БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2025. – № 2 (117). – 40–51

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004 DOI: 10.17212/2782-2230-2025-2-40-51

РАЗРАБОТКА КРИТЕРИЕВ ДЛЯ ПРОВЕДЕНИЯ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ*

К.Е. КИТЛЯЙН[1], В.В. СЕЛИФАНОВ[2]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: kitlyajn.2020@stud.nstu.ru*
[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, старший преподаватель кафедры защиты информации. E-mail: sfo1@mail.ru*

В настоящей статье, основанной на более ранних работах авторов, нормативных и методических документах, рассматриваются актуальные проблемы, связанные с процессом аттестации. Основное внимание уделяется нехватке объективных критериев и влиянию субъективных факторов на результаты аттестации. Автор подчеркивает важность о необходимости создания стандартизированных методов оценки эффективности нейтрализации угроз и соответствия объектов информатизации требованиям регуляторов в области защиты информации. В результате сформирована методика оценки эффективности аттестационных испытаний объектов информатизации. В заключение поднимается вопрос о значимости процесса аттестации, а также приводятся рекомендации по улучшению аттестации, включая использование методов оценки.

Ключевые слова: аттестация объектов информатизации, объект информатизации, оценка соответствия, требования безопасности информации, системы защиты информации, оценка эффективности, информационная безопасность

ВВЕДЕНИЕ

Оценка соответствия системы защиты информации различного рода систем требованиям регуляторов в сфере информационной безопасности осуществляется путем аттестации.

Аттестация объекта информатизации представляет собой комплекс организационных и технических мероприятий – аттестационных испытаний, подтверждающих его соответствие установленным требованиям.

* Статья получена 13 мая 2025 г.

Аттестация является единственной административной процедурой, подтверждающей факт нейтрализации актуальных угроз на объекте информатизации. Аттестация ориентирована на решение двух критически важных вопросов: на объекте информатизации нейтрализованы все актуальные угрозы, и он соответствует установленным требованиям регулятора в области защиты информации, определенным приказом ФСТЭК России № 77 (далее – Порядок) [1].

Анализ требований к аттестации [1–7], показывает, что в них не определены количественные критерии, позволяющие с полной уверенностью утверждать, что получение аттестата соответствия подтверждает реализацию решения вопросов аттестации в полном объеме. Отсутствие критериев не позволяет оценить полноту реализации мер защиты информации.

В соответствии с существующими требованиями любой вид объекта информатизации проходит процедуру аттестации по единым критериям (требованиям). И по результатам устанавливается единая оценка для всех видов, уровней защищенности, категорий значимости объектов (систем).

Актуальностью настоящей работы является разработка подхода к оценке полноты аттестационных испытаний объектов информатизации на соответствие установленным требованиям. Признаком, подтверждающим актуальность, является отсутствие единого подхода к оценке эффективности рассматриваемого процесса аттестации.

В статье представлена разработка методики оценки эффективности (полноты) аттестационных испытаний на основе методического подхода к оценке соответствия систем финансовых организаций [7].

Целью работы является разработка методики оценки эффективности процесса аттестации объектов информатизации.

Для достижения цели были решены следующие задачи.

1. Анализ требований регулятора в данной области.

2. Сравнительный анализ существующих методик оценки эффективности аттестационных испытаний и выявление их основных преимуществ и недостатков.

3. Разработка методики оценки эффективности процедуры аттестации объектов информатизации на основе полученных результатов п. 2.

4. Рекомендации для усовершенствования и применения разработанной методики оценки эффективности процедуры аттестации объектов информатизации на соответствие требованиям безопасности информации.

В настоящей работе объектом исследования являются требования безопасности информации [1–5].

1. ВИДЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ, ПОДЛЕЖАЩИХ АТТЕСТАЦИОННЫМ ИСПЫТАНИЯМ

Аттестация может проводиться для следующих типов объектов информатизации:

1) государственных (муниципальных) информационных систем;

2) автоматизированных систем, обрабатывающих конфиденциальную информацию или информацию ограниченного доступа (с ограничительной пометкой);

3) информационных систем персональных данных;

4) автоматизированных систем управления технологическими процессами обработки информации;

5) значимых объектов критической информационной инфраструктуры.

Под объектом информатизации в настоящей работе подразумевается совокупность информации (информационных ресурсов), технических и программных средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также иные элементы, рассматриваемые с учетом эксплуатации объекта информатизации [6].

2. ОПРЕДЕЛЕНИЕ УСЛОВИЙ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ

На основании п. 3 Порядка определено, что аттестация может быть как обязательной, так и добровольной.

Обязательное требование по проведению оценки соответствия систем защиты информации в форме аттестации установлено для государственных (муниципальных) информационных систем.

Во всех остальных случаях аттестация носит добровольный характер и осуществляется по инициативе владельца объекта информатизации.

Непосредственно аттестационные испытания проводит аттестационная комиссия, создаваемая органом по аттестации, состоящая их руководителя и экспертов (не менее двух). При этом в состав комиссии не должны входить эксперты, принимавшие участие в разработке и (или) внедрении системы защиты объекта информатизации. Также обязательным условием при формировании аттестационной комиссии является независимость экспертов органа аттестации от владельца объекта информатизации.

3. ОЦЕНКА ЭФФЕКТИВНОСТИ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ

Анализ требований регулятора и иных источников по защите информации [1–5] показал, что обобщенно процесс аттестации представляет собой ряд последовательных шагов [9]:

1) анализ исходных данных;
2) разработка и согласование программы и методик испытаний;
3) проведение испытаний;
4) подготовка и отправка документов.

Оценка эффективности аттестационных испытаний заключается в следующем:

– в формировании критериев оценки;

– в анализе критериев оценки на предмет соответствия требованиям регуляторов в области обеспечения информационной безопасности;

– в оценке свойств процесса аттестации (расчет значений метрик на основе анализа критериев оценки);

– в расчете значения оценки эффективности аттестационных испытаний объекта информатизации на основе значений метрик.

В данном случае оценка эффективности является итоговым значением процесса аттестации. Под критериями будем понимать оцениваемые свойства процесса аттестации, под метриками – конкретные свидетельства аттестации (свойств объекта информатизации), подлежащие оценке соответствия.

Оценка эффективности аттестационных испытаний осуществляется в виде расчета заданных метрик. Под метрикой понимается числовое значение соответствия критерия оценки требованиям безопасности информации.

В основе данной методики оценки эффективности аттестационных испытаний лежит процесс проведения оценки соответствия по ряду нормативно-правовых документов [1–5], ГОСТов [6, 7], а также по ранее опубликованным работам авторов [8–17].

3.1. ОПРЕДЕЛЕНИЕ УРОВНЯ ЗНАЧИМОСТИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

Как отмечалось ранее, любой вид объекта информатизации проходит процедуру аттестации по единым критериям (требованиям). Соответственно, по результатам аттестационных испытаний устанавливается единая оценка для всех видов, уровней защищенности, категорий значимости объектов информатизации.

В настоящей работе при разработке методики оценки эффективности введено понятие «уровень значимости объекта информатизации» с целью разграничения критериев оценки. Для уровня значимости введены следующие лингвистические значения: низкий, средний, высокий.

Ранжирование уровня значимости объекта информатизации представлено в табл. 1.

Таблица 1

Определение уровня значимости объекта информатизации

Критерий	Высокий	Средний	Низкий
Категория значимости	К1	К2	К3
Класс защищенности	К1	К2	К3
Уровень защищенности	УЗ1	УЗ2	УЗ, УЗ4

Согласно разработанной методике если хотя бы один из критериев соответствует высокому или среднему уровню значимости, то объекту информатизации присваивается соответствующая группа независимо от того, что другие показатели входят в группы уровней меньшей значимости.

