UDC 528.4:004.056 **doi:** https://doi.org/10.20998/3083-6298.2025.01.01

Eyyub Abdul oglu Abbasquliyev[1]

[1]Azerbaijan Technical University, Baku, Azerbaijan

SECURITY AND FUNCTIONALITY OF GEOGRAPHIC INFORMATION SYSTEMS: CLASSIFICATION APPROACHES AND USAGE MODELS

Abstract. Topicality. In the context of the rapid growth of the volume and importance of geospatial information, geographic information systems (GIS) are becoming an integral element of digital infrastructure, especially in critical industries such as transport, defense, energy, and healthcare. The relevance of the study is due to the need for a comprehensive understanding of architectural features, usage models, and risks associated with information security in modern GIS. The **subject of the study** is classification approaches to geographic information systems, their usage models, and the characteristic cybersecurity threats to which they are exposed. The study analyzed the key criteria for classifying GIS, reflecting both the technical aspects of building systems and the features of their application in applied tasks. Particular attention was paid to the connection of architectural models with vulnerabilities and attack vectors characteristic of each type of system. The **purpose of the study** is a comprehensive analysis of usage models and classification features of GIS from the point of view of information security, as well as the identification of effective protection mechanisms aimed at reducing cyber threats. As a **result**, a comparison of typical threats with GIS architectural models was carried out, and the most effective means of protection were also identified - from multi-factor authentication and network segmentation to the use of incident monitoring systems and cryptographic methods. **Conclusions**. The results of the study confirm the need to adapt security mechanisms to a specific architecture and model of GIS use. A comprehensive approach to classification, threat analysis and selection of protective measures allows significantly increasing the resilience of geographic information systems to cyberattacks and ensuring their safe operation in the conditions of digitalization and increasing technological risks.

Keywords: geographic information systems, information security, cyber threats, data protection, attack resistance, system division.

1. Introduction

The relevance of the problem. With the rapid growth of geospatial information volumes and its importance for management, monitoring and planning, geographic information systems (GIS) are taking an increasingly important place in the digital infrastructure of various industries. Today, GIS are used not only in traditional areas such as cartography, ecology or urban planning, but also in critical areas, including transport, defense, energy and healthcare. GIS usage models determine both the nature of the tasks solved by the system and the approaches to organizing interaction with users and other information platforms. They serve as a basis for analyzing the functionality, scope of application and architectural features of specific GIS implementations.

However, as the scope of application expands and the technical architecture becomes more complex, the risks associated with the cybersecurity of such systems also increase. GIS are increasingly becoming targets for attacks by intruders, especially in cases where they are associated with critical information infrastructure objects. Potential threats include unauthorized access to spatial data, interference in analysis and visualization processes, compromise of communication channels, and violations of the integrity and availability of information.

In this regard, a necessary stage of the study is the systematization of existing GIS by key features reflecting both their technical organization and applied tasks. Classification of geographic information systems allows structuring the diversity of platforms and solutions, which is important both for understanding their functional capabilities and for choosing adequate information protection mechanisms. Particular attention should be paid to classifications and models of GIS use, since they set the context of the system's functioning, determine its vulnerable components and influence approaches to ensuring security.

The aim of the studyis to conduct a comprehensive analysis of the classification features of GIS, models of GIS use and their functional features, as well as interaction with current threats to information security in the modern digital environment. At the same time, special attention is paid to the analysis of existing protection mechanisms that make it possible to increase the resistance of GIS to cyber threats and ensure their safe operation in the context of increasing digital vulnerability.

2. Main part

2.1. Classification of geographic information systems and models of their use. Classification of geographic information systems is a tool that allows you to select or develop a solution that best meets the requirements established at the preliminary stage of analysis. It makes it possible to identify typological features of various GIS, as well as systematize existing solutions according to a number of criteria covering both technical parameters and functional aspects.

Geoinformation systems can be classified by a variety of features and characteristics [1-3]. However, it is important to consider that high competition among leading developers of specialized software stimulates constant updating and improvement of GIS products. As a result, classification criteria remain relevant only within a specific stage of technological development.

