УДК 004.056.5:004.738.5
DOI: 10.26102/2310-6018/2025.50.3.034

Тензорные методы повышения устойчивости цифровых экосистем к DDoS-атакам: интегрированный подход на основе CP-разложения и энтропийного анализа

Н.Г. Аснина[1]✉, Е.В. Нетесов[2], А.К. Ушакова[1]

[1]Воронежский государственный технический университет, Воронеж, Российская Федерация
[2]Российский экономический университет имени Г.В. Плеханова, Москва, Российская Федерация

Резюме. В статье рассматривается метод обнаружения DDoS-атак в цифровых экосистемах с использованием тензорного анализа и энтропийных метрик. Сетевой трафик формализован как 4D-тензор с измерениями: IP-адреса, временные метки, типы запросов и страны происхождения. Для анализа данных применено CP-разложение с рангом 3, что позволяет выявлять скрытые закономерности в трафике. Разработан алгоритм расчета показателя аномальности (AS), который учитывает факторные нагрузки тензорного разложения и энтропию временных распределений. Эксперименты на реальных данных показали, что предложенный метод обеспечивает точность обнаружения атак 92 % при уровне ложных срабатываний 1,2 %. В сравнении с традиционными сигнатурными методами точность повысилась на 35 %, а количество ложных срабатываний снизилось на 86 %. Метод показал эффективность при выявлении сложных low-rate атак, которые трудно обнаружить стандартными способами. Результаты исследования могут быть полезны для защиты различных цифровых экосистем, включая финансовые сервисы, телекоммуникационные сети и государственные платформы. Предложенный подход расширяет возможности анализа сетевого трафика и может быть интегрирован в современные системы кибербезопасности. Дальнейшие исследования могут быть направлены на оптимизацию вычислительной сложности алгоритма и адаптацию метода для различных типов сетевых инфраструктур.

Ключевые слова: тензорный анализ, DDoS-атаки, кибербезопасность, цифровые экосистемы, CP-разложение, энтропийный анализ, обнаружение аномалий.

Для цитирования: Аснина Н.Г., Нетесов Е.В., Ушакова А.К. Тензорные методы повышения устойчивости цифровых экосистем к DDoS-атакам: интегрированный подход на основе CP-разложения и энтропийного анализа. 2025;13(3). URL: https://moitvivt.ru/ru/journal/pdf?id=2030
DOI: 10.26102/2310-6018/2025.50.3.034

Tensor methods for increasing the resilience of digital ecosystems to DDoS attacks: an integrated approach based on CP-decomposition and entropy analysis

N.G. Asnina[1]✉, E.V. Netesov[2], A.K. Ushakova[1]

[1]Voronezh State Technical University, Voronezh, the Russian Federation
[2]Plekhanov Russian University of Economics, Moscow, the Russian Federation

Abstract. The article discusses a method for detecting DDoS attacks in digital ecosystems using tensor analysis and entropy metrics. Network traffic is formalized as a 4D tensor with the following dimensions: IP addresses, timestamps, request types, and countries of origin. The CP decomposition with rank 3 is used to analyze the data, which allows revealing hidden patterns in traffic. An algorithm for calculating the anomaly score (AS) is developed, which takes into account the factor loadings of the tensor decomposition and the entropy of time distributions. Experiments on real data have shown that

the proposed method provides 92 % attack detection accuracy with a false positive rate of 1.2 %. Compared to traditional signature-based methods, the accuracy increased by 35 %, and the number of false positives decreased by 86 %. The method has proven effective in detecting complex low-rate attacks that are difficult to detect by standard methods. The results of the study can be useful for protecting various digital ecosystems, including financial services, telecommunication networks, and government platforms. The proposed approach expands the capabilities of network traffic analysis and can be integrated into modern cybersecurity systems. Further research could be aimed at optimizing the computational complexity of the algorithm and adapting the method to different types of network infrastructures.

Keywords: tensor analysis, DDoS attacks, cybersecurity, digital ecosystems, CP decomposition, entropy analysis, anomaly detection.

