УДК 330.46

doi: 10.53816/23061456_2025_3–4_31

МЕТОДИКА ОЦЕНИВАНИЯ РИСКОВ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВОЕННОГО УПРАВЛЕНИЯ

METHODOLOGY FOR ASSESSING RISKS OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES APPLICATION IN THE INFORMATION AND ANALYTICAL ACTIVITIES OF MILITARY AUTHORITIES

Д-р экон. наук А.Е. Николаев, И.А. Абрамов

D.Sc. A.E. Nikolaev, I.A. Abramov

Военный университет радиоэлектроники

Статья посвящена вопросу оценивания рисков применения технологий искусственного интеллекта в информационно-аналитической деятельности органов военного управления. Дано теоретическое описание категории «риск» и уточнено её значение для среды применения технологии. Определены системность риска и его зависимость от подсистем системы искусственного интеллекта, необходимость его исследования посредством учета созависимого риска. Дана классификация вероятных рисков, частных факторов и описывающих их угроз. Разработана система показателей оценивания рисков применения технологий искусственного интеллекта в информационно-аналитической деятельности органов военного управления, предложен порядок их расчета.

Ключевые слова: технологии искусственного интеллекта, информационно-аналитическая деятельность, органы военного управления, риск применения, фактор риска.

The article is devoted to the issue of assessing risks of using artificial intelligence technologies in the information and analytical activities of military authorities. It provides a theoretical description of the «risk» category and clarifies its significance for the technology application environment. The systemic nature of the risk and its dependence on the subsystems of the artificial intelligence system are determined, the need for its research is determined by considering the codependent risk. The classification of probable risks, particular factors and threats describing them is given. A system of indicators for assessing risks of using artificial intelligence technologies in the information and analytical activities of military authorities has been developed, and the procedure for calculating them has been proposed.

Keywords: artificial intelligence technologies, information and analytical activities, military authorities, application risk, risk factor.

В настоящее время искусственный интеллект (ИИ) является одной из передовых технологий, применение которой предоставляет пользователям высокие функциональные возможности и обеспечивает конкурентные преимущества в любой прикладной среде. При этом вопрос использования данных технологий в деятельности вооруженных сил (ВС) в современных условиях военно-политической обстановки приобретает все большую актуальность. Их внедрение и приме-

нение в интересах ВС рассматривается и реализуется практически повсеместно. Представляя собой частный способ обработки информации, ИИ может выступать важным инструментом обеспечения информационно-аналитической деятельности (ИАД) органов военного управления (ОВУ).

Следует отметить, что наряду с высокими возможностями по обработке и анализу информации, применение данной, еще относительно «молодой» технологии может сопровождаться проявлением непредвиденных событий, возникновение которых приводит к невозможности достижения задач ИАД ОВУ. Их можно описать как риски использования ИИ.

Под термином «риск» в широком смысле рассматривается возможность возникновения каких-либо неблагоприятных событий, которые препятствуют достижению запланированной цели операции, обуславливают неуспех планируемых действий, опасность негативного исхода. Применительно к предметной области использования технологий искусственного интеллекта в информационно-аналитической деятельности органов военного управления под риском подразумевается возможность наступления такого события, когда по причине одного или совокупности факторов становится невозможным выполнение информационных задач. При этом под фактором риска рассматриваются условия, которые могут вызвать или способствовать проявлению подобного события.

Следует отметить, что в целом риск представляет собой исключительно системный показатель. Его системность состоит в том, что для сложного изделия (организационно-технической системы) он определяется не только безотказностью отдельных компонентов и подсистем, но и их взаимным влиянием. Поэтому риски технологии необходимо рассматривать исходя из того, что она является одной из обеспечивающих подсистем системы ИИ, наряду с другими её подсистемами, к которым можно отнести саму технологию, техническое обеспечение (аппаратный комплекс), а также информационное обеспечение и персонал [1, 2]. Порядок организации взаимодействия указанных элементов обуславливает наличие между ними вероятности созависимого риска. Это когда отказ одного из элементов системы приводит к отказу всех её элементов и системы в целом. Следовательно, оценивание рисков технологии ИИ в ИАД ОВУ не может реализовываться обособленно. Следует рассматривать вероятность проявления всех факторов созависимого риска, приводящих к отказу технологии ИИ, то есть вероятность проявления рисков самой системы ИИ. Непосредственно отказ представляет собой переход системы из рабочего состояния в нерабочее, характеризующееся невозможностью достижения информационных задач в соответствии с установленными требованиями и в имеющихся условиях.

