Educational Research and Human Development
ISSN: 3007-6943
DOI: https://doi.org/10.61784/erhd3019

EXPLORATION OF INTEGRATION SCHEMES FOR INFORMATION SECURITY AND PROGRAMMING COURSES

Yu Hao*, Weihua Liu, Ying Liu, Na Li, WeiDong Zhang
School of Communications and Information Engineering, Xi'an University of Posts and Telecommunications, Xi'an 710121, China.
Corresponding Author:Yu Hao, Email: haoyu@xupt.edu.cn

Abstract: Despite the fact that universities have paid sufficient attention in accordance with national information security policies, information security education during the college period is still constrained by issues such as limited coverage and insufficient training hours. Considering that programming courses are offered in the majority of engineering and science majors, this paper proposes a scheme to integrate the cultivation of information security awareness into the teaching of various programming courses. Through studying the integrated cases, students can develop their information security awareness while mastering theoretical knowledge points. Results indicate that students' information security awareness has been significantly enhanced after studying the integrated cases. Leveraging the high proportion of programming courses in the teaching system, this scheme is expected to greatly expand the coverage of information security education in universities.

Keywords: Information security; Programming course; Integration schemes

1 INTRODUCTION

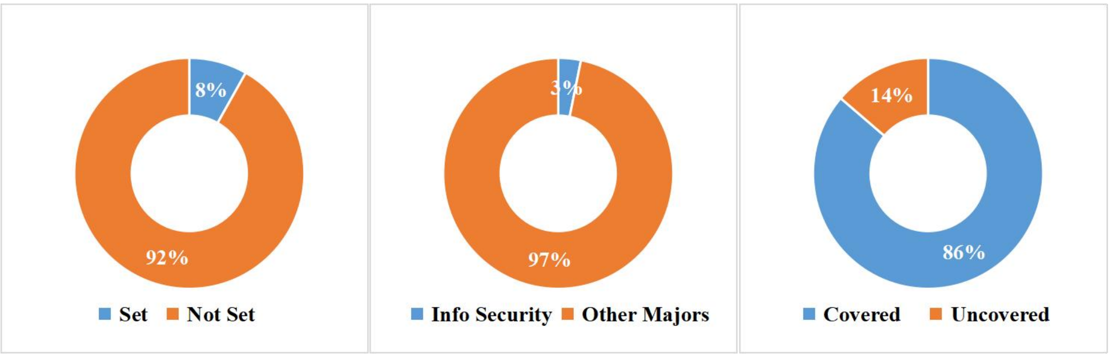
In recent years, with the intensification of international competition, information security incidents such as cyberattacks and breaches that jeopardize national and social security have occurred repeatedly. China has passed laws including the Data Security Law of the People's Republic of China and the Network Security Law of the People's Republic of China to enhance information security capabilities and prevent information from being tampered with, damaged, leaked, or illegally obtained or utilized during economic and social development. The primary causes of information security incidents are technical vulnerabilities and a lack of security awareness. Technical defects or vulnerabilities in systems or networks can be exploited by attackers. Therefore, some institutions have established relevant mechanisms to eliminate the possibility of information leaks from both technical and institutional perspectives. For example, Sinopec has constructed a relatively comprehensive information security management system such as the "Five-in-One" network security risk management and control mechanism to ensure the safe operation of critical infrastructure [1]. However, many breaches are caused by a lack of information protection awareness and disregard for confidentiality regulations or policies. Thus, merely establishing regulations cannot completely eliminate such incidents.