For citation: Asnina N.G., Netesov E.V., Ushakova A.K. Tensor methods for increasing the resilience of digital ecosystems to DDoS attacks: an integrated approach based on CP-decomposition and entropy analysis. *Modeling, Optimization and Information Technology*. 2025;13(3). (In Russ.). URL: https://moitvivt.ru/ru/journal/pdf?id=2030 DOI: 10.26102/2310-6018/2025.50.3.034

Введение

Современные цифровые экосистемы представляют собой сложные сети взаимосвязанных сервисов, объединяющих облачные платформы, IoT-устройства, финансовые системы, медиаресурсы и государственные порталы. Как отмечает Softline, такие экосистемы формируются через интеграцию разнородных технологий – от публичных облаков до промышленных IoT-решений, что создает расширенную «поверхность атаки» для злоумышленников. Актуальность темы исследования обусловлена стремительной эволюцией DDoS-атак, представляющих серьезную угрозу для цифровых экосистем[1].

Современные исследования в области кибербезопасности активно используют методы тензорного анализа для обнаружения аномалий в сетевой активности. Фундаментальные работы, такие как исследование Kolda и Bader (2009), демонстрируют эффективность CP-разложения для анализа многомерных данных, что особенно актуально при обработке сетевого трафика [1]. Дальнейшее развитие этих методов представлено в работах Cichocki и соавторов, где исследуются возможности неотрицательных тензорных разложений для анализа сложных данных и разделения источников [2].

Важным вкладом в развитие методов тензорного анализа стали работы Anandkumar и соавторов [3], где детально исследованы возможности тензорных разложений для обучения скрытых переменных моделей, а также исследование Sun и Sun [4], предложившее новые подходы к классификации зашумленных тензорных данных с использованием методов машинного обучения.

Интересным представляется направление современных исследований комбинации тензорных методов с энтропийным анализом. Panagakis и соавторы (2021), а также Wang и Chen (2020) обосновали применение энтропийных метрик для выявления аномалий и оценки сложности атакующих воздействий [5, 6]. Эти подходы особенно эффективны при анализе low-rate атак, которые трудно обнаружить традиционными методами.

В российских исследованиях также отмечается растущий интерес к комплексным методам анализа угроз. При этом, как отмечает Раменская [7, 8], экосистемный подход к анализу сложных систем позволяет выявлять скрытые взаимосвязи и закономерности, что особенно важно при построении моделей кибербезопасности цифровых экосистем.

[1] DDoS-атаки в мире и России: отчёт StormWall за 2024 год. StormWall. URL: https://stormwall.pro/resources/blog/ddos-2024-godovoj-otchet (дата обращения: 14.07.2025).

Орехов и соавторы (2023) предложили методику обнаружения аномалий, сочетающую фрактальный анализ и машинное обучение, что позволяет учитывать пространственно-временные характеристики угроз [9]. Мишин и Былевский (2023) разработали методы прогнозирования кибератак в цифровых экосистемах, демонстрирующие высокую точность при анализе многомерных данных [10].

Однако, существующие методы демонстрируют недостаточную эффективность против современных полиморфных DDoS-атак, особенно при обработке трафика в реальном времени.

Целью данной работы является разработка усовершенствованного алгоритма, сочетающего CP-разложение тензоров сетевого трафика с энтропийным анализом для обнаружения сложных полиморфных атак ($AS(i)\geq 0{,}3$), анализа пространственно-временных корреляций в 4D-тензоре трафика и снижения ложных срабатываний до 1,2 %.

Материалы и методы

В условиях глобальной цифровой трансформации, пронизывающей все сферы социально-экономических взаимодействий, обеспечение киберустойчивости инфраструктур приобретает стратегическое значение.

DDoS-атаки признаются серьёзной опасностью, способной нарушить функционирование веб-сервисов, дестабилизировать информационные системы и причинить существенный материальный ущерб [11].

DDoS-атака (Distributed Denial-of-Service) представляет собой распределённое воздействие, создающее избыточную нагрузку на серверные ресурсы, что приводит к системному отказу. Подобные ситуации лишают пользователей доступа к сетевым ресурсам, а владельцев инфраструктуры – ожидаемой прибыли [12].

Традиционные методы противодействия, включая перенаправление трафика и блокировку IP-адресов, демонстрируют снижающуюся эффективность в условиях наблюдаемого роста не только количества, но и сложности DDoS-атак, выражающейся в их многогранности и мощности2.

