

上海电子信息职业技术学院

人才培养方案

2024 级三年制高职适用

申安网络安全产业学院

教务处汇编

2024 年 7 月

目录

信息安全技术应用专业人才培养方案	1
一、专业名称及代码	1
二、入学要求	1
三、修业年限	1
四、职业面向	1
五、培养目标与培养规格	1
六、课程设置	3
七、教学进度总体安排	11
八、实施保障	15
九、毕业要求	18
十、附件	18
附件 1 信息安全技术应用专业人才需求与专业改革调研报告	19
密码技术应用专业人才培养方案	53
一、专业名称及代码	53
二、入学要求	53
三、修业年限	53
四、职业面向	53
五、培养目标与培养规格	53
六、课程设置	55
七、教学进度总体安排	62
八、实施保障	65
九、毕业要求	70
十、附件	70
附件 1 密码技术应用专业人才需求与专业改革调研报告	71

信息安全技术应用专业人才培养方案

一、专业名称及代码

专业名称：信息安全技术应用

专业代码：510207

二、入学要求

普通高中毕业生、中等职业学校毕业生或具备同等学力人员

三、修业年限

三年，可以根据学生灵活学习需求合理、弹性安排学习时间。

四、职业面向

信息安全技术应用专业的职业面向见表 1 所示。

表 1 职业面向表

所属专业 大类 (代码)	所属专业类 (代码)	对应行业(代 码)	主要职业类别 (代码)	主要岗位群或技 术领域举例	职业技能等级证 书举例
电子与 信息大 类51	电子信息 类5101	互联网及相 关服务 (64) 和互联网安 全服务 (6440)	网络与信息安 全管理员 (4-0 4-04-02)	网络安全系统集成 工程师; 网络安全运维工 程师; Web 安全工程师 网络安全应急响 应工程师	1+X 证书-网络安 全应急响应 华为 HCIA-安全 红帽认证工程师 (RHCE) CISP-PTE 渗透测 试工程师

五、培养目标与培养规格

(一) 培养目标

本专业培养理想信念坚定，德、智、体、美、劳全面发展，具有一定的科学文化水平，良好的人文素养、职业道德和创新意识，精益求精的工匠精神，较强的就业能力和可持续发展能力，掌握本专业知识和技术技能，面向互联网和相关服务、软件和信息服务业的计算机网络工程技术人员，能够从事信息安全系统集成、网络安全运维、Web 安全管理与评估、网络安全应急响应、数据安全、企业网络等保测评等工作的高素质技术技能人才。

(二) 培养规格

1. 素质

(1) 思想政治素质：坚定拥护中国共产党领导和我国社会主义制度，在习近平新时代

中国特色社会主义思想指引下，践行社会主义核心价值观，具有深厚的爱国情感和中华民族自豪感。热爱社会主义祖国，具有正确的世界观、人生观、价值观；

(2) 身心素质：掌握常规体育运动项目的基础知识和基本技能，掌握有关身体健康的知识和健身方法，体能测试基本合格，提高大学生心理健康水平，增强自我调适的能力；使学生能正确认识自我，热爱生命，善待他人，增强调控自我、承受挫折、适应环境的能力；

(3) 文化素质：提升大学生的人文素养和文化底蕴，培养沟通交流、阅读理解、应用写作、文学鉴赏，促进学生的专业学习和综合素质提升；

(4) 职业素质：树立正确的职业价值观、良好的职业精神、遵守职业法规、坚守职业理想；

(5) 基本通用能力：提升通用基础能力，包括自我学习管理能力、数字运用能力、信息处理能力和中文外语能力；

(6) 关键社会能力：促进有效参与社会实践、提升社会担当意识，包括交流沟通、团队合作、社会责任和社会认知能力；

(7) 创新创业能力：培养良好的创新精神、创造性思维，促进参与创业实践，提升复合型能力和综合素质。

(8) 具有语言文字应用能力和自觉规范使用国家通用语言文字的意识、自觉传承弘扬中华优秀传统文化的意识。

2. 知识

(1) 掌握必备的思想政理论、科学文化基础知识和中华优秀传统文化知识；

(2) 达到英语应用能力 A 级水平、计算机应用达到计算机等级考试一级水平；

(3) 熟悉信息安全相关法律法规和标准；

(4) 掌握计算机系统、信息系统架构、网络拓扑、信息安全理论与安全技术、网络协议的基础知识；

(5) 掌握 Windows 和 Linux 操作系统方面的知识；掌握数据库方面知识；

(6) 掌握 DNS、DHCP 和 WEB 服务器等常用服务器方面的知识；

(7) 掌握交换机、路由器、防火墙的常用网络设备方面的知识；

(8) 网络安全设备的配置管理等方面的知识；

(9) 掌握系统安全架构、信息系统日常检测与维护、网络系统集成、信息系统安全管理知识；

(10) 初步掌握信息系统安全测评、渗透测试、应用服务安全加固等方面的知识；

(11) 初步掌握安全事件分类、应急响应级别、启动、预案、处理等规范；

(12) 熟悉信息安全管理体系、风险管理方法；

(13) 了解常用 WEB 开发语言，中间件框架，JavaScript 框架；

(14) 了解应用开发的基本流程及关键点。

(15) 能够根据企业的业务需求，阐述数据分级分类、配置使用数据安全治理产品。

(16) 掌握专业文本的撰写规范，包括结构、语言、格式等方面的要求。

3. 能力

(1) 具有设计、组建、维护与安全管理中小型企业网络能力；

(2) 具有对网络操作系统、服务器搭建、网络管理软件或工具的使用能力；

(3) 具有对网络设备如路由器、交换机、无线设备安装、配置、调试、维护的基本能力，对网络设备安全特性的配置与调试能力；

(4) 具有对网络安全设备如防火墙、VPN、入侵检测等硬件设备配置、调试、维护的基本能力；

(5) 初步具有应用服务安全检测、评估和安全服务加固能力；

(6) 具有信息系统集成)、安全管理与维护能力；

(7) 能撰写工程文件和渗透测试评估工作报告，会查阅技术文献；

(8) 具有至少一种脚本语言（如 python、perl、bash）开发能力；

(9) 具有至少一种开源的渗透测试工具的使用能力；

(10) 具有网络数据分析能力；

(11) 具备一定的针对安全事件，编制响应预案，并当事件发生时及时应急响应的能力；

(12) 能够准确理解专业文献、报告、合同等文本；

(13) 能够撰写本专业领域的常见应用文本；

(14) 具有初步创业与学习、创新、岗位迁移能力。

六、课程设置

(一) 公共基础课程

公共基础课主要包括：

毛泽东思想和中国特色社会主义理论体系概论、习近平新时代中国特色社会主义思想概论、思想道德修养与法律基础、应用数学、实用英语、体育与健康、信息技术、军事理论与训练、职业生涯规划与职业指导、形势与政策、心理健康教育、大学语文等。

表 2 公共基础课程设置

序号	课程	主要教学内容与要求	参考学时
1	毛泽东思想和中国特色社会主义理论体系概论	内容：毛泽东思想及其历史地位、新民主主义革命理论、社会主义改造理论、社会主义建设道路初步探索的理论成果、“三个代表”重要思想、习近平新时代中国特色社会主义思想及其历史地位。 要求：全面认识我国革命、建设和改革的基本国情，了解马克思主义中国化的历史进程和理论成果，理解社会主义本质论、社会主义初级阶段论、社会主义市场经济论等，深入认识和理解中国共产党领导是中国特色社会主义最本质的特征和中国特色社会主义制度的最大优势。	32
2	习近平新时代中国特色社会主义思想概论	内容：历史方位、鲜明主题、奋斗目标、发展方式、总体布局、战略布局、发展动力、发展保障、安全保障、外部环境、政治保证、治国理政世界观方法论、价值观等 要求：教育学生认识中国特色社会主义的新理论形态，养成严密理论新逻辑。	48
3	思想道德修养与法律基础	内容：坚定理想信念、弘扬中国精神、践行社会主义核心价值观、明大德守公德严私德。 要求：教育学生加强思想道德修养，继承和弘扬中华传统美德和中国革命道德，树立为人民服务的思想，弘扬集体主义精神，培养良好的道德品质和高尚的道德人格。	48
4	应用数学	内容：函数、导数的概念、导数的运算、微分函数的单调性与极值不定积分的概念、不定积分的计算、定积分的概念、定积分的计算、定积分的应用 要求：熟练掌握函数的基本概念和基本特性、掌握极限的四则运算法则、导数在函数单调性判定上的应用、基本积分公式的应用。注重实用性和职场意识，培养学生创新能力和自主学习能力。	64
5	实用英语	内容：课堂交流；介绍、问候、感谢、致谦、道别、指路等日常交际；阅读与翻译科普、人物、政治、商贸等一般题材的文字材料。 要求：培养学生实际应用英语的能力，侧重培养职场环境下语言交际能力，使学生逐步提高用英语进行交流与沟通的能力，掌握有效的英语学习方法和策略，培养学生的英语学习兴趣和自主学习能力，提高学生的综合文化素养和跨文化交际意识，为提升学生的就业竞争力及未来的可持续发展打下必要的基础。	128
6	体育与健康	内容：体育理论、身体素质、篮球、排球。 要求：掌握各项项目的动作技能、培养吃苦耐劳，顽强拼搏的意志品质。	108

