Research on Cybersecurity Talents Cultivating in Higher Vocational Education Based on OBE and Project Integration

Fahong Yu[1], Meijia Chen[2,*]

[1]Center of Intelligent Computing and Security Research, Shanwei Institute of Technology, Shanwei, 516600, China
[2]Shanwei Institute of Technology, Shanwei, 516600, China

jxfhyu@126.com, *jxmjchen@zjxu.edu.cn

Abstract. In the current situation where network security threats are becoming increasingly complex and talent demand continues to grow, vocational education in network security urgently needs innovation to meet the development needs of the industry. This article focuses on the application of the results oriented (OBE) project-based training model in the network security major of vocational colleges, aiming to enhance the on-site skills application ability of vocational college students in network security. By reverse designing the talent cultivation path, clarifying the expected learning outcomes based on industry needs and professional standards, and constructing a curriculum system and selecting teaching methods accordingly. Carefully select and design representative and practical network security projects, run through each teaching stage, and ensure learning effectiveness through project assessment and evaluation. Practical analysis shows that this model can effectively enhance students' professional skills, practical abilities, and professional ethics. This research provides new ideas and practical paradigms for the cultivation of network security talents in higher vocational education, which helps to promote the deep integration of higher vocational education and the network security industry.

Keywords: Cybersecurity, Talents Cultivating, OBE, Talents Cultivating

1 Introduction

With the rapid development of network information technology, the importance of network security is becoming increasingly prominent. From personal privacy to corporate trade secrets, from government critical information infrastructure to national sovereignty security, cybersecurity has become a key factor in ensuring social stability, economic development, and national security [1]. The frequent occurrence of cybersecurity incidents, such as data breaches, cyber-attacks, and the spread of malicious software, has brought enormous losses and threats to individuals, businesses, and countries. This not only requires continuous upgrading of network security technology, but also puts forward an urgent need for the cultivation of network security talents.

H. Kannan et al. (eds.), *Proceedings of the 5th International Conference on Internet, Education and Information Technology (IEIT 2025)*, Atlantis Highlights in Social Sciences, Education and Humanities 40,
https://doi.org/10.2991/978-94-6463-803-5_23

It is an indispensable battlefield ensuring the training of applied technical talents in the cultivation of network security talents [2]. Ready to play such leading technical personnel performing in the network security field is adequate professional knowledge and rich practical experience to solve practical problems with capability. Particularly, they should be able to perform key functions in network security projects, i.e., system deployment, security operation and maintenance, and emergency response [3]. Although the traditional industrial vocational network security talent training model is facing problems of being disconnected from industry needs, insufficient practical teaching, and insufficient development of the students' innovative abilities, they are unable to meet the needs of the current demand for high-quality local engineers in the network security industry.

The OBE concept can offer new ideas and measures for cultivating talents in network security in higher vocational education. The OBE philosophy is to organize educational and teaching activities on the expected learning outcomes of students as a goal with an ability orientation [4]. Through reverse design of the curriculum system, teaching content is closely centered around the abilities that students should possess after graduation, effectively promoting consistency between teaching and learning. Integrating the OBE concept into the entire process of cultivating network security talents in higher vocational education and conducting project-based teaching can help break the constraints of traditional teaching models, improve students' practical and innovative abilities, and cultivate on-site skilled application talents that meet market demand [5]. Therefore, studying the talent training model for on-site application of network security skills in vocational colleges based on the OBE project has important practical significance and value.

Nowadays, The OBE has received incomplete research in the proceedings of its implementation process, and there is a lack of specific practical guidance on how to accurately define the students' learning outcomes and then transform them into teaching objectives [6]. However, there is still an urgent problem of how to establish a closer school-enterprise cooperation mechanism and realize the seamless integration of talent cultivation with enterprise needs. Currently, there is not much study of how to integrate the characteristics of building higher vocational education and fully exploit the advantages of OBE integrated teaching project teaching to cultivate high-quality network security talent with practice skills of on-site application in the cultivation of network security talents in higher vocational education. More work and more practice are needed.