Taking into account the generalized features and parameters, when analyzing modern GIS, it is advisable

to rely on the classification characteristics presented in Table 1.

Table 1 – **Parameters of classification of geographic information systems**

Parameter name	GIS type
Level of specialization	universal (ecological, transport, cadastral, nature protection, geological, engineering communications and urban economy, emergency situations, industrial cartographic, socio-economic GIS) and specialized (navigation, GIS for business, health protection, agriculture, archaeological, etc.)
Scope of coverage	local, regional, national, global
Architecture	desktop, server, cloud, distributed
Data type	raster, vector, combined, two-dimensional, three-dimensional, etc.
Purpose	analytical, monitoring, navigation, management, information and reference, research, publishing, educational, multi-purpose
Form of interaction	user-oriented, integration (API, WebGIS), automated
Industry application	in urban development, agriculture, national defense, healthcare, etc.

As can be seen from Table 1, modern geographic information systems are characterized by significant diversity, which reflects the breadth of their application and the complexity of the tasks they solve. When classifying GIS, it is necessary to take into account a number of parameters: from the level of specialization and scale of coverage to the architecture and form of interaction. This allows for flexible adaptation of GIS to specific needs - be it local solutions in urban development or large-scale national monitoring systems. Thus, classification features serve as the basis for selecting, designing and assessing the effectiveness of GIS depending on the tasks, area of application and technical conditions.

A visual representation of some types of GIS is shown in Fig. 1.

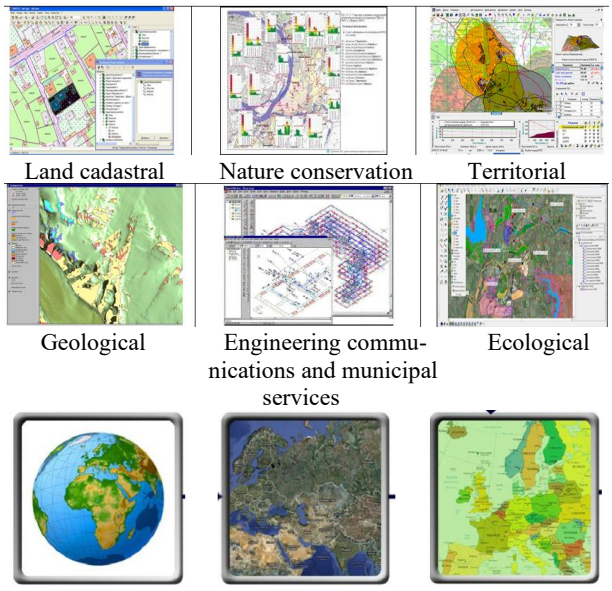

Fig. 1. Types of geographic information systems according to various classification criteria

As can be seen from Figure 1, a significant number of diverse geographic information systems have been created over the past decades. This has led to the emergence of a large number of classification approaches, each of which systematizes this diversity in a different way, grouping systems into homogeneous categories based on one or more characteristics. In general, existing GIS classifications can be divided into three main areas [1], which are based on the following features:

by functional purpose, that is, depending on the purposes for which the system is used;

by subject-thematic orientation, which reflects the specifics of the area of application;

by the scale of territorial coverage, which is determined by the volume of spatial data and the size of the territory covered by geodata within a specific GIS.

Table 2 provides a systematic classification of GIS by purpose, subject matter and territorial coverage.

Table 2 – **Systematized classification of geographic information systems according to classification criteria**

Types of GIS	Characteristic
Classification criterion:	
By appointment	
Multipurpose	They are used for a wide range of tasks, most often at the regional level.
Specialized:	They solve one or more specific problems
information and reference	Quick access to spatial data
monitoring	Monitoring the state of the natural environment, infrastructure, etc.
inventory	Accounting of objects (forests, reservoirs, buildings)
decision support (DSS)	Scenario analysis, forecasting
research	Scientific analysis, modeling
educational	Educational goals, students' practice
By application topic	
Land cadastral	Land registration, cadastre, legal information
Ecological and natural resource	Environmental assessment, natural resource management
Engineering communications and housing and communal services	Urban Infrastructure Management
For emergency situations	Modeling, response, forecasting of disasters
Navigation	GPS navigation, routing