Современные DDoS-атаки отличаются многоуровневой структурой, применяя разнообразные многоцелевые стратегии для преодоления сигнатурных средств защиты. Воздействия одновременно направлены на различные системные компоненты, включая программные модули, сервисы и аппаратное обеспечение[2]. Основные типы атак систематизированы в Таблице 1.

Таблица 1 – Классификация типов DDoS-атак
Table 1 – Classification of DDoS attack types

Класс атак	Механизм воздействия	Потенциальный ущерб
Объемные атаки (Volume-based)	Использование значительного объема данных для превышения пропускной способности канала связи. Перегрузка каналов связи	Материальные потери, утрата клиентской базы вследствие недоступности сервисов
Атаки на протокол (Protocol-level)	Эксплуатация уязвимостей стека TCP/IP с целью перегрузки системы.	Дестабилизация сетевой инфраструктуры
Атаки на приложение (Application-layer)	Целенаправленное воздействие на приложения	Сбои в функционировании приложений, ущерб репутации, материальные потери

[2] Малюк А.А. *Информационная безопасность: концептуальные и методологические основы защиты информации.* Москва: Горячая линия–Телеком; 2004. 280 с.

В основе метода, предложенного в статье, лежит представление сети как тензорного пространства с ограниченной метрикой. Пространство организуется вдоль направлений, заданных структурой сети, что отражает реальные взаимодействия между её элементами. Каждое направление характеризуется собственным весом, определяющим значимость соответствующих связей.

Метрика пространства формируется через тензор второго ранга, компоненты которого зависят от интенсивности взаимодействий между узлами, топологических характеристик сети, временных параметров соединений.

Особенность подхода – вырожденность метрики в направлениях, не соответствующих реальным сетевым соединениям. Это позволяет эффективно снижать размерность задачи без потери ключевых характеристик системы.

Для анализа сетевого трафика строится специальная геометрическая модель, где базовые координаты соответствуют IP-адресам, дополнительные измерения отражают временные параметры, типы запросов задают внутреннюю структуру пространства.

Тензорная модель цифровой экосистемы. Цифровую экосистему можно формализовать как тензор *N*-го порядка:

$$T \in R^{I_1 \times I_2 \times \ldots \times I_N}. \quad (1)$$

В нашем случае это будет 4D-тензор:

$$T \in R^{N \times T \times F \times G}, \quad (2)$$

где в качестве измерений применяются признаки аномалии: IP-адрес (*N*), временная метка (*T*), тип запроса (*F*), страна (*G*).

Алгоритм обнаружения аномалий. Для преодоления проблемы «проклятия размерности», проявляющейся в экспоненциальном росте объема данных при увеличении размерности пространства, применяется метод тензорной декомпозиции. В частности, используется каноническая аппроксимация тензора (CP-разложение), которая позволяет представить исходный многомерный массив данных в виде суммы пересекающихся компонент. Каждая такая компонента описывает определенный тип взаимосвязанных аномалий в данных, обеспечивая тем самым их эффективное сжатие и выявление скрытых закономерностей. В рамках данного исследования оптимальный ранг аппроксимации был установлен равным трем, что подтверждено экспериментальными результатами и обеспечивает баланс между точностью представления данных и вычислительной сложностью.

1. CP-разложение с рангом R = 3:

$$T \approx \sum_{r=1}^{R} \lambda_r \, (a_r \circ b_r \circ c_r \circ d_r). \quad (3)$$

2. Расчет показателя аномальности $AS(i)$для каждого IP-адреса (i):

$$AS(i) = \sum_{r=1}^{R} \lambda_r |a_r(i)| \cdot H(b_r), \quad (4)$$

$$H(b_r) = -\sum_{t=1}^{T} p_t \log p(t), \quad (5)$$

$$p(t) = \frac{b_r(t)}{\sum_{t'} b_r(t')}. \quad (6)$$

Здесь факторные нагрузки $a_r(i)$, полученные в результате канонической аппроксимации тензора, количественно характеризуют вклад *i*-го объекта в соответствующую аномальную компоненту. Сингулярные значения λ_r отражают значимость каждой компоненты в общем разложении, в то время как энтропия Шеннона $H(b_r)$ (5) служит мерой неопределенности временного распределения аномальной активности.

