UDC 378.147:004.056:519.17
https://doi.org/10.31612/2616-4868.6.2026.16

METHODOLOGY FOR TEACHING GRAPH THEORY IN CYBERSECURITY PROBLEMS OF MEDICAL INFORMATION SYSTEMS FOR MEDICAL AND BIOTECHNOLOGY STUDENTS

Yurii M. Litvin, Pavlo V. Mykytenko, Liliia B. Desiatniuk, Svetlana V. Kolpakova, Inna I. Kucherenko

Bogomolets National Medical University, Kyiv, Ukraine

Abstract

Introduction. The rapid digitalization of healthcare has increased the reliance of medical institutions on complex information systems, making cybersecurity a critical component of healthcare practice and an essential competence for future healthcare and biotechnology professionals. Graph theory provides an effective mathematical framework for modeling medical information networks, identifying critical infrastructure components, analyzing vulnerabilities, and optimizing cybersecurity strategies.
Aim. To develop and scientifically substantiate a methodology for teaching graph theory methods through problems involving the minimization of the set of protected network nodes for students of medical and biotechnology specialties.
Materials and methods. The study employed theoretical, mathematical, and pedagogical methods. A review of the scientific literature on graph theory, cybersecurity, medical informatics, and professionally oriented education was conducted. Medical information systems were modeled as graphs, and the cybersecurity task was formulated as the minimum vertex cover problem. A systems approach was applied to analyze healthcare information infrastructures as interconnected digital environments.
Results. A methodology integrating graph theory, medical informatics, and cybersecurity was developed and demonstrated using a hospital information network model. The proposed approach enabled students to represent medical information systems as graphs, analyze communication structures, identify critical network components, and determine the minimum set of protected nodes required to secure all communication channels. The use of professionally oriented cybersecurity tasks promoted the development of algorithmic thinking, systems analysis skills, and a practical understanding of information security principles.
Conclusions. The application of graph-theoretical models, particularly the minimum vertex cover problem, provides an effective framework for analyzing network vulnerabilities, identifying critical infrastructure components, and developing evidence-based cybersecurity strategies. The use of real-world healthcare scenarios promotes algorithmic and systems thinking, strengthens analytical skills, and enhances students' motivation to study mathematical disciplines.

Keywords: **medical information systems, graph theory, cybersecurity.**

INTRODUCTION

The rapid digitalization of healthcare has significantly increased the reliance of medical institutions on complex information systems, including electronic health records, laboratory information systems, telemedicine platforms, diagnostic devices, and bioinformatics databases. While these technologies improve the efficiency and accessibility of healthcare services, they also increase the vulnerability of healthcare infrastructures to cyber threats and unauthorized access to sensitive medical data. As a result, cybersecurity has become a critical component of modern healthcare systems and an important area of professional competence for future healthcare and biotechnology professionals.

Graph theory is one of the most effective mathematical tools for modeling and analyzing complex network structures. Graph-based approaches enable the representation of medical information systems as interconnected nodes and communication links, allowing the identification of critical infrastructure components,

assessment of potential attack pathways, and optimization of cybersecurity strategies. In particular, graph-theoretical problems such as the minimum vertex cover problem, network connectivity analysis, and critical node detection have shown considerable potential for improving the security and resilience of information systems.

At the same time, the growing demand for digitally competent healthcare professionals requires the integration of cybersecurity concepts into medical and biotechnological education. However, discrete mathematics and graph theory are often perceived by students as highly abstract disciplines with limited practical relevance to their future professional activities. This perception may reduce students' motivation to learn and hinder the development of applied analytical skills. Therefore, the use of professionally oriented educational approaches that connect mathematical concepts with real healthcare challenges is becoming increasingly important.

In this context, cybersecurity scenarios involving medical information systems offer a valuable framework for teaching graph theory through interdisciplinary learning. The application of graph models to analyze network vulnerabilities, identify critical nodes, and determine the minimum set of network nodes requiring protection enables students to develop algorithmic thinking, systems analysis skills, and an understanding of information security principles within healthcare environments. Such an approach supports the integration of discrete mathematics, medical informatics, and cybersecurity while enhancing the practical relevance of mathematical education.