Types of GIS	Characteristic
Socio-economic	Demography, urban studies, territorial development analysis
Geological	Study of the structure of the earth's crust, deposits
Transport	Transport logistics, traffic modeling
Trade and marketing	Consumer behavior analysis, market zoning
Archaeological	Registration of archaeological monuments and territories
Military	Spatial planning, tactical maps
Others	New or mixed directions, developing areas of application
By territorial coverage	
Global	The entire planet or large regions
National	GIS covering the entire territory of the country
Regional	Administrative areas, drainage basins, etc.
Local / Municipal	Small areas: cities, municipalities

A study of the data in Table 2 allows us to conclude that the classification of geographic information systems plays a key role in:

simplifying the process of selecting a platform that corresponds to the specifics of the tasks being solved;

coordinating functional requirements with the architectural features of the selected solution;

more rational distribution of resources and ensuring the system's resilience to failures;

increasing the level of security and manageability of the information infrastructure.

A well-conducted classification helps to adapt the GIS architecture to specific operating conditions, taking into account both technical parameters and applied goals. It is closely related to use models that describe practical scenarios for implementing geographic information systems in areas such as cybersecurity, incident management, logistics, environmental monitoring, and others.

The specifics of research and operation of geoinformation systems directly influence the formation of approaches to their practical use. Depending on the tasks set, emphasis is placed on optimizing spatial resource management, increasing the effectiveness of response in emergency situations, ensuring the sustainability of infrastructure and its information security, and reducing potential risks.

Based on this, GIS application models can be divided into the following types:

analytical, which are focused on strategic planning and long-term forecasts, including threat analysis and development of directions for creating a secure digital infrastructure;

situational, which allow identifying anomalies and potential threats based on the analysis of spatio-temporal data;

operational, which are aimed at supporting decision-making in real time, which is especially relevant when responding to cyber incidents or natural disasters.

Table 3 presents the relationship between the characteristics of geographic information systems, their usage models, and an example of the application of these models in the field of cybersecurity with an emphasis on GIS tools.

Table 3 – **Relationship between the features of geographic information systems and their usage models and cybersecurity**

Peculiarity	Characteristics of the feature	Impact of a feature on the usage pattern	Cybersecurity Use Case
Heterogeneity of subsystems and data	Data of different types (spatial, text, time), complex relationships	Building Multi-Level Embedded Models for Attack Analysis	Integrate attack logs and device geolocations to detect suspicious patterns
A large number of interrelated tasks	Data analysis, forecasting, visualization, decision making	Creation of analytical and operational response models	Automatic detection of broken nodes and construction of threat propagation routes
The presence of uncertainty	Inaccurate, incomplete or noisy incident data	Implementation of risk-aware and fuzzy data models (fuzzy models, probabilistic models)	Predicting the Probability of a Successful Attack Based on Incomplete Data
The need to combine quantitative and qualitative analysis	Combination of numerical methods and expert assessments	Using Hybrid Models for Decision Making	Combining Machine Learning and Expert Ratings to Rank Risks
Dynamics of processes	Constant changes in the real information environment	Using real-time models and situational monitoring	Visualize attacks in real time on network maps for rapid response

As Table 3 shows, the spatial nature of many modern threats makes the use of geographic information systems in cybersecurity particularly important. Cyberattacks can be associated with specific geographic areas, affect distributed infrastructure facilities, or require rapid coordination of actions across different territories. GIS tools not only display such threats on a map, but also conduct spatial analysis of possible attack vectors, identify critically vulnerable areas, and build effective defense strategies based on geodata.

This approach forms the basis for a comprehensive threat analysis and the implementation of analytical, situational and operational models adapted to various levels of management – from strategic to tactical and operational. This relationship between the levels of application of GIS models and cybersecurity tasks is clearly presented in Table 4.