序号	课程	主要教学内容与要求	参考学时
7	军事理论与训练	内容: 中国国防、军事思想、信息化战争、战略环境 要求: 了解我国国防历史和国防建设的现状及其发展趋势,熟悉国防法规和国防政策的基本内容,明确我军的性质、任务和军队建设的指导思想,了解信息化战争的形成、发展趋势和与国防建设的关系,熟悉信息化战争的特征,树立打赢信息化战争的信心。了解国际战略格局的现状、特点和发展趋势,正确认识我国的周边安全环境,现状和安全策略,增强国家安全意识。	32
8	职业生涯规划与职业指导	内容: 掌握职业生涯设计、职业道德、职场法律、职业礼仪、职业精神、求职申请与面试准备、求职面试技巧、创业规划和实施。 要求: 培养学生通用的职业意识,提高其可雇用能力。	16
9	大学生安全教育	内容: 饮食安全、学习安全、交通安全、人身安全、财产安全、网络安全、心理安全、社会实践安全、消防安全、国家安全以及救护知识等。 要求: 养成良好的安全习惯,提高安全意识,掌握安全知识和防范技能,增强自我防范能力。	38
10	形势与政策	内容: 根据教育部每学期发布的最新形势与政策课教学要点,结合学校实际灵活选择相应主题开展教学。 要求: 帮助学生认清国内外形势,增强学生的爱国主义责任感和使命感。	32
11	心理健康教育	内容: 心理保健知识。 要求: 培养创造性思维,训练坚强意志,优化心理品质,培养健全人格,开发心理潜能,促进全面人才。	32
12	大学语文	内容: 日常生活中常用的应用文体。 要求: 能按岗位要求完成书面写作。	32
13	劳动教育	内容: 劳动观点、劳动习惯。 要求: 树立学生正确的劳动观点,培养学生热爱劳动和劳动人民的情感,养成劳动的习惯。	16
14	中华优秀传统文化	内容: 涵盖中华优秀思想、文学、艺术、科技、民俗等。通过讲授和体悟中国传统文化,提高学生人文素养,传承中国民族精神,弘扬优秀传统文化。 要求: 讲授中国传统文化,提高学生人文素养,传承中国民族精神,弘扬优秀传统文化。	32
15	人工智能 (AGI) 技术	内容: 大语言模型原理、现有主流大语言模型平台介绍,大语言模型应用案例	32

序号	课程	主要教学内容与要求	参考学时
	应用	要求: 了解元宇宙的内涵,熟悉基本技术知识及其应用,掌握元宇宙的发展趋势,启发学生关于元宇宙的思考和探索。	
16	元宇宙技术与应用	内容: 元宇宙基本概念和发展历程,相关基本技术知识和应用场景 要求: 了解元宇宙的内涵,熟悉基本技术知识及其应用,掌握元宇宙的发展趋势,启发学生关于元宇宙的思考和探索。	32
17	应用物理	内容: 质点和刚体运动及其应用、静电场和恒定磁场及其应用、电磁感应及其应用、光学及其应用、学生实验等。 要求: 通过了解物理学基本概念,掌握基本计算方法,具备一定运用物理学方法解决实际问题的能力,能从物理学角度分析和解决生产生活中的相关问题中的应用,增加实际操作能力。发展物理观念与应用、科学思维与创新、科学实践与探究、科学态度与责任四个方面物理核心素养。	32
18	信息技术	内容: 课程主要介绍人工智能相关概念,通过各种学习工具讲解机器学习等相关知识,结合大量的案例讲解人工智能技术在现实生活中的应用,通过对人工智能现状的深入剖析,展望人工智能的发展方向与未来。包括人工智能发展历史、人工智能基本概念、机器学习、计算机视觉、自然语言处理、人工智能应用、人工智能未来发展。 要求: 理解人工智能的基本概念和原理;掌握人工智能的关键技术并了解它们在各个领域的应用;关注人工智能在法律、伦理和道德方面的问题,培养批判性思维能力;了解我国在人工智能领域的成就和贡献,树立文化自信。	32
19	互联网+创业实践	内容: 创新创业、互联网+创业本质、互联网+商业模式、创业机会识别与开发、互联网创业团队、产品设计与开发、市场运营、互联网创业企业的股权结构设计、互联网创业企业融资、创业孵化、商业计划书撰写和路演、中国国际大学生创新大赛等内容。 要求: 学生具备互联网创业的基本素养,了解互联网创业的流程等相关知识,掌握互联网创业的方法,为学生未来的创业之路提供有力的支持。	32

(二) 专业课程

专业课程包括专业必修课程和专业选修课程,并涵盖相关实践性教学环节。

1. 专业必修课程

包含专业基础课程和专业核心课程。

(1) 专业基础课程: 包括计算机网络技术、信息安全技术、Python 程序设计、Windows 系统管理与应用、网络安全标准与法律法规等。

(2) 专业核心课程: 包含 Linux 服务与安全管理、网络设备安全配置、渗透测试、WEB 应用安全、网络安全应急响应、数据库安全管理等。课程名 后带有★标识。

2. 专业选修课程

为专业拓展课程: 包含创新创业教育、C 语言程序设计、信息安全管理、计算机系统配

置、WEB 应用开发、云安全技术与应用、安全运维技术、数字取证技术、Python 安全工具开发、安全检测与评估等。

其中纯实践性教学课程为：Windows 系统安全实训、Linux 服务安全管理实训、网络安全应急响应项目实战、网络攻防项目实战、认知实习以及岗位实习等。

（三）专业核心课程内容与要求

1. 主要专业必修课程教学内容如表 3 所示。

表 3 专业必修课程内容与要求

序号	课程	主要教学内容与要求	参考学时
1	数据库安全管理	要求: 培养学生构建数据库系统的创新思维能力以及运用数据库分析和解决实际问题能力, 并且了解数据库作为软件系统的基础部件, 保证其安全性的基本方法。 内容: 围绕数据库设计、数据库管理、数据库编程、数据库优化、数据库安全、数据库维护等职业能力, 设置了10个学习项目。分析过程中尤其注意了整个内容的完整性, 以及知识与技能的相关性, 知识与技能内容则依据工作任务完成的需要进行确定。	64
2	网络设备安全配置	要求:使学生能够熟练运用各种网络安全技术, 掌握各种网络设备的安全配置方法, 并能根据实际应用需求进行网络安全策略的设计, 实施和检测。 内容: 网络风险分析、网络设备的管理安全、AAA认证授权审计、二层交换安全、IOS防火墙技术、IPS、加密技术和IPSEC VPN技术。将思科安全认证的内容融入课程。	64
3	Linux服务与安全管理	要求:学生能够进行日常企业工作中的Linux系统安全防护管理工作。对系统安全有一个整体的认识, 全方位、立体化的综合掌握系统平台安全管理知识。 内容: 服务器的安全管理、保障数据传输安全、架设CA服务器; 能对WEB、FTP服务器进行安全维护, 架设SSL网站; PKI公钥基础架构基础知识, 申请与签发证书; 邮件的数字签名与加密; 使用网络管理工具等。	64
4	WEB应用安全	要求:学生能够担负起中小型WEB服务器的安全管理工作。熟悉WEB应用中常见的安全漏洞, 对WEB服务安全有较为完整的认识, 较全面地掌握维护WEB服务安全的管理技能。 内容: WEB OWASPTop10、以典型的WEB应用为例讲解各功能模块存在的安全漏洞, 使用何种检测工具, 如何对已检出漏洞进行有效预防。	96
5	渗透测试	要求:学生能按照信息安全渗透测试基本操作流程, 依据渗透测试的四步模型法, 能够规范、准确、熟练地完成渗透测试全部流程。	64

序号	课程	主要教学内容与要求	参考学时
		内容: 渗透测试的定义与漏洞检测的区别、WEB应用架构分析、owasp top 10、渗透测试的信息收集, 漏洞检查, 漏洞利用, 访问维持及漏洞测试报告的书写规范等。	
6	网络安全应急响应	要求: 学生能在网络安全应急响应工作中进行安全防御、检测分析、等级保护、安全响应。 内容: 挖矿木马应急响应, 网页篡改应急响应, DDOS应急响应, 勒索病毒应急响应, 流量劫持应急响应。	64
7	计算机网络技术	要求: 学生能通过本课程的教学, 使学生对计算机网络从整体上有一个初步的了解, 培养学生在TCP/IP协议和LAN上的实际工作能力, 学会计算机网络管理和维护的最基本方法, 为后续专业课程的学习打下扎实理论基础。 内容: 网络认知、网络体系结构、局域网组建、网络编址、网络寻址、网络传输控制、网络服务、广域网接入。	64
8	网络安全标准与法律法规	要求: 通过该课程的学习, 使学生具有基本的信息安全常识和安全理念, 提高信息安全意识, 对国内外信息安全标准及法律法规有一个较为全面的了解, 掌握信息法律法规的基本知识, 在今后从事信息安全管理等实际工作中加以遵守和运用。 内容: 结合典型案例, 国内外信息安全标准和法律法规的背景知识、发展状况, 讲授网络安全法律法规的基本知识, 帮助学生树立信息安全法律意识, 从而在今后实际工作中加以遵守和运用。	32
9	Python程序设计	要求: 学生能通过本课程学习, 学生具备熟练使用python语言进行基础编程的能力, 能理解Python的编程模式(命令式编程、函数式编程)。 内容: 数据类型、程序控制结构、正则表达式、函数、面向对象编程、文件操作、异常及其处理、数据库操作、科学计算	64
10	Windows系统管理与应用	要求: 通过本课程学习, 学生具备网络组建、帐户管理、AD 配置管理、文件服务器、组策略、磁盘管理等技能, 对不同类型和规模企业网络进行综合管理, 达到 windows 平台的网络管理人才的基本需求。 内容: 网络组建、帐户管理、AD 配置管理、文件服务器、组策略和磁盘设备管理、windows 系统环境安全的配置能力, 能熟练使用安全工具进行安全维护, 使用安全策略, 证书服务器进行系统安全配置	64
11	信息安全技术	要求: 学生能通过该课程的学习, 使生理解基本的信息安全理念, 具备基本的安全常识和信息安全意识, 了解和掌握基本的信息安全技术原理和应用常识, 能使用信息安全技术防护基本信息安全。 内容: 信息与信息安全认识、密码技术、信息隐藏与数字水印、网络安全技	48

序号	课程	主要教学内容与要求	参考学时
		术、病毒防治、数据安全、信息安全新领域、信息安全法律法规案例分析	
12	Linux服务安全管理实训	要求: 学生能通过本课程的学习训练, 能够了解Linux系统安全机制。 内容: 查看安全日志, 系统的审计功能, Linux防火墙、Linux平台的扫描工具使用, 脚本工具的使用与脚本程序的编制。	30
13	网络攻防项目实战	要求: 学生能通过本课程学习, 学生具备从事网络安全行业攻防实战的基本素养, 能在网络安全标准和法律法规的约束下, 按照企业的工作流程和标准, 根据项目需求, 掌握网络攻击的正确思路和方法, 掌握网络攻击的主要工具, 掌握针对攻击的防范措施和防御技术, 内容: 信息探测攻击与防御、系统漏洞攻击与防御、主机操作系统安全攻防、数据库攻击与防御、口令破解攻击与防御、WEB应用攻击与防御	30
14	数据安全 管理	要求: 通过该课程的学习, 学生们能够依据相关法律法规, 对数据安全相关的涉及领域、工作范围等有一个较为全面了解, 掌握数据安全相关的管理手段、实用技术、主要工具的使用等, 为今后从事数据安全管理的实际工作积累实用知识与技能。 内容: 数据治理、风险评估、应急响应、数据脱敏技术、制定共享规则、建立监控审计机制等方面。帮助学生掌握数据安全管理制度, 数据分级分类, 用户隐私保护, 内部数据治理, 数据脱敏与共享, 以及数据安全计算与传输技术等。	64

