ISSN 2522-6398 Vol. 7, Issue 9: 66-71, DOI: 10.25236/FER.2024.070911

Design and research of information security professional platform

Xiaomei Xiong

Jiangxi Police Institute, Nanchang, China
18970868930@163.com

Abstract: *The new era of the global Internet poses new challenges for the training of information security professionals. Traditional curriculum teaching methods lack the development of students' comprehensive analytical and application skills. To address this problem, an online and face to face combination of case-modular mixed learning based on a curriculum information system platform has been proposed. We have improved the course teaching plan by adjusting the structure of traditional course teaching modules, innovating the curriculum system, and employing various teaching methods in course implementation, such as online and blended face-to-face teaching, project-driven teaching, and modular case teaching. To meet the teaching needs of multidisciplinary information security courses through the introduction of different teaching cases, project-driven teaching, etc, it can provide reference for the reform of traditional engineering curricula such as information security, computer science and technology.*

Keywords: *systems security; mixed methods; undergraduate universities; information security specialties*

1. Introduction

On 28 August 2023, China Internet Network Information Centre (CNNIC) released the 52nd Statistical Report on the State of Internet Development in China (hereinafter referred to as the "Report"). The report shows that as of June 2023, the size of China's Internet users reached 10.7 billion people, an increase of 11.9 million compared to December 2022, the Internet prevalence rate reached 76.4%[1].In order to maintain national security, information security and network security, it is necessary to further strengthen the training of information and cybersecurity professionals in the new era.

In response to the new round of technological and industrial revolution and transformation, the information security specialty and the transformation of information security professional industries, the systematic development of innovative information security becomes a long-term strategic task. Information security is a huge system project and requires the support of a large number of professional and technical personnel with the spirit of innovation and practical ability.

The teaching methodology of the specialized "interdisciplinary cross-cutting" course needs to be improved in the training practice of information security professionals. The teaching methodology of the specialized "interdisciplinary cross-cutting" course needs to be established in a timely manner. Due to the wide range of expertise in the information security specialty curriculum system, traditional teaching methods lack the development of students' comprehensive analytical and application capabilities, therefore, it is necessary to integrate and optimize the linkage of curricula and relevant knowledge points according to the characteristics of the information safety specialty.

The intrinsic rule of logic of the course, on the basis of the traditional professional curriculum to integrate the optimization, form the innovating "interdisciplinary cross-crossing" of the professional course, the integration of the link between optimizing the course and the relevant knowledge points, the formation of the "inter-discipline cross" of innovative courses and the course logic close, modular knowledge interconnected innovation of the teaching system. Through the "interdisciplinary cross-discipline" innovative curriculum design, the innovation of the curricular system, systematized in-depth teaching, effectively promote the overall quality of teaching.

ISSN 2522-6398 Vol. 7, Issue 9: 66-71, DOI: 10.25236/FER.2024.070911

2. Literature Review

Information systems and cybersecurity play a vital role in modern society. Cybersecurity threats have also become increasingly complex and diversified as technology develops and the level of informatization increases. The researchers covered many aspects of this area, including data privacy protection, cyber attack defence strategies, and security management practices.

Data privacy protection is a central issue in information system security.Data Quality Campaign (2015)[2] and ExcelinEd.org (2016)[3] focused on legislative progress on student data privacy and put forward specific model legislative proposals. These studies emphasize the importance of protecting sensitive data in the field of education and provide valuable guidance to legislators and educational institutions. These studies indicate that, as data privacy threats increase, the development and implementation of effective privacy protection policies becomes crucial.

At the same time, cyber-attack defence strategies are also a focus of the study. McCrea (2016) demonstrates the severity and complexity of the current cyber attack by describing the case of a ransomware attack in a school district[4]. Such an attack constitutes a major threat not only to information systems, but also to the operations and finances of the targeted entities. Therefore, understanding and developing effective defence strategies is crucial to reducing the impact of cyber attacks.

In addition, the study also involved the exploration of security management practices. Studies by the National Conference of State Legislators (2016) [5]and the Privacy Rights Clearinghouse (2016) [6]respectively introduced a database of time sequence of security vulnerability notification laws and data security vulnerabilities, providing empirical support for security management. Through the analysis of different security management practices, these studies help organizations to better understand how to address security vulnerabilities and act quickly after incidents to reduce potential damage.