Table 4 – **Use of geographic information systems models in cybersecurity by levels of model application**

GIS model view	Use in GIS	Use in GIS-based cybersecurity
Strategic level of application of the model		
Analytical	Construction of conceptual models of territorial use, strategic infrastructure planning	Identifying Geospatial Risks to Critical Infrastructure, Strategic Cyber Defense Planning
Tactical level of application of the model		
Situational	Route optimization, resource management	Modeling Possible Cyberattack Routes Through Geo-Referenced Network Nodes
*Operational*level of application of the model		
Operational	Monitoring environmental changes, rapid response	Real-time attack detection, rapid visualization of cyber threats on geomaps
*Tactical and operational*level of application of the model		
Situational, operational	Localization of accidents, management of response services	Localization of security incidents, coordination of response teams using geospatial data

The analysis of Table 4 demonstrates that the application of geographic information system models in the field of cybersecurity covers all key management levels – from strategic to operational. At the strategic level, analytical GIS models allow identifying critical vulnerabilities in infrastructure and developing long-term plans for ensuring cybersecurity taking into account spatial analysis. The tactical level involves the use of situational models to predict possible attack routes and assess the degree of threats. Operational models ensure rapid detection of cyber incidents and their visual display in real time. At the tactical and operational level, GIS are used to accurately determine incident locations and effectively coordinate the actions of response teams.

Among the approaches to classifying models that use geoinformation systems, an important place is occupied by the division into centralized, decentralized, cloud and distributed models [4-8]. The analysis showed that each of them differs in both functional capabilities (in the field of collecting, processing, storing, analyzing and visualizing spatial data) and the way of interaction with other information systems. Let us consider these types of models in more detail.

1. Centralized GIS models assume the concentration of all data and computing resources in a single data processing center (DPC). Their functions include centralized collection of geodata (via sensors, satellites, and field research), information processing on powerful servers, storage in a single database, centralized analysis, and visualization on local workstations. Integration with other information systems (IS) is implemented at the level of corporate applications and databases. The advantages of these models are high control over the system and data, and the limitations are poor scalability with increasing load.

2. Decentralized GIS models distribute data and computing resources across different organizations or departments. Data collection, storage, and processing are performed locally, with the ability to combine information when needed. Analytics are performed both locally and at an aggregated level. Visualization is performed through interfaces of individual nodes, and interaction between systems is ensured through standardized protocols (e.g., OGC, API). The advantages of such models are: resilience to failures and flexibility in management, the disadvantage is the difficulty in synchronizing and coordinating data.

3. Cloud GIS models host both data and services in the infrastructure of cloud platforms (such as AWS, Azure, Google Cloud). Data comes directly to the cloud from sensors and IoT devices, is processed using scalable cloud computing and is stored in distributed storage. Analysis is performed using Big Data and artificial intelligence, visualization is via web interfaces. Integration with other IS is possible via API and microservice architectures. Advantages: high scalability and availability, ease of collaboration. The main limitation is the need to ensure the security and reliability of the cloud infrastructure.

4. Distributed GIS models combine geodata and computing resources located at different points into a single logically connected system. Data is collected in a decentralized manner, processed both locally and on server nodes, and stored in distributed storage. An important feature is the ability to simultaneously analyze spatial information from different regions in real time and display it in a unified interface. Interaction with external IS is provided through spatial data exchange standards (WMS, WFS, WCS). The advantages of these models are: flexibility of architecture and high scalability. Limitation is the increased complexity of data management and maintaining their consistency.

Thus, the conducted analysis shows that when choosing a model for using geographic information systems, it is necessary to take into account not only the goals of a specific project, requirements for processing speed and scale of data coverage, but also pay attention to the level of system reliability, as well as the specifics of ensuring information security. An effective solution should take into account both the functional tasks and the vulnerabilities inherent in various GIS architectures.

2.2. Threats and security mechanisms in GIS. Analysis of models of using geographic information systems and approaches to ensuring information security within various GIS architectures shows that the choice of one or another model directly depends on the specifics of tasks in the field of cybersecurity. In this regard, a comprehensive study of the key threats that accompany the functioning of GIS in different application scenarios, as well as a thorough analysis of information protection mechanisms at all stages of the life cycle of geographic information systems, becomes especially relevant.

