}$ для всех ЛП.

Соответствующие числовые значения исходных данных на отрезке [0;1]:

– переменная «Возможности нарушителя, достаточные для использования уязвимости»: $x^{ВН} = 0{,}33$;
– переменная «Оценка уязвимости CVSS»: $x^{CVSS} = 0{,}6$;
– переменная «Статистика использования уязвимости»: $x^{стат} = 0{,}75$;
– переменная «Защищенность системы»: $x^{МЗ} = 0{,}5$;
– переменная «Последствия успешной реализации УБИ»: $x^{НП} = 0{,}25$.

Ниже приведены результаты фаззификации для каждой ЛП с использованием ФП, представленных на рис. 2:

$$\begin{gathered}
\mu_{VL}^{T^{ВН}}(0{,}33) = 0;\ \mu_{L}^{T^{ВН}}(0{,}33) = 0{,}68;\ \mu_{M}^{T^{ВН}}(0{,}33) = 0{,}32; \\
\mu_{H}^{T^{ВН}}(0{,}33) = 0;\ \mu_{VH}^{T^{ВН}}(0{,}33) = 0 \\
\mu_{VL}^{T^{CVSS}}(0{,}6) = 0;\ \mu_{L}^{T^{CVSS}}(0{,}6) = 0;\ \mu_{M}^{T^{CVSS}}(0{,}6) = 0{,}65; \\
\mu_{H}^{T^{CVSS}}(0{,}6) = 0{,}35;\ \mu_{VH}^{T^{CVSS}}(0{,}6) = 0 \\
\mu_{VL}^{T^{стат}}(0{,}75) = 0;\ \mu_{L}^{T^{стат}}(0{,}75) = 0;\ \mu_{M}^{T^{стат}}(0{,}75) = 0; \\
\mu_{H}^{T^{стат}}(0{,}75) = 1;\ \mu_{VH}^{T^{стат}}(0{,}75) = 0 \\
\mu_{VL}^{T^{МЗ}}(0{,}5) = 0;\ \mu_{L}^{T^{МЗ}}(0{,}5) = 0;\ \mu_{M}^{T^{МЗ}}(0{,}5) = 1; \\
\mu_{H}^{T^{МЗ}}(0{,}5) = 0;\ \mu_{VH}^{T^{МЗ}}(0{,}5) = 0 \\
\mu_{VL}^{T^{НП}}(0{,}25) = 0;\ \mu_{L}^{T^{НП}}(0{,}25) = 1;\ \mu_{M}^{T^{НП}}(0{,}25) = 0; \\
\mu_{H}^{T^{НП}}(0{,}25) = 0;\ \mu_{VH}^{T^{НП}}(0{,}25) = 0
\end{gathered} \quad (4)$$

В (4) $\mu_{H}^{T^{CVSS}}(0{,}6) = 0{,}35$ означает, что значение ЛП «Оценка уязвимости CVSS» $t^{CVSS} = H$ («Высокая») соответствует $x^{CVSS} = 0{,}6$ со степенью уверенности, определяемой значением ФП $\mu_{H}^{T^{CVSS}}(0{,}6) = 0{,}35$ на отрезке [0;1].

Значение ЛП «Серьезность уязвимости» $t^{СУ}$ определяется ЛП «Оценка уязвимости CVSS» и «Статистика использования уязвимости» с помощью продукционных правил (табл. 3).

Таблица 3. Продукционные правила для определения значения $t^{СУ}$ (фрагмент)

№ правила	t^{CVSS}	$t^{стат}$	$t^{СУ}$
	…		
14	M	H	M
	…		
19	H	H	H
	…		

Согласно базе продукционных правил (табл. 3) и с применением операции логического И получаются следующие значения ФП для соответствующих значений $t^{СУ}$:

– правило 14:
$t^{СУ} = M : \mu_{M}^{T^{СУ}} = \min(0{,}65; 1) = 0{,}65$;
– правило 19:
$t^{СУ} = H : \mu_{H}^{T^{СУ}} = \min(0{,}35; 1) = 0{,}35$.

Значение ЛП «Вероятность реализации УБИ» $t^{ВУБИ}$ определяется ЛП «Возможности нарушителя, достаточные для использования уязвимости», «Серьезность уязвимости» и «Защищенность системы» с помощью продукционных правил (табл. 4).

