DOI: 10.52363/passa-2026.1-19
UDC: 004.738

Borysova L., *Candidate of Legal Sciences, Associate Professor, Senior Lecturer at the Department of Civil Protection and Information Technologies, National University of Civil Protection of Ukraine, Cherkasy*
ORCID: 0000-0001-6554-1949

Dendarenko V., *Candidate of Technical Sciences, Associate Professor, Associate Professor at the Department of Civil Protection and Information Technologies, National University of Civil Protection of Ukraine, Cherkasy*
ORCID: 0000-0001-5833-1257

Zazhoma V., *Candidate of Technical Sciences, Associate Professor, Associate Professor at the Department of Civil Protection and Information Technologies, National University of Civil Protection of Ukraine, Cherkasy*
ORCID: 0000-0003-2083-2472

Борисова Л., *кандидат юридичних наук, доцент, старший викладач кафедри цивільного захисту та інформаційних технологій, Національний університет цивільного захисту України, Черкаси.*

Дендаренко В., *кандидат технічних наук, доцент, доцент кафедри цивільного захисту та інформаційних технологій, Національний університет цивільного захисту України, Черкаси.*

Зажома В., *кандидат юридичних наук, доцент, старший викладач кафедрицивільного захисту та інформаційних технологій, Національний університет цивільного захисту України, Черкаси.*

APPLICATION OF CLOUD TECHNOLOGIES IN THE PUBLIC SECTOR AND THE SESU OF UKRAINE

ЗАСТОСУВАННЯ ХМАРНИХ ТЕХНОЛОГІЙ В ПУБЛІЧНОМУ СЕКТОРІ ТА ДСНС УКРАЇНИ

The article analyses the legal regime, service models and approaches to risk assessment of cloud technologies in the public sector of Ukraine, with particular reference to the State Emergency Service of Ukraine (SESU). The methodological foundation rests on regulatory-legal, comparative and risk-oriented approaches. On the basis of the Law of Ukraine "On Cloud Services" and subordinate legislation, the terminology has been systematised, the roles of the parties and the requirements for providers defined. The Ukrainian classification of cloud services, specifically SECaaS and the "collective cloud," has been compared with the NIST approach to service models and cloud infrastructure characteristics.

Separate attention is given to the risk-oriented approach in evaluating cloud solutions for public users, drawing on ISO/IEC 27005, NIST SP 800-30 and cloud security assurance practices (CSA CCM). Acceptability criteria for cloud solutions in the public sector have been identified: lawfulness of data processing, compliance with established provider requirements, incident control, auditability, continuity of service provision and minimization of single-vendor dependency. It has been concluded that the adoption of cloud technologies in Ukraine's public sector is taking place within the framework of an established legal regime that combines legislative definitions, specific rules for government users, and a risk-based approach to the activities of providers.

Keywords: *cloud technologies, cloud services, public sector, legal regulation, public users, civil protection, information security, risk management, service continuity, audit of cloud solutions.*

Стаття присвячена аналізу правового режиму, моделей обслуговування та підходів до оцінки ризиків хмарних технологій у публічному секторі України, зокрема в контексті діяльності Державної служби з надзвичайних ситуацій (ДСНС). Методологічну основу

становлять нормативно-правовий, порівняльний і ризик-орієнтований підходи. На основі Закону України «Про хмарні послуги» та підзаконних актів систематизовано термінологію, визначено ролі суб'єктів і вимоги до провайдерів. Українську класифікацію хмарних сервісів, зокрема, SECaaS і «колективну хмару» зіставлено з підходом NIST до моделей сервісів і характеристик хмарної інфраструктури.

Окрему увагу приділено ризик-орієнтованому підходу до оцінки хмарних рішень для публічних користувачів із залученням положень ISO/IEC 27005, NIST SP 800-30 та практик cloud security assurance (CSA CCM). Визначено критерії прийнятності хмарних рішень для публічного сектору як правомірність обробки даних, відповідність установленим вимогам до надавачів, контроль інцидентів, аудитність, безперервність надання послуг та мінімізація залежності від одного постачальника. Зроблено висновок, що впровадження хмарних технологій у публічному секторі України відбувається в межах сформованого правового режиму, який поєднує законодавчі дефініції, спеціальні правила для публічних користувачів і ризик-орієнтований підхід до діяльності провайдерів.

