"Competition" Drives New Heights of Industry-Education Integration in the Network Information Security Major

Jie Qiu

School of Artificial Intelligence, Yulin Normal University, Yulin, Guangxi, China

Abstract: In the digital era, the gap between traditional practical teaching of network information security majors and industry demands has become prominent. This study takes Yulin Normal University as an example to explore a new path of industry-education integration with competition-promoted learning as the link for practical teaching reform. It first analyzes the current problems of practical teaching, such as disconnected teaching content from actual needs, weak practical links, and insufficient practical experience of teachers. Then, it elaborates on the connotation, advantages of competition-promoted learning and characteristics of typical competitions like CTF. Furthermore, it introduces the construction and practice of the new industry-education integration path, including university-enterprise co-construction of practical teaching bases and curriculum & teaching method reform. Finally, it presents the reform effects, such as students' outstanding competition achievements and improved comprehensive abilities, and discusses future development trends under the impact of new technologies. This study provides a reference for improving the quality of network information security talent cultivation.

Keywords: Network Information Security; Competition-Promoted Learning; Industry-Education Integration; Practical Teaching Reform; CTF Competition; Talent Cultivation

1. Introduction

In the digital era, network information security has become a crucial cornerstone of national security, economic development, and social stability [1]. With the rapid advancement of information technology, the boundaries of cyberspace are constantly expanding, and methods of cyberattacks are becoming increasingly complex and diverse, exposing network information security to unprecedented challenges. From the leakage of personal privacy and theft of corporate trade secrets to attacks on critical infrastructure and national-level cybersecurity threats, various cybersecurity incidents occur frequently, causing significant losses to individuals, organizations, and the country.

The cultivation of network information security talents has become an urgent priority [2]. As a key field for nurturing such professionals, the quality of practical teaching in the network information security major directly impacts the standard of talent development. However, traditional practical teaching in this major faces numerous issues, including the disconnection between teaching content and practical application, weak practical teaching links, and students' lack of hands-on operational capabilities and innovative thinking. These problems make it difficult to meet the industry's demand for high-quality network information security talents. Therefore, promoting the reform of practical teaching in the network information security major is extremely urgent.

As an innovative teaching concept and method, "competition-promoted learning" provides new ideas and approaches for the reform of practical teaching in the network information security major [3-4]. By participating in various network information security competitions, students can hone their professional skills in a real competitive environment and enhance their ability to solve practical problems. Meanwhile, competition-promoted learning can strengthen cooperation and communication between universities and enterprises, facilitate industry-education integration, align teaching content more closely with the actual needs of the industry, and cultivate network information security talents who are more in line with market demands. Taking Yulin Normal University as an example, this paper will deeply explore the application of the new industry-education integration path (with competition-promoted learning as the link) in the reform of practical teaching for the network information security major, aiming to provide useful references for improving the quality of talent cultivation in this field.

2. Analysis of the Current Situation of Practical Teaching in the Network Information Security Major

2.1 Disconnection between Teaching Content and Actual Needs

At present, the teaching content of the network information security major has a certain degree of lag. With the rapid development of emerging technologies such as cloud computing, big data, artificial intelligence, and the Internet of Things, technologies and application scenarios in the field of network information security are constantly updated and iterated. However, the teaching content of some universities is still limited to traditional network security knowledge, such as basic network attack and defense, principles of cryptography, and firewall technology, with little coverage of network security issues under emerging technologies, such as cloud computing security, big data security, and artificial intelligence security [5-6]. According to relevant surveys, in the network information security courses of more than 60% of universities, the content related to emerging technology security accounts for less than 20%. This leads to a large gap between the knowledge students have learned and the actual needs of enterprises, making it difficult for graduates to quickly adapt to their job positions.

The depth and breadth of teaching content also need to be improved. In actual teaching, some courses focus too much on the imparting of theoretical knowledge, with insufficient explanation of practical operations and real cases. Although students have mastered certain theoretical knowledge, they lack the ability to analyze and solve problems when facing actual network security issues. In the course of Network Security Laws and Regulations, some teachers only simply explain legal provisions without combining them with real network security cases for analysis, resulting in students' insufficient ability to understand and apply legal knowledge.