Therefore, the development of a methodology for teaching graph theory through cybersecurity tasks in medical information systems represents an important educational challenge that addresses both the digital transformation of healthcare and the need to prepare future healthcare and biotechnology professionals for work in secure and technologically advanced healthcare environments.

AIM

To develop and scientifically substantiate a methodology for teaching graph theory methods in problems related to minimizing the set of protected network nodes, intended for students of medical and biotechnological specialities.

MATERIALS AND METHODS

The study was based on a theoretical and methodological analysis of teaching graph theory in the context of cybersecurity of medical information systems for students of medical and biotechnological specialities. The research employed a combination of theoretical, mathematical, and pedagogical methods. Theoretical analysis was used to examine scientific literature on graph theory, discrete mathematics, cybersecurity, medical informatics, and professionally oriented education. Mathematical modelling was applied to represent medical information systems as graphs and to formulate the problem of minimizing the set of protected network nodes using the minimum vertex cover approach. A systems approach was utilized to consider medical information systems as interconnected information, technical, and organizational components within a unified digital environment. Pedagogical modeling and instructional design methods were employed to develop a teaching methodology based on professionally oriented cybersecurity case studies. The proposed methodology integrates graph-theoretical concepts, medical informatics, and cybersecurity tasks, enabling students to analyze network vulnerabilities, identify critical nodes, and develop algorithmic and systems-thinking skills through real-world healthcare scenarios.

RESULTS

Network analysis has emerged as a powerful interdisciplinary framework for understanding complex systems in healthcare. By representing healthcare entities – such as hospitals, medical devices, healthcare professionals, patients, or biological components – as nodes and their relationships as edges, researchers can uncover critical patterns of interaction, influence, and information flow. Among the various analytical tools available, network centrality measures play a central role in identifying the most important entities within these systems.

Centrality measures quantify the structural importance of individual nodes based on their position and connectivity within a network. The most widely used metrics include degree centrality (the number of direct connections), betweenness centrality (control over information flow between other nodes), closeness centrality (the efficiency of reaching other nodes), and eigenvector centrality (influence derived from connections to other highly influential nodes). These metrics translate abstract graph-theoretical concepts into practical insights for healthcare management, epidemiology, and clinical decision-making.

In the healthcare domain, network centrality analysis has found diverse and impactful applications. It is used to identify super-spreaders in infectious disease transmission networks, key opinion leaders in professional collaboration networks, central hospitals in patient-sharing and referral networks, and critical components of medical information infrastructures. Such analyses support more effective resource allocation, targeted interventions, infection control strategies, and cybersecurity measures in increasingly digitalized healthcare environments.

The ongoing digitalization of healthcare, including the widespread adoption of electronic health records, laboratory information systems, and medical imaging archives, has created highly interconnected networks that are vulnerable to disruptions and cyber threats. In this context, understanding which nodes play pivotal roles is essential not only for optimizing operational efficiency

but also for strengthening the resilience and security of healthcare information systems.

This study applies the minimum vertex cover problem – a fundamental graph-theoretical problem closely related to network protection strategies – to a typical hospital medical information network. By modelling the system as a graph and identifying the minimum set of network nodes requiring protection to secure all communication channels, the study demonstrates how discrete mathematics and network analysis can be effectively integrated into medical education and practical cybersecurity in healthcare settings.

The following sections present the mathematical model, visual and pedagogical analysis, computational solution using Microsoft Excel Solver, and broader implications for teaching graph theory in the context of medical cybersecurity.

Mathematical Model of the Study

The medical information system is modeled as a graph:

$$G = (V, E)$$

where V – the set of system nodes (vertices), E – the set of data transmission channels (edges).