Таблица 4. Продукционные правила для определения значения $t^{ВУБИ}$ (фрагмент)

№ правила	$t^{ВН}$	$t^{СУ}$	$t^{МЗ}$	$t^{ВУБИ}$
		…		
38	L	M	M	H
		…		
43	L	H	M	H
		..		
63	M	M	M	M
		…		
68	M	H	M	M
		…		

Аналогично получаются следующие значения $t^{ВУБИ}$:

– правило 38:
$t^{ВУБИ} = H : \mu_{H_{38}}^{T^{ВУБИ}} = \min(0{,}68; 0{,}65; 1) = 0{,}65$;
– правило 43:
$t^{ВУБИ} = H : \mu_{H_{43}}^{T^{ВУБИ}} = \min(0{,}68; 0{,}35; 1) = 0{,}35$;
– правило 63:
$t^{ВУБИ} = M : \mu_{M_{63}}^{T^{ВУБИ}} = \min(0{,}32; 0{,}65; 1) = 0{,}32$;
– правило 68:
$t^{ВУБИ} = M : \mu_{M_{68}}^{T^{ВУБИ}} = \min(0{,}32; 0{,}35; 1) = 0{,}32$.

Правила 38, 43 и 63, 68 дают одинаковые значения $t^{ВУБИ} = H$ и $t^{ВУБИ} = M$ соответственно. Очевидно, что $\mu_{M}^{T^{ВУБИ}} = \mu_{M_{63}}^{T^{ВУБИ}} = \mu_{M_{68}}^{T^{ВУБИ}} = 0{,}32$. Итоговое значение $\mu_{H}^{T^{ВУБИ}}$ определяется с использованием операции логического ИЛИ (5):

$$t^{ВУБИ} = H : \mu_{H}^{T^{ВУБИ}} = \max(0{,}65; 0{,}35) = 0{,}65. \quad (5)$$

Значение ЛП «Риск» t^{R} определяется ЛП «Вероятность реализации УБИ» и «Негативные последствия реализации УБИ» с помощью

продукционных правил (табл. 5), заданных на основе матрицы риска, предложенной в [12].

Таблица 5. Продукционные правила для определения значения t^R (фрагмент)

№ правила	$t^{ВУБИ}$	$t^{НП}$	t^R
	…		
12	M	L	L
	…		
17	H	L	M
	…		

Согласно базе продукционных правил (табл. 5) и с применением операции логического И получаются следующие значения ФП для соответствующих значений t^R:

– правило 12:

$t^R = L : \mu_L^{T^R} = \min(0,32; 1) = 0,32;$

– правило 17:

$t^R = M : \mu_M^{T^R} = \min(0,65; 1) = 0,65.$

Выполненная нечеткая оценка риска (нахождение t^R) означает, что искомый риск определяется как «Низкий» со степенью уверенности 0,32 и как «Средний» со степенью уверенности 0,65. Следует отметить, что понятие степени уверенности в принадлежности нечеткому множеству (значение ФП в нечеткой логике) не связано с понятием вероятности в теории вероятностей [22].

Дефаззификация производится путем вычисления средневзвешенного значения x^R [23]:

$$x^R = \frac{x_{\mu_L^{T^R}\max} \cdot \mu_L^{T^R} + x_{\mu_M^{T^R}\max} \cdot \mu_M^{T^R}}{\mu_L^{T^R} + \mu_M^{T^R}} = \\ = \frac{0,25 \cdot 0,32 + 0,5 \cdot 0,65}{0,32 + 0,65} = 0,42, \quad (6)$$

где $x_{\mu_L^{T^R}\max} = 0,25$ — значение, при котором $\mu_L^{T^R}(x)$ достигает максимума (см. рис. 2);

$x_{\mu_M^{T^R}\max} = 0,5$ — значение, при котором $\mu_M^{T^R}(x)$ достигает максимума (см. рис. 2).

В результате итоговое значение риска x^R при заданных исходных данных равно 0,42 на отрезке [0;1], где значение 0 соответствует минимальному значению риска, а 1 — максимальному.

Если, согласно действующей политике ИБ, риск $x^R = 0,42$ признается приемлемым, система защиты остается в неизменном состоянии. В случае если риск признается неприемлемым, система принятия мер обеспечения ИБ ИСВТ вырабатывает и реализует защитные мероприятия. При этом предполагается, что внесение изменений в систему защиты может повлиять на функциональность ИСВТ, что также является риском. Кроме того, даже после введения соответствующих мер защиты может существовать остаточный риск. Остаточные риски и риски, признанные приемлемыми, должны отслеживаться и контролироваться системой мониторинга ИБ ИСВТ (см. рис. 1).