The issues of information security (IS) and the corresponding protective mechanisms in geographic information systems are the subject of many scientific

studies. The works [9-11] consider IS threats in government information systems, including GIS: the features of their categorization are analyzed, as well as approaches to ensuring security in conditions of uncertainty and instability. The authors of the study [12] propose a classification of key threats to geographic information systems, such as unauthorized access, data forgery and distributed attacks such as DDoS, and develop corresponding methods for their prevention.

A number of studies [13-15] focus on identifying vulnerabilities in systems that use geospatial data to restrict access. These studies propose technical and organizational security measures, including cryptographic methods, authentication and identification mechanisms, and risk assessment procedures in the context of digitalization and increased information security requirements.

Some studies, in particular [16-18], analyze in more depth the models and technologies of information security in modern geographic information systems. Particular attention is paid to protecting the confidentiality, integrity, and availability of geospatial data and services, especially in distributed environments, critical infrastructures, and in the presence of active cyber threats. Various technical solutions are studied: from access control policies and cryptographic algorithms to intrusion detection systems and risk assessment methods.

Modern trends also show the active implementation of intelligent approaches: neural networks and machine learning algorithms. These technologies are used to identify anomalies, predict threats and adaptive response, which significantly increases the effectiveness of GIS protection in a dynamically changing and complex cyber environment. [9,10,14,17,18]

Summarizing the research in this area, we can highlight the following relationships between the main threats to information security characteristic of GIS, the corresponding protective mechanisms and the above-considered models of GIS construction – centralized, decentralized, cloud and distributed (Table 5).

Table 5 – **Correspondence between key security threats, models of geographic information systems that are susceptible to these threats and the protection mechanisms applied**

Security threat	Affected GIS models	Appropriate protective mechanisms
Unauthorized access (via weak passwords, lack of MFA, software vulnerabilities)	Centralized, cloud, decentralized	- Role-based access model (RBAC) - Multi-factor authentication (MFA) - Action logging - Network segmentation and firewalls
Forgery/distortion of spatial data (coordinates, routes, zones, etc.)	All models, especially distributed and cloud	- Digital signatures - Hash control of data integrity - Encryption of spatial information - Audit of GIS component code
Attacks on network infrastructure (DDoS, exploits, traffic interception)	Distributed, cloud	- Firewalls, VPN - SIEM systems, IDS/IPS - TLS/SSL encryption - Geoanalytics of incidents
Malware, injection attacks (SQL injections, malware injection via web interfaces and APIs)	Cloud, centralized	- Web filtering - Regular updates and patches - Behavioural detection (UEBA) - Input data validation
Data leakage or corruption (storage breach, data interception, failures or internal actions)	Cloud, centralized, distributed	- Encryption at rest (AES, etc.) - Backup and backup integrity check - Access control - Secure cloud storage configurations

An analysis of Table 5 shows that threats to information security in geographic information systems vary depending on their construction model. Thus, cloud and distributed GIS are more vulnerable to network attacks, data leaks and malware, which requires the use of a wide range of protective mechanisms: from encryption and authentication to SIEM systems and data integrity control. Centralized models, although easier to manage, require enhanced access control and protection of the central node. Decentralized systems face problems of coordination and synchronization of security measures between segments. Thus, the choice and implementation of protective mechanisms should take into account the GIS architecture, as well as the nature and scale of potential threats.

3. Conclusions and prospects for further development

Based on the conducted research, it can be concluded that effective information security of geographic information systems is impossible without taking into account the architectural specifics of their construction and the characteristics of the threats that such systems face. The variety of GIS models determines both technical characteristics and potential attack vectors. Connection to external data sources, the use of open source software, online work, distributed computing increase the risks associated with data compromise, denial of service, violation of the integrity and availability of services. The most critical threats remain such as forgery and distortion of spatial data, unauthorized access, DDoS attacks, exploits of web interfaces and physical impact on sensory elements of the infrastructure. A particularly high degree of vulnerability is observed in GIS used in critical sectors: energy, defense, industry and smart control systems.