3.2. ОПРЕДЕЛЕНИЕ КРИТЕРИЕВ И МЕТРИК ОЦЕНКИ ЭФФЕКТИВНОСТИ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

При проведении оценки соответствия объекта информатизации требованиям безопасности информации необходимо осуществить сбор необходимых критериев для оценки.

Набор критериев оценки эффективности аттестационных испытаний сформирован на основе нормативного сопровождения процесса обеспечения безопасности информации [1–5] от идентификации и аутентификации (ИАФ) до информирования и обучения персонала (ИПО).

При разработке критериев учитываются как «внутренние», так и «внешние» показатели. Под «внутренними» показателями подразумеваются показатели эффективности объекта информатизации, под «внешними» – показатели системы защиты информации, «наложенной» поверх объекта информатизации.

После получения критериев оценки необходимо получить численные показатели – метрики.

Метрики сгруппированы в соответствии с [1–5] в 19 групп, каждая из которых является тем или иным свойством процесса защиты информации.

Значения метрик лежат в промежутке [0; 1], где 0 – низкая оценка, а 1 – высокая оценка.

3.3. РАСЧЕТ ОЦЕНКИ ЭФФЕКТИВНОСТИ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Для проведения оценки эффективности аттестационных испытаний на соответствие требованиям безопасности предлагается однозначное соответствие количественных и качественных показателей произвольного процесса.

При разработке методики будем утверждать, что можно оценить количество предполагаемых нарушений.

Для обозначения количества критериев, предъявляемых к объекту информатизации в рамках одной группы мер, примем обозначение k_p, а для обозначения количества выявленных нарушений – обозначение $n_{\text{нар}}$.

Для расчета процентного значения нарушений в рамках одной группы мер (p_i) применяется формула

$$p_i = \frac{n_{\text{нар}}}{k_p}, \tag{1}$$

где $n_{\text{нар}}$ – сумма метрик, равных нулю; k_p – максимальное возможное количество нарушений в рамках одной группы мер.

3.4. РАСЧЕТ ВЕРОЯТНОСТИ ПРОПУСКА НАРУШЕНИЙ

По завершении испытаний на основе полученных критериев рассчитывается вероятность пропуска нарушений. Для удобства введем обозначение вероятности пропуска нарушений – $p_{\text{нар}}$.

Для расчета вероятности пропуска нарушений будем использовать формулу

$$p_{\text{нар}} = p_{\text{ИАФ}} p_{\text{УПД}} \cdots p_i, \tag{2}$$

где p_i – это процентное значение нарушений в рамках одной группы мер.

Обобщенная функция эффективности аттестационных испытаний объектов информатизации определяется по формуле

$$S = 1 - \frac{p_{\text{нар}}}{K + m}, \tag{3}$$

где K – суммарное количество требований (k_p); m – количество дополнительных мер, необязательных для выполнения рассматриваемого уровня значимости.

Числовое значение S классифицируется согласно табл. 2.

Таблица 2

Оценка эффективности аттестационных испытаний

Значение S	Уровень соответствия	Интерпретация
0	Нулевой	Аттестационные испытания не проведены в установленном порядке
$0 < S <= 0,6$	Базовый	Аттестационные испытания проведены не в полном объеме, процент невыявленных нарушений высок
$0,6 < S <= 0,85$	Средний	Аттестационные испытания проведены не в полном объеме, требуется проведение дополнительных аттестационных испытаний
$0,85 < S <= 1$	Высокий	Аттестационные испытания проведены в полном объеме, процент невыявленных нарушений мал

Полученное числовое значение позволяет оценить полноту проведенных аттестационных испытаний объекта информатизации.

ЗАКЛЮЧЕНИЕ

В ходе исследования была разработана методика оценки эффективности на соответствие требованиям безопасности информации. Критерии и метрики оценки эффективности к процессу аттестации сформированы на основе стандартов по безопасности финансовых организаций [7]. ГОСТ 57580.2–2018 взят за основу как наиболее проработанная методика оценки защиты информации, опирающаяся не только на качественную, но и на количественную оценку.