Заключение

Оценка рисков ИБ является важным инструментом в обеспечении ИБ ИСВТ и предназначена для формирования полных и достоверных информационных свидетельств, достаточных для принятия решения о необходимости обработки выявленных рисков ИБ. В условиях непрерывного развития технологий ИСВТ и возникновения новых видов уязвимостей и угроз безопасности информации, автоматизация процесса оценки рисков ИБ ИСВТ является необходимой.

Разработанная модель нечеткой системы оценки рисков ИБ ИСВТ представляет собой иерархическую структуру в виде дерева, где каждая вершина соответствует лингвистической переменной, характеризующей риски ИБ ИСВТ. Значения лингвистических переменных концевых вершин дерева определяются методом экспертной оценки, а значения лингвистических переменных вершин более высокого уровня — методами нечетких множеств и нечеткой логики, что определяет разработанную модель системы оценки рисков как основанную на технологиях гибридного интеллекта.

[12] Проект национального стандарта ГОСТ Р ИСО/МЭК 27005. Информационная безопасность, кибербезопасность и защита частной жизни. Руководство по управлению рисками информационной безопасности. Требования и руководства. URL: https://fstec.ru/tk-362/standarty/proekty/proekt-natsionalnogo-standarta-gost-r-iso-mek-27005?ysclid=lsakd3b9i41408646

Предложенный метод оценки рисков ИБ учитывает множество факторов, необходимых для рассмотрения при оценке рисков ИБ ИСВТ, среди которых:

- возможности нарушителя, достаточные для использования имеющихся в ИСВТ уязвимостей;
- применяемые в ИСВТ меры защиты информации;
- оценка уязвимостей CVSS;
- статистика использования уязвимостей;
- негативные последствия успешной реализации УБИ.

Преимуществом разработанной модели системы оценки рисков ИБ является ее адаптируемость под различные критерии рисков, типы входных данных и степень необходимой детализации анализа рисков.

Дальнейшее развитие этого метода предполагает интеграцию экспертной оценки рисков ИБ с методами машинного обучения для создания более эффективной системы оценки рисков ИБ. ▲