Ключові слова: *хмарні технології, хмарні послуги, публічний сектор, правове регулювання, публічні користувачі, цивільний захист, інформаційна безпека, управління ризиками, безперервність послуг, аудит хмарних рішень.*

Problem statement. The digitalization of the public sector places demands on data processing, storage and protection that traditional on-premise IT infrastructure does not always meet above all in terms of scalability, fault tolerance and cost-effectiveness under crisis loads.

For the SESU this problem is particularly acute. The effectiveness of emergency response hinges on prompt access to information, the resilience of the digital infrastructure and the ability to exchange data rapidly between units and other government bodies. These are precisely the requirements that most often become a bottleneck when working with legacy on-premise solutions; the experience of the large-scale cyber-attacks on Ukrainian state registries in

late 2024 only underscored how vulnerable concentrated local infrastructure can be without proper redundancy.

Cloud technologies emerge as one possible avenue for modernising information support. Yet their adoption in the public sector calls for separate scholarly scrutiny not only from the standpoint of technical fitness but also in light of the security and organisational-legal constraints that are specific to state structures and, most acutely, to services handling restricted-access information.

Analysis of recent research and publications. The foundational work for the study of cloud computing remains that of P. Mell and T. Grance [1], which outlined five key characteristics of cloud infrastructure on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service and systematised models of service delivery and deployment. This work still serves as the "common denominator" in discussions of cloud computing, although some of its provisions (particularly those concerning deployment models) no longer capture the full diversity of today's hybrid and multi-cloud architectures.

In the Ukrainian academic literature, cloud technology research develops along two markedly different lines. Where V. Ya. Yurchyshyn [2, p. 59] takes a predominantly economic view cloud technologies as a model for cutting the costs of maintaining local infrastructure the authors of the handbook edited by D. V. Lande [3] shift the focus toward processing very large datasets, which is considerably closer to the needs of the SESU as a service whose work is tightly bound up with large volumes of operational, analytical, reference and geospatial information.

None of these approaches, however, addresses the specifics of departmental implementation.

Risks and security of cloud services form a separate line of inquiry, and the pattern here is much the same: the works of L. O. Nikitina, N. V. Dzheniuk and L. V. Borysova [4], I. A. Kotiashichev and E. A. Byrylova [5, pp. 30–34], T. H. Bilova and V. O. Yaruta [6, pp. 71–73] deal with expert risk assessment, data protection mechanisms, access control and operational continuity, but mostly in general terms, without tying the analysis to specific departmental

systems. For the SESU this aspect is key: what is at stake are information resources on which the management of forces and assets, the coordination of response and decision support under crisis conditions all depend. Put differently, if the works cited above lay the theoretical and methodological groundwork for cloud risk assessment, what we propose is to bring that lens down to the applied level – to the resilience of specific alert and operational management systems.

For the SESU this aspect is key: what is at stake are information resources on which the management of forces and assets, the coordination of response and decision support under crisis conditions all depend. Put differently, if the works cited above lay the theoretical and methodological groundwork for cloud risk assessment, what we propose is to bring that lens down to the applied level – to the resilience of specific alert and operational management systems.

Formulation of the task. Notwithstanding the existence of these studies, the question of applying cloud technologies specifically within the SESU system has been insufficiently explored. What remains outside the researchers 'field of vision are the specifics of operational response, inter-agency coordination (in particular the interaction between the SESU, the State Special Communications Service and the General Staff of the Armed Forces of Ukraine in matters of cyber defence), the continuity of information systems and the protection of restricted information in the domain of civil protection. It is this gap that drives the need for further research.

The aim of this work is to analyse the legal regime, service models and risk assessment approaches for cloud technologies in the context of the Ukrainian public sector, and specifically the SESU.

Presentation of the main material. The concept of cloud computing traces its origins to the 1960s and John McCarthy's idea of "computer utility." The classical NIST definition describes it as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort and/or service provider interaction" [1]. Douglas Parkhill, in The Challenge of

e-ISSN 2786-5533

the Computer Utility (1966), sketched the basic outlines of what would later come to be called cloud computing [2].

The distance between that early concept and today's reality is vast: from a model of shared mainframe use to complex distributed architectures that blend machine learning, big-data processing and IoT protocols.