(四) 实践性教学环节

实践性教学环节主要包括实训、项目实战、岗位实习等。实训、项目实战可在校内实训室以及校外实训基地等开展完成; 岗位实习可由学校组织在信息安全相关企业开展完成。

实践性教学课程设置如表 4 所示。

表 4 纯实践教学课程安排表

序号	课程名称	内容、要求	学期	周数	场地	备注
1	Windows 系统安全实训	要求: 学生能进行 windows 系统环境安全的配置, 能熟练使用安全工具进行安全维护, 使用安全策略, 证书服务器进行系统安全配置。 内容: WINDOWS 安全的基本知识、WINDOWS 安全的实现原理、WINDOWS 安全通信的配置与管理、WINDOWS 安全策略配置与管理。	3	1		
2	Linux 服务安全管理实训	要求: 学生能进行中小企业 linux 系统及服务的运维。 内容: Linux 系统安全机制、查看安全日志、系统的审计功能、设置 Linux 防火墙、Linux 平台的扫描工具、脚本工具的使用与脚本程序的编制。	4	1		
3	防火墙与 VPN 技术项目实战	要求: 使学生理解防火墙的工作原理, 掌握防火墙的安全策略配置、NAT 策略配置及 VPN 技术配置。 内容: 防火墙基础配置、防火墙的安全策略配置, NAT 策略配置, VPN 技术配置。	3	1		
4	网络安全应急响应项目实战	要求: 培养学生的更高级别的渗透测试能力, 提高学生在“高级阶段”的风险评估与处置等方面的技能水平。为学生考取 1+X 网络安全应急响应 (中级) 证书、胜任网络安全应急响应方向的就业岗位打下坚实的基础。 内容: 了解和掌握网络安全应急响应技术的知识。该课程的内容主要是讲述系统日志分析、安全工具的使用、恶意代码排查分析、高级别的渗透测试及网络设备的安全加固等。	4	1		
5	网络攻防项目实战	要求: 使学生了解网络攻防的基本概念, 熟练掌握网络攻击的常见思路、常用方法、常用工具, 以及针对攻击的防范方法和措施, 具备网络攻击和网络防御的能力, 以适应企业相应岗位的需求。 内容: 课程内容分为 Windows 攻防实战和 Linux 攻防实战两大模块, 围绕网络攻击能力和网络防御能力的培养, 分别设置了信息探测攻击与防御、主机系统安全加固、系统漏洞攻击与防御、数据库攻击与防御、口令破解攻击与防御、WEB 应用攻击与防御等 6 个项目。	5	1		

序号	课程名称	内容、要求	学期	周数	场地	备注
6	认识实习	内容：企业岗位认识实习 要求：在企业岗位进行技能训练	5	2	校外实践基地	
7	岗位实习 1、2★	内容：企业顶岗实习 要求：在企业岗位进行技能训练	5、6	22	校外实践基地	
总计				31		

（五）相关要求

专业课程思政教育全覆盖。创新创业教育除了开设必修课程外，还通过信息安全技术项目实践创新等环节，鼓励学生积极申报国家专利、发表论文等，提高学生的创新创业能力。安全教育贯穿于每门课程中，在专业课程的教学过程中，安全教育贯穿于教学过程始终。在公共选修课中开设人文素养、科学素养等。

七、教学进度总体安排

学时根据学生的认知特点和成长规律，注重各类课程学时的科学合理分配。

（一）学时安排

信息安全技术应用专业教学活动周进程安排表如表 5 所示。

表 5 教学活动周进程安排表

单位：周

学期	入学教育	军训	课堂教学	实训（实验）	实习	考试	机动	总计
第一学期	1	(1)	16	0	0	1	*	20
第二学期	0	0	16	*	0	1	*	20
第三学期	0	0	16	*	0	1	*	20
第四学期	0	0	16	*	0	1	*	20
第五学期	0	0	8	*	8		*	20
第六学期	0	0	0	*	16		*	20
总计								

说明：1. 军训周不统计到总计里去；

第一学期安排新生入学教育 1 周。

（二）教学进度表

表6 2024级信息安全技术应用专业教学进程表

课程类别	课程类别	课程名称	学分	总学时	考试(考查)	实践学时	各学期周数、学分分配					
							1	2	3	4	5	6
公共基础必修	思想政治类	思想道德与法治	3	48	考试	8		3				
		毛泽东思想和中国特色社会主义理论体系概论	2	32	考试	0		2				
		习近平新时代中国特色社会主义思想概论	3	48	考试	8	3					
		形势与政策1	0.5	8	考查	0	0.5					
		形势与政策2	0.5	8	考查	0		0.5				
		形势与政策3	0.5	8	考查	0			0.5			
		形势与政策4	0.5	8	考查	0				0.5		
	身体素质类	体育与健康1	2	32	考查	30	2					
		体育与健康2	2	32	考查	30		2				
	身体素质类	体育与健康3	1	22	考查	16			1			
		体育与健康4	1	22	考查	16				1		
	综合素养类(科学、人文素养)	应用数学	4	64	考试	0	4					
		应用物理	2	32	考试	0	2					
		实用英语1	3	48	考试	0	3					
		实用英语2	3	48	考试	0		3				
		实用英语3	2	32	考试	0			2			
		大学语文	2	32	考查	0		2				
		中华优秀传统文化	2	32	考查	0	2					
		信息技术(人工智能基础)	2	32	考查	18		2				
		人工智能(AGI)技术应用	2	32	考查	18	2					
		元宇宙技术与应用	2	32	考查	18		2				
	综合	职业生涯	1	16	考	0	1					

课程类别	课程类别	课程名称	学分	总学时	考试(考查)	实践学时	各学期周数、学分分配					
							1	2	3	4	5	6
	能力类	规划与职业指导			查							
		互联网+创业实践	2	32	考查	16	2					
		心理健康教育	2	32	考查	0	2					
		大学生安全教育	2	32	考查	0	*	*	*	2		
		军事理论与训练	2	32	考查	16		2				
	综合能力类	劳动教育	1	16	考查	16					1	
总计			50	812		210	23.5	18.5	3.5	3.5	1	0
公共基础选修	通识、艺术、传统文化类	公共艺术选修	2	32	考查	0		2				
		公共通识选修	4	64	考查	0		4				
		小计	6	96					4	2		
专业必修	专业基础	计算机网络技术	4	64	考试	32	4					
		Python 程序设计	4	64	考试	32	4					
		计算机系统配置	0.5	16	考查	16		0.5				
		Windows 系统管理与应用	4	64	考查	32		4				
		网络安全标准与法律法规	2	32	考查	0			2			
		信息安全技术	3	48	考查	32			3			
		Linux 服务安全管理实训	1	30	考查	30			1			
		网络安全产品配置	3	48	考查	32			3	0		
		网络安全应急响应项目实战	1	30	考查	30				1		
		网络攻防项目实战	1	30	考查	30				1		
专业必修	专业核心	★Linux 服务与安全管理	4	64	考试	32		4				
		★网络设备安全配置	4	64	考试	32		4				
		★渗透测	4	64	考	32			4			

课程类别	课程类别	课程名称	学分	总学时	考试（考查）	实践学时	各学期周数、学分分配					
							1	2	3	4	5	6
		试			试							
		★数据安全 管理	4	64	考试	32			4			
		★WEB 应用安全	6	96	考试	48				6		
		★网络安全应急响应	4	64	考试	32				4		
		岗位实习1	8	240	考查	240					8 周	
		岗位实习2	16	480	考查	480						16 周
		小计	73.5	1562		1194	8	12.5	17	12	8	16
专业选修	专业拓展	云安全技术与应用	3	48	考查	32			3			
		WEB 应用开发										
		C 语言程序设计	4	64	考试	32				4		
		Java 程序设计基础										
		数据库安全管理	3	48	考查	16				3		
		数字取证技术										
		信息安全管理	3	48	考查	16				3		
		安全检测与评估										
		Python 安全工具开发	3	48	考查	32					3	
		商用密码应用安全性评估				16						
		小计	16	256		112	0	0	3	10	3	0
合计			145.5	2726		1516	31.5	31	27.5	27.5	12	16

八、实施保障

（一）师资队伍

1. 队伍结构

学生数与本专业专任教师数比例不高于 25:1，双师素质教师占专业教师比例一般不低于 60%，专任教师队伍要考虑职称、年龄，形成合理的梯队结构。

2. 专任教师

专任教师应具有高校教师资格；有理想信念、有道德情操、有扎实学识、有仁爱之心；具有计算机等相关专业本科及以上学历；具有扎实的本专业相关理论功底和实践能力；具有较强信息化教学能力，能够开展课程教学改革和科学研究；有每 5 年累计不少于 6 个月的企业实践经历。

3. 专业带头人

专业带头人原则上应具有副高及以上职称，能够较好地把握国内外信息安全行业、专业发展，能广泛联系行业企业，了解行业企业对本专业人才的实际需求，教学设计、专业研究能力强，组织开展教科研工作能力强，在本区域或本领域具有一定的专业影响力。

4. 兼职教师

兼职教师主要从本专业相关的行业企业聘任，具备良好的思想政治素质、职业道德和工匠精神，具有扎实的专业知识和丰富的实际工作经验，具有中级及以上相关专业职称，能承担专业课程教学、实习实训指导和学生职业发展规划指导等教学任务。

（二）教学设施

1. 专业教室

专业教室配备黑（白）板、多媒体计算机、投影设备、音响设备，互联网接入或 Wi-Fi 环境，并实施网络安全防护措施；安装应急照明装置并保持良好状态，符合紧急疏散要求，标志明显，保持逃生通道畅通无阻。