Активное внедрение технологий ИИ в ИАД ОВУ в рамках процесса цифровизации деятельности вооруженных сил вызывает необходимость расширения границ военно-экономического анализа в части, касающейся оценивания вероятности рисков их применения в прикладной среде. Объективные сложности в решении данной научной задачи возникают ввиду отсутствия на сегодняшний день глубоких исследований, посвященных рассмотрению данного вопроса. В работе предлагается методика, которая предполагает оценивание показателя риска применения технологий ИИ в ИАД ОВУ в пять основных этапов (рис. 1).

На первом этапе методики изучается структура системы ИИ. В рамках этого устанавливаются основные элементы системы искусственного интеллекта, как организационно-технической системы, а также определяются порядок и направления их взаимодействия в контексте вероятности проявления факторов созависимого риска. На основе анализа литературы предлагается следующая эталонная структура организации системы ИИ (рис. 2) [2, 3].

В состав системы входят четыре основные подсистемы: программный компонент, аппаратный компонент, информационное обеспечение (ИО) и персонал. Каждая из этих подсистем включает в себя совокупность функциональных элементов. Все четыре подсистемы взаимодействуют между собой для обеспечения выполнения целей и задач системы. Порядок их организации (соединения) обуславливает различные подходы к определению вероятности проявления риска и обеспечения безотказной работы. Рассмотрим два основных подхода к соединению элементов системы ИИ: последовательное и параллельное.