The main innovation of this study is the deep integration of the OBE concept and project-based teaching and forming a unique model. Based on OBE, the instructional objectives that students are expected to achieve must clarified, which can be concreted throughout the whole teaching process. By using projects as a carrier, students are invited to actively learn and apply knowledge and skill in the mission of completing projects, educating the ability of solving practical problems and teamwork spirit. This paper therefore reports the major research on the OBE project-based integrated training model and the research results of cultivating the professional of the vocational network security with a solid theoretical basis, strong application ability of on-site skills, and an

innovative spirit to provide new ideas and methods for vocational network security personnel training.

2 Insight into Talents Cultivation of Cybersecurity

2.1 Analysis of Current Teaching

Against the backdrop of the continuous increase in demand for cybersecurity talents, the cultivation of cybersecurity talents in vocational colleges is facing many difficulties, which seriously restrict the quality and quantity of talent cultivation and make it difficult to meet the urgent needs of the industry for high-quality skilled talents.

(1) Lack of solid skill mastery: Specifically for network security, because network security is a practical subject, and it relies on students having strong network security technology and rich practical experience. Although, in real teaching, students have poor practical teaching resource limitations, there are fewer opportunities for practical operation, and students' mastery of network security technology is simply theoretical [7]. Given that students may have a theoretical understanding of different attack methods and defensive strategies in the field of network security attack and defense, they cannot perform quick and precise analysis and fixing of network security vulnerabilities in real practice.

(2) Unreasonable curriculum system: There are many unreasonable aspects in the current curriculum system of vocational network security majors. On the one hand, the curriculum lacks systematicity and foresight, and fails to closely integrate with the latest development trends and practical needs of the network security industry [8]. Some course content is outdated and disconnected from actual work, resulting in students' knowledge after graduation not meeting the needs of enterprises. On the other hand, the connection between courses is not tight enough, resulting in knowledge duplication and gaps, which affects the construction of students' knowledge system and the improvement of their comprehensive abilities.

(3) Weak practical teaching: In the current stage, the teaching of network security majors at vocational college is relatively weak. The cultivation of students' practical ability is limited by the lack of enough practical teaching resources, the badly outdated and backward practical teaching equipment, and the lack of ability to simulate a real network security environment for teaching [9]. Furthermore, the initial teaching staff for practical teaching is weak, and some of them are not experienced in the practical work of network security, so it is unlikely for us to offer effective guidance to students. Additionally, there is also a non-perfection assessment and evaluation mechanism for practical teaching, which cannot make a complete and accurate assessment of students' practical ability and comprehensive quality.

2.2 Compatibility between OBE Project-based and Talent Cultivation

The OBE concept emphasizes clear and measurable learning outcomes, which is in line with the goal of cultivating network security talents in higher vocational education. According to the OBE concept, the training objectives for vocational network security

talents can be refined to enable students to proficiently use network security tools for vulnerability detection and repair, master the configuration and management of network security equipment, possess the ability to respond to network security incidents, and other specific achievements, so that both students and teachers can clearly know the direction of their efforts.

From the curricular system point of view, with its OBE concept, reverse design is advocated as a curriculum system that is designed with predicted learning outcomes. According to the OBE, the curriculum system should be designed based on the network security abilities that the students must own, including the network security protection ability, the ability to operate and maintain the security, etc. Based on these ability requirements, the courses, their teaching objectives, and content are determined so as to render each course as tightly connected as possible and yet prevent redundancy and the missing or disjoint course content. The basic course of network security focuses on explaining the basic concepts, principles, and technologies of network security, laying a foundation for subsequent courses. In the course of network security device configuration and management, students are taught various configuration methods and application scenarios of network security devices, combined with practical cases, to cultivate their practical operation ability. In the comprehensive training course of network security, by simulating real network security projects, students can comprehensively apply their learned knowledge and skills, solve practical problems, and enhance their comprehensive abilities.