2. 校内实训室（基地）

信息安全应用技术目前建有，计算机网络管理实训室、计算机网络互联实训室（Cisco 设备）、计算机网络互联实训室（H3C 设备）、无线网络安全管理实训室、综合布线实训室、虚拟安全综合实训室、攻防沙场演练实训室等七个专业实训室，工位 280 个，能够承担包括日常教学、认证培训和社会服务等多种任务。校内实训室主要功能如表 7 所示。

表 7 校内主要实训教学条件配置表

实训室名称	教学与训练	工位数量
网络安全虚实结合实训室	网络空间安全导论、操作系统管理及应用、Linux 基础与服务管理、路由交换技术、终端安全管理、漏洞扫描与防护、虚拟化技术及应用、行为安全管理、项目实战、Web 应用防火墙技术及应用、Ctf 比赛课程、企业网渗透测试、网络安全应急响应	40

实训室名称	教学与训练	工位数量
密码技术应用实训室	网络安全攻防技术、信息安全管理、防火墙技术及应用、数据安全	40
程序设计开发实训室	Python 程序设计、WEB 应用开发、渗透测试、PHP 动态网站开发	40
应用安全实训室	网络安全法律法规与标准、数据库原理及应用、应用程序安全原理分析与实践、企业网应用安全防护、Python 安全工具开发 WEB 应用安全、漏洞扫描与防护	40
计算机系统配置实训室	计算机系统配置	40

3. 校外实训基地

校外实训基地基本要求为：具有稳定的校外实训基地；实训设施齐备，实训岗位、实训指导教师确定，实训管理及实施规章制度齐全；能够接纳一定规模的学生开展网络安全应急响应等有关实训。

4. 学生实习基地

学生实习基地基本要求为：具有稳定的校外实习基地；能提供日常网络安全检测、渗透测试和安全运维、信息系统安全测评、信息系统安全规划实施、信息系统安全运维管理等工作，能涵盖当前相关产业发展的主流技术，可接纳一定规模的学生实习；能够配备相应数量的指导教师对学生实习进行指导和管理；有保证实习生日常工作、学习、生活的规章制度，有安全、保险保障。

（三）教学资源

1. 教材和讲义选用

（1）教材和讲义优先选用自编校本教材，自编校本教材不仅是高职院校教材的补充，还是高职院校自身教学特色的一种体现，本专业已拥有一定数量特色鲜明、有较高水平的自编校本教材及讲义。

（2）除自编校本教材外，还可选用反映计算机网络技术最新发展水平、特色鲜明，并能够满足高等职业教育培养目标要求的规划教材，并尽量选用近三年出版的高职高专教材。

2. 数字化（网络）教学资源

（1）专业信息库

专业信息库包括专业概况、对接的产业概况、专业建设、人才培养、质量评估、建设成果。

（2）课程资源

课程资源包括课程简介、课程标准、教学设计（整体设计、单元设计、项目设计）、说

课录像、授课录像、素材资源（电子教材、电子课件、参考资料、习题试题库、任务单、项目指导书、学生作品等）。

（3）教学案例库

包括：课程案例、项目案例、学生作品。

（4）专业工具库

专业工具库包括专业知识动画资源库、专业设备组件库、专业图片库、工具使用手册库、项目工程视频库、音频库。

（5）培训资源库

培训资源库包括行业企业证书和培训、师资培训、职业资格培训、学生竞赛培训、社会服务与对外交流。

（6）行企资源库

行企资源库包括行业概况、技术前沿、行业相关岗位描述、合作企业信息及企业真实案例、政策法规、标准规范。

（四）教学方法

依据课程标准，结合课程教学内容、学生学习基础、教学资源等，坚持学中做、做中学，倡导因材施教、按需施教，创新教学方法和策略，加强信息化技术在教育教学中的应用。

1. 以立德树人为根本，思政教育引领，将思政元素融入课程教学，实现价值塑造、能力培养、知识传授三位一体，培养学生精益求精的工匠精神和严谨踏实的职业素养。

2. 以学生为中心，注重“教”与“学”的互动，以个体练习、小组活动、模拟仿真、展示分享和示范纠错等不同形式开展教学。让学生通过执行完整的项目任务来锻炼综合职业能力，改变教师本位观念，充分发挥学生主观能动性。

3. 以工程项目为载体，依托实训室、教学资源平台等，采用理实一体化教学、案例教学、任务驱动式项目化等教学方法。教师采用“任务驱动”教学方法，进行“任务引领式”教学，各任务的完成通过“案例展示、任务分析、知识讲解、操作示范、课堂模仿、课后实践、问题解析、归纳总结”等步骤进行。

4. 以产教融合为抓手，依托协同创新中心，学生参与项目开发，搭建自主创新学习平台。

（五）学习评价

通过对课程教学评价体系改革，突出能力考核，引入企业参与学生考核评价，建立多元化的课程考核评价体系，实现专业技能和岗位技能的综合素质评价。

建立“知识+技能+实践”的教学评价体系；以过程考核为主体，突出专业核心能力和学生综合素质的考核评价；注重课程评价与职业资格鉴定的衔接；建立多元评价机制，加强行业、企业和社会评价。评价体系包括理论考核、项目过程考核、职业资格认证、行业认证、技能竞赛等多种考核方式。课程考核可以选用以下一种或多种方式：

1. 建立“知识+技能+实践”的教学评价内容体系，突出项目成果评价。

2. 以过程考核为主体，突出专业核心能力和学生综合素质的考核评价。

3. 注重课程评价与职业资格鉴定的衔接。
4. 建立多元评价机制，加强行业、企业和社会评价。

（六）质量管理

为确保人才培养质量，学院建立质量监控体系。质量监控包括人才培养目标监控、人才培养方案和教学大纲监控、教学过程监控、学生信息反馈、教材质量监控。

1. 人才培养目标监控。通过行企业调研和评估，及时跟踪人才培养效果，不断完善人才培养模式，确保专业人才培养目标适应社会发展需要。

2. 人才培养方案和教学大纲制订与执行监控。人才培养方案和教学大纲是组织和实施人才培养工作的核心教学文件，也是开展教学工作和对教学工作监控与评估的主要依据。

3. 教学过程监控。主要通过听课、教学检查、教学督导、学生评教、教师评学、考试等实现监控目的。

4. 学生信息反馈。建立学生教学信息员制度，定期召开院系两级学生座谈会。

5. 教材质量监控。学院建立教材招标工作组，采用教材三级审核制：教研室申报、教学单位审核、教务处审定。

九、毕业要求

学生通过规定年限的学习，修满人才培养方案规定的全部学分，准予毕业。鼓励学生毕业前考取一张或多张与专业相关的职业技能等级证书，尤其是与专业相关的 1+X 证书。

十、附件

附件 1 信息安全技术应用专业人才需求与专业改革调研报告

附件 2 专业建设指导委员会审定意见

附件 3 学术委员会审批意见

附件1 信息安全技术应用专业人才需求与专业改革调研报告

信息安全技术应用专业

2024 年人才需求与专业改革调研报告

一、基本思路与方法

（一）调研思路

深入与专业联系较为紧密的典型企业、行业协会和职业培训鉴定机构，通过与企业人事部门的主管、工程技术人员、各层次管理骨干以及职业培训鉴定专家进行有效的沟通、访谈，了解行业的发展趋势、行业对高职人才知识结构和职业能力要求，以及相应的职业资格证书和鉴定需求；结合学校的教学和资源现状、学生就业去向等相关问题，切实把握行业的人才需求与职业教育、技能培训之间的内在联系。

结合《上海市建设网络安全产业创新高地行动计划（2021-2023 年）》《关于促进网络安全保险规范健康发展的意见》《信息安全技术 关键信息基础设施安全保护要求》的发布，聚焦基础技术创新、应用技术创新、服务业态创新，分析信息安全技术应用专业和上海现代服务业、先进制造业的密切联系；跟踪和了解企业、行业的“双赢”需求，关注网络与信息安全技术应用行业发展的现状和趋势，了解行业从业人员的基本情况，分析网络与信息安全技术应用专业人才培养的优势。

（二）调研方法

1. 调研内容

此次调研的内容是：通过对信息安全技术应用专业人才市场需求情况及信息安全技术应用专业人才培养现状的调研，分析是否有必要对原信息安全技术应用专业的人才培养进行新的调整。

2. 调研方式

（1）文献查阅

以上海市教委发展规划处、高教处、职教处公布的各校网络安全专业、信息安全技术应用专业招生和就业数据及科研课题资料为目标，进行文献查阅，为进一步调研提供线索。

（2）电话访谈

选择行业协会和 25 家典型企业，邀请信息安全技术应用专业毕业生就业企业的人力资源主管、部门直接负责人、企业一线技术人员电话咨询，了解人才需求情况。

（3）网络调查

通过对各大权威报告的数据进行汇总分析，了解信息安全技术应用专业人才需求情况及趋势，主要以 2023 网络安全产业人才发展报告为主。

3. 调研范围

上海市各单位企业负责人、人事专员、部门经理、企业一线的技术人员、工程施工人员。

4. 调研对象

(1) 企业选择

- 1) 网络安全服务公司；
- 2) 与信息安全行业相关的科技及咨询公司；
- 3) 从事网络空间安全标准制定的企事业单位。

本次主要调研了 25 家企业，包括奇安信科技集团股份有限公司、杭州安恒信息技术股份有限公司、上海三零卫士信息安全有限公司、上海纽盾科技股份有限公司、上海豌豆信息技术有限公司、公安部第三研究所、神州数码、上海观安信息技术股份有限公司、上海仁恒物业管理有限公司、内蒙古信元网络安全技术股份有限公司、万司信息技术（上海）股份有限公司、上海树盈信息技术有限公司、上海信昊信息科技有限公司、上海蓝叶信息科技有限公司、上海飒智智能科技有限公司、上海诺康信息科技有限公司、上海恒驰信息系统有限公司、智巡密码（上海）检测技术有限公司、上海成集电子科技有限公司、上海嘉韦思信息技术有限公司、上海毓赢网络安全技术有限公司、上海彼德网络安全技术有限公司、上海前景网络科技有限公司、上海惠拓信息技术有限公司、精英教育等。企业情况如表 1 所示：