The objective is to find the minimum set of vertices of the given graph, specifically:

$$S \subseteq V, \quad |S| \to \min$$

where is the set of nodes that must be protected to ensure the security of the entire network under the condition:

$$\forall\, e \in E, \quad e \cap S \neq \emptyset$$

This model corresponds to the Minimum Vertex Cover problem [1].

Example task for teaching graph theory in the context of cybersecurity of a medical network

Problem Statement: A hospital operates an information network consisting of the following nodes: A – Electronic Medical Records Server; B – Laboratory Information System; C-MRI Scanner; D – Physician Workstation; E – Medical Imaging Archive Server.

The following communication channels are established between the nodes:

$$E = \{(A, B); (A, C); (B, D); (C, D); (D, E)\}$$

It is required to determine the minimum set of nodes that need to be protected so that every communication channel is protected from at least one side.

Step I. Mathematical model of the study.

The medical information system is represented as a graph:

$$G = (V, E)$$

where – the set of system nodes, – the set of data transmission channels.

In this case, the set of nodes consists of 5 elements:

$$V = \{A, B, C, D, E\}$$

$$S \subseteq V, |\, S \,| \to \min$$

where represents the nodes that must be protected to ensure the security of the entire network under the condition:

$$\forall\, e \in E, e \cap S \neq \emptyset$$

This model corresponds to the Minimum Vertex Cover problem [1].

Step II. Visual analysis (Pedagogical aspect) (Fig. 1).

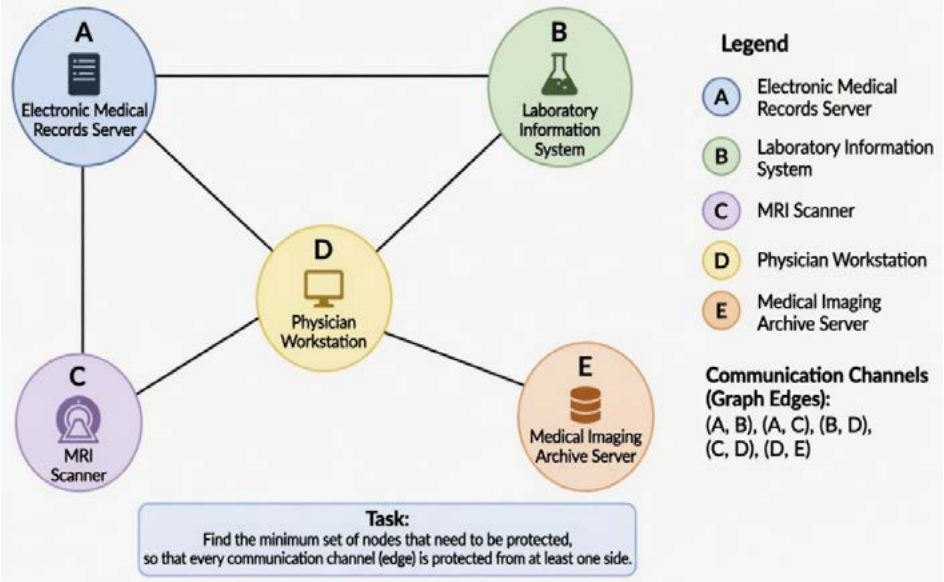


Figure 1. Medical information network graph

For students, it is important to first consider the network as a real hospital structure and explore alternative hypotheses. For example:

- If only node A is protected, the channels (B, D), (C, D), and (D, E) remain vulnerable;

- If node D is protected, three connections are covered immediately.

This approach develops practical thinking rather than purely formal mathematical problem-solving.

Step III. Solution Search.

Let us consider the set.

Verification of all edges: (A, B) – covered by A; (A, C) – covered by A; (B, D) – covered by D; (C, D) – covered by D; (D, E) – covered by D.

Thus, we conclude that all communication channels are protected. Solution: The minimum number of protected nodes is $|S| = 2$.