Cultivating students' awareness of information protection early in their college education helps safeguard confidential information they may encounter in their future careers. The cultivation of information security concepts in higher education primarily stems from the establishment of information security disciplines and the implementation of general education courses on information security. The curriculum of information security disciplines generally includes cryptography, network security, application security, and other related content, which enables students to effectively cultivate their information security awareness while learning relevant technologies [2]. However, in 2024, only 69 universities in China offered information security majors, accounting for only 8% of the 845 public universities nationwide, indicating a low coverage rate. Additionally, the number of students majoring in information security does not constitute a high proportion of the total student population. Taking Xi'an University of Posts and Telecommunications as an example, in 2024, there were 603 undergraduate students majoring in information security, which is only 3% of the total undergraduate population of 19,000. Therefore, the strategy of cultivating students with good information security awareness through information security disciplines cannot achieve widespread coverage.

Another approach currently employed by universities to cultivate knowledge of information security is to offer general education courses on information security to all students on campus. In recent years, many universities have explored methods to popularize information security education among their students, by inviting experts in the field of information security to conduct lectures, organizing students to take online open courses on information security, and other means, in order to cultivate the concept of information security among non-major students [3]. The main issue faced by such methods is the insufficient duration of training, which is usually only around 2 academic hours, making it impossible to deeply instill the concept in students. Additionally, non-major students often adopt a perfunctory attitude when taking online open courses [4], so cultivating the concept of information security through this method tends to become a mere formality, failing to achieve the expected results.

The offering of programming courses is very common in China, covering almost all universities nationwide, including comprehensive key universities, ordinary institutions, and vocational colleges. Furthermore, various programming courses have also achieved wide coverage among non-computer majors in universities [5]. Taking Xi'an University of Posts and Telecommunications as an example again, the university has a total of 51 undergraduate majors, among which 44 majors offer programming courses, mainly including C++, Java, Python, etc., accounting for 86.3% of all majors.

Compared to majors related to information security, programming courses have an absolute advantage in terms of coverage within the university. On the other hand, programming courses explain some of the mechanisms for the transmission of computer information, and object-oriented computer languages possess mechanisms such as encapsulation and inheritance for achieving information protection and separation [6]. These concepts are highly complementary to the concept of information security. Therefore, a teaching mode that integrates the knowledge points of programming courses with the cultivation of information security awareness can be designed. With the understanding of relevant knowledge points in computer languages, students are more likely to accept the integrated concept of information security. At the same time, the wide coverage of language courses can ensure synchronous coverage of the cultivation of security awareness, potentially addressing the shortcomings of the two current main training modes (Figure 1).



(a) (b) (c)

Figure 1 Comparison of Coverage Rates Among Several Strategies for Cultivating Information Security Awareness. (a) The Proportion of Universities in China that Offer Information Security Majors. (b) The Proportion of Students Majoring in Information Security at XUPT to the Total Student Population. (c) The Coverage Rate of Computer Language Courses at XUPT.

2 OVERALL STRATEGY FOR INTEGRATING PROGRAMMING COURSES WITH THE INFORMATION SECURITY

The strategy explored in this paper for integrating and cultivating programming courses with the concept of information security generally consists of four main steps, as illustrated in Figure 2 below. Firstly, based on the characteristics of the selected programming courses, the knowledge points are dissected and correlated with the main concepts of information security. Secondly, through the analysis of actual cases from actual cases completed by scientific research teams, and publicly sourced cases, a collection of cases suitable for matching with the course knowledge points is screened and summarized. After completing the dissection of knowledge points and case research, the third step involves matching the dissected knowledge points with the cases in the collection according to the corresponding information security concepts, and designing specific training plans. Finally, the training plan is implemented in actual course, and the training effect of the plan is evaluated based on relevant evaluation mechanisms to optimize it. At the same time, this process achieves the cultivation of students' information security protection awareness.