表 1 调研企业一览表（部分公司）

序号	企业名称	所在省（市）	企业性质	主营业务
1	公安部第三研究所	上海市	国家机关	安全标准制定，安全产品（硬软件）安全检测与评估，信息安全师认证
2	奇安信科技集团股份有限公司	北京市	民营	提供新一代企业级网络安全产品、服务和硬件，包括终端安全、边界安全、数据安全、实战型态势感知等四大类安全产品
3	上海豌豆信息技术有限公司	上海市	民营	面向信息安全专业的教学实训设备产品研发、生产、销售及服务
4	上海纽盾科技股份有限公司	上海市	民营	产品研发基于公司自主知识产权的“区块链安全技术”和“人工智能技术”，为客户构建“全场景、可管理、实战化”的安全运营能力，深度融合与应用客户不断发展的安全需求，向“平台化、工具化、集成化、智能化”演进。
5	上海三零卫士信息技术有限公司	上海市	民营	面向上海市大中型企业及机关事业单位提供信息安全技术外包服务，信息安全保障集成服务
6	杭州安恒信息技术股份有限公司	杭州市	民营	服务：信息安全设备、网络安全设备、网络安全软件、计算机软硬件、系统集成的技术开发、技术服务，信息安全设备、网络安全设备、计

序号	企业名称	所在省（市）	企业性质	主营业务
				计算机设备；
7	神州数码	北京市	民营	神州数码围绕企业数字化转型的关键要素，开创性的提出“数云融合”战略和技术体系框架，着力在云原生、数字原生、数云融合关键技术和信创产业上架构产品和服务能力
8	上海观安信息技术股份有限公司	上海市	民营	信息技术咨询服务；技术服务、技术开发、技术咨询、技术交流、技术转让、技术推广；信息系统集成服务；计算机软硬件及辅助设备批发；计算机软硬件及辅助设备零售；软件开发；数据处理和存储支持服务；

（2）被调研人员选择

- 1）企业的总监、总经理、副总经理；
- 2）企业人事部门经理；
- 3）企业技术部门的经理；
- 4）企业一线的技术人员、工程施工人员；
- 5）我院信息安全技术专业历届毕业生。

5. 调研过程

2023 年 11 月～2024 年 1 月，进行走访企业现场调查，问卷调查。

2024 年 3 月～2024 年 4 月，采用电话或者视频方式进行询问。

2024 年 5 月，调研结果分析、完成调研总结报告。

二、专业人才需求调研

（一）欧美等发达国家网络安全产业及人才发展概况

1. 欧美网络安全领域立法不断加强

今年 6 月，美国众议院军事网络、信息技术和创新小组委员会发布《2024 财年国防授权法案》（NDAA），以技术和网络为重点制定新战略，促进对五角大楼网络安全计划的更全面审查。美国证券交易委员会提出的网络安全和隐私规则草案将要求上市公司披露具有安全知识或经验的董事会成员。美国康涅狄格州发布《康涅狄格州数据隐私法》的相关指南，对大型科技公司提出了全面的隐私要求，还要求更广泛实体进行儿童隐私保护。

欧洲议会成员就《网络弹性法案》（Cyber Resilience Act）中有关制造商的义务以及如何适用于开源软件的条款进行了讨论。英国信息专员办公室（ICO）发布了对拟议的《数据保护和数字信息法案》（Data Protection and Digital Information Bill）的意见。荷兰政府宣布将各分散的网络安全机构融并为一个单独的国家机构。新西兰内政部（DIA）公

布了一项提案，呼吁建立一个新的全行业监管机构，以保护新西兰人免受社交媒体和其他数字平台上的有害内容的侵害。

总体来说，欧美网络安全立法有不断加强的趋势，网络安全与国家安全、个人隐私、商业活动等紧密联系，欧美从各维度加强了对网络安全的监管。

2. 全球网络安全产业稳步增长

根据 IDC 于 2023 年发布的《全球网络安全支出指南》，2022 年全球网络安全总投资规模预计将达到 1955.1 亿美元，有望在 2026 年增至 2979.1 亿美元。另据 Gartner《2021-2023 年全球信息安全与风险管理细分市场终端用户支出报告》，2022 年全球的信息安全与风险管理产品和服务支出 1691 亿美元，2023 年预计将超过 1883 亿美元，增长 11.3%。

近年来，全球网络安全行业创新风向标——美国 RSAC 大会创新沙盒竞赛的入围十强企业，主要集中在云安全、数据安全、软件供应链安全、身份安全四个热门赛道。2023 年，受 AI 技术爆发的影响，智能化网络安全应用成为新热点。今年创新沙盒公布的十强企业中，有三家是通过智能技术应用来提升网络安全能力，应用方向分别为智能 SOC、智能网络攻防和智能数据治理与隐私安全。在安全自动化赛道，来自美国和以色列的公司实现了自动化的事件分析和快速响应，以及与用户企业业务互动的工作流程。今年 3 月，美国微软公司推出了基于 GPT-4 的网络安全助手 Security Copilot，可帮助防御者识别网络入侵。该安全助手集成了 OpenAI 的 GPT-4 生成式人工智能和微软的安全专用模型，网络安全人员可输入文件、网址或代码片段进行网络安全分析、询问某个特定漏洞的概要或从其他安全工具中获取安全事件及警报信息。Security Copilot 是第一个生成式人工智能安全产品，可服务于安全团队，以人工智能的速度和规模执行工作。

综合来看，无论从产业规模，还是技术应用落地来看，网络安全产业在全球都实现了快速发展。随着各行各业的数字化转型，网络安全产业还将具有长足的发展空间。

3. 全球网络安全人才缺口较大

网络安全专业人才是数字经济下劳动力市场不可或缺的组成部分，但人才缺口较大，据相关数据调查，当前已有数以百万计的相关职位空缺有待填补。

例如，目前全球有 340 万网络安全职位正在招聘但未能找到相应人才。同时，美国也有超过 70 万的网络安全职位空缺，主要集中于那些能专职保护公司、客户和基础设施安全的人才。

据美国信息系统审计和控制协会（ISACA）的研究，网络安全的两个主要技能缺口是软技能和云计算知识。为了帮助建立网络安全劳动力职业路径并填补现今的空缺职位，需要来自各种不同背景的专业人员，把这些软技能带到网络安全前线。麦肯锡认为，企业可以拓宽潜在应聘者的寻找范围，识别并保留背景更多样的候选人。另外，还应该培养网络安全团队领导人合作解决问题的能力，帮助其重新审视团队内的职业发展策略，消除传统的职业发展障碍，建立更具包容性的工作场所文化。为了更好防范安全威胁，企业除了引进软技能及云计算方面的技术人才外，还应加强全体员工的网络安全培训。一些安全事件往往由业务项目

和网络钓鱼而起，通过改善各行业、各岗位的网络安全培训，企业可以推动建立安全第一的文化，让安全成为每个人的职责。例如，亚马逊正在帮助更多人认识到网络安全的重要性，联合美国国家网络安全防范联盟发起“保护和连接”网络安全意识宣传活动，并向全世界个人和企业免费提供网络安全意识培训。

结合全球网络安全人才现状，可以看出网络安全岗位需求与人才供给不匹配的矛盾仍然存在，全球网络人才缺口较大，领先的科技公司已经在培养发掘人才方面做出了表率。

（二）我国网络安全产业及人才发展概况

1. 我国网络安全领域政策规定不断完善

今年1月，《工业和信息化部等十六部门关于促进数据安全产业发展的指导意见》（以下简称《指导意见》）发布。《指导意见》聚焦数据安全保护及相关数据资源开发利用需求，提出促进数据安全产业发展的总体要求，并按2025年、2035年两个阶段提出产业发展目标。指导意见分两个层面明确促进数据安全产业发展的七项重点任务，明确了提升产业创新能力、壮大数据安全服务、推进标准体系建设和推广技术产品应用四项重点任务。

今年5月，国家互联网信息办公室发布《数字中国发展报告（2022年）》，要求强化数字中国关键能力。构筑自立自强的数字技术创新体系。筑牢可信可控的数字安全屏障。推动网络安全法律法规和政策体系持续完善，不断增强网络安全保障能力。

2. 我国网络安全产业发展更加清晰明确

2022年我国全年国内生产总值（GDP）超121万亿元，其中数字经济规模达50.2万亿元，占GDP比重为41.5%。其中，典型网络安全产业规模达到900亿元，在数字经济中的占比达到0.18%。与2021年数字经济在GDP的占比（40.7%）及网络安全在数字经济中的占比（0.16%）相比，2022年均有显著提升。

根据《指导意见》的官方解读，数据安全产业聚焦数据全生命周期安全保护和开发利用的需求，支持相关技术、产品和服务的研究开发。网络安全产业主要从保护数据存储、处理、传输等载体的角度，实现对网络数据完整性、机密性、可用性保护，主要包含网络边界防护、计算环境防护等方面的技术、产品和服务。

当前我国网络安全企业在学习国外先进技术的同时，国内需求侧对创新的驱动更为显著。数据安全在创新方面的比重已接近传统安全领域，我国网络安全重视攻防、安全运营、SOAR等更具实战化的赛道，工业安全、汽车安全、安全芯片等赛道符合我国新型行业对网络安全的需求。海外市场为我国网络安全企业带来新的机遇，网络安全国际市场、国家海外利益保护、中东/东南亚数字化加速带来的配套网络安全市场均是潜在增长点。

3. 我国网络安全人才培养加快

目前，我国网络安全人才培养加快。截至2023年3月，国内已有80所高校开设网络空间安全专业，132所高校开设信息安全专业，2所高校开设保密技术专业，17所高校开设信息对抗技术专业，28所高校开设网络安全与执法专业。同时，我国各高校正在逐步加强网络安全高层次人才培养力度。

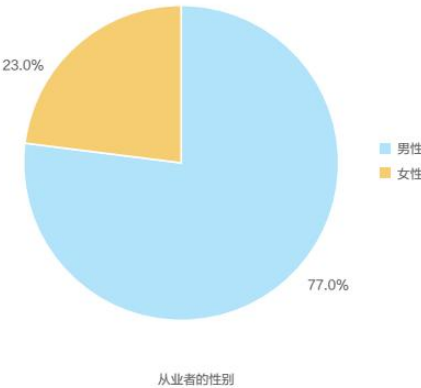
对于企业而言，当前网络安全业务份额越来越重，但是招到匹配和适合的网络安全技术人才却并不容易。从人才培养角度来看，深耕研究的定向人才十分缺乏，实战人才也处于供不应求的状态。日益增加的网络安全招聘岗位数，愈发精确地面向专业人才。