In summary, these studies show that the research of information systems and cybersecurity requires not only a technical level of exploration, but also a multi-faceted coordination and coordination of law and management. As cybersecurity threats evolve, researchers need to keep an eye on emerging threats and develop more sophisticated defence and management strategies to protect the integrity of information systems and data security.

3. Information Security Professional Course System Setup

The information security major requires students to master knowledge and skills from multiple interdisciplinary fields such as computer science, communications, mathematics, physics, law, and management. It primarily studies information science and technology to ensure information security and aims to cultivate high-quality professionals who can work in the field of information security.

The curriculum of the university's information safety specialization should be fully reflected in the training of technology application capabilities as the main line, to "apply as a subject setting curricula, build their own curricular system, enhance the practicality and relevance, so that students master the analysis of problem thinking and solving complex engineering problems practical ability.

Teachers focus on strengthening the cultivation of five types of thinking abilities in students: computational thinking, logical thinking, dialectical thinking, systemic thinking, and innovative thinking, in order to enhance students' comprehensive application skills.

3.1. Principles for the establishment of basic and professional courses

In order to reflect the professional competence and professional skills necessary for the position targeted to the career, the students have the skills and skills to apply the practice of vocational application and practice, the principle of professional basic lessons and the establishment of professional lessons is: master information security related theoretical knowledge, applied techniques, experimental training techniques, etc. The vocational courses include compulsory courses and electives, the obligatory courses are the skills that must be mastered by students. The electives are designed to expand the student's multi-directional learning needs or cutting-edge technology perspectives, in combination with the vocational characteristics, enrich the students' understanding of the professional knowledge, techniques, tools and methods of learning information security specialization. The

ISSN 2522-6398 Vol. 7, Issue 9: 66-71, DOI: 10.25236/FER.2024.070911

professional course is the core key course to strengthen students' vocational skills, to expand students' depth and breadth of the information security profession, focus on students' application of new knowledge, new technologies, new tools and new methods and vocational capacity improvement, and progress, according to the new era of information security function needs, adjust the professional direction of learning, and build the teaching content that is compatible with the integrated application of students.

3.2. Modular "Interdisciplinary Crossing" Curriculum Structure

Information security specialty courses can generally be divided into professional basic courses and professional orientation courses.

In order to integrate traditional professional curricula with information security disciplines, it is necessary to promote the intersection of existing curriculum with emerging information security knowledge and technologies. The curriculum combines with emerging knowledge and technologies such as data science, computer science and technology, artificial intelligence, and integrates the knowledge of different curricula into different courses. Therefore, we must break the traditional linear curriculum system and form a modular curricular structure for information security specialties. For example, based on the specialty of the discipline, the information security knowledge modules (including information network security monitoring, network intelligence collection and research, cybersecurity techniques and prevention, etc.) are constructed, the network system security application modules, including advanced language program design, website building and analysis, software system assessment, the system engineering security management module, including software development techniques, software engineering, software systems project integration, etc., as well as the big data science modules and other specialized course modules. Each module consists of several different specialty courses, thus forming a "cross-fusion" curriculum system(as shown in Figure 1).This platform consists of many modules,such as Information Security Expertise Platform(ISEP),Professional Basic Course Module (PBCM),Professional Core Course Modules(PCCM),Network System Security Application Module(NSSAM),Information Security Knowledge Module(ISKM),Data Science Security Technical Module(DSSTM)and Software System Security Management Module(SSSMM).Through this way, students have a certain understanding of innovative technologies in the latest cutting edge of China's development, from the professional basis, better master information security expertise and new technology in the integrated application in the field of information security, while developing students' systemic thinking skills, computational thinking ability, innovative thinking ability and so on, so as to improve the theoretical basic level and comprehensive practical application ability.