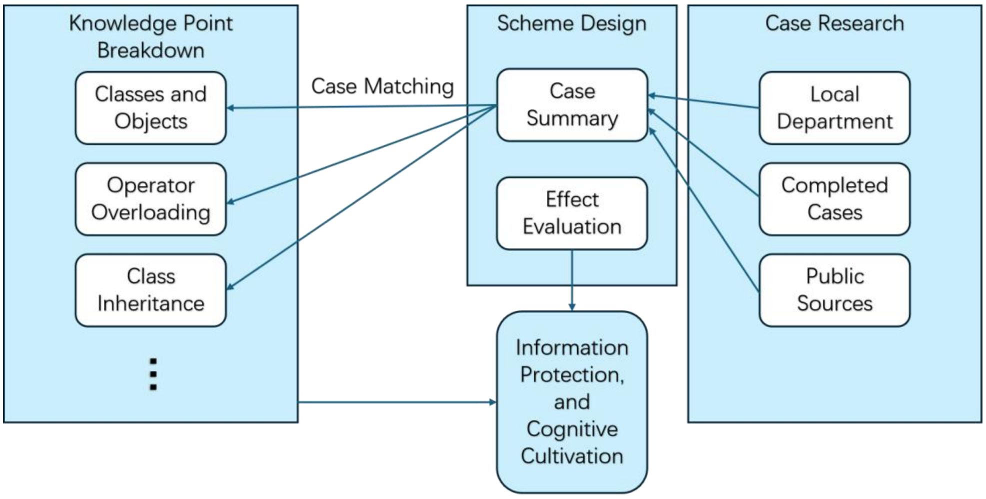


Figure 2 Framework for Integration Strategy of Computer Language Courses and Information Security Concepts

3 PATTERNS OF KNOWLEDGE POINTS IN PROGRAMMING COURSES

Currently, the language courses offered in universities mainly include five mainstream advanced programming languages: C++, Java, Python, C#, and Matlab, among which C# and Matlab account for a relatively low proportion, while the other three languages dominate. Mainstream advanced languages typically share characteristics of object-oriented programming, which are also key focus areas during the course of study. These include classes and objects, encapsulation, inheritance, polymorphism, abstraction, message passing, etc. By conducting an in-depth analysis of these characteristics, matching information security cases are identified for integration, ultimately generating an upgraded set of teaching plans for each characteristic. This plan enables students to cultivate relevant security awareness through integrated information security cases while deeply studying the technical characteristics. The concept of information security can be mainly divided into three categories: (1) Physical security achieved through physical isolation; (2) Communication security during information transmission; and (3) System security, including operating systems, databases, vulnerability and virus detection, etc. Each knowledge point within the characteristics of computer languages can be matched with the most suitable category from the above three, in order to explore suitable cases for integration. The specific analysis results are as follows.

(1) Classes and objects, as fundamental concepts introduced in object-oriented programming languages, reversed the process-oriented programming paradigm, significantly enhancing efficiency in developing large-scale software. By introducing the concepts of object attributes and methods within classes and objects, and implementing access control through access specifiers to isolate visitors, system security can be achieved by setting different levels of object states and behaviors. (2) The encapsulation characteristic combines an object's attributes and methods into an independent unit, hiding the internal details of the object as much as possible to ensure that its internal state cannot be arbitrarily changed by external programs. External programs can only interact with the encapsulated data through interfaces, thereby improving code security and maintainability. This characteristic controls the physical isolation and openness of member information by setting interfaces. (3) The inheritance characteristic enhances code reusability, maintainability, and extensibility by allowing subclasses to inherit attributes and methods from their parent classes. By selecting inheritance methods, invisible hiding of related members of the parent class can be achieved, thereby realizing physical isolation. (4) Polymorphism refers to the ability of different objects to respond differently when calling the same member function. This characteristic enables program architects to focus on top-level design and programmers to focus on specific programming during large-scale software development, facilitating efficient collaboration. The concept of overloading in polymorphism ensures that the program can handle multiple different situations using the same method, which requires considering multiple possibilities during program design to ensure smooth operation and safeguard the security of the program or system. (5) Similarly, abstract classes and virtual functions are commonly used abstraction means in inheritance behavior to meet the needs of software division development and polymorphism, aligning with the concept of system security. (6) The message-passing mechanism is the primary information exchange mechanism between objects, achieving decoupling and loose coupling between objects, making the program more flexible. Friend functions or classes are often used during the exchange process to break access restrictions between classes. Therefore, attention should be paid to the use of the friend mechanism to ensure the security of the information transmission process. The detailed correspondence between advanced language characteristics and information security classifications is shown in Table 1 below.