Thus, ensuring the sustainability of geoinformation infrastructure requires a comprehensive and multi-level approach, including cryptographic protection, multi-factor authentication, isolation of network segments,

continuous auditing, a monitoring and incident management system, as well as reliable backup and recovery mechanisms.

Prospects for further research in this direction may include:

development of adaptive threat management models using machine learning and neural networks;

integration of mechanisms for trusted transmission and verification of geodata in distributed and cloud GIS;

creation of standard threat models for specific industry GIS (transport, housing and communal services, defense);

study of the impact of digital sovereignty and regulatory requirements on GIS architecture and security in different jurisdictions;

expanding risk analysis methods to take into account geospatial dependencies and user behavior patterns.

Such research will increase the resilience of geographic information systems to modern cyber threats and ensure their reliable operation in critical conditions.

REFERENCES

1. Heoinformatsiini systemy i bazy danykh: monohrafiia (2014) / V. I. Zatserkovnyi, V. H. Burachek, O. O. Zhelezniak, A. O. Tereshchenko. – Nizhyn: NDU im. M. Hoholia. – 492 s.
2. Rich S. (2011) Geograficheskie informacionnye sistemy (GIS) dlja administrativno-hozjajstvennogo upravlenija / Stjuart Rich, Kevin H. Djevis. – IFMA Foundation.; per. s angl. – M.: Data+.
3. Geographic Information Systems and Pandemic Influenza Planning and Response. – Режим доступа: http://www.esri.com/library/index.html.
4. Alekseev M.M. (2016) Geoinformacionnye sistemy: Uchebnoe posobie. – M.: Aspekt Press. – 287 s.
5. Kudrjashov I.F., Shishkin A.G. (2017) Geoinformacionnye tehnologii v upravlenii territorijami. – M.: Logos. – 296 s.
6. Longley P.A., Goodchild M.F., Maguire D.J., Rhind D.W. (2015) Geographic Information Systems and Science. – Wiley. – 500 p.
7. Goodchild M.F. (2010) Twenty years of progress: GIScience in 2010 // *Journal of Spatial Information Science*. – № 1. – Pp. 3-20.
8. Yang C., Huang Q., Li Z., Liu K., Hu F. (2017) Big Data and Cloud Computing: Innovation Opportunities and Challenges for GIS // *Computers, Environment and Urban Systems*. – T. 61. – Pp. 93-102.
9. Prokushev Y. E., Ponomarenko S. V., Ponomarenko S. A. (2021) Modeling the processes of designing information security systems in state information systems // *Computational Nanotechnology*. – Vol. 8, Iss. 1. – Pp. 26-37.
10. Gryzunov V. V. (2021) Konceptual'naja model' adaptivnogo upravlenija geoinformacionnoj sistemoj v uslovijah destabilizacii // *Problemy informacionnoj bezopasnosti. Komp'juternye sistemy*. – № 1. – S. 102-108.
11. Gavdan G. P., Penerdzhi R. V. (2020) Obespechenie bezopasnosti informacii gosudarstvennyh informacionnyh sistem v uslovijah neopredelennosti // *Bezopasnost' informacionnyh tehnologij*. – T. 27, № 3. – S. 3-10.
12. Tatarnikova T. M., Jagotinceva N. V. (2016) Ugrozy informacionnoj bezopasnosti GIS // *Regional'naja informatika i informacionnaja bezopasnost'*. – Vyp. 2. – S. 137-142.
13. Shahtorin M. S. (2023) Analiz ugroz informacionnoj bezopasnosti v sistemah cifrovogo upravlenija // *Vestnik nauki*. – № 2 (83), t. 2. – S. 93-100.
14. Zarubina Ju. V., Turkin M. E. (2023) Informacionnaja bezopasnost' v uslovijah cifrovoj jekonomiki // *Sbornik nauchnyh trudov Angarskogo gosudarstvennogo tehnicheskogo universiteta*. – № 1. – S. 365-368.
15. Borshheva N. V. (2019) Osobennosti postroenija modeli ugroz bezopasnosti informacii dlja gosudarstvennyh informacionnyh sistem // *Sovremennye problemy proektirovanija, proizvodstva i jekspluatacii radiotehnicheskih sistem*. – S. 163-166.
16. Tatarnikova T. M., Jagotinceva N. V. (2016) Model' obespechenija informacionnoj bezopasnosti GIS // *Nauchnyj al'manah*. – № 1-1 (15). – S. 521-523.
17. Pavlenko E. Ju., Kudinov K. V. (2019) Obespechenie kiberustojchivosti krupnomasshtabnoj setevoj infrastruktury s ispol'zovaniem murav'inogo algoritma // *Problemy informacionnoj bezopasnosti. Komp'juternye sistemy*. – № 4. – S. 85-92.
18. Krundyshev V. M. (2019) Obespechenie kiberbezopasnosti cifrovogo proizvodstva s pomoshh'ju sovremennyh nejrosetevyh metodov // *Problemy informacionnoj bezopasnosti. Komp'juternye sistemy*. – № 4. – S. 75-84.