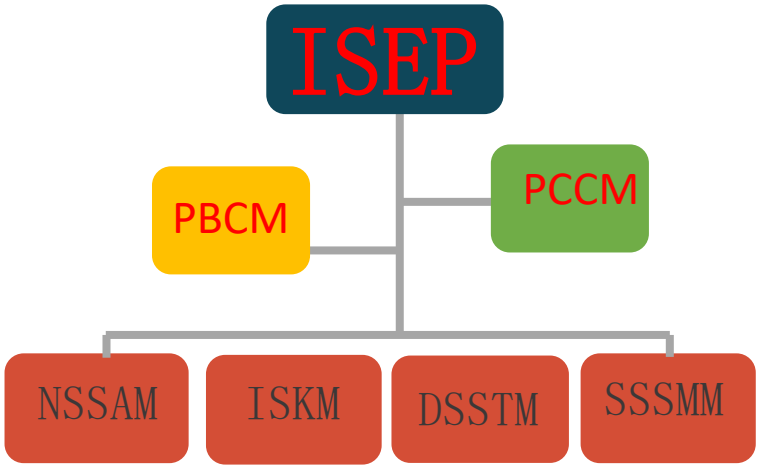

Figure 1: Design of the architecture of the modular curriculum for information security specialists

In order to focus on cultivating students' innovative abilities, practical skills, and social adaptability, as well as to enhance their overall quality and professional competence, a corresponding curriculum teaching platform and training system have been established[7].

On the basis of respect for the rules of education development, to promote high-quality applied talent as the goal of cultivation, is an important manifestation of the fundamental task of LIDER, in the cultivation of applied highly qualified talents, in setting up the professional curricular system, take into account the technical, practicality, applied, scientific setting curricula[8].

ISSN 2522-6398 Vol. 7, Issue 9: 66-71, DOI: 10.25236/FER.2024.070911

Considering that students should aim for work competence, it is essential to emphasize the improvement of practical skills. Therefore, it is necessary to integrate knowledge and skills from multiple disciplines to enrich the curriculum, such as fields like computer science and technology, management information systems, and law.

4. Create multi-faceted and synergistic educational resource platforms and teaching methods

In order to combine information security expertise with the latest technology in industry positions, we explored the "Management Department + Schools + Enterprises + Institute of Sciences" in collaboration with the education resource platform (CEP) and teaching methods of the professional curriculum(as shown in Figure 2).

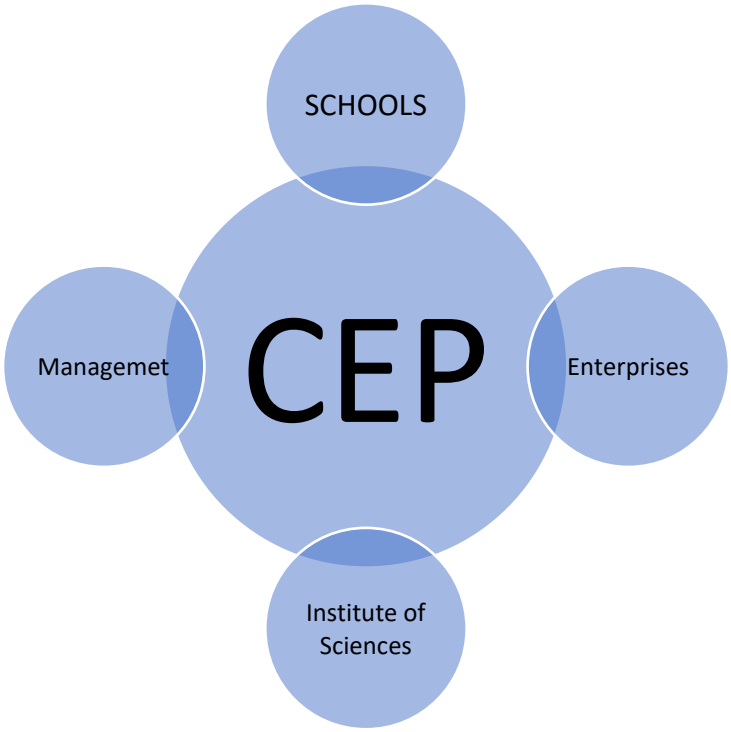

Figure 2: Information security vocational teaching resource platform design

One important aspect of information security is the competence of cybersecurity talents. The Cybersecurity and Law Enforcement program requires students to focus on information network security regulation, network information monitoring, network intelligence collection and analysis, cybercrime detection, and electronic data verification. Students should master fundamental theories, basic knowledge, and essential skills, and possess the ability to maintain the security of the national cyberspace[9].

Therefore, we believe it is essential to integrate the resources of management departments, schools, enterprises, and research institutions to enhance students' practical skills. We encourage students to form innovation teams, apply for innovative projects, and focus on scientific research, inventions, and technical services related to safety technology during their entrepreneurial practices.