Solving the problem in Microsoft Excel

Input Data: Binary variables (1 or 0); Objective function – minimization of the sum of the «Protection Status» cells for nodes A, B, C, D, E; Constraints – for each communication channel, the sum of the protected nodes must be more than 1.

1. Represent the graph structure as an incidence matrix (a rectangular table describing the connections between vertices and edges of the graph), where rows correspond to communication channels (edges E) and columns correspond to system nodes (V). At the intersections, logical values 1 and 0 are used (1 – the node is part of this channel, 0 – the node is not connected).

Table 1

Incidence matrices

Nodes (V) / Communication channels (Edges)	A (V1)	B (V2)	C (V3)	D (V4)	E (V5)
(A, B)	1	1	0	0	0
(A, C)	1	0	1	0	0
(B, D)	0	1	0	1	0
(C, D)	0	0	1	1	0
(D, E)	0	0	0	1	1

In Table 1, the value 1 is placed under the nodes that form the communication channel; the rest are 0.

Add a row for the objective function (S) «Protection Status» and a column «Verification».

2. Minimize the total number of protected nodes by entering the formula =SUM(B8: F8) in the cell at the intersection of the «Protection Status» row and the «Verification» column.

3. Enter the following formula in the «Verification» column: =SUMPRODUCT(B3: F3, $B$8:$F$8) for the first channel and copy it for the other channels. This formula multiplies the channel row by the «Protection Status» row. If the result is ≥ 1, the channel is protected (Fig. 2).

	A	B	C	D	E	F	G
1	Nodes (V)	A (V1)	B (V2)	C (V3)	D (V4)	E (V5)	Verification
2	Communication channels (Edges)						
3	(A, B)	1	1	0	0	0	=SUMPRODUCT(B3:F3;$B$8:$F$8)
4	(A, C)	1	0	1	0	0	=SUMPRODUCT(B4:F4;$B$8:$F$8)
5	(B, D)	0	1	0	1	0	=SUMPRODUCT(B5:F5;$B$8:$F$8)
6	(C, D)	0	0	1	1	0	=SUMPRODUCT(B6:F6;$B$8:$F$8)
7	(D, E)	0	0	0	1	1	=SUMPRODUCT(B7:F7;$B$8:$F$8)
8	Protection Status						=SUM(B8:F8)

Figure 2. Creation of a table with formulas in Microsoft Excel

4. Configure the Solver add-in as follows (Fig. 3):

- Set the objective cell: $G$8 (set the value to Minimum);

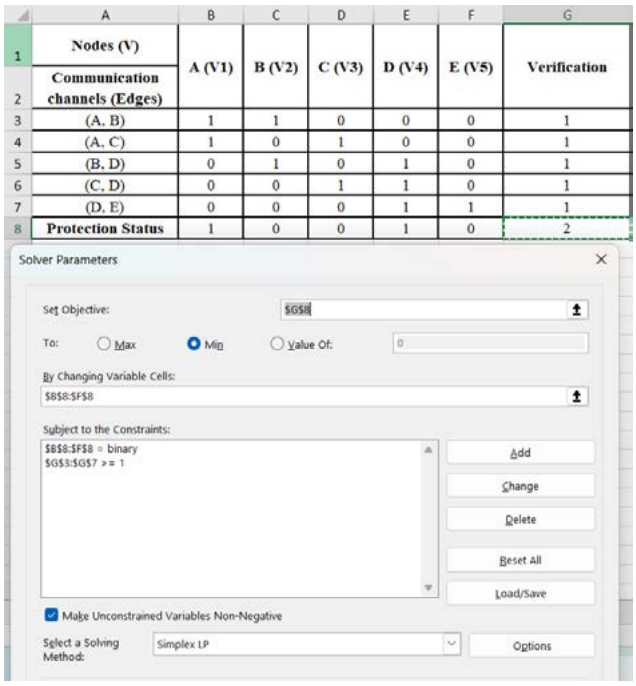
- By changing variable cells: $B$8:$F$8 (your «Protection Status» row);

- Add constraints:

- $B$8:$F$8 = binary (this will restrict values to only 0 or 1);

- $G$3:$G$7 ≥ 1 (each channel must be covered by at least one node).