2.2 Weak Practical Teaching Links

The lack of authenticity in practical projects is an important factor affecting the effect of practical teaching. Practical projects in many universities are often simulated scenarios, which are quite different from actual network security work scenarios. During the practical process, students cannot truly experience the complexity and challenges of network security work, making it difficult to develop the skills and capabilities required for actual work. Some practical projects only simply set up some network attack scenarios for students to defend against, without involving content such as security strategy formulation and security risk assessment in actual work.

There are also deficiencies in the organization and management of practical teaching. The practical teaching of some universities lacks scientific planning and arrangement, with insufficient practical teaching time and lack of coherence and systematicness between practical teaching links. At the same time, the assessment and evaluation system for practical teaching is not perfect, often focusing only on practical results while ignoring the practical process and the cultivation of students' practical abilities.

2.3 Insufficient Practical Experience of the Teaching Staff

Most teachers in the network information security major have rich theoretical knowledge but lack practical work experience in enterprises. In the teaching process, they mainly rely on teaching materials and theoretical knowledge, and it is difficult for them to integrate cases and experience from actual work into teaching. This leads to the disconnection between teaching content and actual work, making it difficult for students to learn about the latest industry trends and actual needs from teachers' teaching. The insufficient practical ability of teachers also limits the quality of practical teaching. In practical teaching, teachers need to have strong practical guidance capabilities and be able to promptly solve problems encountered by students during the practical process. However, due to the lack of practical experience of some teachers, they often cannot provide effective guidance and help when facing students' problems. This not only affects students' enthusiasm for practice but also reduces the effect of practical teaching.

The structure of the teaching staff is also unreasonable. In the teaching staff of the network information security major in some universities, there is a lack of "double-qualified" teachers with industry background and practical experience. At the same time, there are certain problems in the age structure and professional title structure of teachers: the proportion of young teachers and teachers with professional titles below the intermediate level is relatively large, and their teaching experience and professional level still need to be improved.

3. Competition-Promoted Learning: An Innovative Link for Industry-Education Integration

3.1 Connotation and Advantages of Competition-Promoted Learning

Competition-promoted learning refers to integrating various competition activities into the teaching process, with competitions as the driving force to stimulate students' interest and initiative in learning. It encourages students to enhance their professional skills, develop innovative thinking and teamwork abilities through competitions, thereby achieving effective mastery of knowledge and comprehensive improvement of overall capabilities. In the field of network information security, competition-promoted learning has unique connotations and significant advantages [7].

Competition-promoted learning can greatly stimulate students' interest in learning. Traditional classroom teaching usually focuses on the imparting of theoretical knowledge, with relatively single teaching methods, which easily makes students feel boring. In contrast, competition activities are challenging, interesting and competitive, which can attract students' attention and arouse their curiosity and desire for knowledge. In network security competitions, students need to face various complex network security issues, such as prevention of network attacks and response to data leakage. These practical problems enable students to deeply recognize the importance and urgency of network information security, thus proactively learning relevant knowledge and skills and seeking solutions to problems. According to surveys, more than 80% of students who have participated in network security competitions reported a significant increase in their interest in the network information security major, and their enthusiasm and initiative in learning have also been significantly improved [8].

Competition-promoted learning helps to enhance students' comprehensive abilities. During competitions, students need to apply their professional knowledge and formulate solutions based on actual situations. This not only requires students to have a solid theoretical foundation, but also demands strong practical abilities, innovative thinking and problem-solving skills. At the same time, competitions are usually conducted in the form of teams, so students need to cooperate closely with team members to complete competition tasks together. This helps to cultivate students' teamwork, communication and leadership abilities. In CTF (Capture the Flag) competitions, students need to complete a series of network security challenge tasks through analysis, cracking, defense and other means within a specified time. In this process, students need to apply knowledge in multiple fields such as network security, cryptography, operating systems and databases, and at the same time cooperate closely with team members and divide work reasonably to achieve good results. By participating in such competitions, students' comprehensive abilities are fully exercised and improved.