Библиографический список

1. Mikhalevich I. F. Problemic Issues of Deploying Cooperative Intelligent Transport Systems During of Digital Transformation. In 2021 International Conference "Systems of Signals Generating and Processing in the Field of on Board Communications". DOI: 10.1109/IEEECONF51389.2021.9415999.
2. Баранов Л. А. Иванова Н. Д., Михалевич И. Ф. и др. Информационная безопасность системы автономного судовождения в контексте специфических для интеллектуальных транспортных систем угроз // Сборник трудов международной научной конференции «Проблемы управления безопасностью сложных систем». Москва, 13 декабря 2023 г. (статья принята к публикации).
3. Andrej Androjna, Marko Perkovic. Impact of Spoofing of Navigation Systems on Maritime Situational Awareness. September 2021. Transactions on Maritime Science 10(2). DOI: 10.7225/toms.v10.n02.w08.
4. Goudosis A., Katsikas S. Secure Automatic Identification System (SecAIS): Proof-of-Concept Implementation // Journal of Marine Science and Engieneering. 2022, 10, 805. J. Mar. Sci. Eng. 2022, 10, 805. DOI: 10.3390/jmse10060805.
5. Svilicic B., Brčić D., Žuškin S., et al. (2019, March). Raising Awareness on Cyber Security of ECDIS // TransNav, The International Journal on Marine Navigation and Safety of Sea Transportation. 2019. Vol. 13, no. 1. P. 231–236. DOI: 10.12716/1001.13.01.24.
6. Karahalios H. Appraisal of a Ship's Cybersecurity efficiency: the case of piracy // J Transp Secur. 2020. Vol. 13. P. 179–201. DOI 10.1007/s12198-020-00223-1.
7. Kavallieratos G., Katsikas S. Managing Cyber Security Risks of the Cyber-Enabled Ship // Journal of Marine Science and Engineering. 2020. No. 8 (768). 19 p. DOI: 10.3390/jmse8100768/.
8. Иванова Н. Д., Михалевич И. Ф., Якунчиков В. В. Управление рисками информационной безопасности интеллектуальных транспортных систем внутреннего водного транспорта // Сборник трудов Международной научно-практической конференции «Транспорт России: проблемы и перспективы». Санкт-Петербург, 14–15 ноября 2023 г.
9. Kharchenko V., Illiashenko O., Fesenko H., et al. AI Cybersecurity Assurance for Autonomous Transport Systems: Scenario, Model, and IMECA-Based Analysis. In: Dziech, A., Mees, W., Niemiec, M. (eds) Multimedia Communications, Services and Security. MCSS 2022. Communications in Computer and Information Science. 2022. Vol. 1689. Pp 66–79. Springer, Cham. DOI: 10.1007/978–3–031–20215–5_6.
10. Kharbanda Varun. Journal: Application of Artificial Intelligence in Cyber security (IJSPPC). 2023. Vol. 15, no. 1. P. 1–13. DOI: org/10.4018/ijsppc.318676.
11. Ryjov A. P., Mikhalevich I. F. Hybrid intelligence framework for improvement of information security of critical infrastructures. In book: Handbook of Research on Cyber Crime and Information Privacy. Hershey, PA, US 2021. DOI: 10.4018/978–1–7998–5728–0.ch016.
12. Mikhalevich I. F., Ryjov A. P. Augmented Intelligence Framework for Protecting against Cyberattacks, 2018 // Engineering and Telecommunication (EnT-MIPT), Moscow, Russia, 2018. P. 143–145. DOI: 10.1109/EnT-MIPT.2018.00039.
13. Карякин В. В. Гибридные интеллектуальные системы как симбиоз естественного и искусственного интеллектов // Россия: тенденции и перспективы развития. 2022. № 17 (1). С. 652–655.
14. Лецкий Э. К., Панкратов В. И., Яковлев В. В. Информационные технологии на железнодорожном транспорте / под ред. Э. К. Лецкого, Э. С. Поддавашкина, В. В. Яковлева. М.: УМК МПС России, 2000. 678 с.
15. Рыжов А. П. Об агрегировании информации в нечетких иерархических системах // Интеллектуальные системы. 2001. Т. 6, Вып. 1–4. С. 69–79.
16. Рыжов А. П. Оценка и мониторинг процессов в социотехнических системах и связанные с ними задачи // Интеллектуальные системы. 2001. Т. 22, Вып. 2. С. 129–140.
17. Kerimkhulle S., Dildebayeva Z., Tokhmetov F., et al. Fuzzy Logic and Its Application in the Assessment of Information Security Risk of Industrial Internet of

Things, Symmetry. 2023. 15 (10). 1958. DOI: 10.3390/sym15101958.
18. Azam M. H., Hasan M. H., Hassan S., et al. Fuzzy Type-1 Triangular Membership Function Approximation Using Fuzzy C–Means, 2020 // International Conference on Computational Intelligence (ICCI), Bandar Seri Iskandar, Malaysia, 2020. P. 115–120. DOI: 10.1109/ICCI51257.2020.9247773.
19. Карелин В. П. Методы и средства нечеткого логического вывода, представления и защиты данных в интеллектуальных системах управления и поддержки принятия решений // Вестник ТИУиЭ. 2016. № 2 (24). С. 5.
20. Cahyaningrum Y., Suryono S., Warsito B. Fuzzy-Expert System for Indicator and Quality Evaluation of Teaching and Learning Processes Online Study Programs // The 6th International Conference on Energy, Environment, Epidemiology, and Information System (ICENIS 2021). 2021. Vol. 317. 11 p. DOI: 10.1051/e3sconf/202131705021.
21. Rizvi S. S., Mitchell J., Razaque A., et al. A fuzzy inference system (FIS) to evaluate the security readiness of cloud service providers // Journal of Cloud Computing. 2020. № 9 (1). 17 p. DOI:10.1186/s13677–020–00192–9.
22. Dubois D., Prade H. Fuzzy sets and probability: misunderstandings, bridges and gaps // 2nd IEEE International Conference on Fuzzy Systems (FUZZY 1993), IEEE, Mar 1993, San Francisco, United States. P. 1059–1068. DOI: ff10.1109/FUZZY.1993.327367ff.
23. Jain D., Sharma S. K., Dhiman P. Comparative Analysis of Defuzzification Techniques for Fuzzy Output // Journal of algebraic statistics. 2022. Vol. 13, no. 13. P. 874–882.