– Select the solving method Simplex LP and get results.



Nodes (V) / Communication channels (Edges)	A (V1)	B (V2)	C (V3)	D (V4)	E (V5)	Verification
(A, B)	1	1	0	0	0	1
(A, C)	1	0	1	0	0	1
(B, D)	0	1	0	1	0	1
(C, D)	0	0	1	1	0	1
(D, E)	0	0	0	1	1	1
Protection Status	1	0	0	1	0	2

Figure 3. Solver configuration and calculation results

Step IV. Analysis and Analytical Conclusions.

Teaching graph theory in the context of cybersecurity to students of medical and biotechnological specialties requires moving away from a purely engineering approach dominated by programming. The goal of teaching this topic is to develop in future doctors an understanding of network technologies and cyber hygiene, as well as the ability to perceive a hospital's infrastructure as a single organism.

For conducting classes, particularly with this task, it is advisable to present the pedagogical explanation to students through the following question: «Which two devices in the hospital need to be protected to minimize the risk of information leakage?».

The proposed approach, schematically presented in Figure 4, effectively integrates abstract graph theory, a real-world medical case, and fundamental cybersecurity concepts. Such types of tasks develop in students: logical thinking; understanding of network security; the ability to find solutions on a graph without complex coding or manual matrix calculations; the ability to apply discrete mathematics in medicine using information technologies (Microsoft Excel).