The school opens specialized laboratories for students during their spare time, providing a favorable environment to enhance their practical skills and increase credits for practical internship courses. Through joint training programs with enterprises, it helps students improve their practical experience, validate the theories they have learned, and strengthen their ability to solve problems in practice.

ISSN 2522-6398 Vol. 7, Issue 9: 66-71, DOI: 10.25236/FER.2024.070911

Figure 3: Professional methods of information security

4.1. Online and offline mixed method

Using the online school's information system teaching application platform and the online enterprise's network technical practical resources, the mixed learning and design of online information security professional courses, teachers conduct offline teaching activities in the school, and introduce enterprise mentors to conduct on-site or online teaching, conduct mixed teaching methods exchange(as shown in Figure 3), carry out modular multidisciplinary cross-fusion education training, promote the systematic course building of the theoretical foundation of information security professionals and practical skills, effectively realize the organic combination of online and on-line teaching in the campus, forming the "multi-discipline interfusion" innovative teaching model.

4.2. Case-based method

Through a pre-prepared case database, from different case material perspectives, students are inspired to analyze and think from different angles on specific issues in the field of actual information security. In this way, it is possible to cultivate students' computational thinking, abstract thinking, dialectical thinking, innovative thinking and system thinking, to the development of students' comprehensive application skills, scientific innovation skills and practical skills.

4.3. Project-based method

Teachers at the school select foundational or specialized courses based on relevant knowledge content, allowing students to learn through project-based group work. By addressing these issues, students' interest in learning can be stimulated.

Students as team members need to earnestly invest time and energy to continuously solve the phased tasks of each project, in the process of solving problems, the project manager arises when the team collaborates to complete tasks. As the course progresses and develops, complex professional problems are addressed through continuous questioning, group discussions, and collaboration.

5. Conclusion

The curriculum is structured to develop and form a multi-module "cross-fusion" of knowledge points.

On this basis, a diversified curriculum teaching methodology of online, offline, mixed teaching,

ISSN 2522-6398 Vol. 7, Issue 9: 66-71, DOI: 10.25236/FER.2024.070911

case-inspired teaching and project-based teaching has been developed, and effective feasibility measures have been proposed. The research results are applied to information security-related specialties and provide reference to other specialties' curriculum reform and upgrading.

Acknowledgements

This study was supported by the Provincial Project of Science and Technology of Jiangxi Provincial Department of Education in 2022: "Research on the Protection of Users' Personal Information Security under the Perspective of Cybernetics" (No. GJJ2202309).

References

[1] China Internet Network Information Centre. (2023). 52nd Statistical Report on the State of Internet Development in China [EB/OL]. Retrieved from [URL].
[2] Data Quality Campaign. (2015, May). Student Data Privacy Legislation: What Happened in 2015, and What Is Next? Retrieved from Data Quality Campaign website: http://www.dataquality campaign.org/ resource/student-data-privacy-legislation-happened-2015-next/
[3] ExcelinEd.org. (2016, May). Model Legislation. Retrieved from ExcelinEd website: http://www.excelined.org/wp-content/uploads/Student-Data-Privacy-Accessibility-and-Transparency-Act-Model-Legislation-03.2015.pdf
[4] McCrea, B. (2016). How Hackers Held a District Hostage for Almost $10,000. Retrieved from eSchool News website: http://www.eschoolnews.com/2016/06/08/ how-hackers-held-a-district-hostage- ransomware/
[5] National Conference of State Legislators. (2016, June). Security Breach Notification Laws. Retrieved from NCSL website: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx
[6] Privacy Rights Clearinghouse. (2016, June). Chronological Database of Data Security Breaches. Retrieved from Privacy Rights Clearinghouse website: http://www.privacyrights.org/data-breach
[7] Zhu, J. (2023). Public security education. Chongqing Public Security Education, (09), 53-56.
[8] Nongu, Z., & Zhu, Y. (2018). Cultivation goals: Value leadership of talent development modeling reform—Based on the enlightenment of Stanford University's "Ring University" programme. Modern University Education, (04), 103-111.
[9] Li, J. (2015). National standards of teaching quality for the training of cybersecurity and law enforcement professional talent training programme. Sichuan Police Academy Study Report, 27(06), 91-96.