TRANSPORT AUTOMATION RESEARCH. 2024. Vol. 10, no. 1. P. 7–17
DOI: 10.20295/2412-9186-2024-10-01-7-17

Fuzzy system for assessing the information security risk of intelligent water transport systems

Information about authors
Baranov L. A., Doctor in Engineering, Head of the Department.
E-mail: baranov.miit@gmail.com
Ivanova N. D., Postgraduate Student. E-mail: ivanovand.nina@yandex.ru
Mikhalevich I. F., PhD in Engineering, Associate Professor, Senior Researcher. E-mail: mif-orelf@mail.ru

Russian University of Transport (MIIT), Department of Control and Protection of Information, Moscow

Abstract. The intellectualization of water transport is accompanied by an expansion of the landscape of threats to transport security, caused by the characteristics and weaknesses of the technologies being introduced, which are the convergence of information and telecommunication technologies, automated and automatic control technologies and artificial intelligence. The peculiarity of these technologies is working with large volumes of information. Violation of the security of information processed in intelligent systems of water transport (illegal access, modification, deletion and similar unauthorized influence) causes a violation of transport security and, as a consequence, the security of critical information infrastructure and the country's critical infrastructure, national security. Convergent technologies used in intelligent transport systems are characterized by multiple and poorly formalized manifestations of the consequences of threats. The article presents a model for assessing the risks of information security of intelligent water transport systems, based on the methods of the theory of fuzzy sets and fuzzy logic, the use of which makes it possible to take into account the above-mentioned features of the technologies being implemented. The hierarchical structure of the model and the use of fuzzy set theory and fuzzy logic methods make it possible to adapt the model to various risk criteria, types of input data and the level of detail of risk analysis. For the presented model, a methodology for assessing information security risks has been developed and an example of risk calculation is given. The developed model and methodology are intended to build an information security risk management system for autonomous shipping, implementing technologies of hybrid (augmented, extended) intelligence, providing for the use of artificial intelligence controlled by people.

Keywords: transport security; natural intelligence; artificial intelligence; intelligent systems; linguistic variables; information aggregation systems.

References

1. Mikhalevich I. F. Problemic Issues of Deploying Cooperative Intelligent Transport Systems During of Digital Transformation. In 2021 International Conference "Systems of Signals Generating and Processing in the Field of on Board Communications". DOI: 10.1109/IEEECONF51389.2021.9415999.
2. Baranov L. A., Mihalevich I. F., Ivanova N. D., Sokolov S. S. Informacionnaya bezopasnost' sistemy avtonomnogo sudovozhdeniya v kontekste specificheskih dlya intellektual'nyh transportnyh sistem ugroz // Sbornik trudov mezhdunarodnoj nauchnoj konferencii "Problemy upravleniya bezopasnost'yu slozhnyh sistem", Moscow, Russia, December 13, 2023 (accepted for publication) (In Russian)
3. Andrej Androjna, Marko Perkovic. Impact of Spoofing of Navigation Systems on Maritime Situational Awareness. September 2021. Transactions on Maritime Science 10(2). DOI: 10.7225/toms.v10.n02.w08.
4. Goudosis A., Katsikas S. Secure Automatic Identification System (SecAIS): Proof-of-Concept Implementation. Journal of Marine Science and Engieneering. 2022. 10. 805. J. Mar. Sci. Eng. 2022. 10. 805. DOI: 10.3390/jmse10060805.
5. Svilicic B., Brčić D., Žuškin S., et al. (2019, March). Raising Awareness on Cyber Security of ECDIS. TransNav, The International Journal on Marine Navigation and Safety of Sea Transportation. 13 (1). 231–236. DOI: 10.12716/1001.13.01.24.
6. Karahalios H. Appraisal of a Ship's Cybersecurity efficiency: the case of piracy. J Transp Secur 13. 179–201 (2020). DOI: 10.1007/s12198–020–00223–1.
7. Kavallieratos G., Katsikas S. Managing Cyber Security Risks of the Cyber-Enabled Ship // Journal of Marine Science and Engineering. 2020. № 8 (768). 19 c. DOI: 10.3390/jmse8100768/.
8. Ivanova N. D., Mihalevich I. F., Jakunchikov V. V. Upravlenie riskami informacionnoj bezopasnosti intellektual'nyh transportnyh sistem vnutrennego vodnogo transporta // Sbornik trudov Mezhdunarodnoj nauchno-prakticheskoj konferencii "Transport Rossii: problemy i perspektivy". Sankt-Peterburg, 14–15 nojabrja 2023 g. (In Russian)
9. Kharchenko V., Illiashenko O., Fesenko H., et al. (2022). AI Cybersecurity Assurance for Autonomous Transport Systems: Scenario, Model, and IMECA-Based Analysis. In: Dziech, A., Mees, W., Niemiec, M. (eds) Multimedia Communications, Services and Security. MCSS 2022. Communications in Computer and Information Science. Vol. 1689. P. 66–79. Springer, Cham. DOI: 10.1007/978–3–031–20215–5_6.