The NIST definition (prepared by the Information Technology Laboratory) covers five essential characteristics, three service models and four deployment models and remains the generally accepted framework for comparing cloud services. It does, though, capture an architectural snapshot rather than the dynamics of technological development. For a paradigm that is constantly evolving, this is a tangible limitation. The distance between that early concept and today's reality is vast: from a model of shared mainframe use to complex distributed architectures that blend machine learning, big-data processing and IoT protocols.

Legal regime of cloud services in the public sector. The Law of Ukraine "On Cloud Services" defines a "cloud service" as a service involving the provision of cloud resources by means of cloud computing technology, and "cloud resources" as technical and software assets access to which is provided by cloud technologies: computing power, storage, networks, databases, applications, and so on [7]. The wording is broad enough to encompass virtually any remote computing resource. This can create difficulties when it comes to drawing a line between cloud services and other forms of IT infrastructure outsourcing; in our view, the exact location of that boundary still awaits clarification from the regulator.

The Law tackles two interrelated tasks. First, the formalisation of the conceptual apparatus and models of cloud services at the legislative level. Second, the creation of instruments for admitting providers through the register mechanism, and the standardisation of cloud service consumption by state bodies by means of catalogues, a model contract and provider requirements [8].

A cornerstone of the Law is the distinction between public and commercial users. The concept of "public user" covers state bodies, local self-government bodies, state enterprises and institutions; for this category, additional

e-ISSN 2786-5533

restrictions and requirements apply that are absent for the commercial sector. The regulatory function rests with the State Special Communications Service.

The four service models enshrined in the Law IaaS, PaaS, SaaS and SECaaS are far from equivalent in practical weight. The inclusion of SECaaS in the list is, in our opinion, one of the legislature's most consequential decisions: it "embeds" cyber defence into the normative architecture of cloud services rather than leaving it as an optional add-on. These models differ markedly in how responsibility is distributed between provider and consumer, as the responsibility matrix makes clear (see Table 1). It is the IaaS model, specifically, that leaves the departmental administrator in control of encryption keys and security parameters critical for restricted-access data handled by SESU structures. Under SaaS, by contrast, control over encryption, updates and environment configuration is delegated entirely to the provider. PaaS sits somewhere in between. SECaaS functions as a complement compatible with any of the three base models, though in practice its integration with existing departmental software particularly the document-management and operational command systems of the SESU remains a methodologically unresolved question.

Table 1. Comparison of cloud service models: distribution of responsibility and key risks (summary). Compiled from NIST SP 800-145 and approaches to the classification of cloud risks/controls

Model	What the consumer controls	Typical benefits for the public sector	Key risks (examples)	Minimum "must-have" controls
IaaS	OS, configurations, network policies at the VM/container level; application services, data	rapid infrastructure scaling, recovery/redundancy, service migration	configuration errors, weak network segmentation, account compromise, DDoS/availability	hardening, network segmentation, MFA/PAM, logging, backup/DR plans

e-ISSN 2786-5533

PaaS	application logic, data, access policies, application lifecycle	accelerated development of government services, standardization of environments, DevSecOps	reduced infrastructure-level transparency, platform dependency, supply chain risks	CI/CD controls, SAST/DAST, secrets management, data policies, independent monitoring
SaaS	data, roles/access, security and compliance settings within the service	rapid deployment of capabilities (document management, collaboration), minimization of own infrastructure	data exfiltration via access errors, vendor lock-in, limited auditability	DLP policies, data classification, contractual SLA/audit rights, access control, user training
SECaaS	security policies (partially), integrations, response (partially)	scalable monitoring, centralized response, anti-phishing/endpoint protection	dependence on the security provider, integration errors, telemetry privacy risks	log/retention requirements, IR procedures, access control, independent validation of effectiveness
Community cloud (deployment)	shared governance rules, inter-participant agreements	possibility of a "government/departmental" cloud for similar functions	complexity of responsibility allocation, inter-organisational access risks	shared responsibility model, unified security profiles, centralised audit, segmentation

For structures that work simultaneously with open information in the alert system and with restricted information of operational units, a single service model is simply not viable. What is needed is a hybrid architecture whose parameters are shaped not only by technical reasoning but also by the

compliance requirements of the Law "On Cloud Services" and subordinate acts. We believe that designing such a hybrid architecture with a clear segregation of data by classification level and the corresponding service models is one of the most pressing practical tasks the SESU faces.