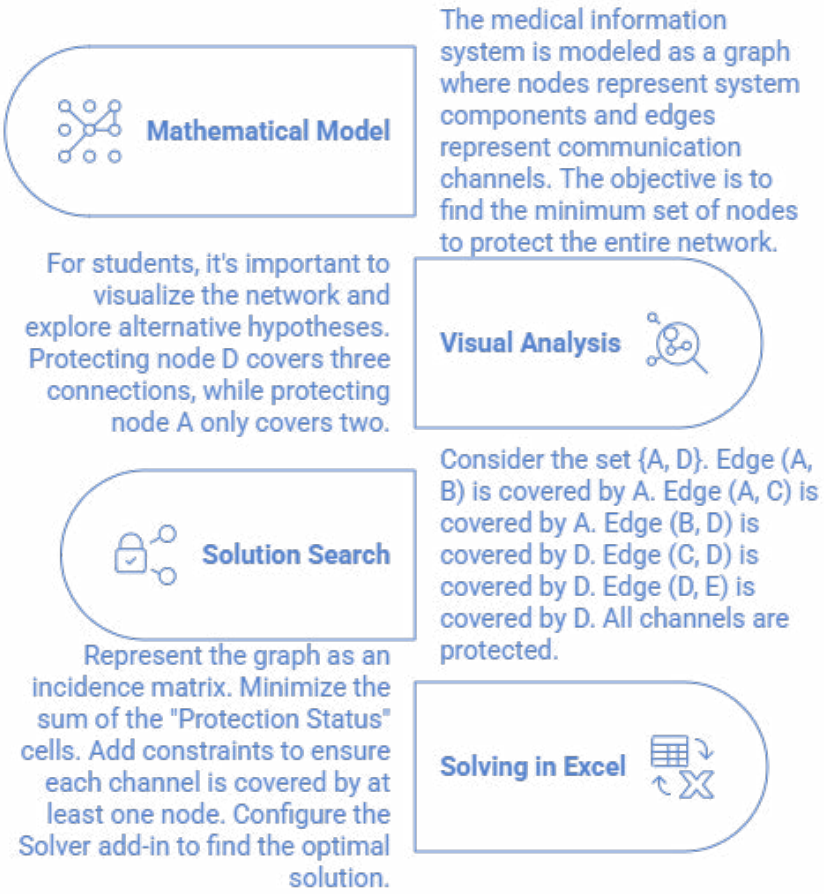


Figure 4. Framework for teaching graph theory method

DISCUSSION

Cybersecurity threats to healthcare organizations, medical information systems (MIS), and patient safety are becoming increasingly significant as healthcare undergoes rapid digital transformation. Modern healthcare institutions depend on interconnected digital infrastructures that integrate electronic health records, laboratory information systems, medical imaging platforms, telemedicine services, and network-connected medical devices. While these technologies improve the efficiency and quality of healthcare delivery, they simultaneously expand the attack surface available to cybercriminals. Consequently, ensuring cybersecurity has become not only a technical challenge but also an educational priority for future healthcare professionals [2].

The findings of this study support the growing body of research emphasizing the value of graph-theoretical approaches for modeling and protecting healthcare information systems. Previous studies have demonstrated that graph theory provides an effective framework for representing network structures, analyzing vulnerabilities, and identifying critical nodes within complex digital environments [3-6]. In healthcare settings, graph-based models have been successfully applied to attack graph construction, intrusion detection, network segmentation, and risk assessment [7-9]. The present study extends these applications to the educational domain by demonstrating how graph-theoretical methods can be incorporated into the training of medical and biotechnology students through professionally oriented cybersecurity tasks.

Graph-based models also facilitate the implementation of microsegmentation in medical information systems. Graph-theoretical algorithms can identify critical nodes whose compromise or removal may either fragment the network or provide unauthorized access to system resources. The protection of these critical nodes can be strengthened through the implementation of multifactor authentication and other advanced cybersecurity measures [10].

A distinctive feature of the proposed methodology is the integration of mathematical modeling with authentic healthcare scenarios. The application of the minimum vertex cover problem is particularly valuable from both educational and practical perspectives. From a cybersecurity standpoint, this model illustrates the principle of resource optimization by enabling students to determine the minimum set of network nodes requiring protection to secure all communication channels. Such optimization problems closely reflect real-world decision-making processes in healthcare organizations, where financial, technical, and human resources are often limited. Understanding how to allocate protective measures efficiently is therefore an important competency for future healthcare professionals, who will increasingly interact with digital infrastructures and cybersecurity policies.

Overall, the results indicate that graph-theoretical modeling provides a valuable bridge between mathematical education and professional healthcare practice. By connecting discrete mathematics with cybersecurity challenges in medical information systems, the proposed methodology enhances the practical relevance of mathematical training, promotes interdisciplinary learning, and contributes to preparing future healthcare professionals to function effectively in digitally transformed healthcare environments. The proposed approach demonstrates that graph theory can serve not only as a mathematical discipline but also as a practical tool for developing cybersecurity awareness, analytical competence, and systems thinking in medical and biotechnology education.

CONCLUSIONS

The application of graph-theoretical models, particularly the minimum vertex cover problem, provides an effective framework for analyzing network vulnerabilities, identifying critical infrastructure components, and developing evidence-based cybersecurity strategies. The use of real-world healthcare scenarios promotes algorithmic and systems thinking, strengthens analytical skills, and enhances students' motivation to study mathematical disciplines.

The successful implementation of this interdisciplinary approach contributes to the development of the digital, analytical, and professional competencies required for work in modern healthcare environments. The integration of mathematical modeling, cybersecurity principles, and digital tools supports the preparation of future healthcare professionals to understand and address information security challenges in the context of the ongoing digitalization of healthcare.

Perspectives for further research. Future research should focus on the development of interactive educational simulators, the incorporation of artificial intelligence technologies, and the experimental evaluation of the proposed methodology in medical and biotechnological education.

Study limitations. The authors explicitly acknowledge that this study has several methodological limitations arising both from its predefined scope and from the characteristics of the proposed approach. In particular, the proposed cybersecurity scenarios and graph models are educational models of medical information systems and do not fully reflect the complexity of real healthcare information infrastructures. Furthermore, the proposed methodology is illustrated using the Minimum Vertex Cover problem; therefore, the findings cannot be directly generalized to all graph-theoretical methods or other cybersecurity problems. Future research should focus on the experimental validation of the proposed methodology, the evaluation of its pedagogical effectiveness, and comparison with alternative approaches to teaching graph theory to medical and biotechnology students.