Разработанная методика оценки эффективности аттестационных испытаний объектов информатизации на соответствие требованиям безопасности информации является одной из составляющих процесса аттестации и содержит объективные доказательства оценки эффективности аттестационных испытаний, охватывающих основные процессы информационной безопасности.

Методика проведения аттестационных испытаний по требованиям безопасности информации позволяет определить порядок выполнения требований законодательства и обеспечения безопасности объектов информатизации.

Методика может применяться при разработке Программы и методик аттестационных испытаний с целью повышения эффективности процесса аттестации.

На этапе анализа документов аттестационная комиссия с помощью методики может выдавать рекомендации по внесению необходимых изменений в документы по технической защите информации.

СПИСОК ЛИТЕРАТУРЫ

1. Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну: утв. приказом ФСТЭК России от 20.04.2021 № 77.

2. Приказ ФСТЭК России от 11 февраля 2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

3. Приказ ФСТЭК России от 18 февраля 2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

4. Приказ ФСТЭК России от 25 декабря 2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

5. Методический документ ФСТЭК России от 11 февраля 2014 «Меры защиты информации в государственных информационных системах».

6. ГОСТ Р 51275–2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения: дата введ. 2008–02–01. – М.: Стандартинформ, 2007. – 11 с.

7. ГОСТ Р 57580.2–2018. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия: дата введ. 2018–09–01. – М.: Стандартинформ, 2018. – 28 с.

8. *Вантеева А.Е., Омельченко Т.А., Никишова А.В.* Исследование возможности повышения эффективности процесса аттестации объекта информатизации // НБИ технологии. – 2022. – Т. 16, № 1. – С. 5–9. – DOI: 10.15688/NBIT.jvolsu.2022.1.1.

9. *Карганов В.В.* Основные положения по требованиям безопасности информации в части аттестация объектов информатизации // Национальная безопасность России: актуальные аспекты: сборник избранных статей Всероссийской научно-практической конференции. – СПб., 2020. – С. 22–27.

10. *Ефремов А.В., Панамарев Г.Е.* Анализ существующих методик оценки средств аудита информационной безопасности // Вестник Военного инновационного технополиса «Эра». – 2021. – Т. 2, № 4. – С. 38–45. – DOI: 10.1134/S2782375X21040031.

11. *Токарев В.Л., Сычугов А.А.* Метод аудита защищенности автоматизированных систем // Моделирование, оптимизация и информационные технологии. – Т. 7, № 1. – С. 548–559. – DOI: 10.26102/2310-6018/2019.24.1.036.

12. Методика разработки программы аудита информационной безопасности с учетом весовых коэффициентов значимости свидетельств аудита на основе метода анализа иерархий / В.А. Воеводин, П.В. Маркин, М.С. Маркина, Д.С. Буренок // Системы управления, связи и безопасности. – 2021. – № 2. – С. 96–129. – DOI: 10.24412/2410-9916-2021-2-96-129.

13. *Шлыков А.И., Шабуров А.С.* О формализации подходов к разработке моделей многокритериальной оценки эффективности систем защиты информации // Автоматизированные системы управления и информационные технологии: материалы Всероссийской научно-технической конференции. В 2 т. Т. 2. – Пермь, 2020. – С. 408–414.

14. *Воеводин В.А., Маркина М.С., Маркин П.В.* Определение весомости аудиторских свидетельств методом балльных оценок при аудите информационной безопасности // Computational nanotechnology. – 2020. – Т. 7, № 1. – С. 57–62. – DOI: 10.33693/2313-223X-2020-7-1-57-62.