Cloud technologies in the practice of the SESU and the alert system. For the SESU, moving to cloud infrastructure is not about optimizing costs. It is a strategic necessity – the survivability under peak loads. In the event of a failure at one provider, data can be promptly transferred or restored from other resources; remote secured servers offer a level of protection that exceeds the capabilities of a typical local setup; users can access data from any location and any device.

A telling example is the deployment of the alert system based on Cell Broadcast technology in cooperation with mobile operators. During testing, messages appeared on the screen on top of applications and the lock screen, accompanied by a loud signal carrying timely information about threats and a recommended course of actions [9]. Cell Broadcast as a state e-communications service shows that the "cloudification" of the public sector goes beyond simply migrating storage facilities and registries – it is a shift to platform-based models of delivering information to citizens, where SLA availability, cyber resilience and incident management become critical. As of the completion of testing, the system covered 67% of mobile phone subscribers [10]. Whether that coverage is adequate for zones with damaged base infrastructure particularly in the Kharkiv, Zaporizhzhia and Kherson oblasts, where some towers have been destroyed or operate in a degraded mode remains an open question.

Plans for phased expansion of coverage to 95% of subscribers envisage the involvement of all mobile operators, but the pace of implementation hinges on factors well beyond technical capabilities: restoration of infrastructure in de-occupied areas, availability of equipment and the willingness of operators to invest in high-risk zones.

Cloud services are already present in the SESU's departmental environment, though perhaps not in the way one might expect. Materials available on the research and educational component of the system describe

the use of commercial cloud file-sharing services (Dropbox, Google Drive) for information storage a fact that speaks more to the organic penetration of commercial cloud solutions into departmental practice than to any purposeful migration strategy. For operational information systems, the compliance requirements of the Law "On Cloud Services" remain the first priority. From a privacy-by-design standpoint, it is of fundamental significance that the emergency alert system collects no personal data and works on the principle of broadcast delivery via base stations, which sets it apart technologically from SMS-based distribution [10].

Cyber defence in the cloud environment: national and international dimensions. The regulatory framework described above maps out the formal contours of cyber defence but does not exhaust the problem of putting it into practice. Ukrainian regulation builds cyber defence into cloud services along two tracks: by including SECaaS in the legislatively defined list of cloud service types, and by imposing requirements on providers in the areas of risk management, incident response, business continuity (BCP/DR), monitoring and incident reporting to the regulator and CERT-UA [10]. How fully these requirements are met in practice is a separate matter. Public data on the results of inspections of providers on the State Special Communications Service register have not, to our knowledge, been made available. We are compelled to note that the current oversight mechanism for providers remains opaque both to the academic community and, it would seem, to public users themselves.

At the international level, a comparable function is performed by the Cloud Security Alliance (CSA) – a non-profit organization that specializes in developing cyber security standards for cloud computing [11].

At the international level, a similar role is played by the non-profit organization Cloud Security Alliance (CSA), which specializes in developing cybersecurity standards for cloud computing [9].

The CSA CCM v4.1 controls matrix (207 controls across 17 domains) and the accompanying CAIQ v4.1 questionnaire provide a structured instrument for verifying a provider's security maturity [12]. Juxtaposing these with Ukrainian requirements reveals areas of overlap – incident management, business

continuity, audit – but also gaps: the CSA's requirements on the transparency of subcontracting chains are considerably more granular than the corresponding provisions of domestic legislation.

The architecture of the SESU's alert system creates a distinctive cyber defence profile. The system works on the principle of broadcast delivery via base stations and does not collect subscribers 'personal data. This rules out the targeted compromise of individual subscribers. It does, however, open up a different risk vector – mass-scale disruption of the alert infrastructure, where a failure hits not a particular user but the entire coverage zone of a base station. This threat profile is unlike the typical one for government information systems and, in our view, calls for a dedicated risk assessment model, one that takes into account not just the classical CIA triad but also a specific metric: the time to recovery of alert capability.