（三）网络安全人才从业现状

1. 我国网络安全从业人才画像

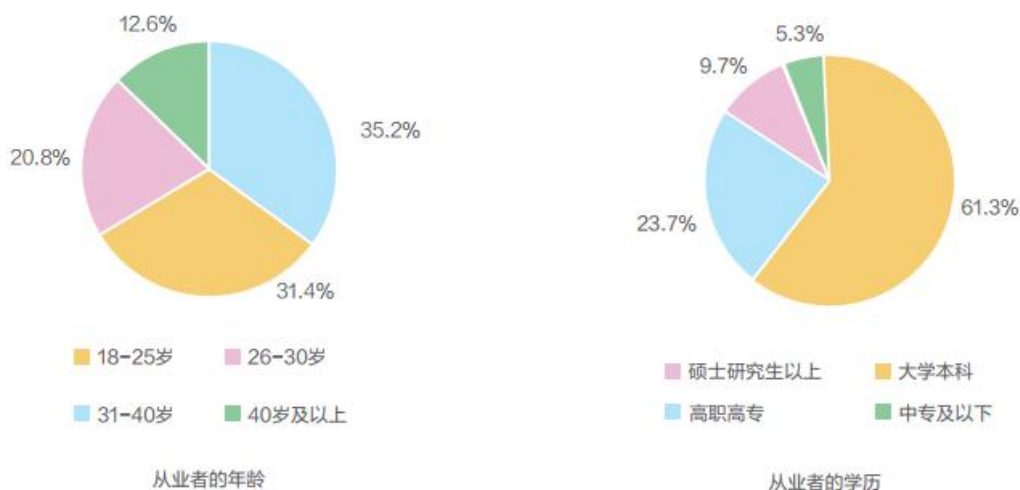
（1）男女比重为 77:23

问卷调研数据显示，2023 年，网络安全从业人才中，男性和女性分别占比 77%、23%。一方面，从专业学习来看，就读于网络安全相关理工科专业的男性比重更高，因而在后续就业中的占比也高于女性；另一方面也表明在当前的网络安全领域，男性仍是产业劳动力的主体。



（2）行业从业者逐渐年轻化

从年龄来看，2023 年，31-40 岁的网络安全从业者占比最高，达到 35.2%，但低于 2022 年的 50.8%和 2021 的 59.7%，该年龄段从业者的占比呈逐年下降趋势。相比之下，18-25 岁网络安全从业者的占比呈逐年上升趋势，2021 年、2022 年、2023 年的占比依次为 3.2%、11.2%、31.4%。另外，2023 年 26-30 岁的从业者占比为 20.8%，40 岁以上占比 12.6%。由此可见，网络安全从业者逐渐年轻化，更多的年轻从业者涌入该行业，为行业的未来发展注入了新鲜的活力。



（3）本科毕业生占比超 6 成

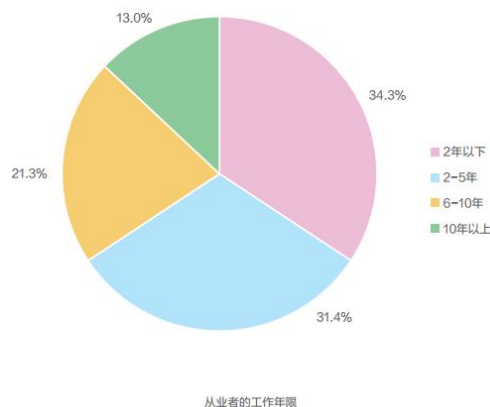
从学历来看，2023 年，本科毕业的网络安全从业者占比最高，达到 61.3%。其次是高职高专和硕士研究生以上学历的从业者，分别占比 23.7%、9.7%。本科学历从业者一直是网络安全领域的主要人才供给，在 2022 年、2021 年的调研数据中，分别占比 59.3%、63.9%。可见，网络安全从业者学历素质整体偏高。

（4）6 成以上网络安全从业者专业为计算机与网络

问卷调研结果显示，受访者中，63.8%的最高学历专业为计算机与网络相关专业，其次是网络安全相关专业，占比 15.9%。可以看出 6 成以上网络安全从业者的业务领域与所学专业有所区分，一方面，网络安全一级学科和专业开设时间较晚，目前新一代科班毕业生刚刚进入网络安全产业，导致网络安全相关专业的从业者占比较低，另一方面，这也表明网络安全行业凭借行业优势及学科交叉特性，吸引了较多“跨专业”人才就业。

（5）5 年以下工作年限从业者占比超 6 成

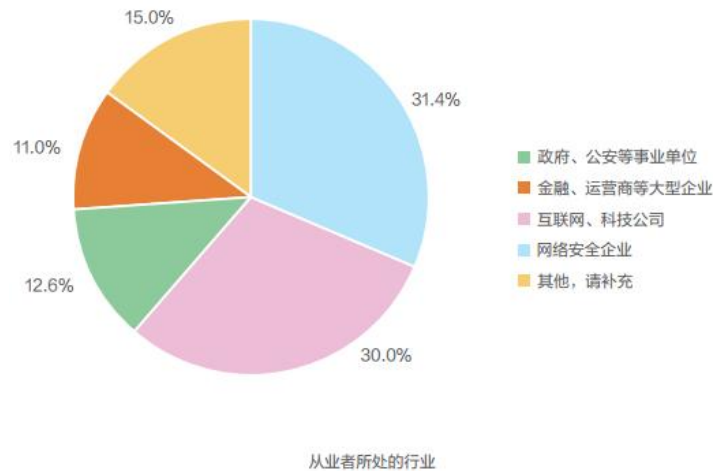
从工作年限来看，34.3%的受访者工作 2 年以下，占比最高。其次是 2-5 年、6-10 年工作者，占比分别为 31.4%、21.3%。由于网络安全产业兴起时间不长，目前处于稳步上升阶段，从业者整体上也处于探索和成长阶段，拥有较长工作经验的从业者占比较低。



2. 网络安全产业人才的从业现状

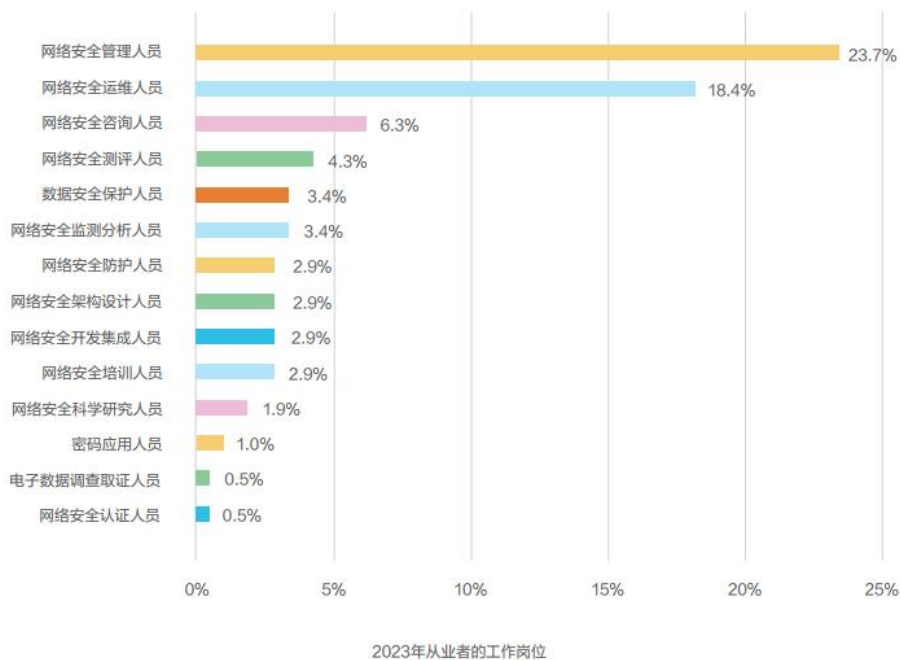
（1）网络安全企业和 IT 行业成产业人才汇聚地

从问卷调研结果可以发现，网络安全企业是网络安全产业人才的主要聚集领域，占比 31.4%，排名第一。其次是互联网、科技公司，占比 30%。此外，政府、公安等事业单位，以及金融、运营商等大型企业，占比分别为 12.6%、11%。可见，网络安全企业和 IT 行业是当前网络安全专业人才的主要汇聚地。



（2）安全管理和安全运维人员占比较高

从岗位来看，受访者中，从事网络安全管理工作的人才占比最高，达到 23.7%。其次是网络安全运维人员，占比 18.4%。而网络安全咨询、网络安全测评、数据安全保护等其他岗位的从业者占比均低于 7%。在具体的工作中，管理及运维类职能范畴相对宽泛，是网络安全人才的两大主要就业领域。