Primary data and materials. The authors confirm that no primary medical documentation (including patient medical records, outpatient records, examination protocols, or the results of laboratory and instrumental investigations), as well as no statistical databases containing individual patient-level data, were used in this study. The materials used in the study consisted of scientific publications, theoretical graph models, educational case studies, mathematical problem formulations, and illustrative examples developed by the authors.

COMPLIANCE WITH ETHICAL REQUIREMENTS.

The research did not involve human participants, personal data collection, clinical interventions, biological materials, or experimental procedures involving patients or animals. Therefore, informed consent and formal ethical approval were not required.

The study was conducted in accordance with the principles of academic integrity, research ethics, and responsible scientific practice. All sources used in the research were appropriately cited, and the proposed educational methodology was developed for academic and educational purposes aimed at improving the professional training of students in medical and biotechnological specialties.

Declaration of AI use. No artificial intelligence tools were used in the preparation of this manuscript for text generation, data analysis, or image creation. All content was developed by the authors, who bear full responsibility for its accuracy, originality, and compliance with ethical standards

Funding and conflict of interest. The authors declare the absence of any financial or personal interest that could have influenced the objectivity of the presentation of the study results. The study was conducted as a fragment of the scientific project «Ensuring the quality of computer science and physics and mathematics training of future healthcare professionals in the classroom and distance learning environment» (2024-2026, state registration № . 0124U000724).

AUTHORS' CONTRIBUTION

Yurii M. Litvin[A, B, C, F]
Pavlo V. Mykytenko[D, E]
Liliia B. Desiatniuk[A, B, C, F]
Svetlana V. Kolpakova[A, B, C, F]
Inna I. Kucherenko[D, E]

REFERENCES

1. Shevchenko, S., Zhdanova, Y., Skladannyi, P., et al. (2021). Matematychni metody v kiberbezpetsi: Hrafy ta yikh zastosuvannia v informatsiinii ta kibernetychnii bezpetsi [Mathematical methods in cybersecurity: Graphs and their applications in information and cyber security]. Cybersecurity: Education, Science, Technology, 13(1), 133-144. https://doi.org/10.28925/2663-4023.2021.13.133144
2. U.S. Department of Health and Human Services. (n.d.). Health industry cybersecurity practices: Managing threats and protecting patients. https://405d.hhs.gov/Documents/HICP-Main-508.pdf
3. Borysenko, I. I., & Vinkovska, I. S. (2025). Teoriia hrafiv yak osnova metodiv vbudovuvannia informatsii [Graph theory as the basis of information embedding methods]. Informatics and Mathematical Methods in Simulation, 15(1), 39-47. https://doi.org/10.15276/imms.v15.no1.39
4. Sowrirajan, R., & Manimekalai, S. (2024). Graph-theoretic approaches to optimizing connectivity and security in ubiquitous healthcare systems. In A. S. Kumar et al. (Eds.), Ubiquitous computing and technological innovation for universal healthcare (pp. 327-351). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-2268-0.ch015
5. Al-Jawadi, A. M. A., & Al-Shumam, A. A. K. (2020). A review on the relationship between computer engineering, discrete mathematics and graph theory. Tikrit Journal of Engineering Sciences, 27(3), 38-44. https://doi.org/10.25130/tjes.27.3.05
6. Rumiantseva, O. V. (2023). Analiz modelei system zakhystu informatsii, pobudovanykh z vykorystanniam teorii hrafiv [Analysis of models of information protection systems built using graph theory]. In Radioelectronics and Youth in the 21st Century: Materials of the 27th International Youth Forum (Vol. 4, pp. 46-47). https://openarchive.nure.ua/handle/document/26639
7. Angel, D. (2022). Protection of medical information systems against cyber attacks: A graph theoretical approach. Wireless Personal Communications, 126(4), 3455-3464. https://doi.org/10.1007/s11277-022-09873-x
8. Ünözkan, H., Ertem, M., & Bendak, S. (2022). Using attack graphs to defend healthcare systems from cyberattacks: A longitudinal empirical study. Network Modeling Analysis in Health Informatics and Bioinformatics, 11, Article 52. https://doi.org/10.1007/s13721-022-00391-1
9. Taylor, C. R., Venkatasubramanian, K., & Shue, C. A. (2014). Understanding the security of interoperable