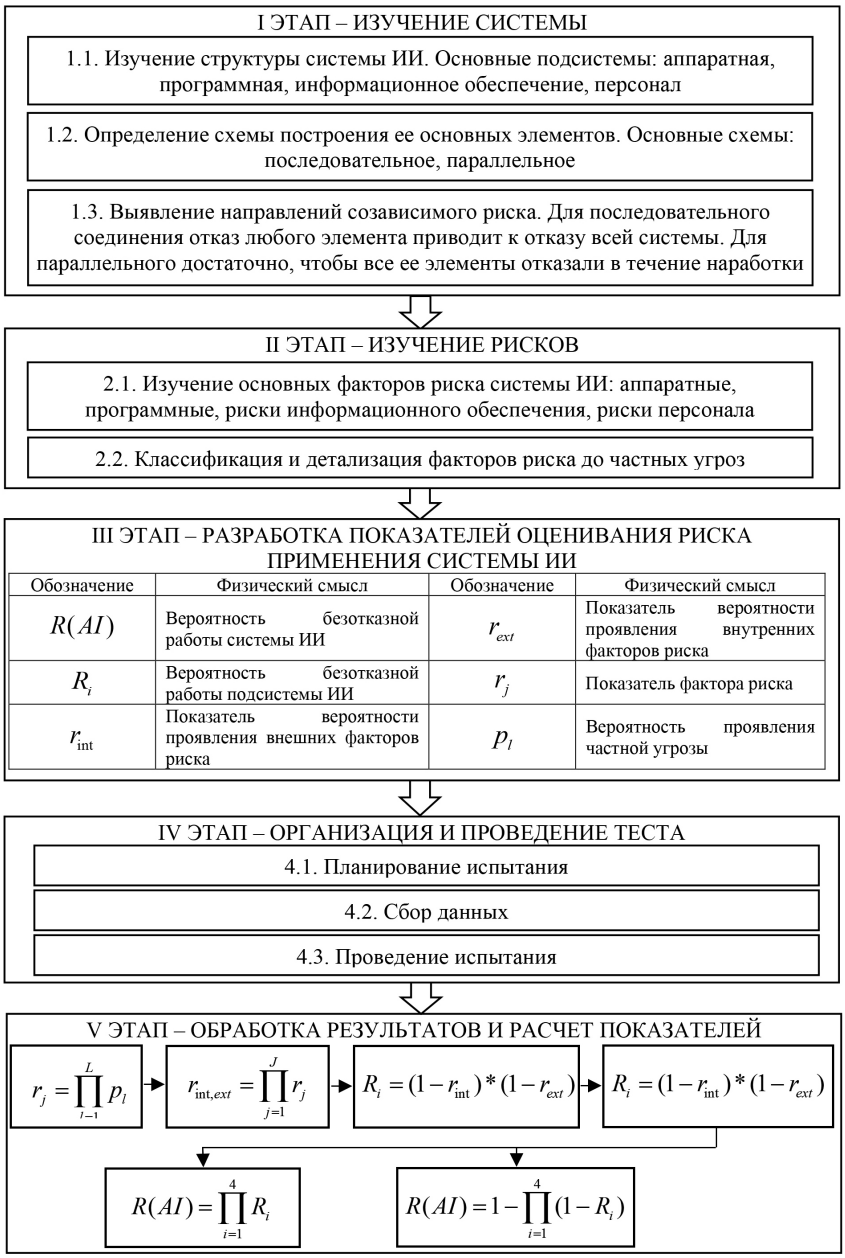

Рис. 1. Структура методики оценивания рисков применения технологий ИИ в ИАД ОВУ

Системой с последовательным соединением элементов называется система, в которой отказ любого элемента приводит к отказу всей системы (рис. 3) [3].

В системе ИИ с параллельным соединением элементов отказ происходит только в случае отказа всех её элементов (рис. 4). Для отказа системы с параллельным соединением элементов в течение наработки необходимо и достаточно, чтобы все её элементы отказали в течение этой наработки. Такие структуры характерны для устройств, в которых элементы дублируются или резервируются, потому что параллельное соединение применяется как основной метод повышения надежности [1].

На втором этапе методики определяется набор вероятных факторов риска системы. Исходя из её ранее обозначенной структуры риски могут быть аппаратными, программными, риски информационного обеспечения и риски, касающиеся деятельности персонала. Каждый из них может проявляться как от внутренних, так и от внешних факторов. Внутренние факторы каса-

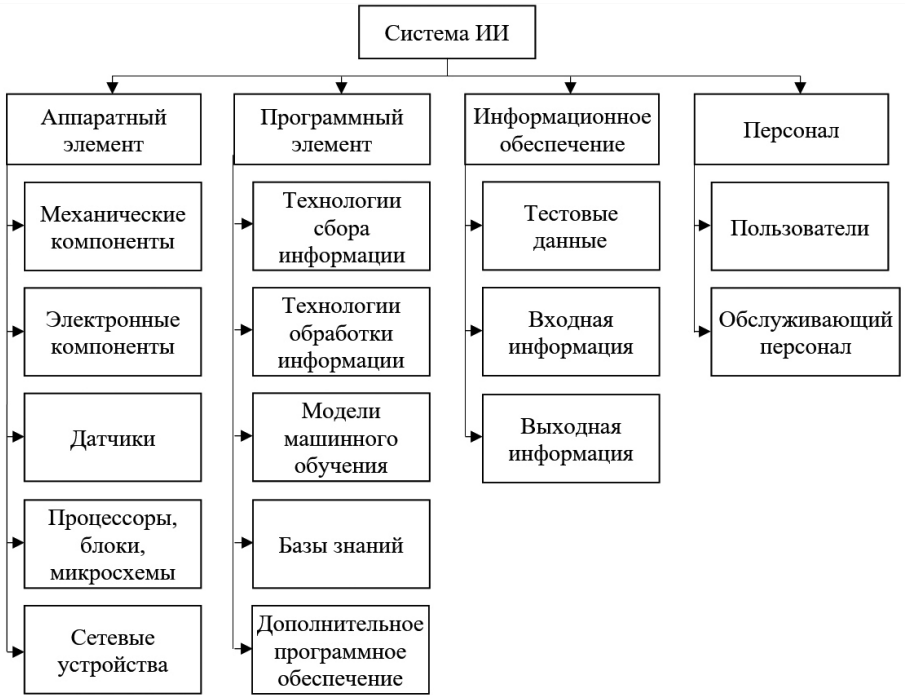

Рис. 2. Эталонная структура организации системы ИИ

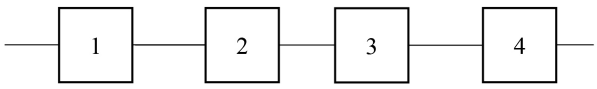

Рис. 3. Система ИИ с последовательным соединением элементов

ются в большей степени внутренней организации элементов системы, а внешние вызваны как условиями применения самих элементов системы, так и условиями проведения целевой операции. Основные факторы, определяющие риски для систем искусственного интеллекта представлены в таблице [4–10].