In terms of teaching methods, the OBE concept emphasizes student-centered approach and focuses on cultivating students' active learning and practical abilities. According to the OBE concept, teachers can adopt diverse teaching methods such as project driven teaching, case teaching, and group cooperative learning to stimulate students' interest and initiative in learning, allowing them to learn and master knowledge and skills through practice. In project driven teaching, teachers break down network security projects into multiple subtasks and have students complete them in groups. Each group is responsible for one subtask, and in the process of completing the task, students need to independently search for information, analyze problems, and solve problems, thereby improving their practical and teamwork abilities; In case teaching, teachers select actual network security cases and guide students to analyze and discuss them, so that students can understand the causes, hazards, and response measures of network security incidents, and cultivate their ability to analyze and solve problems.

Given the evaluation system, the OBE principle involves diversity in the system and evaluation of students' learning outcomes through the view of evaluating students' learning process, in the whole, and in an objective manner. It could compensate for the weakness of the past evaluation systems and provide a better evaluation of the students' learning processes and outcomes and promote the all-round development of the students. To evaluate such exams as total score or classroom work performance, results of student practice on projects, completion rate in homework, teamwork ability, and so on in various manners, the evaluation system based on the OBE concept is used. The system of diversified and procedural evaluation allows us to find out students' problems and shortcomings, which are in the course of learning, so that in time we can be given

the basis on which the teachers can readjust the teaching strategy and means in order to bring 100 percent students' learning and growth.

3 Construction of Obe Project-based Talent Cultivation

3.1 Objectives of Talent Cultivation

By conducting in-depth research on the current situation and future development trends of the network security industry, extensively communicating and discussing with enterprises and experts in the industry, accurately grasping the industry's ability requirements and job requirements for network security talents, and using this as a basis for reverse deduction to determine the training objectives of vocational network security talents, the training objectives of vocational network security talents were given as table 1.

Table 1. Objectives of talent cultivation

Objective	Sub-objectives	Description
Professional knowledge objective	1.1	systematically master basic knowledge such as computer network principles, basic theories of network security, operating system security, database security, and laws and regulations related to network security.
	1.2	Master the basic knowledge of computer network principles, network security fundamentals, operating system security, database security, and network security laws and regulations.
	1.3	Master the knowledge related to network security architecture. Familiar with the Open Systems Interconnection Reference Model (OSI) and the hierarchical structure of the Internet network architecture.
	1.4	Deeply understand the principles of network security protection technology, including firewalls, intrusion detection and defines systems VPN、 Encryption technology, etc.
Practical skill objective	2.1	Proficiently master the configuration and management skills of network security equipment, be able to configure firewalls, IDS/IPS, VPN and other devices reasonably according to the needs of enterprise network security.
	2.2	Capable of detecting and repairing network security vulnerabilities, able to use professional vulnerability scanning tools to conduct comprehensive vulnerability detection of network systems and applications, and develop effective repair plans based on the detection results.
	2.3	Master the configuration and application of SSL/TLS protocol in network communication. Configure SSL/TLS certificates in a web server or client environment, establish a secure HTTPS communication connection, and analyse the SSL/TLS handshake process using packet capture tools such as Wireshark.

	2.4	Master the emergency response process and technology for network security incidents, and be able to quickly take measures for emergency handling when a network security incident occurs, including incident investigation, evidence collection, system recovery, etc..
	2.5	Cultivate students' scientific literacy and rigorous attitude, comprehensive design and emergency response abilities, group collaboration abilities, innovation abilities, and aesthetic abilities, and enhance students' ability to solve practical problems.
Professional ethics objective	3.1	Produce students' serious, rigorous, and highly responsible work attitude.
	3.2	In terms of network security tasks, students should be able to communicate and collaborate effectively with team members to jointly complete the tasks.
	3.3	Guide students to pay attention to the international political and economic factors behind cybersecurity threats, make them realize that cybersecurity is an important component of national comprehensive security, and enhance their national security awareness and sense of responsibility.
	3.4	By continuously refining interface details, we cultivate a rigorous attitude and a spirit of innovation and craftsmanship.

Based on the needs of enterprises and industries, refine network security requirements into specific technical requirements such as firewall technology, intrusion detection and defense technology, corresponding to the professional knowledge objectives of mastering the principles and configurations of firewalls, intrusion detection and defense systems, etc.; Proficient in configuring firewalls, IDS/IPS devices, and other skills in practical skill objectives.

3.2 Design of Project-based Curriculum System

Curriculum System.