medical devices using attack graphs. In Proceedings of the 3rd International Conference on High Confidence Networked Systems (pp. 31-40). https://doi.org/10.1145/2566468.2566482

10. Bilot, T., El Madhoun, N., Al Agha, K., et al. (2023). Graph neural network for intrusion detection: A survey. IEEE Access, 11, 49114-49139. https://doi.org/10.1109/ACCESS.2023.3275789

Резюме

МЕТОДИКА НАВЧАННЯ ТЕОРІЇ ГРАФІВ У ЗАДАЧАХ КІБЕРБЕЗПЕКИ В МЕДИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ ДЛЯ СТУДЕНТІВ МЕДИЧНИХ ТА БІОТЕХНОЛОГІЧНИХ СПЕЦІАЛЬНОСТЕЙ

Юрій М. Литвин, Павло В. Микитенко, Лілія Б. Десятнюк, Світлана В. Колпакова, Інна І. Кучеренко

Національний медичний університет імені О. О. Богомольця, м. Київ, Україна

Вступ. Стрімка цифровізація сфери охорони здоров'я зумовила зростання залежності медичних установ від складних інформаційних систем, що робить кібербезпеку критично важливим компонентом медичної практики та необхідною компетентністю майбутніх фахівців медичних і біотехнологічних галузей. Теорія графів забезпечує ефективний математичний апарат для моделювання медичних інформаційних мереж, виявлення критичних компонентів інфраструктури, аналізу вразливостей та оптимізації стратегій кіберзахисту.

Мета. Розробити та науково обґрунтувати методику навчання методів теорії графів на основі задач, пов'язаних із мінімізацією множини захищених вузлів мережі, призначену для студентів медичних і біотехнологічних спеціальностей.

Матеріали та методи. У дослідженні використано теоретичні, математичні та педагогічні методи. Медичні інформаційні системи змодельовано у вигляді графів, а задачу кібербезпеки сформульовано як задачу мінімального вершинного покриття. Для аналізу інформаційної інфраструктури закладів охорони здоров'я як взаємопов'язаного цифрового середовища застосовано системний підхід.

Результати. Розроблено методику, що інтегрує теорію графів, медичну інформатику та кібербезпеку, і продемонстровано її застосування на моделі лікарняної інформаційної мережі. Запропонований підхід дає змогу аналізувати структуру комунікацій, визначати критичні компоненти мережі та знаходити мінімальну множину захищених вузлів, необхідну для забезпечення безпеки всіх каналів зв'язку. Використання професійно орієнтованих задач із кібербезпеки сприяє розвитку алгоритмічного мислення, навичок системного аналізу та практичного розуміння принципів інформаційної безпеки.

Висновки. Застосування графових моделей, зокрема задачі мінімального вершинного покриття, забезпечує ефективний інструментарій для аналізу мережевих вразливостей, виявлення критичних компонентів інфраструктури та розроблення обґрунтованих стратегій кіберзахисту. Використання реалістичних сценаріїв із галузі охорони здоров'я сприяє розвитку алгоритмічного та системного мислення, посиленню аналітичних навичок і підвищенню мотивації студентів до вивчення математичних дисциплін.

Ключові слова: **медичні інформаційні системи, теорія графів, кібербезпека**

Received: 04.05.2026
Accepted: 02.07.2026
Published: 11.09.2026