15. Approach of determining process maturity in information security management systems / M. Naumann, F. Pitz, G. Lampe, S. Olaru // Proceedings of the 7th International Conference on Economics and Social Sciences, Bucharest, Romania. – Editura ASE, 2024. – P. 221–230. – DOI: 10.24818/ICESS/2024/023.

16. Towards the creation of a unified information systems certification system / P. Danilak, S. Lins, M. Greilich, A. Sunyaev // 24th IEEE Conference on Business Informatics (CBI). – IEEE, 2022. – Vol. 1. – P. 186–195. – DOI: 10.1109/CBI54897.2022.00027.

17. *Seeba M., Mäses S., Matulevičius R.* Method for evaluating information security level in organisations // Lecture Notes in Business Information Processing. – 2022. – Vol. 446: Research Challenges in Information Science. RCIS 2022. – Springer, 2022. – P. 644–652. – DOI: 10.1007/978-3-031-05760-1_39.

Китляйн Ксения Евгеньевна, лаборант кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – информационная безопасность. E-mail: kitlyajn.2020@stud.nstu.ru

Селифанов Валентин Валерьевич, старший преподаватель кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – информационная безопасность. E-mail: sfo1@mail.ru

DOI: 10.17212/2782-2230-2025-2-40-51

Development of criteria for conducting certification tests*

K.E. Kitlyayn[1], V.V. Selifanov[2]

[1] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, laboratory assistant of the Department of Information Security. E-mail: kitlyajn.2020@stud.nstu.ru*
[2] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, Senior Lecturer at the Department of Information Security. E-mail: sfo1@mail.ru*

This article, based on the authors' earlier works, normative and methodological documents, discusses current issues related to the certification process. The main focus is on the lack of objective criteria and the influence of subjective factors on the assessment results. The author emphasizes the importance of the need to create standardized methods for assessing the effectiveness of threat neutralization and the compliance of information facilities with the requirements of regulators in the field of information protection. As a result, a methodology for evaluating the effectiveness of certification tests of informatization facilities has been developed. In conclusion, the issue of the importance of the certification process is raised, and recommendations for improving certification, including the use of assessment methods, are given.

Keywords: certification of informatization facilities, informatization facility, conformity assessment, information security requirements, information security systems, efficiency assessment, information security

REFERENCES

1. “The procedure for organizing and carrying out work on certification of informatization facilities for compliance with the requirements for the protection of restricted access information that does not constitute a State Secret” was approved by Order No. 77 of the FSTEC of Russia dated 04.20.2021. (In Russian).

2. FSTEC of Russia Order No. 17 dated February 11, 2013 “On Approval of Requirements for the Protection of Information Not Constituting a State Secret Contained in State Information Systems”. (In Russian).

3. FSTEC of Russia Order No. 21 February 18, 2013 “On Approval of the Composition and Content of Organizational and Technical Measures to Ensure the Security of Personal Data during their Processing in Personal Data Information Systems”. (In Russian).

4. FSTEC of Russia Order No. 239 December 25, 2017 “On Approval of Requirements for Ensuring the Security of Significant objects of the Critical Information Infrastructure of the Russian Federation”. (In Russian).

* *Received 13 May 2025.*

5. FSTEC of Russia Methodological document, February 11, 2014 “Information protection measures in state information systems”. (In Russian).

6. State Standard R 51275–2006. *Protection of information. Object of informatisation. Factors influencing the information. General*. Moscow, Standartinform, 2007. 11 p. (In Russian).

7. State Standard R 57580.2–2018. *Security of financial (banking) operations. Information protection of financial organizations. Conformity assessment methods*. Moscow, Standartinform, 2018. 28 p. (In Russian).

8. Vanteeva A.E., Omelchenko T.A., Nikishova A.V. Issledovanie vozmozhnosti povysheniya effektivnosti protsessa attestatsii ob“ekta informatizatsii [Study of the possibility of improving the efficiency of the certification process of the information object]. *NBI tekhnologii = NBI Technologies*, 2022, vol. 16, no. 1, pp. 5–9. DOI: 10.15688/NBIT.jvolsu.2022.1.1.