Совместное использование этих параметров позволяет получить комплексную оценку аномальности, учитывающую как пространственные, так и временные характеристики сетевого поведения.

3. Классификация угроз:
- нормальный трафик: $AS(i) < 0{,}1$;
- подозрительный трафик: $0{,}1 \leq AS(i) < 0{,}3$;
- DDoS-атака (блокируется, как источник атаки): $AS(i) \geq 0{,}3$.

Результаты

Предложенный в статье подход на основе тензорного анализа и энтропийных метрик может найти практическое применение в различных типах цифровых экосистем, каждая из которых имеет специфические требования к кибербезопасности.

Крупные IT-платформы и агрегаторы, такие как Яндекс, Mail.ru Group, СберМаркет и Wildberries, могут использовать данный метод для защиты от DDoS-атак в периоды пиковых нагрузок, анализа аномального поведения ботов и скрейперов, а также выявления скоординированных атак на API-интерфейсы. В финансовом секторе, включая Сбербанк, Тинькофф и Альфа-Банк, разработанный алгоритм позволит обнаруживать сложные атаки на интернет-банкинг, защищать платежные шлюзы от multi-vector атак и мониторить подозрительную активность в транзакционных операциях.

Телекоммуникационные операторы, такие как МТС, МегаФон и Ростелеком, могут использовать метод для защиты сетевой инфраструктуры, обнаружения атак через IoT-устройства и анализа low-rate атак на оборудование 5G-сетей. В промышленных IoT-экосистемах (Росатом, Газпромнефть, РЖД) подход обеспечит защиту SCADA-систем, обнаружение аномалий в работе датчиков и предотвращение атак на критическую инфраструктуру.

Игровые и стриминговые платформы, включая VK Play, RuStore и Okko, могут применять алгоритм для защиты от атак во время киберспортивных турниров, выявления бот-сетей в многопользовательских играх и мониторинга атак на системы доставки контента.

Особенности применения варьируются в зависимости от типа экосистемы. Для B2C-платформ критически важно обнаружение low-rate атак, маскирующихся под легитимный трафик. Финансовые системы требуют минимизации ложных срабатываний при блокировке подозрительной активности. В государственном секторе особую значимость приобретает географическая привязка атак и анализ их политического контекста. Для телекоммуникационных операторов ключевое значение имеет масштабируемость методов обработки экстремально больших объемов сетевого трафика.

Все перечисленные типы цифровых экосистем сталкиваются с современными DDoS-угрозами, против которых традиционные методы защиты демонстрируют недостаточную эффективность, что подтверждает актуальность предложенного в статье тензорного подхода.

Экспериментальная проверка метода. Для валидации предложенного подхода был проведен сравнительный анализ эффективности тензорного метода и традиционного сигнатурного анализа на реальных данных сетевого трафика российской цифровой платформы.

Результаты представлены в Таблице 2.

Таблица 2 – Сравнительные показатели эффективности методов обнаружения DDoS-атак
Table 2 – Comparative performance of DDoS attack detection methods

Метрика	Тензорный метод	Сигнатурный метод	Улучшение, %
Точность (Precision)	92 %	68 %	+35,3
Полнота (Recall)	89 %	54 %	+64,8
Ложные срабатывания (FPR)	1,2 %	8,7 %	−86,2

Анализ данных эксперимента. Исследуемый набор данных включал анонимизированные записи сетевого трафика для тензора $T \in R^{1000\times3600\times5\times20}$, со следующими характеристиками (Таблица 3):

Таблица 3 – Структура входных данных
Table 3 – Input data structure

Обозначение	Параметр	Характеристики
N	Количество IP-адресов	1000 уникальных узлов
T	Период наблюдения	1 час (3600 секунд)
F	Типы запросов	HTTP_GET, HTTP_POST, UDP, ICMP, DNS
G	География трафика	20 стран

Пример выявленных аномалий представлен в Таблице 4:

Таблица 4 – Примеры обнаруженных аномальных паттернов
Table 4 – Examples of detected abnormal patterns

IP-адрес	Время	Тип запроса	Страна	Интенсивность	AS(i)	Заключение
E8G2H5	12:05:06	ICMP	CN	1,00	0,42	DDoS-атака
C7D4E1	12:05:04	UDP	US	0,92	0,37	Flood-атака
A3F9B2	12:05:03	HTTP_GET	RU	0,15	0,05	Нормальный трафик