Table 1 The Correspondence Between Programming Characteristics and Information Security Classifications

Characteristics of Programming Languages	Knowledge Points	Classification of Information Security
Classes and Objects	Member Functions and Attributes	System Security
Encapsulation of Classes	Access Specifiers and Interfaces	Physical Security
Inheritance of Classes	Inheritance and Code Reuse	Physical Security
Polymorphism	Overriding and Overloading	System Security
Abstraction of Classes	Abstract Classes and Virtual Functions	System Security
Message Passing	Friend Functions and Friend Classes	Communication Security

4 ACQUISITION OF INFORMATION SECURITY CASES

Based on the analysis of knowledge points in the Advanced Programming Language course and the corresponding information security classifications obtained, it is necessary to disassemble actual information security cases and match them with the types of information security. So teaching cases for programming languages that integrate the concept of information security can be devised. To achieve the above objectives, a large number of information security cases need to be acquired and screened. To ensure that the cases align with national development strategies, the overall direction should first be established according to relevant laws and regulations formulated by the country, and then relevant cases that conform to this direction should be obtained from various sources. From the perspective of national security, China's laws such as the State Secrets Law and Data Security Law establish relevant obligations related to national security in information activities. In terms of information system security, regulations such as the Network Security Law and Regulations on the Security Protection of Computer Information Systems provide behavioral norms for computer and internet security. Finally, amendments to the criminal law provide practical grounds for punishing computer-related crimes. Therefore, the acquisition of relevant integrated cases needs to comply with the overall direction of the above laws and regulations, so that students can understand the background knowledge of these laws and regulations during the learning process.

The main sources for acquiring cases are public information on the internet and relevant professional departments. With the increase in information security incidents in recent years, the relative department has expanded the promotion of such cases, leading to their widespread dissemination on the internet. By searching for keywords such as "leak" on domestic search engines, it is easy to obtain information security cases on various topics. This type of data is abundant and diverse, serving as an excellent source of cases. However, due to privacy concerns, many details are often removed from these cases. Although such omissions have no practical impact on the cultivation of security awareness, they can create a sense of distance for students during the learning process, reducing students' interest in learning. When relevant cases occur close to students and may have an impact on them, it will stimulate their interest and effectively improve learning efficiency. Local public security departments and public security laboratories usually have a large amount of historical case data, including cases of information security incidents. This study relies on the research team's laboratory resources and long-term cooperation with local public security departments to compile a series of real information security cases after removing confidential and sensitive information. These cases are rich in non-confidential details, serving as a good supplement to publicly available internet cases in the process of designing teaching cases.

Based on the overall design strategy and combining the sources of the aforementioned cases, this research compiles 12 practical cases concerning information security protection, including incidents such as the leakage of user data from medical equipment monitoring systems and the theft of communication content from encrypted communication software. These cases are matched with the knowledge points of encapsulation, inheritance, and code reuse in computer language courses. Using the matched case collection, a teaching scheme integrating information security and knowledge points is designed.