Competition-promoted learning plays an important role in promoting industry-education integration. Competition activities are often organized with the joint participation of multiple parties such as universities, enterprises and industry associations, which builds a bridge for communication and cooperation between universities and enterprises. Enterprises can understand the teaching level of universities and the professional abilities of students through competitions, providing a channel for enterprises to select outstanding talents; at the same time, enterprises can also introduce practical projects and cases into competitions, making the competition content more in line with the actual needs of the industry and providing a direction for the teaching reform of universities. Universities, on the other hand, can rely on the resources and technical advantages of enterprises to strengthen practical teaching links, improve teachers' practical teaching abilities, and cultivate professional talents more in line with market demands. Some network security enterprises provide technical support and competition platforms for competitions, and at the same time send enterprise experts to serve as competition judges to comment on and guide students' performance. This competition model of industry-education integration achieves a win-win situation for universities, enterprises and students.

3.2 Analysis of Competition Types and Characteristics

In the field of network information security, there are various types of common competitions. Different types of competitions have their own unique characteristics, and the focus of training students' abilities also differs.

CTF competitions are highly representative and influential events in the field of network information security. Originating from the DEF CON Global Hacking Conference held in 1996, they have now developed into one of the most popular competition models in the global network security community, known as the "World Cup" of CTF competitions - DEFCON CTF. CTF competitions usually simulate typical network security vulnerabilities or cases through a virtual platform environment, requiring participants to solve a series of challenges to obtain answers called "Flags" [9]. Their competition models mainly include Jeopardy (problem-solving mode), Attack-Defense (attack-defense mode) and Mix (hybrid mode).

Jeopardy-mode CTF competitions are similar to ACM programming competitions and informatics Olympiads. Participating teams take part through the Internet or on-site networks, and are ranked based on the scores of solved network security technical challenge questions and the time spent. The questions cover multiple categories such as reverse engineering, vulnerability exploitation, Web penetration, cryptography, forensics, steganography and secure programming. This mode focuses on training students' mastery of different network security technologies and their ability to solve problems, requiring students to have solid professional knowledge and the ability to learn and analyze problems quickly. In reverse engineering questions, students need to analyze binary files, restore their code logic, and identify vulnerabilities or hidden information within them; in cryptography questions, students need to apply knowledge of various cryptographic algorithms to crack encrypted cipher text and obtain Flags.

In Attack-Defense-mode CTF competitions, participating teams attack and defend against each other in cyberspace. Each team needs to maintain its own services and attack the services of other teams, and obtain or protect Flags in the attack-defense confrontation. This mode not only tests students' attack techniques, but also focuses on their defense capabilities and real-time adaptability. At the same time, it has high requirements for the division of labor and cooperation among team members. Competitions usually last for 48 hours or more, which is also a test of the physical strength and endurance of participants. In actual competitions, students need to constantly monitor the status of their own servers, promptly detect and fix vulnerabilities to prevent attacks from other teams; at the same time, they need to actively find vulnerabilities in the servers of other teams, launch attacks and obtain Flags. This requires students to have comprehensive network security knowledge and rich practical experience, and be able to make quick decisions in complex network environments.

The hybrid mode combines the characteristics of the Jeopardy mode and the Attack-Defense mode. Participating teams obtain some initial scores by solving problems, and then engage in a zero-sum game of score increase and decrease through attack-defense confrontation. The final ranking is determined by the total score. This mode is more complex and closer to actual application scenarios, comprehensively training students' overall abilities. In some hybrid-mode CTF competitions, students need to obtain certain resources and information by solving problems in the early stage to prepare for the subsequent attack-defense confrontation; in the attack-defense stage, students use the knowledge and experience accumulated from solving problems in the early stage to engage in fierce confrontation with other teams.