Географическое распределение аномального трафика показало значительную концентрацию подозрительной активности из определенных регионов (Таблица 5):

Таблица 5 – География DDoS-атак
Table 5 – Geography of DDoS attacks

Страна	Доля трафика	Аномальность (AS(i))	Тип атаки
США (US)	25 %	0,52 ± 0,03	UDP-flood (45 %)
Китай (CN)	10 %	0,48 ± 0,05	ICMP (30 %)
Россия (RU)	60 %	0,08 ± 0,01	Нормальный трафик

Данные показывают концентрацию атак из США и Китая при низкой аномальности российского трафика.

Анализ временных характеристик выявил существенные различия в энтропийных показателях:

– нормальный трафик: $H = 0{,}8 \pm 0{,}2$;

– аномальная активность: $H = 2{,}1 \pm 0{,}3$.

Обсуждение

Полученные результаты демонстрируют, что предложенный тензорный метод существенно превосходит традиционные подходы по ключевым метрикам, обеспечивая надежное обнаружение сложных multi-vector атак при минимальном уровне ложных срабатываний.

Однако метод имеет некоторые ограничения:

– производительность: при обработке более 1 млн запросов/сек наблюдается снижение скорости на 15 %;

– зависимость от качества входных данных: требуется предварительная фильтрация DNS-трафика;

– необходимость ручной настройки параметров: оптимальный ранг разложения R = 3 требует верификации для разных типов экосистем.

Заключение

Проведенное исследование подтвердило эффективность предложенного подхода, основанного на комбинации тензорного разложения и энтропийного анализа, для обнаружения сложных DDoS-атак в цифровых экосистемах. Экспериментальные результаты продемонстрировали значительное превосходство метода над традиционными сигнатурными подходами, выражающееся в повышении точности обнаружения на 35 % и снижении ложных срабатываний на 86 %. Разработанная тензорная модель позволила выявлять скрытые пространственно-временные корреляции в сетевом трафике, недоступные для классических методов анализа. Особую ценность представляет способность алгоритма детектировать low-rate атаки, успешно маскирующиеся под легитимный трафик. Полученные результаты имеют важное практическое значение для защиты критически важных цифровых инфраструктур, включая финансовые системы, телекоммуникационные сети и государственные платформы. Перспективы дальнейших исследований связаны с оптимизацией вычислительной сложности метода и разработкой адаптивных механизмов автоматического выбора параметров анализа. Теоретическая значимость работы заключается в развитии математического аппарата тензорного анализа для задач кибербезопасности. Практическая реализация предложенного подхода может существенно повысить устойчивость цифровых экосистем к современным киберугрозам.

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Kolda T.G., Bader B.W. Tensor Decompositions and Applications. *SIAM Review*. 2009;51(3):455–500. https://doi.org/10.1137/07070111X
2. Cichocki A., Zdunek R., Phan A.H., Amari Sh.-I. *Nonnegative Matrix and Tensor Factorizations: Applications to Exploratory Multi-Way Data Analysis and Blind Source Separation.* Singapore: John Wiley & Sons; 2009. 504 p.
3. Anandkumar A., Ge R., Hsu D., Kakade Sh.M., Telgarsky M. Tensor Decompositions for Learning Latent Variable Models. *Journal of Machine Learning Research*. 2014;15:2773–2832. https://doi.org/10.1007/978-3-319-24486-0_2