ENISA [13] stresses the multi-dimensional character of cloud risks, ranging from organisational and contractual ones (provider dependency, subcontractor obligations) to technical ones (multi-tenancy, loss of control over data). The Agency points to a paradox worth commenting on separately: the massive concentration of resources and data makes the cloud a more attractive target for attackers, yet cloud security tools thanks to the provider's economies of scale and specialization can actually be more reliable and more cost-effective than on-premise solutions. For the public sector, where migration decisions are frequently held up by security fears, this is an argument for a measured approach to migration, not a blanket refusal.

Risk assessment methodology for public users. From the regulatory field and cyber defence we now turn to the methodological toolkit, without which the requirements set out above remain little more than declarations.

The methodology we propose brings together the logic of ISO/IEC 27005 (context, assessment, risk treatment) and NIST SP 800-30 (identification of threats and vulnerabilities, assessment of likelihood and impact, determination of risk level) [14]. A caveat: neither standard was designed with the specifics of cross-border data transfer in an active combat zone in mind – a situation where data centres may be physically destroyed and communication channels degraded or intercepted. We adapt these frameworks to Ukrainian conditions,

e-ISSN 2786-5533

but the limitations of the base models should be kept in view. The methodology spans eight stages, which we present not as co-equal steps but with emphasis on those that prove most problematic for the public sector in particular.

The starting point defining the context is inseparable from the subsequent classification of data and the construction of a responsibility matrix. In practice these three steps form a single analytical frame: first, the system's objectives, user base, migration perimeter (which components move to the cloud, which stay on-premise) and cloud type are delineated; then data and services are classified according to CIA triad criteria and legal regime (personal data, restricted information, state secrets); finally, a matrix is built that maps out the zones of control of the provider and the consumer depending on the chosen service model. Splitting these stages apart means analysing context without understanding what data and at what sensitivity level will actually be processed.

Next comes the identification of threats (human error, malicious activity, technical failures, vulnerabilities in configurations, access mechanisms and integrations) and the assessment of likelihood and impact on a 1–5 scale, separately for each CIA triad parameter and additionally for "legal impact": sanctions, fines, reputational damage, service suspension. The sixth stage is the selection of response measures (avoidance, mitigation, transfer or acceptance of risk), accompanied by the formulation of a controls plan tied to the relevant standards.

The hardest stage in practice turns out to be the seventh: contractual assurance and compliance. The model contract and the provider requirements laid down by legislation set a minimum baseline. But for systems with heightened availability needs, that baseline is not enough. For the SESU's alert system, where even a short outage has direct implications for public safety, the contract must lock in an SLA with clearly specified penalties for breaching recovery-time targets not simply invoke general language about "continuity." Whether the providers on the State Special Communications Service register are actually prepared for commitments of this kind is a question that demands separate empirical investigation.

The final stage is continuous monitoring and reassessment: regular verification that controls are working, updating the risk assessment in light of

e-ISSN 2786-5533

incidents, testing recovery plans. And here an open methodological question arises: how often should the risk assessment be revisited for a system operating under conditions of active hostilities, where the threat landscape can shift in a matter of hours?

A problem in its own right is vendor lock-in. The limited number of providers in the register approved by the regulator effectively narrows the public user's options to a handful of suppliers. There is a paradox here: the register mechanism, whose purpose is to guarantee quality, simultaneously deepens dependence on a specific vendor – the very contradiction it was supposed to alleviate. We are forced to acknowledge that the current mechanism for updating the register does not keep pace with the dynamics of the cloud services market, and for public users with critical continuity needs this is a real risk. To the acceptability criteria for a cloud solution we propose adding not just lawfulness of data processing, compliance with provider requirements, incident control, continuity and auditability, but also a clearly articulated exit plan. Without one, the public user ends up in a situation where switching providers is technically feasible but organisationally and financially prohibitive. For the SESU the problem has a further dimension: the choice of provider for the alert system is not merely an IT-architecture question but a national-security question, one that, in our view, warrants a separate procedure for verifying the ultimate beneficial owners of cloud companies and their jurisdiction.

Conclusions. Cloud technologies in the Ukrainian public sector operate within a defined legal regime combining legislative definitions, special rules for public users and the mandatory risk-orientation of providers, with a focus on incidents, continuity and international standards. The regulatory field has been created. But whether it is sufficient is a different matter.