In addition to CTF competitions, the National College Student Information Security

Competition is also one of the important events in the field of network information security. This competition mainly includes the Information Security Works Competition and the Innovative Practical Ability Competition. The Information Security Works Competition requires participating teams to submit hardware and software works related to network and information security. The works should be designed around the application and innovation of information security technologies, and can involve multiple fields such as cryptographic algorithms, security chips, firewalls and intrusion detection systems [10]. The "Fuxing Cup" National College Student Network Security Elite Competition is also a well-known brand event with wide influence. With the purpose of "popularizing network security knowledge, discovering network security talents and safeguarding the cyber power strategy", this competition strictly selects outstanding college students in network security with solid theoretical foundations, outstanding practical abilities and innovative potential through a multi-track and multi-level competition mechanism. The competition sets up multiple tracks such as the "Network Security Attack-Defense Track", "Network Security Awareness and Laws & Regulations Track" and "Artificial Intelligence Application and Security Track". This multi-track competition setup can comprehensively examine students' knowledge and skills in different fields, meet the interests and strengths of different students, and provide a platform for cultivating interdisciplinary network security talents.

4. Construction and Practice of a New Path for Industry-Education Integration

4.1 University-Enterprise Cooperation in Building Practical Teaching Bases

Universities establish close cooperative relationships with well-known enterprises in the field of network information security to jointly build practical teaching bases. These bases provide students with a real project practice environment, enabling them to practice and enhance their professional skills in actual work scenarios. The School of Artificial Intelligence of Yulin Normal University has established a Network Security Offense and Defense Laboratory. Equipped with advanced network security equipment and software, the laboratory simulates real network environments, including enterprise internal networks, Internet borders, and various application systems. In the laboratory, students can participate in actual enterprise network security projects, such as network security vulnerability detection and repair, network attack prevention strategy formulation, and security incident emergency response. By participating in these projects, students can gain in-depth understanding of the processes and methods of enterprise network security work, master the latest network security technologies and tools, and improve their practical abilities and skills in solving real-world problems.

The joint construction of practical teaching bases also realizes resource sharing between universities and enterprises. Universities can utilize enterprises' technical equipment, project resources, and industry experience to enrich practical teaching content and improve the quality of practical teaching; enterprises, on the other hand, can leverage universities' teaching resources and talent advantages to carry out employee training, technological research and development, and other work, achieving mutual benefit and a win-win situation. Enterprises provide universities with the latest network security equipment and software for students' practical use; meanwhile, enterprise technical experts regularly conduct lectures and training sessions at universities to impart the latest industry knowledge and practical experience to students. Universities provide enterprises with venues and equipment to support their technological research and development and employee training activities; university teachers can also participate in enterprises' project research and development, providing technical support and intellectual services to enterprises.

4.2 Reform of Curriculum System and Teaching Methods

4.2.1 Curriculum content optimization based on competitions

Cases and technologies from various network information security competitions are integrated into curriculum teaching content, making the content more closely aligned with practical applications. In network security courses, typical questions and cases from CTF competitions—such as Web penetration testing cases and cryptography cracking cases—are introduced, allowing students to analyze and practice them in class. Through learning these cases, students can gain in-depth understanding of the principles and methods of network security attacks and defenses, master relevant technologies and tools, and improve their network security skills. At the same time, teachers can update curriculum content in a timely manner based on the latest developments in competitions and technological trends, exposing students to the most up-to-date network security knowledge and technologies. As artificial intelligence technology is increasingly applied in the field of network security, teachers can add content related to artificial intelligence security to courses, introducing the application principles and methods of artificial intelligence in network security detection, defense, and risk assessment, so as to cultivate students' interdisciplinary thinking and innovative abilities.

The practical links in competitions are combined with curriculum experimental teaching to strengthen the cultivation of students' practical abilities. In curriculum experiments, practical projects similar to those in competitions—such as simulated network attack and defense experiments and security vulnerability mining experiments—are set up, enabling students to consolidate the knowledge they have learned and improve their practical abilities through practice. Meanwhile, students are encouraged to participate in various network information security competitions, so that they can further enhance their comprehensive abilities through actual competition participation. Universities can also organize internal network security competitions to provide students with more practical opportunities and platforms for demonstration, stimulating their interest in learning and sense of competition.