10. Kharbanda Varun. "Journal: Application of Artificial Intelligence in Cyber security." IJSPPC. 2023. Vol. 15, no. 1. P. 1–13. DOI: org/10.4018/ijsppc.318676.
11. Ryjov A. P., Mikhalevich I. F., "Hybrid intelligence framework for improvement of information security of critical infrastructures". In book: Handbook of Research on Cyber Crime and Information Privacy. Hershey, PA, US. 2021. DOI: 10.4018/978–1–7998–5728–0.ch016.
12. Mikhalevich I. F., Ryjov A. P. "Augmented Intelligence Framework for Protecting against Cyberattacks". 2018 Engineering and Telecommunication (EnT-MIPT), Moscow, Russia. 2018. P. 143–145. DOI: 10.1109/EnT-MIPT.2018.00039.
13. Karyakin V. V. Gibridnye intellektual'nye sistemy kak simbioz estestvennogo i iskusstvennogo intellektov // Rossiya: tendencii i perspektivy razvitiya. 2022. № 17 (1). S. 652–655. (In Russian)
14. Leckij Je. K., Pankratov V. I., Jakovlev V. V. Informacionnye tehnologii na zheleznodorozhnom transporte / pod red. Je. K. Leckogo, Je. S. Poddavashkina, V. V. Jakovleva. M.: UMK MPS Rossii, 2000. 678 s. (In Russian)
15. Ryjov A. P. Ob agregirovanii informacii v nechetkih ierarhicheskih sistemah // Intellektual'nye sistemy. 2001. T. 6, Issue. 1–4. S. 69–79. (In Russian)
16. Ryjov A. P. Ocenka i monitoring processov v sociotekhnicheskih sistemah i svyazannye s nimi zadachi // Intellektual'nye sistemy. 2001. T. 22, Issue 2. S. 129–140. (In Russian)
17. Kerimkhulle S., Dildebayeva Z., Tokhmetov F., et al. "Fuzzy Logic and Its Application in the Assessment of Information Security Risk of Industrial Internet of Things", Symmetry 2023, 15 (10), 1958. DOI: 10.3390/sym15101958.
18. Azam M. H., Hasan M. H., Hassan S., et al. Fuzzy Type-1 Triangular Membership Function Approximation Using Fuzzy C–Means, 2020 International Conference on Computational Intelligence (ICCI), Bandar Seri Iskandar, Malaysia, 2020, P. 115–120. DOI: 10.1109/ICCI51257.2020.9247773.
19. Karelin V. P. Metody i sredstva nechyotkogo logicheskogo vyvoda, predstavleniya i zashchity dannyh v intellektual'nyh sistemah upravleniya i podderzhki prinyatiya reshenij // Vestnik TIUiE. 2016. № 2 (24). 5 s. (In Russian)
20. Cahyaningrum Y., Suryono S., Warsito B. Fuzzy-Expert System for Indicator and Quality Evaluation of Teaching and Learning Processes Online Study Programs // The 6th International Conference on Energy, Environment, Epidemiology, and Information System (ICENIS 2021). 2021. Vol. 317. 11 p. DOI: 10.1051/e3sconf/202131705021.
21. Rizvi S. S., Mitchell J., Razaque A., et al. A fuzzy inference system (FIS) to evaluate the security readiness of cloud service providers // Journal of Cloud Computing. 2020. № 9 (1). 17 p. DOI:10.1186/s13677–020–00192–9.
22. Dubois D., Prade H. Fuzzy sets and probability: misunderstandings, bridges and gaps // 2nd IEEE International Conference on Fuzzy Systems (FUZZY 1993), IEEE, Mar 1993, San Francisco, United States. P. 1059–1068. DOI: ff10.1109/FUZZY.1993.327367ff.
23. Jain D., Sharma S. K., Dhiman P. Comparative Analysis of Defuzzification Techniques for Fuzzy Output // JOURNAL OF ALGEBRAIC STATISTICS. 2022. Vol. 13, no. 13. P. 874–882.