5 DESIGN APPROACH OF THE INTEGRATED CASE

The teaching scheme integrating information security consists of five components: Case Background, Overview of Information Security Incident, Technical Solution Approach, Sample Code, and Insights on Information Security Concepts. The derivation relationships among these five components are illustrated in Figure 3 below. (1) The Case Background provides an overview of the current case, introducing the context in which the incident occurred and the relevant computer language knowledge points. (2) Based on the Case Background, the Overview of Information Security Incident section details the vulnerabilities of the information security incident, the conditions and processes leading to information leakage, the consequences and severity of the leakage incident, and other relevant content. (3) In response to the actual situation of the incident, the Technical Solution Approach presents solutions and remedies for the aforementioned vulnerabilities through technical means, combining the teaching knowledge points. (4) The Sample Code resolves the issue in the form of code using the programming language taught, based on the Technical Solution Approach. (5) The Insights on Information Security Concepts summarizes the key technical issues of the case and the corresponding key points for cultivating information security awareness. Among these, Parts 3 and 4 aim to train students on the knowledge points of related courses, while Parts 1, 2, and 5 aim to cultivate students' information security awareness. Below is an intuitive presentation of one of these cases.

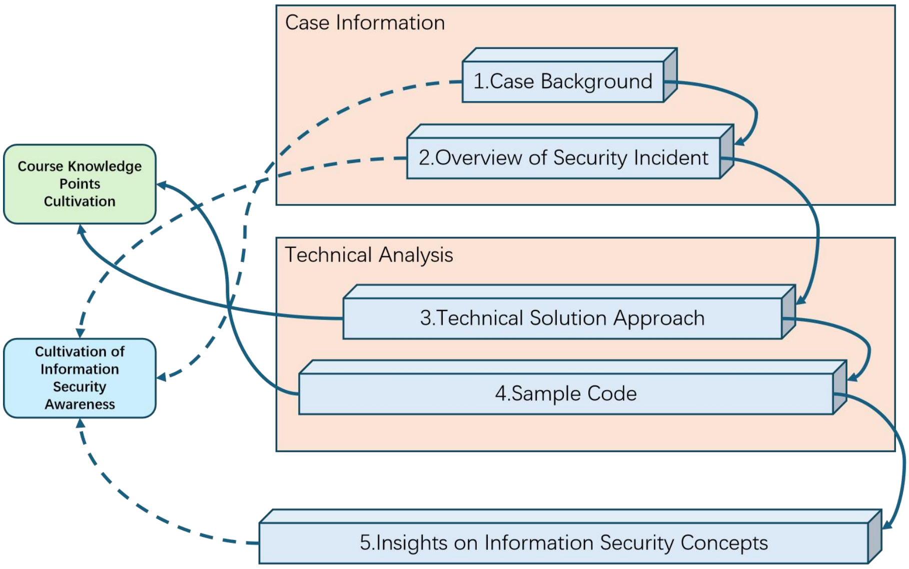

Case Information
1.Case Background
2.Overview of Security Incident
Course Knowledge Points Cultivation
Technical Analysis
3.Technical Solution Approach
4.Sample Code
Cultivation of Information Security Awareness
5.Insights on Information Security Concepts

Figure 3 Framework for Integrated Information Security Case Studies

Case Name: Classes and Objects - Common Encryption Methods

Case Background: A small library, aiming to enhance its management efficiency, developed a C/S architecture library management system implemented in C++. This system encompasses functionalities such as user management, book borrowing, and returning, utilizing C++ classes to encapsulate user information and book details. However, due to inadequate consideration of information security during system design, a user data breach occurred at the library.

Overview of the Security Incident: The library management system harbored certain design flaws. Specifically, the password attribute within the user class was stored in plaintext and could be directly accessed through member functions. Additionally, the system lacked rigorous validation of user inputs, posing risks such as SQL injection. During the attack, hackers attempted an SQL injection attack on the system by maliciously constructing query parameters. Upon successful exploitation, the hackers gained access to the user table structure within the database and downloaded all user data, including usernames and plaintext passwords. Ultimately, users' private information, including borrowing records and contact details, was leaked.