4.2.2 Project-driven and group collaboration teaching methods

The project-driven teaching method is adopted, with actual network information security projects as the guide, to help students learn and master knowledge and skills in the process of completing projects. Teachers assign students a network security project task, such as designing and implementing a network security protection plan for an enterprise. Based on the enterprise's network architecture, business needs, and security risks, students are required to formulate detailed security protection strategies, including firewall configuration, intrusion detection system deployment, and security vulnerability repair. During the project implementation process, students need to apply the network security knowledge and skills they have learned to solve various problems encountered, such as preventing network attacks and responding to data leaks. Through the project-driven teaching method, students can integrate theoretical knowledge with practice, and improve their practical operation abilities and problem-solving skills.

In the process of project implementation, the group collaboration method is adopted, where students form teams to complete project tasks together. The group collaboration teaching method can cultivate students' teamwork, communication, and leadership abilities. In network security projects, team members need to divide work and cooperate with each other, taking charge of tasks such as network security demand analysis, plan design, technical implementation, and test verification. During the collaboration process, students need to communicate and coordinate effectively with team members to jointly solve problems encountered. At the same time, students can give full play to their strengths in the team, and practice their leadership and organizational abilities. In the process of group collaboration, teachers play the role of guides and supervisors, providing students with necessary guidance and support to ensure the smooth progress of the project. Teachers can help students analyze project requirements and provide relevant technical materials and tools; during project implementation, they can identify problems existing in students in a timely manner and provide guidance and suggestions; after the project is completed, they can evaluate and provide feedback on students' project results, and put forward improvement opinions and suggestions.

5. Effects of Practical Teaching Reform and Case Analysis

Through the practical teaching reform of industry-education integration with competition-promoted learning as the link, students have achieved remarkable results in various network information security competitions. In the National College Student Network Security Competition, student teams from the Information Security major of Yulin Normal University have won first, second, and third prizes for consecutive years. In the 2025 competition, the university's student teams successfully solved multiple complex network security problems relying on their solid professional knowledge and excellent teamwork capabilities, standing out among numerous participating teams from universities across the country. Students also demonstrated strong capabilities in CTF competitions.

The achievement of these results fully proves the significant progress of students in practical abilities and innovative thinking. In the process of participating in competitions, students need to continuously learn and master new network security technologies, such as the application of artificial intelligence in network security detection and the application of blockchain technology in data security protection. At the same time, they also need to use innovative thinking to propose unique solutions to address various complex network security challenges. In a network security vulnerability mining competition, students improved traditional vulnerability mining technologies and combined them with machine learning algorithms, successfully discovering multiple previously undetected security vulnerabilities and providing important support for enterprises' network security protection.

Students have also made great progress in teamwork and communication abilities. In competitions, students usually participate in teams and need to cooperate closely with team members to complete competition tasks together. Through teamwork, students have learned how to communicate and coordinate effectively, how to give full play to their strengths, and how to take responsibility in the team. The improvement of these abilities not only helps students achieve good results in competitions but also will have a positive impact on their future career development.

6. Future Development Trends and Outlook

6.1 Impact of Technological Development on the Network Information Security Major

With the rapid advancement of science and technology, new technologies such as artificial intelligence (AI), big data, and blockchain are profoundly reshaping the landscape of the network information security field, and also putting forward brand-new requirements for the cultivation of network information security professionals.

AI technology is increasingly widely applied in the field of network information security, bringing new changes to network security protection. In terms of threat detection, AI analyzes massive volumes of network traffic data and user behavior data through machine learning algorithms, enabling it to quickly and accurately identify abnormal behaviors and potential security threats. Intrusion detection systems built using deep learning algorithms can automatically learn the patterns of normal network behaviors and issue timely alerts when behaviors deviate from these normal patterns. In emergency response, AI can automatically take measures according to preset strategies—such as isolating infected devices and blocking attack sources—greatly shortening response time and reducing losses caused by security incidents. AI can also be used for vulnerability mining, discovering security vulnerabilities in systems through automated means to improve the efficiency and accuracy of vulnerability detection. However, AI technology also poses new challenges to network information security. On one hand, attackers can use AI technology to launch more targeted and concealed attacks: for example, using generative adversarial networks to create realistic phishing emails that bypass traditional email filtering systems, or conducting automated penetration testing on target systems via AI algorithms to find system vulnerabilities. On the other hand, AI models themselves have security risks, such as model attacks and data tampering, which may lead to deviations in model decisions and thus affect the effectiveness of network security protection.