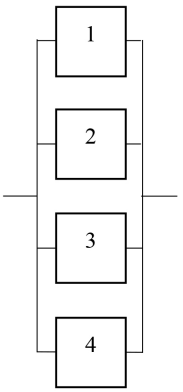

Рис. 4. Система ИИ с параллельным соединением элементов

Таблица

Факторы риска применения систем ИИ

Наименование подсистемы	Факторы риска	
	внешние	внутренние
Аппаратные	1. Условия окружающей среды. 2. Физическое воздействие противника	1. Конструкторско-технологические отказы
Программные	1. Воздействие противника. 2. Условия информационной среды	1. Программные ошибки
Риски ИО	1. Воздействие противника. 2. Низкая интенсивность и информативность информационного потока	1. Ошибки в подборе обучающих данных
Риски персонала	1. Воздействие противника. 2. Чрезвычайные ситуации	1. Ошибки личного состава. 2. Отсутствие эффективных кадров

Каждый из факторов можно описать совокупностью угроз, определяющих вероятность их проявления. Они в большинстве своем соответствуют информационно-аналитическим системам с традиционными способами обработки и анализа данных. Существенным отличием являются именно угрозы программного компонента и информационного обеспечения, что обусловлено особенностью построения и организации функционирования системы ИИ. В частности, если для традиционных систем основными источниками рисков выступают ошибки в алгоритмах и воздействие на них противника, то для систем ИИ к ним относятся ошибки в модели обучения, а также ошибки, искажения и возмущения во входном потоке данных и обучающей информации, и воздействие на них противника.

На третьем этапе разрабатываются основные показатели оценивания риска системы ИИ в ИАД ОВУ. В предлагаемом подходе показатель риска характеризуется вероятностью безотказного функционирования искусственного интеллекта. Он описывается совокупной вероятностью отказов входящих в него основных элементов, которая, в свою очередь, может быть определена вероятностью реализации основных факторов риска, вызванных всем спектром возможных угроз. На основе этого было составлено дерево показателей оценивания рисков систем ИИ в ИАД ОВУ (рис. 5).

На четвертом этапе методики осуществляется тестирование системы ИИ на вероятность проявления каждого из факторов риска. Оно реализуется по следующему алгоритму:

1. Подготовка плана тестирования;
2. Сбор данных;
3. Проведение испытания в реальных условиях эксплуатации.

Тест может быть реализован на стендовом испытательном полигоне или на реальных объектах с использованием различных средств и подходов имитации функционирования системы, а также условий применения её элементов и проведения целевой операции. В рамках испытания искусственный интеллект интегрируется в операционную систему, которая работает в реалистичной среде для соответствующего приложения. Степень детализации имитационных моделей тестирования должна обеспечивать возможность воспроизведения основных функций реальных объектов риска, проведения необходимого количества испытаний и получения статистических данных для оценки риска [11]. В рамках теста оценивается частота проявления угроз, описывающих каждый из возможных частных факторов риска.

На пятом этапе осуществляется обработка результатов тестирования и расчет показателей риска системы ИИ. Вероятность проявления частной угрозы фактора риска оценивается по-

