2025 Program for Talent Cultivation in Information Security

I. Program Overview

Major Code: 080904K

Admission Category: National College Entrance Examination

Discipline and Major Category: Engineering — Computer Category

Standard Duration of Study: 4 Years

II. Educational Objectives

Implement the fundamental task of fostering virtue through education, focusing on the cultivation of high-quality applied talents. To support regional economic transformation and development, industrial upgrading and technological innovation, the program cultivates socialist builders and successors who achieve well-rounded development in morality, intelligence, physical fitness, aesthetics and labor. They are politically firm, professionally skilled, honest and trustworthy, rational and calm, with good political and ideological literacy, humanities and social science literacy, and professional ethics. They possess strong engineering practice ability and innovative spirit, master basic theories, technologies and applied knowledge of natural sciences, computer technology and information security, and are competent for R&D of information security products, information security management, information security services and other work in the information security field.

Approximately 5 years after graduation, through personal effort and professional experience, graduates should be able to become engineers or outstanding professional talents and possess the following capabilities:

Objective 1: Familiar with the development status and trends of industrial information security related fields; be able to use mathematical, natural science and engineering basic knowledge, as well as professional knowledge of industrial automation and information security, to systematically analyze complex engineering problems in industrial information security and propose solutions.

Objective 2: Capable of utilizing modern tools and professional knowledge of industrial information security to engage in industrial network security protection, R&D of industrial information security products, security management of industrial enterprises, information security services and other work.

Objective 3: Possess the fundamental professional qualities and social responsibility of engineers, and abide by professional ethics and norms. In engineering practice, prioritize public interests, and comprehensively consider factors such as law, environment and sustainable development.

Objective 4: Possess healthy physical and mental wellbeing good humanistic literacy, have teamwork spirit and effective communication and expression skills, and be able to serve as technical backbones to play an effective role in enterprise production and management.

Objective 5: Have the ability of lifelong learning and self-improvement, and a certain international vision. Be able to continuously improve professional literacy and personal quality through engineering practice, continuing education and other means.