Solution Approach: During the system design process, implement encrypted password storage by modifying the user class to store password attributes as encrypted strings. Utilize secure encryption algorithms (such as AES, SHA-256, etc.) to encrypt passwords. Secondly, input validation is necessary, adding input validation logic to all functions that accept user input to prevent attacks like SQL injection. Use prepared statements or ORM frameworks to securely execute database queries. Additionally, implement access control, including role-based access control (RBAC), to ensure that only authorized users can access sensitive data. Log access to user data for tracking and auditing purposes. Finally, introduce security audits, including periodic security audits of the system to check for potential vulnerabilities. Utilize automated tools for code scanning to identify insecure programming practices.

Lessons Learned on Information Security Awareness: In this case, it is crucial to prioritize password security by educating students and users about the importance of password safety, such as using strong passwords and regularly changing them. Emphasize that passwords should not be stored or transmitted in plaintext. Secondly, enhance data protection awareness by understanding the basic principles and importance of data encryption, including encryption for transmission and storage. Recognize that sensitive data (such as user information, financial information, etc.) should be specially protected. Thirdly, stress the importance of validating all user inputs to prevent attacks like SQL injection and XSS. Learn how to write secure code to avoid common security vulnerabilities. Finally, guide students in understanding the concept of access control to ensure that only authorized users can access sensitive data. Learn how to implement strategies such as RBAC.

6 ANALYSIS OF THE CULTIVATION EFFECT OF THE INTEGRATED SCHEME

To validate the cultivation effect of the information security awareness integration case proposed in this paper, the author implemented it in the C++ Programming course for the 2023 intake of Information Engineering students at their university. To ensure the comprehensiveness and representativeness of the evaluation results, multiple methods were adopted during the course to collect data on the cultivation effect, including random testing, student interviews, analysis of homework completion, and questionnaire surveys. Firstly, the random testing method required students to answer questions related to information security knowledge covered in the previous class at the beginning of the course. The evaluation scheme recorded the students' test scores as the test evaluation value S_Q for this round of evaluation. Next, students are selected for interviews based on the median score of each round of testing to assess their understanding of relevant knowledge points and information security concepts. Subjective scoring is conducted during these interviews, and the results are recorded as the interview evaluation value S_D for this round of assessment. Subsequently, the completion status of information security-related knowledge points in students' after-school assignments and experiment reports is analyzed, with the accuracy rate of answers serving as the assignment evaluation value S_W for this round of evaluation. Finally, two information security knowledge surveys are conducted at the beginning and end of the course, with the results recorded as S_1 and S_2, respectively. Let $S_P = (S_2 - S_1) * e/E$ represent the survey evaluation value for a given round e, where e is the current evaluation round and E is the total number of evaluation rounds, and $\mathrm{e} \in \mathrm{E}$. Then, the evaluation value S_e for the cultivation effect in the $\mathrm{e-th}$ round of teaching can be derived from S_Q, S_D, S_W and S_P, as shown in Formula 1.

$$S_e = W^T \cdot S \tag{1}$$

Where $\mathrm{W} = [\mathrm{w}_1, \mathrm{w}_2, \mathrm{w}_3, \mathrm{w}_4]$ is the vector of weight coefficients for the evaluation values, set as $w_1 = 0.4, w_2 = 0.15, w_3 = 0.3, w_4 = 0.15$ in the verification process of this paper. $\mathrm{S} = [S_Q, S_D, S_W, S_P]$ represents the evaluation vector for the cultivation effect. A total of 5 rounds of evaluation were conducted in the verification process of this paper, noted as $\mathrm{E} = 5$, and the average evaluation value $\overline{S_e}$ for the cultivation effect of the 2023-grade students in Information Engineering was calculated for each round. The changes in the $\overline{S_e}$ values over the 5 rounds of evaluation are shown in Figure 4 below. The verification results indicate that $\overline{S_e}$ generally maintained an upward trend throughout the 5 rounds of evaluation. The final evaluation value $\overline{S_5}$ was 80.1, representing a significant improvement compared to the initial evaluation value $\overline{S_1}$ of 65.3. This confirms the effectiveness of the proposed scheme in cultivating the concept of information security in teaching process.