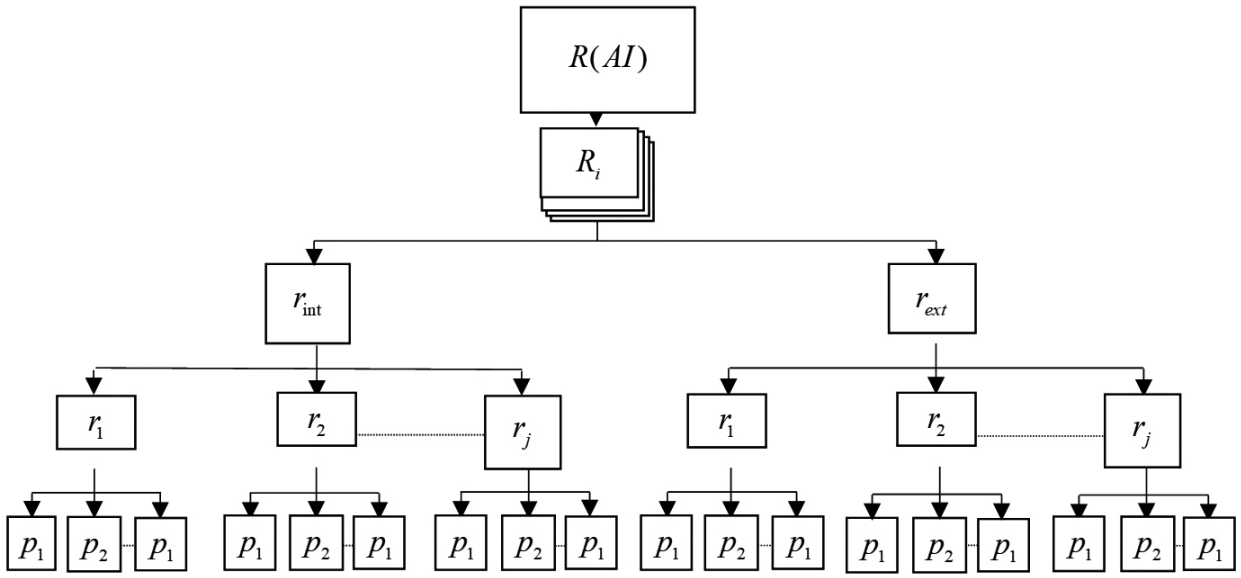

Рис. 5. Дерево показателей оценивания риска системы ИИ в ИАД ОВУ

средством определения частоты её возникновения в ходе проведения испытания и рассчитывается выражением

$$p_l = \frac{U}{N},$$

где U — частота проявления угрозы, приведшей к отказу функционирования системы;

N — число проведенных испытаний.

Принимая предположение, что любая из возникших угроз приводит к сбою работы системы, показатель фактора риска оценивается посредством произведения вероятностей проявления характерных ему угроз:

$$r_j = \prod_{l=1}^{L} p_l \ ,$$

где L — количество возникших угроз при проведении тестирования.

Аналогично производится расчет показателя вероятности проявления внешних/внутренних факторов риска:

$$r_{\text{int},ext} = \prod_{j=1}^{J} r_j \ ,$$

где J — количество проявившихся внешних/внутренних факторов риска при проведении тестирования.

Для эффективного решения информационно-аналитических задач ОВУ необходимо создать такую ситуацию, когда ни один из рисков не будет реализован. В этом случае можно рассчитать вероятность безотказного функционирования каждого из элементов системы ИИ в ИАД ОВУ в условиях реализации всего комплекса рисков:

$$R_i = (1 - r_{\text{int}}) \cdot (1 - r_{ext}) .$$

Расчет безотказного функционирования системы ИИ осуществляется с учетом порядка (схемы) соединения её основных элементов.

В системе с последовательным соединением для безотказной работы в течение некоторого времени необходимо и достаточно, чтобы каждая из её подсистем работала безотказно в течение этого периода времени. Считая отказы элементов независимыми, вероятность одновременной безотказной работы элементов определяется по теореме умножения вероятностей:

$$R(AI) = R_1 \cdot R_2 \cdot R_3 \cdot R_4 = \prod_{i=1}^{4} R_i = \prod_{i=1}^{I} (1 - Q_i) ,$$

где Q_i — вероятность отказа работы подсистемы ИИ;

I — количество подсистем, в которых были отмечены отказы в рамках тестирования.

Для отказа системы с параллельным соединением элементов в течение наработки необходимо и достаточно, чтобы все её элементы отказали в течение этой наработки. Следовательно, вероятность отказа системы (при допущении независимости отказов) может быть найдена по теореме умножения вероятностей как произведение вероятностей отказов элементов:

$$Q_i = \prod_{i=1}^{I} Q_i = \prod_{i=1}^{4} (1 - R_i) .$$

Соответственно, вероятность безотказной работы, описывающая интегральный риск системы ИИ, рассчитывается выражением

$$R(AI) = 1 - \prod_{i=1}^{I} Q_i = 1 - \prod_{i=1}^{4} (1 - R_i) .$$

Значения данного показателя будут находиться в промежутке от нуля до единицы. При этом чем его значение ближе к единице, тем меньше для системы ИИ рисков её применения.

Таким образом, предлагаемый методический подход позволяет решить задачу военно-экономического анализа, состоящую в необходимости оценивания рисков применения технологий ИИ в ИАД ОВУ, что несомненно способно повысить степень объективности дальнейшего обоснования рациональности их использования в рассматриваемой прикладной среде. Одной из ключевых особенностей подхода выступает утверждение необходимости исследования риска как не частного, а системного показателя, зависящего от всех подсистем системы ИИ, которые также могут создавать условия, приводящие к невозможности решения информационных задач технологией. Основу предложенного подхода составляет определение показателя риска как вероятности безотказной работы, описываемой совокупностью вероятностей проявления факторов риска и характеризующих их частных угроз.

Важным шагом на пути реализации методики должна стать разработка единого перечня типовых угроз применения систем ИИ в ИАД ОВУ.