III. Graduation Requirements and Mapping Matrix

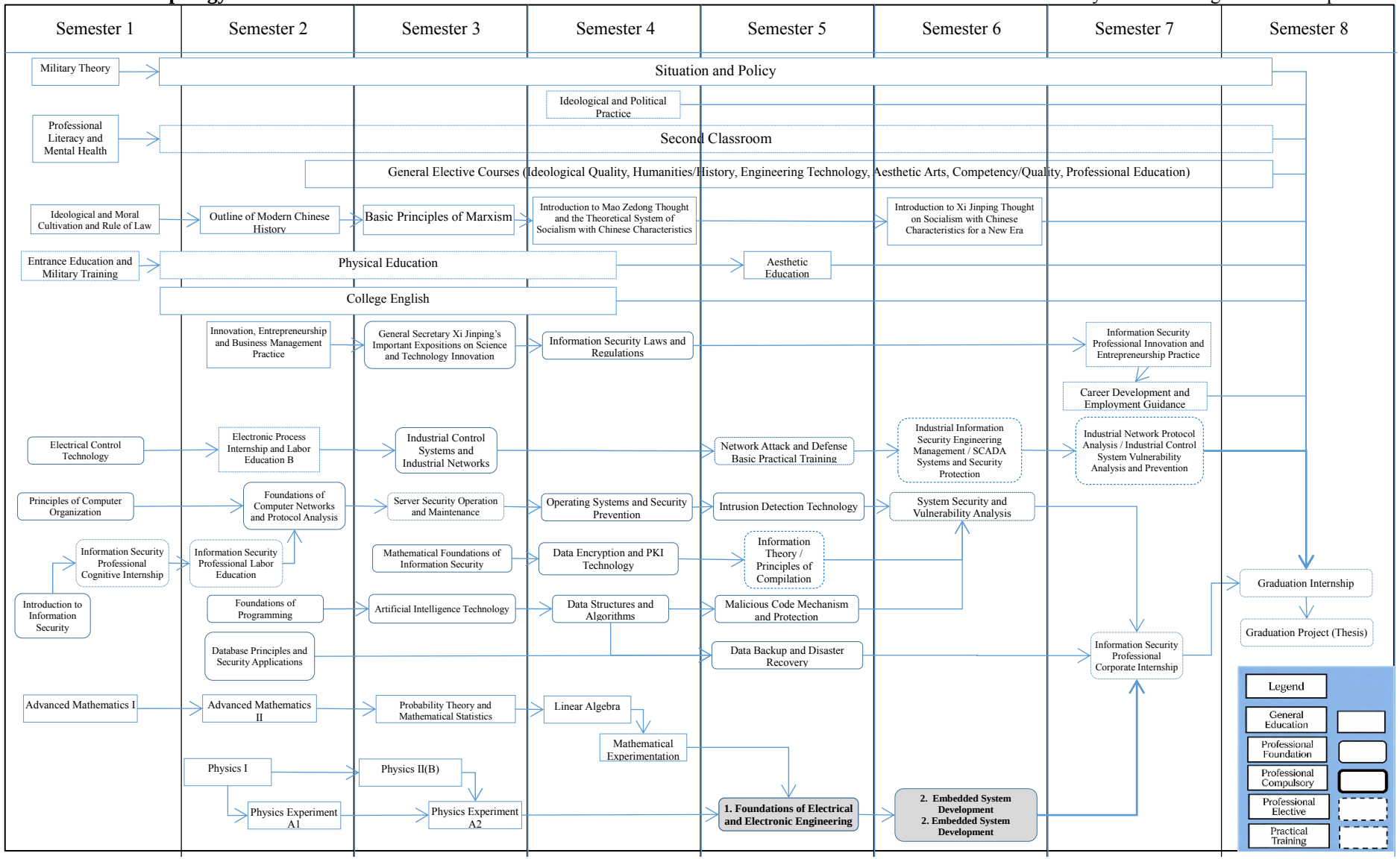
Graduation Requirements	Implementation Components / Channels
1. Engineering Knowledge: Systematically master the knowledge of mathematics, natural sciences, engineering foundations, and professional expertise required for engineering work related to information security, and be capable of comprehensively applying the aforementioned knowledge to solve complex engineering problems in the field of information security.	Advanced Mathematics, Physics, Physics Experiment, Mathematical Experiment, Probability Theory and Mathematical Statistics, Linear Algebra, Fundamentals of Programming, Electrical Control Technology, Fundamentals of Computer Networks and Protocol Analysis, Intrusion Detection Technology, Operating Systems and Security, Fundamentals of Electrical and Electronics
2. Problem Analysis: Capable of applying the basic principles of mathematics, natural sciences, and engineering sciences to identify and express complex engineering problems in the field of information security; be capable of mastering literature research methods and combining experimental practice to analyze complex engineering problems to obtain valid conclusions.	Introduction to Information Security, Principles of Computer Organization, Foundations of Computer Networks and Protocol Analysis, Database Principles and Security Applications, Mathematical Foundations of Information Security, Data Structures and Algorithms, Industrial Network Protocol Analysis, Industrial Control System Vulnerability Analysis and Prevention, Information Theory, System Security and Vulnerability Analysis, Graduation Project (Thesis).
3. Design/Development of Solutions: Capable of comprehensively applying professional knowledge, technologies, and methods to design solutions for complex engineering problems in information security-related fields, including designing information security systems and related components that meet specific needs; be capable of operating, maintaining and responding to information security systems; be capable of demonstrating innovation awareness in the design and development process while comprehensively considering constraints such as society, health, safety, law, culture, and environment.	Industrial Control Systems and Industrial Networks, Artificial Intelligence Technology, Malicious Code Mechanism and Protection, Server Security Operation and Maintenance, Data Encryption and PKI Technology, Data Backup and Disaster Recovery, Embedded System Development, EDA Technology and Application, Industrial Cloud Platform Security, SCADA Systems and Security Protection, Web Application Security, Graduation Project (Thesis).
4. Research: Capable of conducting research on complex engineering problems based on scientific principles related to the information security profession by using scientific methods, including designing simulation/experimental models, formulating research routes, safely conducting experiments, analyzing and interpreting data, and obtaining reasonable and effective conclusions through information synthesis.	Principles of Computer Organization, Mathematical Foundations of Information Security, Data Structures and Algorithms, Data Encryption and PKI Technology, Operating Systems and Security Prevention, Industrial Network Protocol Analysis.
5. Use of Modern Tools: Capable of developing, selecting, and using appropriate technologies, resources, modern engineering tools, and information technology tools during the process of analysis, research, and resolution of complex information security engineering problems, including prediction, simulation, analysis, and solution design for	Malicious Code Mechanism and Protection, Intrusion Detection Technology, SCADA Systems and Security Protection, Industrial Control System Vulnerability Analysis and Prevention, System Security and Vulnerability Analysis, Principles of Compilation, Artificial Intelligence Technology.