Based on the OBE concept, a curriculum system framework for cultivating vocational network security talents is constructed using projects as the carrier. This framework covers three major modules: basic courses, professional core courses, and practical courses. Each module is interrelated and progressive, serving together to achieve students' ultimate learning outcomes.

(1) The basic course module mainly lays a solid knowledge foundation for students, including courses such as computer basics, network basics, programming language basics, etc. The Network Fundamentals course focuses on explaining the basic concepts, topology, network protocols, and other knowledge of computer networks, enabling students to have a preliminary understanding and comprehension of networks and laying the foundation for in-depth learning of network security knowledge.

(2) The professional core course module is the core part of the curriculum system, closely focusing on the professional knowledge and skills required for network security talents, including network security basics, network security equipment configuration and management, network security vulnerability detection and repair, network security incident emergency response, cloud computing security, big data security and other courses. The course on Network Security Equipment Configuration and Management focuses on network security devices such as firewalls, IDS/IPS, VPNs, etc. Through

practical case teaching and operation, students will master the configuration methods, working principles, and application scenarios of these devices, and be able to configure and manage them reasonably according to the needs of enterprise network security. Students will learn to use professional vulnerability scanning tools such as Nessus, OpenVAS, etc. to detect vulnerabilities in network systems and applications, and develop effective repair plans based on the detection results; The emergency response course for network security incidents simulates real network security incident scenarios, allowing students to learn the emergency response process, techniques, and methods for network security incidents.

(3) The practical course module aims to nurture the ability of the students to gain practical knowledge and solve problems. Students can apply the theoretical knowledge that they have learned by project practice, internship, and practical training. Real network security projects are part of the project practice phase, and students are divided into groups. The subtasks of the project are divided among each group. Students independently take on the requirements analysis, scheme design, implementation, and tests of the project under the arrangement of a teacher, developing the ability of their teamwork, project management, and practical operation. The internship and practical training program arrange for students to conduct an intern period at network security companies or related institutions in order to get practical experience in the real environment of work, understand the practical needs and working process of the industry, and enhance their employment competitiveness.

Project Selection and Integration.

The selection and the OBE project integration are important steps in the model of vocational network security talent training. The real network security project is to choose a few pieces that are complete enough to expose the students' professional knowledge and skills. Select enterprise network security protection projects, which include tasks such as security assessment of enterprise network architecture, selection and configuration of network security equipment, detection and repair of network security vulnerabilities, formulation and implementation of security policies, etc.; Select government department information system security reinforcement projects involving security audits, data encryption, user identity authentication, and authorization of information systems. Different foci on the integration methods and the project teaching objectives are made at different stages of the course.

In the basic course stage, simple network security project cases are introduced, mainly in the form of case analysis for teaching, to help students understand the knowledge points in the basic course. In the computer fundamentals course, by analyzing a case of data leakage caused by improper computer operation by employees in a certain enterprise, students are guided to think about the importance of computer security operations and deepen their understanding of basic knowledge such as computer file management and user permission settings.

In the core course stage of the major, project integration is more in-depth, teaching for the projects first using a project-based teaching method to divide the tasks into several courses. In the course of Network Security Equipment Configuration and Management, taking enterprise network security protection projects as the background, students

are required to select suitable security equipment such as firewalls, IDS/IPS, etc., according to the needs of enterprise networks, and configure and manage them to achieve security protection of enterprise networks. In the course of network security vulnerability detection and repair, students apply the vulnerability detection techniques and tools they have learned to conduct comprehensive vulnerability scans of information systems, analyze vulnerability risks, and develop repair plans for information system security reinforcement projects.

In the stage of practice in a course, students undertake a complete network security project practice from the project requirements analysis, scheme design, implementation, testing, and acceptance so as to allow students to carry out the comprehensive practice abilities. Taking the network security emergency response project for the e-commerce platform as the example, students join forces as a project team to play the role of the network security team of the e-commerce platform. Together with the teacher, they construct an emergency response plan for the network security emergency response, set up the emergency environment for the network security emergency response, carry out the network attack simulation exercises, and, in case of an emergency during the exercise, promptly deal with the emergency, record the process, and record the results.