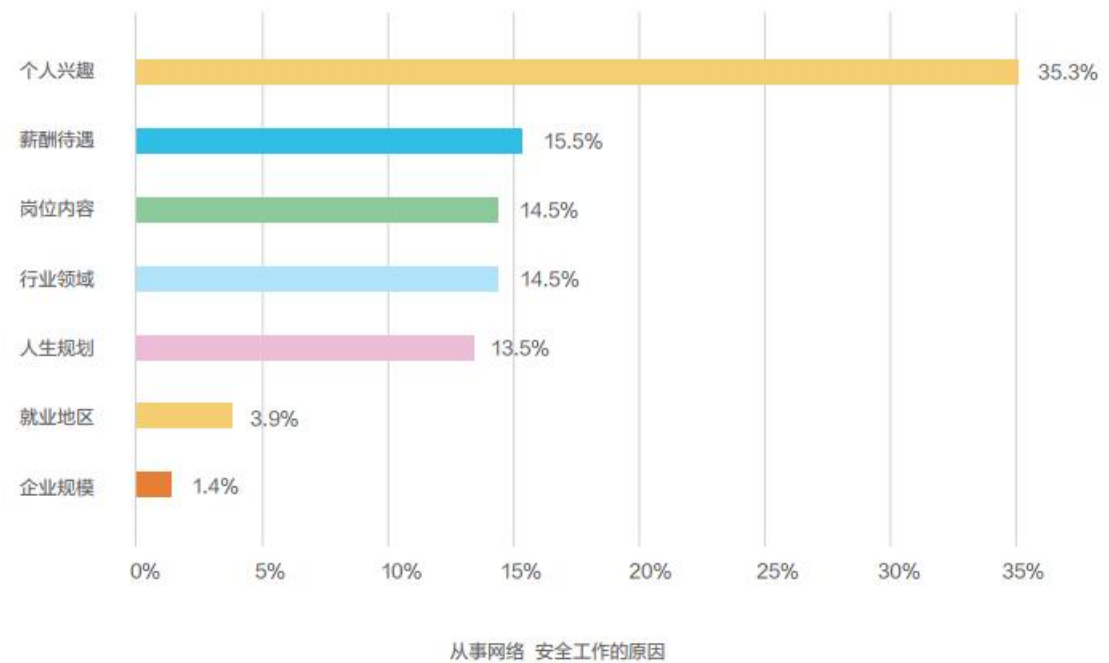


（3）3 成以上人才因个人兴趣选择从事网络安全行业

调研数据显示，在今年的受访者中，35.3%表示因个人兴趣选择从事网络安全行业，高

于选择薪酬待遇的 15.5%，也高于 2022 年选择个人兴趣而入行的 7.2%。

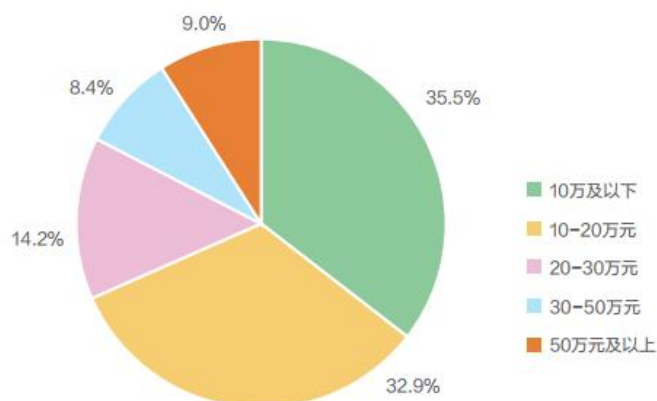
从年龄看，18-25 岁受访者因个人兴趣而入行的占比最高，为 46.2%，其次是 26-30 岁、40 岁以上和 31-40 岁的从业者，选择该项的占比分别为 34.9%、34.6%和 26%。新一代年轻人更倾向于以热爱为激励，把个人兴趣与职业相结合。随着越来越多年轻人加入网络安全行业，与薪酬待遇等“身外物”相比，因“真爱”而入行网络安全也显得更为普遍。



3. 网络安全产业人才的薪酬及福利待遇

(1) 近 2 成从业者税前年薪 30 万元以上

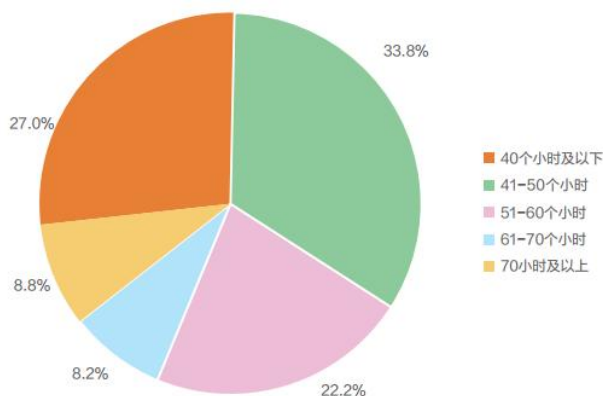
问卷调研结果显示，35.5%的受访者税前年薪不足 10 万元，但更多的从业者拥有较高的薪酬水平。其中，32.9%的从业者薪酬在 10-20 万元之间，14.2%的从业者税前年薪为 20-30 万元，8.4%从业者税前年薪为 30-50 万元，还有 9.0%的从业者拥有 50 万元及以上的高薪。网络安全是一个快速发展的朝阳行业，对从事相关工作从业者的技能要求也较高，因此企业更愿意为保护系统和数据免受网络威胁的专业人员提供优厚的薪酬待遇，预计未来网络安全人才的薪酬及福利待遇也将稳步提升。



从业者的税前年薪水平

(2) 超7成从业者每周工作时长40小时以上

问卷调研数据显示，73%的网络安全从业者每周工作时间超40个小时。其中，33.8%的从业者每周工作41-50小时，22.2%每周工作51-60小时。因工作性质原因，网络安全从业者需要时刻保持警惕，随时应对可能或已经发生的网络安全漏洞和风险，因此工作强度较高，加班情况较为普遍。



从业者的每周工作时长

(四) 网络安全产业人才供需分析

1. 网络安全产业人才需求

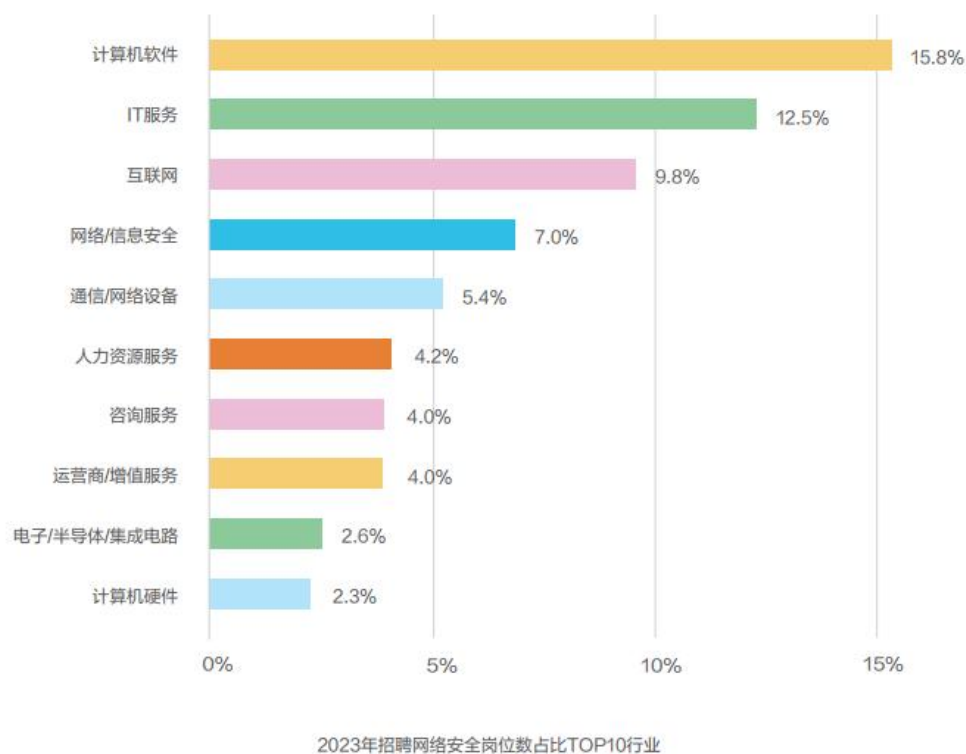
(1) 网络安全产业招聘职位数呈现波动

从网络安全人才需求来看，该产业招聘职位数呈现波动趋势。智联招聘平台数据显示，2021和2022年网络安全相关岗位招聘数量分别同比增长20.0%，2023年则有所下降。考虑到每年平台数据统计周期为上一年7月至今年6月，而2022年下半年疫情较严重，同时受国内外经济波动影响，部分行业在投资、拓展业务等方面有所收缩，企业人员增速放缓，同时内部推荐选才比例有所上升，因而网络安全产业招聘职位需求呈现出波动状态。



（2）计算机软件、IT 服务、互联网招聘需求排名前三

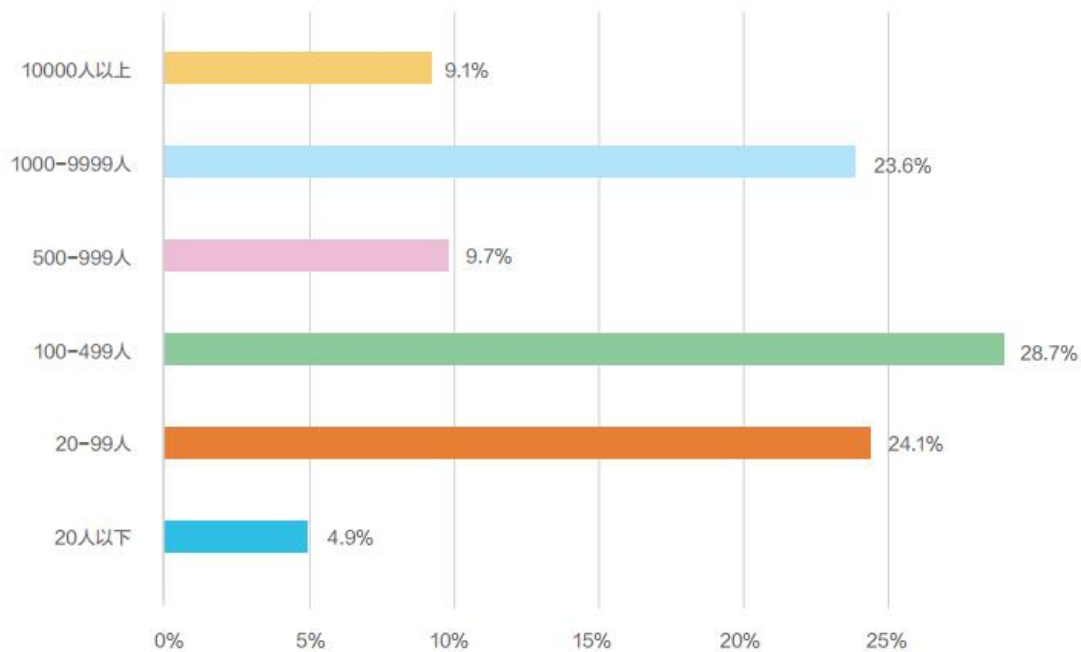
从招聘职位所在行业分布来看，2023 年招聘网络安全岗位数量最多的是计算机软件行业，占比 15.8%。其次是 IT 服务和互联网行业，招聘职位数占比分别为 12.5% 和 9.8%。此外，网络/信息安全、通信/网络设备、人力资源服务、咨询服务等行业，也对网络安全人才有较大需求。