The analysis has brought to light three critical contradictions for which the current regulatory framework offers no exhaustive answer. The allocation of responsibility between provider and public user remains insufficiently detailed for hybrid architectures and yet it is precisely such architectures, as we have shown in the body of this article, that are unavoidable for structures with heterogeneous data flows. Under martial law, when the SESU's need for instantaneous resource scaling is especially acute and the speed of deploying additional capacity can be measured in hours, the bureaucratic inertia of the

e-ISSN 2786-5533

provider-register update mechanism risks becoming a critical factor.

The risk assessment methodology built on ISO/IEC 27005 and NIST SP 800-30 needs to be adapted to the specifics of individual agencies. Neither ISO nor NIST envisions a scenario in which the provider's or the consumer's infrastructure may be physically destroyed by a missile strike yet for the Ukrainian public sector this is not hypothetical but entirely realistic. For the SESU, with its broadcast-alert architecture, the threat profile differs from the standard one for government information systems. Are the existing methodologies adequate for systems where the consequence of a failure is not the loss of data confidentiality or integrity but the disruption of alerts to the civilian population? We believe the answer calls not only for regulatory refinements but also for empirical testing of the proposed methodology on real SESU infrastructure configurations, factoring in the bandwidth constraints of communication channels and the uneven mobile-operator coverage, especially in the eastern and southern oblasts.

References:

1. Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing* (NIST Special Publication 800-145). National Institute of Standards and Technology.

2. Юрчишин, В. Я. (2022). *Хмарні та Грід-технології: конспект лекцій* [Навчальний посібник]. КПІ ім. Ігоря Сікорського.

3. Ланде, Д. В., Субач, І. Ю., & Гладун, А. Я. (2021). *Оброблення надвеликих масивів даних*.

4. Нікітіна, Л. О., Дженюк, Н. В., & Борисова, Л. В. (2024). Експертна система для оцінки ризиків хмарних сервісів. *Системи управління, навігації та зв'язку*, *1*(75), 146–151. https://doi.org/10.26906/SUNZ.2024.1.146

5. Котяшічев, І. А., & Бирилова, Е. А. (2015). Захист інформації в «хмарних технологіях» як предмет національної безпеки. *Молодий вчений, 6.4*, 30–34.

6. Білова, Т. Г., & Ярута, В. О. (2015). Методи підвищення безпеки обробки даних в хмарних обчисленнях. *Збірник наукових праць Харківського національного університету Повітряних Сил, 4*(45), 71–73.

7. Верховна Рада України. (2023). *Про хмарні послуги* (Закон України № 15, ст. 52).

8. Верховна Рада України. (2015). *Про публічні закупівлі* (Закон України № 922-VIII). https://zakon.rada.gov.ua

9. ДСНС України. (2026). ДСНС продовжує розгортання системи оповіщення із використанням високотехнічної технології. https://www.rv.gov.ua/news/dsns-prodovzhuye-rozgortannya-sistemi-opovishchennya-iz-vikoristannyam-visokotehnichnoyi-tehnologiyi

10. Суспільне. (2022). Система екстреного сповіщення населення охоплює 67% абонентів мобільних – ДСНС. https://suspilne.media/286942-sistema-ekstrenogo-spovisenna-naselenna-ohoplue-67-abonentiv-mobilnih-dsns/

11. Cloud Security Alliance. (2024). *Cloud Controls Matrix (CCM) v4.1*. https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4-1

12. European Union Agency for Cybersecurity (ENISA). (2012). *Cloud computing: Benefits, risks and recommendations for information security*. https://www.enisa.europa.eu/sites/default/files/all_files/ENISA%20-%20Cloud%20Computing%20-%20final.pdf

13. National Institute of Standards and Technology. (2011). *Special publication 800-145: The NIST definition of cloud computing*. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

14. Cloud Security Alliance (CSA). Official website. URL: https://cloudsecurityalliance.org/

Funding. This research received no external funding.

Use of AI. During the preparation of this article, the authors used artificial intelligence tools for the technical editing of the text in Table 1. All research results, conclusions, and interpretations were obtained by the authors independently. The authors bear full responsibility for the content of the article.

Acknowledgments. The author declares no acknowledgments.

Received: 15.04.26
Accepted: 26.05.26
Published: 26.06.26