Graduation Requirements	Implementation Components / Channels
complex engineering problems while understanding their limitations.	
6. Engineering and Society: Capable of recognizing the interaction between information security system engineering and society; performing rational analysis based on engineering-related background knowledge to evaluate the impact of information security engineering practices and complex engineering problem solutions on society, health, safety, law, and culture, and understanding the responsibilities to be assumed.	Electronic Process Internship and Labor Education B, General Secretary Xi Jinping's Important Expositions on Science and Technology Innovation, Information Security Laws and Regulations, Digital Forensics and Emergency Response.
7. Environment and Sustainable Development: Capable of understanding and evaluating the impact of engineering practices for complex engineering problems on the environment and social sustainable development, and integrating the concept of sustainable development throughout the process of complex information security engineering practices.	Electrical Control Technology, Industrial Control Systems and Industrial Networks, Data Backup and Disaster Recovery, Information Security Professional Corporate Internship.
8. Professional Norms: Possess humanities and social science literacy and a sense of social responsibility; establish a correct worldview, outlook on life, and values; understand the professional nature, ethics, norms, and responsibilities related to the information security profession; and be capable of consciously abiding by professional ethics and norms and fulfilling responsibilities in engineering practice.	Situation and Policy, Ideological and Moral Cultivation and Rule of Law, Outline of Modern Chinese History, Basic Principles of Marxism, Introduction to Mao Zedong Thought and the Theoretical System of Socialism with Chinese Characteristics, Introduction to Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era, Career Development and Employment Guidance Practice, Information Security Laws and Regulations, Information Security Professional Corporate Internship, Graduation Internship.
9. Individual and Team: Capable of assuming the roles of individual, team member, or leader within teams with multidisciplinary backgrounds; possess a spirit of collectivism; and possess certain teamwork, organizational, and independent working abilities, playing an active role within the team.	Military Theory, Orientation and Military Training, Information Security Professional Innovation and Entrepreneurship Practice, Server Security Operation and Maintenance, Network Attack and Defense Basic Practical Training, Graduation Internship, Second Classroom, Ideological and Political Practice.
10. Communication: Capable of communicating and exchanging ideas effectively with industry peers and the public regarding complex engineering problems in the field of information security, including writing reports and design manuscripts, making presentations, and clearly expressing or responding to instructions. Possess a certain international perspective and the ability to communicate in cross-cultural settings.	College English, Professional Literacy and Mental Health, Innovation, Entrepreneurship and Business Management Practice, Information Security Professional Innovation and Entrepreneurship Practice, Graduation Internship, Graduation Project (Thesis), Second Classroom.
11. Project Management: Understand and master engineering management principles	Information Security Professional Cognitive Internship, Information Security Professional Innovation and