Список источников

1. Белик А.Г. Качество и надежность программных систем: учеб. пособие. Омск: ОмГТУ, 2018. 80 с.

2. Hong Y., Lian J., Xu L., Min J. et al. Statistical Perspectives on Reliability of Artificial Intelligence Systems, Department of Statistics, Virginia Tech, Blacksburg, 2021. 40 p.

3. Чекал Е.Г. Надежность информационных систем: учеб. пособие. Ч. 1. Ульяновск: УлГУ, 2012. 118 с.

4. Угрозы информационной безопасности. URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ugrozy-informatsionnoj-bezopasnosti/ (дата обращения: 17.09.2024).

5. Konstantopoulos S. On the Reliability of Artificial Intelligence Systems: 13th EETN Conference on Artificial Intelligence (SETN). Piraeus, Greece, 2024. 5 p.

6. Намиот Д.Е., Ильюшин Е.А., Чижов И.В. Основания для работ по устойчивому машинному обучению // International Journal of Open Information Technologies. 2021. Вып. 9. № 11. С. 68–73.

7. Намиот Д.Е., Ильюшин Е.А. Об устойчивости и безопасности систем искусственного интеллекта // Международный журнал открытых информационных технологий. 2022. Вып. 10. № 9. С. 126–132.

8. Лаврищева Е.М., Зеленов С.В., Пакулин Н.В. Методы оценки надежности программных и технических систем // Труды ИСП РАН. 2019. Т. 31. № 5. С. 95–108.

9. Mortajia S.T.Y., Sadeghi M.E. Assessing the Reliability of Artificial Intelligence Systems: Challenges, Metrics, and Future Directions // International Journal of Innovation in Management Economics and Social Sciences. 2024. Vol. 4. No 2. Pp. 1–13.

10. Hamon R., Junklewitz H., Sanchez I. Robustness and Explainability of Artificial Intelligence — From technical to policy solutions, Publications Office of the European Union, Luxembourg, Luxembourg, 2020. 36 p.

11. Антонов С.Г., Климов С.М. Методика оценки рисков нарушения устойчивости функционирования программно-аппаратных комплексов в условиях информационно-технических воздействий // Надежность. 2017. Т. 17. № 1. С. 32–39.

References

1. Belik A.G. Kachestvo i nadezhnost' programmnyh system: textbook. Omsk: OmSTU, 2018. 80 p.

2. Hong Y., Lian J., Xu L., Min J. et al. Statistical Perspectives on Reliability of Artificial Intelligence Systems, Department of Statistics, Virginia Tech, Blacksburg, 2021. 40 p.

3. Chekal E.G. Nadezhnost' informacionnyh sistem: textbook. Ulyanovsk: UlSU, 2012. Vol. 1. 118 p.

4. Information security threats. URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ugrozy-informatsionnoj-bezopasnosti/. (date of reference: 17.09.2024).

5. Konstantopoulos S. On the Reliability of Artificial Intelligence Systems: 13th EETN Conference on Artificial Intelligence (SETN). Piraeus, Greece, 2024. 5 p.

6. Namiot D.E., Ilyushin E.A., Chizhov I.V. Basis for sustainable machine learning searches // International Journal of Open Information Technologies. 2021. Vol. 9. No 11. Pp. 68–73.

7. Namiot D.E., Ilyushin E.A. On the stability and security of artificial intelligence systems // International Journal of Open Information Technologies. 2022. Vol. 10. No 9. Pp. 126–132.

8. Lavrishcheva E.M., Zelenov S.V., Pakulin N.V. Methods for assessing the reliability of software and technical systems // Proceedings of ISP RAS. 2019. Vol. 31. No 5. Pp. 95–108.

9. Mortajia S.T.Y., Sadeghi M.E. Assessing the Reliability of Artificial Intelligence Systems: Challenges, Metrics, and Future Directions // International Journal of Innovation in Management Economics and Social Sciences. 2024. Vol. 4. No 2. Pp. 1–13.

10. Hamon R., Junklewitz H., Sanchez I. Robustness and Explainability of Artificial Intelligence — From technical to policy solutions, Publications Office of the European Union, Luxembourg, Luxembourg, 2020. 36 p.

11. Antonov S.G., Klimov S.M. Methodology for assessing risks of stability violation of the functioning of software and hardware systems in the conditions of information and technical influences // Reliability. 2017. Vol. 17. No 1. Pp. 32–39.