3.3 Diversified Teaching

By integrating development, distributed teaching methods are used to meet the different content of the course and the different learning needs of students in order to comprehensively improve the professional ability and comprehensive quality of students in the vocational network security skill training model based on the OBE project.

Including one of the core teaching methods of this training model, this is a project-driven teaching method. Network security projects are decomposed into actual tasks, and the project implementation is encouraged through actual participation in groups in the teaching of network security courses. There is a certain enterprise network security protection project that forces one to analyze enterprise network architecture and security requirements and choose corresponding security devices such as firewalls and IDS/IPS suitably and configure and manage these security devices to realize security protection of the enterprise network.

Another of the important teaching methods is the case study teaching method. Large amounts of practical network security cases are introduced in the teaching process in the teaching of the network security knowledge and technology through the analysis, discussion, and resolution of the cases about a given enterprise's network security incident and major network security vulnerability. To explain the network security vulnerability detection and repair process, we choose a particular e-commerce platform that is attacked by SQL injection as an example to make students understand the reasons for the attack, the type and the harm of the vulnerability, and then help students apply the vulnerability detection tools and methods they have learned and make a proposal of the vulnerability detection and repair procedures for the case.

The group collaborative learning method plays an important role in cultivating students' teamwork spirit and communication skills. In project practice and course discussions, students are divided into groups, with each group responsible for a project task or solving a practical problem. Group members need to divide their work and collaborate to complete tasks together. In the comprehensive training course of network security, students complete a complete network security project in groups, including project requirement analysis, scheme design, implementation, and testing. In the process of group collaboration, students need to engage in effective communication and coordination, leverage their respective strengths, and work together to solve problems encountered in the project.

Various teaching methods such as situational teaching and heuristic teaching have been employed. The situational teaching method creates realistic network security work scenarios, allowing students to learn and practice in simulated work environments, improving their professional competence and practical work abilities.

4 Practice of the Obe Project-Based Cultivation

In order to verify the feasibility and effectiveness of the vocational network security talent training model built on the OBE project, two project practices of "system security defense" and "application security defense" were established. Defensive Security System “is an enterprise network security protection project, which builds an enterprise network security protection system including the choice and configuration of network security equipment, the formulation and implementation of security policies, and the network security vulnerability detection and repair tasks to ensure the stable and safe operation of the enterprise network, preventing data leakage and attacks in the network and other types of security events. "The Application Security Defense" is a program of the Government Department Information System security reinforcement project, and the core task is to conduct a system security assessment for the Government Department Information System, and such work consists of finding system vulnerabilities, checking the security configuration, and encrypting the data. By crafting problems found on the assessment, the security reinforcement is done to grow the security of the info system and the governance of the government department info security.

4.1 Implementation Process

In terms of curriculum design, we follow the design concept of a curriculum system OBE project-based.

(1) In the first academic year, basic courses such as computer basics, network basics, and Python programming language basics are offered to lay a solid foundation for students' subsequent learning of network security professional knowledge. In computer fundamentals courses, teachers use practical case demonstrations to help students master basic operations such as installing and configuring computer operating systems, file management, etc; In the course of network fundamentals, network topology simulators

are used to help students understand the characteristics and application scenarios of different network topology structures.

(2) In the second academic year, core courses such as Network Security Fundamentals, Network Security Equipment Configuration and Management, and Network Security Vulnerability Detection and Repair will be offered. In the basic course of network security, a network attack incident suffered by a certain enterprise is introduced, allowing students to analyze the attack principles and defense measures, and deepen their understanding of network security knowledge; In the course of network security device configuration and management, students are grouped into groups to practice the configuration and management of security devices such as firewalls and IDS/IPS, based on real enterprise network security protection projects. Teachers provide on-site guidance and promptly solve problems encountered by students; In the course of network security vulnerability detection and repair, students use vulnerability scanning tools such as Nessus and OpenVAS to detect vulnerabilities in simulated network systems, and develop repair plans based on the detection results.