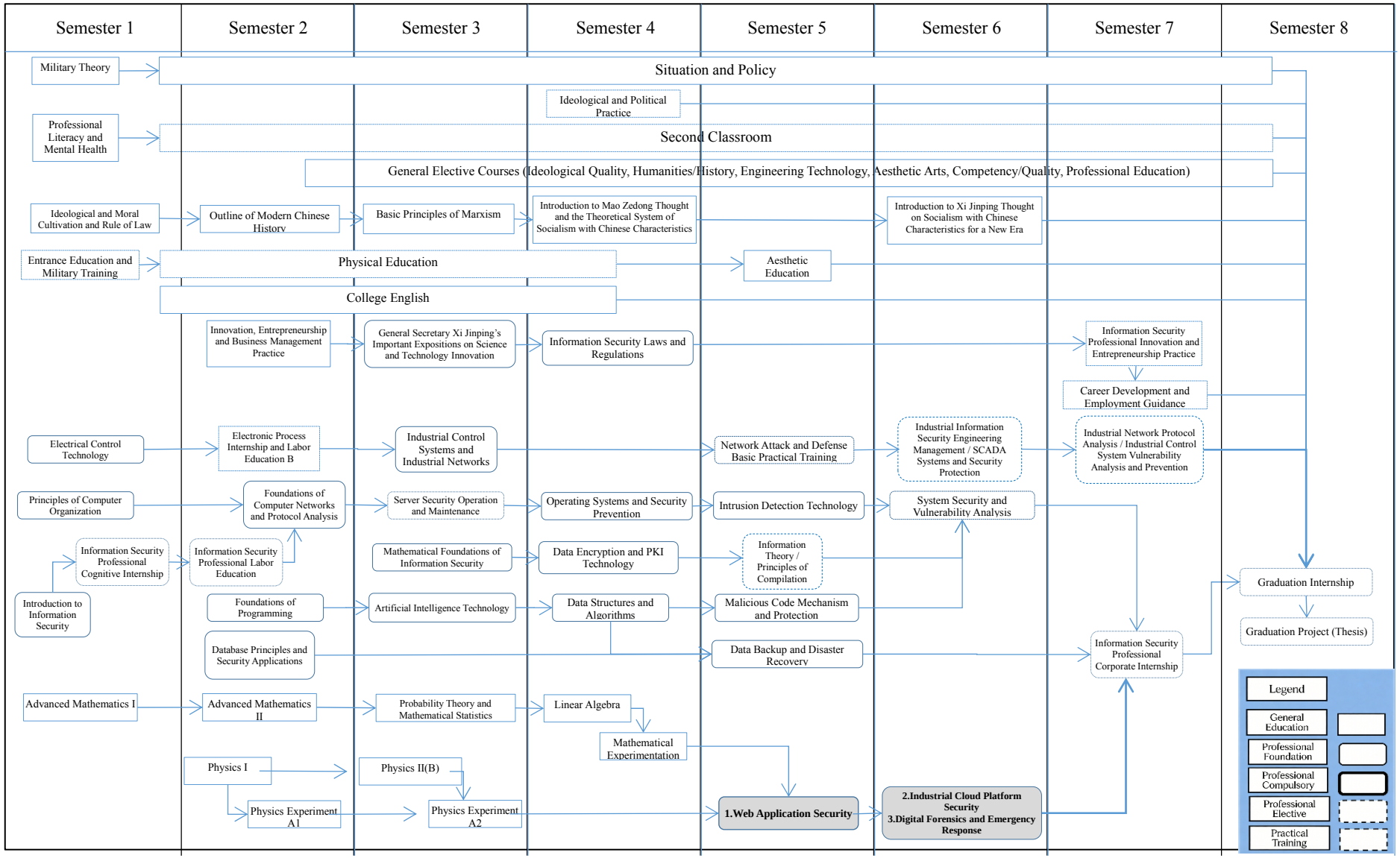
Graduation Requirements	Implementation Components / Channels
and economic decision-making methods, and be able to apply this knowledge in the multidisciplinary environments involved in information security to perform task planning and schedule management for engineering projects.	Entrepreneurship Practice, Information Security Professional Corporate Internship, Graduation Internship, Graduation Project (Thesis), Second Classroom.
12. Lifelong Learning: Possess the awareness of autonomous learning and lifelong learning; be capable of continuously following the frontier development trends of the discipline; and possess the ability to constantly learn emerging information security methods and technologies and adapt to relevant developments and changes.	Physical Education, Aesthetic Education, Information Security Professional Labor Education, Second Classroom, Ideological and Political Practice.

IV. Curriculum Topology

Track 1: Information Security Product Design and Development



Track 2: Information Security Services



V. Core Professional Courses

The following professional core courses are offered in this major:

(1) Foundations of Computer Networks and Protocol Analysis: This course adopts a teaching method combining theory and experiments, enabling students to systematically master the concepts, composition and architecture of computer networks, master basic knowledge in data communication and network interconnection, and master basic methods of network protocols at all layers and protocol analysis. It equips students with a comprehensive, systematic and solid knowledge foundation, laying a solid foundation for the study of other subsequent courses.

(2) Industrial Control Systems and Industrial Networks: This course adopts a teaching method combining theory and experiments, taking industrial network equipment such as Siemens series layer-2 industrial switches, layer-3 industrial switches and industrial firewalls as the teaching core, and integrates industrial equipment such as S7-1200 series PLCs and HMIs. Through industrial Ethernet connection, communication between industrial devices is realized, enabling students to understand the basic principles of data exchange in industrial networks, and master configuration and management of industrial switches, routing configuration and management, VLAN virtual local area network technology, industrial network redundancy technology, industrial network routing technology, and NAT address translation technology. Students can comprehensively apply industrial network technologies to realize the interconnection and interoperability of industrial control systems such as PLCs, HMIs, frequency converters, workstations, servers and industrial control computers in actual engineering projects, and possess the abilities in industrial network hardware selection, network scheme design, industrial network debugging, inspection and maintenance.