The development of big data technology provides rich data resources and powerful analysis tools for network information security. By collecting, storing, and analyzing massive amounts of network security data, security personnel can better understand the network security situation and identify potential security threats. Using big data analysis technology to conduct correlation analysis on network attack incidents makes it possible to trace attack sources, reveal attack paths and methods, and provide a basis for formulating effective defense strategies. Big data can also be used for security risk assessment: through the analysis of historical and real-time data, it can predict the probability and impact of network security incidents and take preventive measures in advance. However, big data technology also brings issues of data security and privacy protection. As the volume of data continues to grow, data storage and transmission face greater risks—once data is leaked, it will cause severe harm to personal privacy and corporate secrets. At the same time, how to ensure the legality, compliance, and security of data during big data analysis is also an important issue that needs to be addressed.

Blockchain technology, with its characteristics of decentralization, immutability, and traceability, provides a new solution for network information security. In terms of data security, blockchain technology can realize encrypted storage and sharing of data, ensuring data integrity and authenticity. By storing important data on the blockchain, data security is guaranteed through cryptography, and only authorized users can access and modify the data. In terms of identity authentication, blockchain technology can build a decentralized identity authentication system to improve the security and credibility of identity authentication. Using blockchain smart contracts to realize user identity verification and authorization avoids problems such as identity theft and authentication information leakage that exist in traditional identity authentication methods. However, blockchain technology also faces challenges in its application, such as performance bottlenecks, insufficient scalability, and inconsistent standards, which require further research and improvement.

Facing the opportunities and challenges brought by these new technologies, network information security professionals need to possess more comprehensive knowledge and skills. On one hand, they must master the basic principles and application methods of new technologies such as AI, big data, and blockchain, and be able to apply these technologies to network information security practices. On the other hand, they need to have strong security awareness and innovative capabilities to cope with the security risks and challenges brought by new technologies. When learning AI technology, they should not only master algorithms such as machine learning and deep learning, but also understand how to prevent security threats caused by the abuse of AI technology. When learning big data technology, they need to master knowledge and technologies related to data security and privacy protection to ensure the secure application of big data.

6.2 Innovation and Expansion of the Industry-Education Integration Model

In the future, the industry-education integration model will continue to innovate and expand, injecting new vitality into the cultivation of network information security professionals. Cross-regional cooperation will become an important trend in industry-education integration. With the development of economic globalization and regional economic integration, the development of the network information security industry is no longer limited to a single region, but requires the integration of cross-regional resources and advantages. Universities and enterprises can break through geographical restrictions, carry out cross-regional cooperation, and achieve resource sharing and complementary advantages. Universities and enterprises in eastern regions have advantages in network information security technology research, development, and innovation, while western regions have potential in network security application scenarios and talent demand. Through cross-regional cooperation, the two sides can jointly carry out activities such as talent cultivation, technology research and development, and project cooperation to promote the coordinated development of the network information security industry. Cross-regional cooperation can also promote cultural exchange and integration between different regions, and cultivate students' cross-cultural communication skills and teamwork capabilities. By organizing cross-regional network security competitions, academic exchange activities, and other events, students are given the opportunity to communicate and compete with peers from different regions, broadening their horizons and improving their comprehensive quality.

7. Conclusion

The new path of industry-education integration with competition-promoted learning as the link holds significant importance that cannot be ignored in the practical teaching reform of the network information security major. It breaks the limitations of traditional teaching, provides students with a more challenging and practical learning environment, and effectively addresses issues such as the disconnection between teaching content and actual needs, weak practical teaching links, and insufficient practical experience of teachers. By participating in various network information security competitions, students have significantly improved their professional skills, achieved excellent results in competitions, and comprehensively developed their innovative thinking, teamwork, and communication abilities. The enhancement of these abilities not only promotes students' academic progress but also lays a solid foundation for their future career development.