(3) In the third academic year, practical courses such as comprehensive cybersecurity training and enterprise internships will be arranged to enable students to comprehensively apply their learned knowledge and skills in practical projects. The comprehensive network security training project selects real network security projects, such as the network security protection project of a certain e-commerce platform. Students form a project team to comprehensively exercise students' comprehensive abilities from project requirement analysis, scheme design, implementation to testing and acceptance.

In terms of evaluation methods, the case university has established a diversified evaluation system to comprehensively and objectively evaluate students' learning outcomes. The evaluation of skill dimensions is conducted through project practice, experimental operations, skill competitions, and other methods. In the project practice of the Network Security Equipment Configuration and Management course, teachers evaluate students based on their equipment configuration plans, operation processes, and ultimately achieved security protection effects; In the experimental operation of the network security vulnerability detection and repair course, teachers evaluate students from the accuracy of vulnerability detection and the feasibility of repair plans. Combining formative evaluation with summative evaluation, formative evaluation runs through the teaching process. Teachers timely understand students' learning situation, identify problems, and provide guidance through classroom questioning, group discussions, project progress checks, and other methods; Summative evaluation is conducted at the end of the course, project completion, or semester, and comprehensively evaluates students' learning outcomes through theoretical exams, practical assessments, project outcome evaluations, and other methods.

4.2 Effect Analysis

By implementing the OBE project based integrated training model for experimental class students and regular class students at the case university, and according to the evaluation index system for the quality of computer network security professional talent training, this study analyzes and compares the quality of training from the aspects of

achieving course objectives and graduation requirements, evaluating employers, and evaluating graduates' feedback abilities. In the evaluation of the achievement of course objectives and graduation requirements, the "credit score" is used to evaluate students' graduation grades and calculate the achievement of course objectives and graduation requirements. The quantitative evaluation standard for achievement is set at 0.7. The achievement of 13 graduation requirements for students majoring in computer network security in the experimental class and regular class is shown in Figure 1, with the horizontal axis representing the graduation requirements and the vertical axis representing the degree of achievement of the graduation requirements.

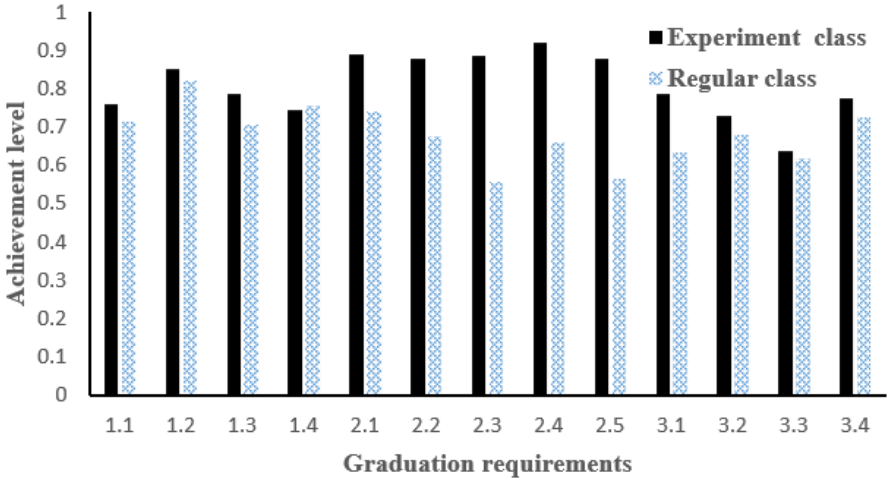

Fig. 1. Completion of graduation requirements for students majoring in cybersecurity

Viewing from Figure 1, it can be seen that this training model has achieved significant results in improving students' knowledge, skills, and employment. The graduation requirements of this class of graduates have all met and exceeded the standard requirement of 0.7. Compared to regular classes, experiment classes can achieve higher levels of achievement, especially in terms of improving practical skills. This indicates that the training model based on the OBE project can enable students to have a more systematic and in-depth understanding of network security professional knowledge. Through the study of practical projects and cases, students have a more thorough understanding of the knowledge and a deeper memory. At the same time, it fully demonstrates that this training model effectively improves students' practical skills. Through project-based teaching and a large number of practical operations, students continuously exercise and improve their skill levels in actual projects, and can more proficiently apply their learned skills to solve practical network security problems.