4. Sun T., Sun X.-M. New Results on Classification Modeling of Noisy Tensor Datasets: A Fuzzy Support Tensor Machine Dual Model. *IEEE Transactions on Systems, Man, and Cybernetics: Systems.* 2022;52(8):5188–5200. https://doi.org/10.1109/TSMC.2021.3119422
5. Panagakis Ya., Kossaifi J., Chrysos G.G., et al. Tensor Methods in Computer Vision and Deep Learning. *Proceedings of the IEEE.* 2021;109(5):863–890. https://doi.org/10.1109/JPROC.2021.3074329
6. Wang Q., Chen L., Wang Q., Zhu H., Wang X. Anomaly-Aware Network Traffic Estimation via Outlier-Robust Tensor Completion. *IEEE Transactions on Network and Service Management.* 2020;17(4):2677–2689. https://doi.org/10.1109/TNSM.2020.3024932
7. Раменская Л.А. Экосистемный подход к анализу объектов архитектуры бизнеса. *Фундаментальные исследования.* 2022;(10–1):147–152. https://doi.org/10.17513/fr.43358
   Ramenskaya L.A. Ecosystem Approach to the Analysis of Business Architecture Objects. *Fundamental Research*. 2022;(10–1):147–152. (In Russ.). https://doi.org/10.17513/fr.43358
8. Раменская Л.А. Обзор подходов к исследованию экосистем бизнеса. *Вестник Алтайской академии экономики и права.* 2019;(12–2):153–158. https://doi.org/10.17513/vaael.890
   Ramenskaya L.A. Overview of Approaches to Research of Business Ecosystems. *Vestnik Altaiskoi akademii ekonomiki i prava.* 2019;(12–2):153–158. (In Russ.). https://doi.org/10.17513/vaael.890
9. Орехов А.В., Орехов А.А. Автоматическое обнаружение аномалий сетевого трафика при DDoS-атаках. *Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления.* 2023;19(2):251–263. https://doi.org/10.21638/11701/spbu10.2023.210
   Orekhov A.V., Orekhov A.A. Network Traffic Anomalies Automatic Detection in DDoS Attacks. *Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes.* 2023;19(2):251–263. (In Russ.). https://doi.org/10.21638/11701/spbu10.2023.210
10. Мишин А.Е. Применение машинного обучения для прогнозирования кибератак. *Hi-Hume Journal.* 2023;(3):80–89.
    Mishin A.E. Using Machine Learning to Predict Cyber Attacks. *Hi-Hume Journal.* 2023;(3):80–89. (In Russ.).
11. Кульмамиров С.А., Баймаманова А.А. Современное состояние обнаружения DDoS-атак и противодействие к ним. *Актуальные научные исследования в современном мире.* 2020;(4–2):50–57.
    Kulmamirov S.A., Baimamanova A.A. Current State of DDoS Attack Detection and Counteraction. *Aktual'nye nauchnye issledovaniya v sovremennom mire.* 2020;(4–2):50–57. (In Russ.).
12. Воеводин В.А., Черняев В.С., Буренок Д.С., Виноградов И.В. Методика оценки защищённости автоматизированной системы управления критической информационной инфраструктуры от DDoS-атак на основе имитационного моделирования методом Монте-Карло. *Вестник Дагестанского государственного технического университета. Технические науки.* 2023;50(1):62–74. https://doi.org/10.21822/2073-6185-2023-50-1-62-74
    Voevodin V.A., Chernyaev V.S., Burenok D.S., Vinogradov I.V. Assessment Methodology for Security of an Automated Control System of Critical Information Infrastructure Against DDoS Attacks Based on Monte Carlo Simulation. *Herald of*

Dagestan State Technical University. Technical Sciences. 2023;50(1):62–74. (In Russ.). https://doi.org/10.21822/2073-6185-2023-50-1-62-74

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Аснина Наталия Георгиевна, кандидат технических наук, доцент, доцент Воронежского государственного технического университета, Воронеж, Российская Федерация.
e-mail: andrey050569@yandex.ru

Natalia G. Asnina, Candidate of Engineering Sciences, Docent, Associate Professor of Voronezh State Technical University, Voronezh, the Russian Federation.

Нетесов Евгений Владимирович, магистр, Российский экономический университет имени Г.В. Плеханова, Москва, Российская Федерация.

Evgeny V. Netesov, Master, Plekhanov Russian University of Economics, Moscow, the Russian Federation.

Ушакова Анастасия Константиновна, аспирант кафедры систем управления и информационных технологий в строительстве, Воронежский государственный технический университет, Российская Федерация.
e-mail: ushakova_nastena@mail.ru

Anastasia K. Ushakova, Postgraduate, Department of Control Systems and Information Technologies in Construction, Voronezh State Technical University, Voronezh, the Russian Federation.

Статья поступила в редакцию 23.07.2025; одобрена после рецензирования 04.08.2025; принята к публикации 07.08.2025.

The article was submitted 23.07.2025; approved after reviewing 04.08.2025; accepted for publication 07.08.2025.