(3) Data Encryption and PKI Technology: This course adopts a teaching method combining theory and experiments. On the basis of mastering the working mechanisms of symmetric encryption, public-key encryption, hash algorithms, security protocols, digital certificates and PKI, students are required to deeply understand their working principles. This course focuses on cultivating students' ability to apply modern cryptographic working mechanisms, and at the same time cultivates students' preliminary abilities in cryptographic analysis and evaluation, as well as innovative design of cryptographic algorithms.

(4) Malicious Code Mechanism and Protection: This course adopts a teaching method combining theory and experiments. On the basis of mastering the basic principles, types and operating mechanisms of malicious code, the course focuses on analyzing the detection and removal technologies of malicious code, and requires students to develop strategies for preventing malicious code and have the ability to write protection plans.

(5) Operating Systems and Security Prevention: This course mainly introduces the basic principles and implementation methods of computer operating systems. The purpose is to enable students to understand the role, status and characteristics of operating systems in computer systems, understand the working principles of operating systems, learn general methods of using operating systems, and understand software design methods and operating environments of software systems from the perspective of systems engineering, so as to lay a foundation for the application and development of system security. In addition, the security protection of the operating system shall be well done according to the security mechanisms of the operating system.

(6) Information Security Laws and Regulations: This course adopts theoretical teaching, teaching basic laws and regulations in the field of information security application, such as *Cybersecurity Law of the People's Republic of China, Regulations on the Protection of Critical Information Infrastructure*, etc., cultivating students' good awareness of laws and regulations.

(7) Intrusion Detection Technology: This course adopts a project-based teaching method combining theory and practice. Through the four-level progressive project system of "commercial product cognition → open-source tool practice → comprehensive system integration → vertical field customization", from shallow to deep, it helps students understand the theoretical basis of intrusion detection / prevention systems such as functions, working modes, deployment methods and key technologies, master the deployment architecture, policy configuration and tuning of commercial equipment such as Cisco IPS, and master the working mechanism and rule syntax of open-source systems such as Snort. On the basis of understanding the visual design logic and the linkage principle with firewalls, students shall integrate third-party open-source tools such as ELK for secondary development to realize visual intrusion defense functions, understand the security characteristics of industrial control network protocols (such as Modbus), expand the support of Snort for the industrial control field, and realize an industrial visual intrusion defense system.

(8) Embedded System Development (Track 1): This course adopts a teaching method combining theory and experiments. With the help of an embedded system development platform, students are required to master the basic working principles and design methods of embedded systems, master the basic use of microcontrollers such as ARM in interfaces, interrupts, protocol communication, operating systems, etc., master software programming such as microcontroller driver programs and application programs, and master the application of embedded system security protection technologies such as data transmission encryption and decryption processing of microcontrollers, and equipment firmware file extraction and analysis, so as to further improve students' professional skills.

(9) Web Application Security (Track 2): This course adopts an integrated teaching method of theory and practice. Taking the Web platform commonly used by enterprises as the service platform, it first introduces the security risks of Web applications and their causes, and introduces defense methods for common Web security vulnerabilities. It introduces methods to improve the security of Web sites, countermeasures against malicious software, and methods to develop secure Web applications.

VI. Main Practical Training Links

(1) Information Security Professional Cognitive Internship: This course is conducted in enterprises. The course is taught by enterprise mentors with the assistance of professional supervisors. Students understand the basic job content of information security positions, and cultivate good professional norms.

(2) Information Security Professional Labor Education: Under the guidance of labor value theory, model worker spirit and craftsmanship spirit, this course improves students' labor morality, labor sentiment, professional skills, scientific and technological innovation, professional literacy and team awareness. Adopting the teaching method of practical case explanation, analysis and modularization, the overall scheme of the information security system is divided into modules for analysis and explanation, and the knowledge and skills learned in other courses are integrated into the practical process, cultivating students' ability to comprehensively apply knowledge and technologies in practice. At the same time, students are required to master basic network cabling knowledge and skills, so that students can further understand the manifestation of network structure in practical applications. Students are required to complete the design of basic network structure and network security scheme, connect the network and security equipment according to their own design, and then conduct security configuration on the network to achieve practical training effect.

(3) Server Security Operation and Maintenance: This course cultivates students' ability to install, configure, manage and securely maintain various enterprise servers based on the Linux platform. The course contents include: Linux network management, SAMBA server configuration, DHCP server configuration, DNS server configuration, APACHE server configuration, FTP server configuration, NFS server configuration, etc.

(4) Basic Network Attack and Defense Training: Professional comprehensive training, conducted on campus for 2 weeks. The course is taught by enterprise mentors with the assistance of professional supervisors. Students master the use methods of basic network penetration attack tools and security defense methods.