Taking Yulin Normal University as an example, in the practice of industry-education integration, the university-enterprise cooperative talent cultivation mechanism has been continuously improved: jointly-built practical teaching bases provide students with a real practical environment, and the joint development of talent training programs makes the teaching content more in line with industry needs. The reform of the curriculum system and teaching methods has achieved remarkable results: the optimization of curriculum content based on competitions and the application of project-driven and group cooperation teaching methods have stimulated students' learning interest and improved teaching quality. In terms of teacher team construction, through measures such as teachers' on-the-job training in enterprises and the introduction of enterprise experts as part-time teachers, both the practical capabilities and teaching levels of teachers have been improved. Although challenges such as the depth and breadth of integration between competitions and teaching, the sustainability of enterprises' enthusiasm for participation, and the integration and optimization of practical teaching resources are encountered in the reform process, these issues are gradually being resolved through response strategies such as rationally coordinating the relationship between competitions and teaching, improving the university-enterprise cooperation mechanism, and increasing investment in practical teaching resources.

Looking forward to the future, with the continuous development of new technologies such as artificial intelligence, big data, and blockchain, the network information security major will face more opportunities and challenges. The industry-education integration model will also continue to innovate and expand, with cross-regional cooperation and international exchanges and cooperation becoming increasingly strengthened. We should actively grasp these development trends, further deepen the reform of practical teaching, and continuously improve the new path of industry-education integration with competition-promoted learning as the link. This will help cultivate more high-quality, innovative, and practical professionals in the field of network information security, and provide strong talent support for the development of national network information security undertakings.

Acknowledgments

This work is supported by 2024 Undergraduate Teaching Reform Project of Yulin Normal University — Research and Practice on the Reform of Network Information Security Talent Cultivation through Industry-Education Integration and Competition-Promoted Learning (2024xjjg03).

References

[1] Pillai, Sanjaikanth E. Vadakkethil Somanathan, and Kiran Polimetla. "Analyzing the impact of quantum cryptography on network security." 2024 International Conference on Integrated Circuits and Communication Systems (ICICACS). IEEE, 2024.

[2] Pillai, Sanjaikanth E. Vadakkethil Somanathan, and Kiran Polimetla. "Integrating network security into software defined networking (SDN) architectures." 2024 International Conference on Integrated Circuits and Communication Systems (ICICACS). IEEE, 2024.

[3] Li, J. H., Qiu, W. D., Meng, K., et al. Thoughts on the connotation construction and talent cultivation of the first-level discipline of cyber space security. Journal of Information Security Research, 2015, 1(02):149-154.

[4] Li, H. Q. On the skill competitions in vocational colleges based on "industry-education integration and competition-promoted learning". Education and Vocation, 2019, (18):104-108. DOI:10.13615/j.cnki.1004-3985.2019.18.020.

[5] Kuik, Cheng-Chwee. "Southeast Asian responses to US-China tech competition: Hedging and economy-security tradeoffs." Journal of Chinese Political Science 29.3 (2024):509-538.

[6] Chen, K. Q., He, Y., Zhong, G. Q. The connotation transformation of information literacy and the orientation of AI education goals from the perspective of artificial intelligence: Also on the implementation path of AI courses and teaching in basic education. Journal of Distance Education, 2018, 36(01):61-71. DOI:10.15881/j.cnki.cn33-1304/g4.2018.01.006.

[7] Liu, L., Liu, C. B., You, C. J., et al. Teaching reform of network security courses combined with CTF competitions. Computer Education, 2019, (04):107-111. DOI:10.16512/j.cnki.jsjjy.2019.04.027.

[8] Lee, Seungjoo. "US-China technology competition and the emergence of techno-economic statecraft in East Asia: High technology and economic-security nexus." Journal of Chinese Political Science 29.3 (2024):397-416.

[9] Gao, J., Liu, C., Su, P. C. Design of network security competition platform based on CTF. Computer Education, 2015, (17):47-50. DOI:10.16512/j.cnki.jsjjy.2015.17.014.

[10]Cai, Z. P., Yao, D. L., Xu, M., et al. Discussion on the experience of participating in the National College Student Information Security Competition. Computer Education, 2009, (22):27-28. DOI:10.16512/j.cnki.jsjjy.2009.22.017.