9. Karganov V.V. [The basic provisions on the requirements information security in the part of certification of informatization objects]. *Natsional'naya bezopasnost' Rossii: aktual'nye aspekty* [National Security of Russia: relevant aspects]. Collection of selected articles of the All-Russian Scientific and Practical Conference. St. Petersburg, 2020, pp. 22–27. (In Russian).

10. Efremov A.V., Panamarev G.E. Analiz sushchestvuyushchikh metodik otsenki sredstv audita informatsionnoi bezopasnosti [Analysis of existing methods for evaluating information security audit tools]. *Vestnik Voennogo innovatsionnogo tekhnopolisa “Era”*, 2021, vol. 2, no. 4, pp. 38–45. DOI: 10.1134/S2782375X21040031. (In Russian).

11. Tokarev V.L., Sychugov A.A. Metod audita zashchishchennosti avtomatizirovannykh sistem [Method of auditing the protection of automated systems]. *Modelirovanie, optimizatsiya i informatsionnye tekhnologii = Modeling, Optimization and Information Technology*, 2019, vol. 7, no. 1, pp. 548–559. DOI: 10.26102/2310-6018/2019.24.1.036.

12. Voevodin V.A., Markin P.V., Markina M.S., Burenok D.S Technique for developing an information security audit program taking into account the weight coefficients of certificates audit based on the hierarchy analysis method. *Sistemy upravleniya, svyazi i bezopasnosti = Systems of Control, Communication and Security*, 2021, no. 2, pp. 96–129. DOI: 10.24412/2410-9916-2021-2-96-129. (In Russian).

13. Shlykov A.I., Shaburov A.S. On the formalization of approaches to the development of models of multi-criteria evaluation of the effectiveness of information security systems]. *Avtomatizirovannye sistemy upravleniya i informatsionnye tekhnologii*. V 2 t. T. 2 [Automated control systems and information technologies. In 2 vol. Vol.2]. Materials of the All-Russian scientific and technical conference. Perm, 2020, pp. 408–414. (In Russian).

14. Voevodin V.A., Markina M.S., Markin P.V. Determination of the weight of audit evidence by the method of pointratings in the information security audit. *Computational nanotechnology*, 2020, vol. 7, no. 1, pp. 57–62. DOI: 10.33693/2313-223X-2020-7-1-57-62. (In Russian).

15. Naumann M., Pitz F., Lampe G., Olaru S. Approach of determining process maturity in information security management systems. *Proceedings of the 7th International Conference on Economics and Social Sciences*, Bucharest, Romania. Editura ASE, 2024, pp. 221–230. DOI: 10.24818/ICESS/2024/023.

16. Danylak P., Lins S., Greulich M., Sunyaev A. Toward a unified framework for information systems certification internalization. *24th IEEE Conference on Business Informatics (CBI)*. IEEE, 2022, vol. 1, pp. 186–195. DOI: 10.1109/cbi54897.2022.00027.

17. Seeba M., Mäses S., Matulevičius R. Method for evaluating information security level in organisations. *Lecture Notes in Business Information Processing*. Springer, 2022, vol. 446. *Research Challenges in Information Science. RCIS 2022*, pp. 644–652. DOI: 10.1007/978-3-031-05760-1_39.

Для цитирования:

Китляйн К.Е., *Селифанов В.В.* Разработка критериев для проведения аттестационных испытаний // Безопасность цифровых технологий. – 2025. – № 2 (117). – С. 40–51. – DOI: 10.17212/2782-2230-2025-2-40-51.

For citation:

Kitlyayn K.E., Selifanov V.V. Razrabotka kriteriev dlya provedeniya attestatsionnykh ispytanii [Development of criteria for conducting certification tests]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2025, no. 2 (117), pp. 40–51. DOI: 10.17212/2782-2230-2025-2-40-51.