(5) System Security and Vulnerability Analysis: The course aims to systematically teach the generation principles of software vulnerabilities (such as stack overflow and heap overflow), analyze the mechanism of malicious code, and cultivate students to master advanced vulnerability mining and analysis methods such as

static / dynamic analysis and vulnerability mining methods (Fuzzing). Through rich experiments and case teaching, students will obtain complete practical experience from vulnerability discovery to simple exploitation and development, laying a solid foundation for engaging in software security analysis, penetration testing and other fields.

(6) Information Security Professional Innovation and Entrepreneurship Practice: According to the characteristics of the information security major, innovation and entrepreneurship education is carried out. Professional teachers carry out professional innovation ability training combined with discipline competitions and other requirements, encourage students to participate in competitions, and recognize credits according to competition results.

(7) Information Security Professional Enterprise Internship: Through the internship practice of this course, students are familiar with the working environment and rules and regulations of enterprises, understand the professional-related positions and actual business operation processes in enterprises, and understand corporate culture. Through the internship practice of this course, students are prepared for graduation internship.

(8) Graduation Internship: Through the internship practice of this course, students are further familiar with the working environment and rules and regulations of enterprises, and deeply understand corporate culture. Students master the professional-related positions and actual business operation processes in enterprises. Through the internship practice of this course, students are prepared for employment or further professional study.

(9) Graduation Project (Thesis): Students comprehensively apply the knowledge they have learned to independently complete the research and practical work of project topics, test the quality and achievements of students' four-year study, and lay a solid foundation for students to participate in practical work after graduation.

VII. Graduation and Degree Requirements

Students who complete all the credits required by this cultivation program with passing grades, obtain a professional-related vocational qualification certificate (see the table below), and meet all other graduation requirements will be awarded a Bachelor's Graduation Certificate in Information Security. Students who meet the graduation requirements and satisfy the criteria set forth in the *Implementation Rules for Bachelor's Degree Awarding of Tianjin Sino-German University of Applied Sciences* and other relevant regulations may be granted a Bachelor of Engineering degree upon review and approval by the University Academic Degree Evaluation Committee.

Table of Vocational Qualification Certificates

No.	Certificate Name	Requirement	Issuing Authority
1	National Information Security Test (NISP)	Junior Level or above	China Information Technology Security Evaluation Center
2	Associate Network Security Engineer	Junior Level or above	Jointly issued by International Webmaster Association (IWA), etc.
3	National Computer Technology and Software Professional Qualification Examination	Programmer or above	Ministry of Human Resources and Social Security; Ministry of Industry and Information Technology
4	Cisco Certified Network Associate (CCNA)	Obtain CCNA or above	Cisco
5	Huawei Certified ICT Associate (HCIA)	Obtain HCIA or above	Huawei
6	PLC Programming and Application Engineer	Junior Level or above	Talent Exchange Center, Ministry of Industry and Information Technology
7	National Computer Rank Examination (NCRE)	Level 2 or above	NEEA, Ministry of Education
Note: Students must obtain at least one of the required certificates listed in the table above. If a listed certificate is cancelled during the period of study, the teaching unit shall provide a replacement certificate of an equivalent level, report it to the Academic Affairs Office for the record, and notify students in advance.			

VIII. Academic Calendar

Semester	Week																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	⊙	⊙	★	★	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	Exam
2	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	R	●	■	Exam
3	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	■	■	Exam
4	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	■	■	Exam
5	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	■	■	Exam
6	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	■	■	Exam
7	○	○	○	○	○	○	○	○	○	○	○	○	○	■	■	Q	Q	Q	Q	Exam
8	◆	◆	◆	◆	◆	◆	※	※	※	※	※	※	※	※	※	※	※	※	--	--

Key to Symbols ： ⊙----Entrance Education ★----Military Training

○----Curricular Teaching Exam----Examination Week

■----Professional Comprehensive Training / Professional Innovation Training ▲----Course Design

●----Engineering Basic Training and Labor Education R----Professional Cognitive Internship (Off-campus)

Q----Corporate Internship (Off-campus) ◆----Graduation Internship (Off-campus)

※----Graduation Project #----Others

IX. Program Development and Approval

Program Director: Wang Xiuying Associate Dean for Academic Affairs: Fan Qiming Dean:

Director of Academic Affairs: Zhang Chunming Vice President for Academic Affairs: Guan Zhiwei