Received (Надійшла) 21.04.2025
Accepted for publication (Прийнята до друку) 12.05.2025

ВІДОМОСТІ ПРО АВТОРІВ/ ABOUT THE AUTHORS

Аббаскулієв Еюб Абдул огли – аспірант по технологічним наукам, Азербайджанський технічний університет, Баку, Азербайджан;
Eyyub Abdul oglu Abbasquliyev – PhD student in Technology, Azerbaijan Technical University, Baku, Azerbaijan;
e-mail: formemaybe23@yahoo.com; ORCID Author ID: https://orcid.org/0009-0003-7714-5494.

БЕЗПЕКА І ФУНКЦІОНАЛЬНІСТЬ ГЕОІНФОРМАЦІЙНИХ СИСТЕМ: КЛАСИФІКАЦІЙНІ ПІДХОДИ І МОДЕЛІ ВИКОРИСТАННЯ

Еюб Абдул огли Аббаскулієв

Анотація. Актуальність теми. В умовах стрімкого зростання обсягів та значущості геопросторової інформації геоінформаційні системи (ГІС) стають невід'ємним елементом цифрової інфраструктури, особливо в критично важливих галузях, таких як транспорт, оборона, енергетика та охорона здоров'я. Актуальність дослідження зумовлена необхідністю комплексного розуміння архітектурних особливостей, моделей використання та ризиків, пов'язаних з інформаційною безпекою у сучасних ГІС. **Предметом дослідження** виступають класифікаційні підходи до геоінформаційних систем, моделі їх використання, а також характерні загрози кібербезпеці, яким вони піддаються. В рамках дослідження проаналізовано ключові критерії класифікації ГІС, що відображають як технічні аспекти побудови систем, так і особливості їх застосування у прикладних задачах. Особливу увагу приділено зв'язку архітектурних моделей з уразливістю та векторами атак, характерними для кожного з типів систем. **Мета дослідження** – всебічний аналіз моделей використання та класифікаційних ознак ГІС з погляду інформаційної безпеки, а також виявлення ефективних механізмів захисту, спрямованих на зниження кіберзагроз. В **результаті** проведено зіставлення типових загроз з архітектурними моделями ГІС, а також визначено найефективніші засоби захисту – від багатофакторної аутентифікації та сегментації мережі до використання систем моніторингу інцидентів та криптографічних методів. **Висновки**. Результати проведеного дослідження підтверджують необхідність адаптації механізмів забезпечення безпеки до конкретної архітектури та моделі використання ГІС. Комплексний підхід до класифікації, аналізу загроз та вибору захисних заходів дозволяє суттєво підвищити стійкість геоінформаційних систем до кібератаків та забезпечити їх безпечну експлуатацію в умовах цифровізації та зростання технологічних ризиків.

Ключові слова: геоінформаційні системи, інформаційна безпека, кіберзагрози, захист даних, стійкість до атак, розподілені системи.