From the point of view of employment, the OBE project implementation in terms of the implementation of a comprehensive training model has significantly increased the competitiveness of students in the market of jobs. Statistically, students majoring in this had an employment rate that increased from 80% to 95% and an employment matching rate that increased from 60% to 85%. Student employment at the enterprises is more

diversified, not only traditional cybersecurity enterprises but also the enterprises in finance, e-commerce, and other industries, because they highly esteem the professional ability and professional quality of students. Whether it be that the salary of students has increased significantly as well, to approximately 1500 yuan per month, or that the population of the students themselves has significantly increased. In other words, this training model can help cultivate more students who can more adequately meet the needs of enterprises and have more competitiveness in the job market, with better employment and development space.

Through the analysis of the process of implementing and the effectiveness of case college, the study indicates that the OBE project-based vocational network security talent training model has obvious positive effects on improving students' knowledge level, skill ability, and employment competitiveness, and the model is feasible and effective for vocational network security talent training.

5 Conclusion

OBE project-based vocational network security talent training model constructed in this study has improved the application system of OBE concept in the field of vocational network security talent training, clarified the method of reverse design of training objectives guided by industry needs, constructed a project-based curriculum system framework, enriched the application strategies of diversified teaching methods in network security teaching, improved the diversified and full process teaching evaluation system, provided new ideas and theoretical basis for the research of vocational network security talent training model, and achieved good results in teaching practice. Future research will further expand the research sample and conduct studies on multiple vocational colleges, comparing the differences and commonalities of different colleges in implementing OBE project-based integrated training mode, summarizing more universal experiences and methods, keeping up with technological development trends, updating teaching content and training objectives in a timely manner, and cultivating high-quality talents that can adapt to the future development needs of network security.

Acknowledgments

This research was supported by Guangdong Key Scientific Research Platform Project under Grant No. 2024CJPT004, Guangdong Higher Vocational Education Teaching Quality and Reform Project under Grant No. 2023JG511, higher education specialization Project for Guangdong Education Science Planning under Grant No. 2023GXJK946, School Quality Engineering and Teaching Reform Project under Grant No. SWJY23-004 and No. SWJY24-009.

References

1. Liu Yandong. Research on the Practice of Project based Teaching Mode in Information Technology Majors in Vocational Colleges Vocational and Technical Education, 2024, 4(35), 56-60.
2. Sloam, J., Kisby, B., Henn, M., and Oldfield, B. Voice, equality and education: the role of higher education in defining the political participation of young europeans. Comp. Eur. Polit. 2021 (19): 296–322.
3. Zeng Peng, Yi Jie. Research on the Talent Training System of Industrial Visual Field Engineers under the Background of Industry Education Integration. Ship Vocational Education, 2025, 13 (1): 1-4.
4. Marland, Joshua, Harrick, Matthew, Sireci, Stephen G., Student Assessment Opt Out and the Impact on Value-Added Measures of Teacher Quality, Journal of educational and psychological measurement, 2024 80(2):365-388.
5. Xu Lan, He Jingshi, Mai Qiang. The practical obstacles and targeted paths for vocational colleges to cultivate on-site engineers under the background of new quality productivity. Education Theory and Practice, 2025, 45 (06): 20-25.
6. Evans Carla M., Lee Jade Caines. Value-added assessment of teacher preparation programs in the United States: a critical evaluation, Journal of assessment in Education Principles Policy & Practice, 2023, 25(5): 519-539.
7. Chen Jie, Fan Yao, Wang Hao. Research on the Innovative Training Model of Industry Education Integration for Computer Field Engineers under the OBE Concept. Innovation and Entrepreneurship Theory Research and Practice, 2024, 7 (23): 153-155.
8. Vladislav, S. G., Oleg, I. B., Sergey, S. S., Pyrkin, A. A., and Karashaeva, F. B. Modeling and control of robotic systems course: from fundamentals to applications. IFAC Pap. 2019 (5): 224–229.
9. Pominova, I. I., and Zaretskaya, L. M. The role of civil society institutions in the development of higher education. Business Inform. 2022 (4): 8-13.