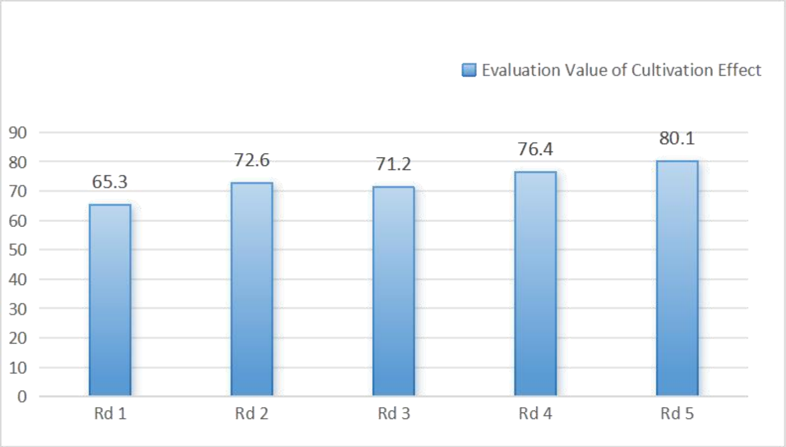


Figure 4 The Trend of Changes in the Average Value $\overline{S_e}$ of the Evaluation of the Cultivation Effect Across Five Rounds for Students Majoring in Information Engineering at XUPT.

7 CONCLUSION

Cultivating students' information security awareness at the university level holds significant strategic importance, as a lack of such awareness may lead to severe national security and economic security incidents in their subsequent professional careers. However, due to the relatively low coverage of specialized information security courses in current universities in China and inadequate cultivation effects of general information security courses, it is challenging to effectively promote the cultivation of information security awareness. To address these issues, considering the widespread offering of programming courses in science and engineering universities and the similarity in the knowledge structures of advanced programming teaching, this paper proposes a fusion scheme that integrates programming courses with the concept of information security. This scheme analyzes the knowledge points of mainstream advanced programming courses in universities and the corresponding directions for cultivating information security awareness that are compatible with these courses. Meanwhile, guided by national policy documents, the scheme screens out multiple real-life information security cases from public internet information and local public security departments and matches them with the cultivation directions. Finally, based on the fusion method proposed in the scheme, information security cases are integrated into the teaching of computer language courses. Practical verification results from computer courses for students at a university indicate that the proposed scheme effectively enhances students' information security awareness. Given the similarity in the knowledge structures of advanced programming teaching, this scheme can be applied to most coding courses, achieving wide coverage among students on campus.

COMPETING INTERESTS

The authors have no relevant financial or non-financial interests to disclose.

FUNDING

This work is funded by Educational Reform Projects of Xi'an University of Posts and Telecommunications (JGSZB202402) and (JGZYB202402).

REFERENCES

[1] Li Jun. Thoughts on the Construction of Information Security Education Courses in Colleges and Universities. Journal of Guangxi Police College for Criminal Justice, 2010.

[2] Shen Xiajuan, Gao Donghuai, Xu Hao, et al. Exploration of Information Security Quality Education for College Students. Information Security & Communications Privacy, 2014.

[3] Zuo Junyu, Sun Xinghua, Ye Simi, et al. Current Situation and Countermeasures of College Students' Network Information Security Awareness in the Context of "Internet +": A Case Study of Hebei University of Economics and Business. Modern Marketing (Information Edition), 2020.

[4] Yang Yongqi. Exploration of Key Issues in Big Data Information Security in Smart Cities. Digital Communication World, 2019.

[5] Zhao Jia. Preliminary Exploration on the Ideological and Political Construction of the Course "Introduction to Information Security". Science and Technology of Confidentiality, 2023.

[6] Huang Li. Comprehensively and Deeply Understanding and Effectively Maintaining Information Security - Learning from General Secretary Important Discussions on Information Security. Journal of Jiangsu Provincial Socialist College, 2023.