（3）中小型企业对网络安全人才招聘需求更高

从企业规模看，2023 年，招聘网络安全岗位数量最多的是 100-499 人企业，招聘职位

数占比达 28.7%。其次是 20-99 人企业、1000-9999 人企业，分别占比 24.1%、23.6%。在全球网络安全人才短缺的背景下，中小型企业普遍进入数字化转型阶段，网络安全业务处于成长期，因而网络安全人才需求相对更加旺盛，有志于在网络安全领域发展的求职者可以重点投递中小型企业，积累经验迅速成长。

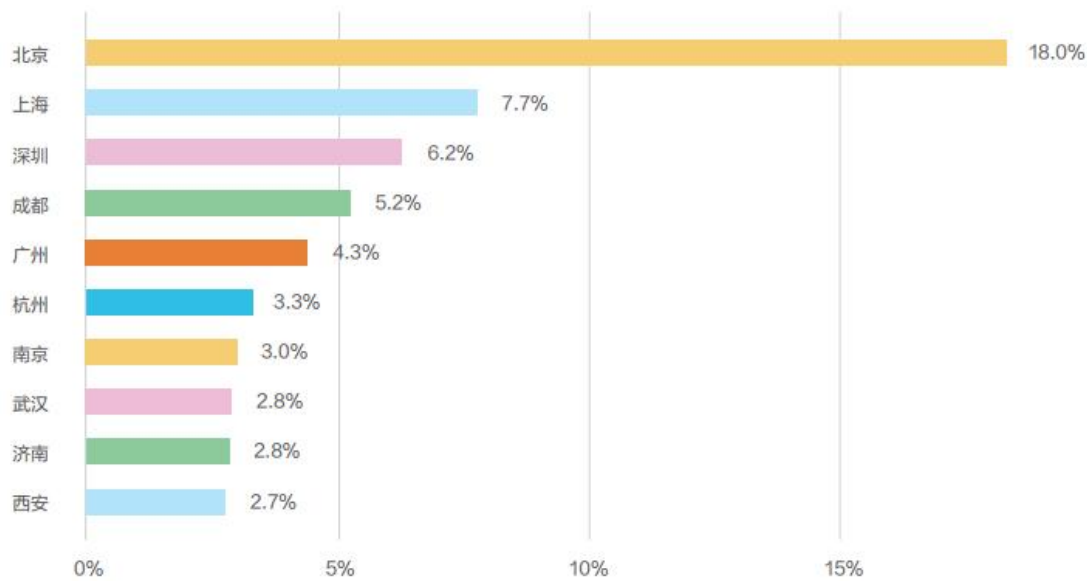


2023年不同规模企业招聘网络安全岗位数量占比

（4）一线城市对网络安全人才招聘需求大

从城市来看，一线城市是对网络安全人才需求最大的城市，2023 年北京市招聘网络安全岗位数量占比为 18%，排名各城市之首，数字安全产业正逐渐成为支撑首都数字经济发展的重点领域之一。其次是上海、深圳、成都，招聘职位数占比均超 5%。

总体来看，除了一线城市，网络安全人才需求主要集中在信息技术、智能制造等新兴产业布局广、数字化程度高的新一线城市。作为唯一进入前十的二线城市，济南高新区入选全国首批国家网络安全教育技术产业融合发展试验区，筑牢网络安全根基，人才需求也相对较大。



2023年招聘网络安全岗位数量占比TOP10城市

(5) 网络安全运营岗位招聘职位数占比 29%

从岗位分布来看，网络安全运营的招聘职位数占比最高，达到 29%。其次是网络安全建设、网络安全管理、数据安全类职位，分别占比 18.6%、17.7%和 10.2%。从典型职位上看，安全运维工程师的招聘职位数占比最高，达到 15.2%。数据安全是网络安全中极为重要的内容，从招聘职位数占比来看，数据安全招聘需求呈现出“少而精”的趋势。

一级职能	二级职能	典型职位	招聘职位数占比
网络安全运营 (29.0%)	网络安全运维	安全运维工程师	15.20%
	网络安全集成	集成方案解决师	7.60%
	网络安全应急响应	网络安全应急响应工程师	6.10%
网络安全建设 (18.6%)	网络安全开发	网络安全开发师	11.50%
	网络安全架构	安全系统架构师	6.60%
	个人信息保护	——	0.30%
	供应链安全	供应链安全管理	0.10%
网络安全管理 (17.7%)	网络安全测试	安全测试工程师	8.30%
	网络安全合规	安全合规工程师	3.50%
	网络安全咨询	安全咨询工程师	2.70%
	网络安全规划	安全规划师	1.90%
	网络安全防护	安全等级保护测评师	1.30%
数据安全 (10.2%)	数据安全体系	数据安全体系工程师	3.20%
	数据安全治理	数据管理师	3.20%
	数据安全评估	数据安全评估师	2.60%
	数据安全保护	数据安全保护工程师	1.00%
	电子数据取证	电子数据取证师	0.30%
网络安全审计和评估	网络安全分析	渗透测试/漏洞挖掘工程师	5.90%

一级职能	二级职能	典型职位	招聘职位数占比
(8.8%)	网络安全评估	网络安全评估师	2.50%
	网络安全认证	安全认证工程师	0.4

(6) Linux、Java、Windows 等技能需求大

考虑到安全研发人员和安全服务人员对攻防技术方面的关注和以往无明显区别,因而本报告中增加了安全研发方面的技能供需分析。从需求端来看,在各种针对研发人员的技能中, Linux、Java、Windows 等技能的招聘需求最高,排名招聘要求技能榜 TOP3。Linux 是一种自由和开放源码的类 Unix 操作系统,在安全领域的应用非常广泛,如网络维护、系统管理等;Java 是一门面向对象的编程语言,具有跨平台性,因此可以在不同的操作系统和硬件上运行。这一特点使得 Java 语言成为开发网络安全应用的理想选择,因此招聘需求也相对较大。其次,招聘企业对 Python、MySQL、TCP/IP 协议等技能的需求也比较高。可见,掌握系统编程和面向对象的编程技术人才,在网络安全领域更受企业青睐。

排名	技能
1	Linux
2	Java
3	Windows
4	Python
5	MySQL
6	TCP/IP协议
7	C++
8	CCNP
9	Oracle
10	SQL

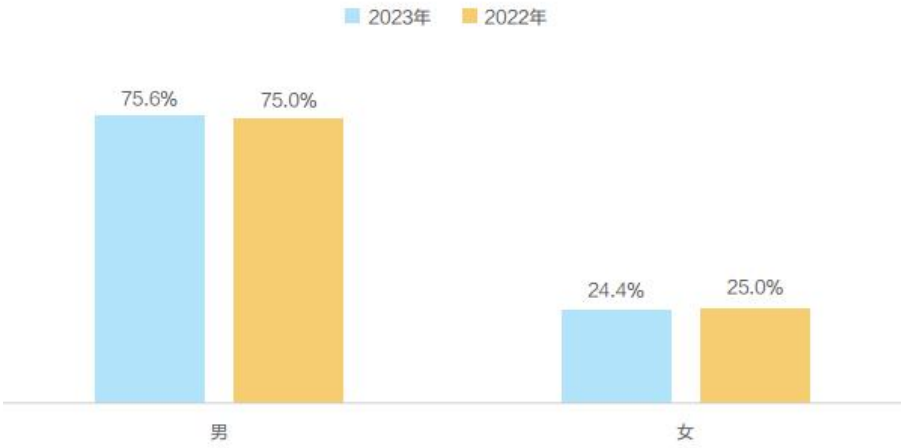
2023年网络安全岗位需求的专业技能TOP10

2. 网络安全产业人才供给

(1) 男性求职者占比超七成

智联招聘平台数据显示,2023 年向网络安全岗位求职的人才中,男性占比 75.6%,女性占比 24.4%。2022 年,男性占比 75%,女性占比 25%。性别结构较为稳定。由于网络安全属于理工科,就读相关专业的男性更多,而该工作对技术升级迭代、工作时间的要求较高,需要持续学习和加班工作,相比之下男性更适应这样的工作要求,因此男性求职者比重持续处

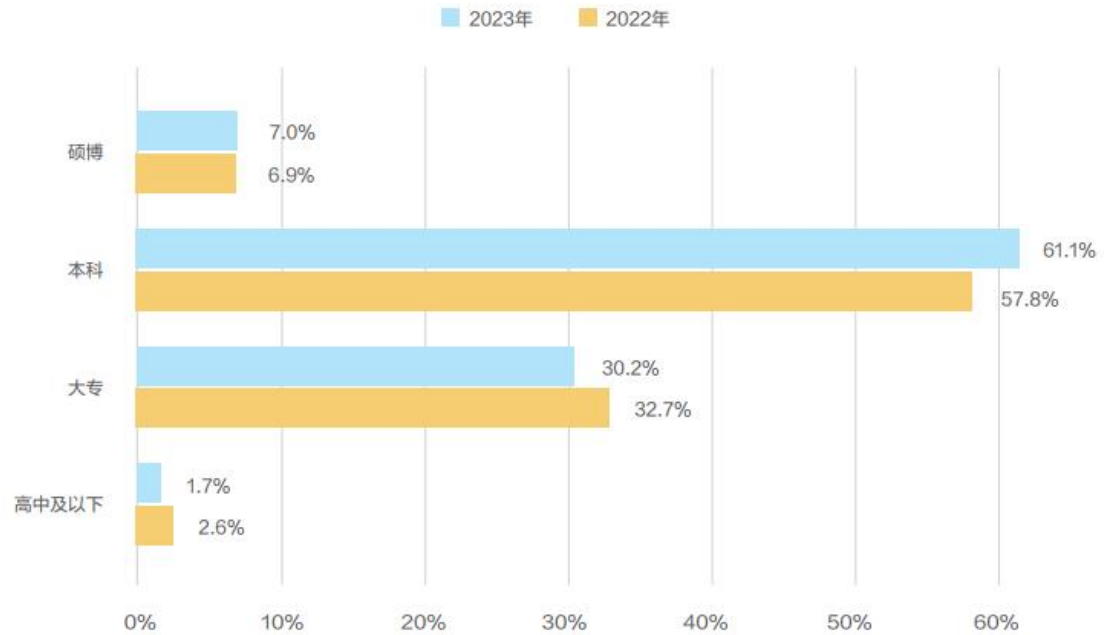
于高位，属于绝对的求职主体。



网络安全求职者的性别分布

（2）本科学历求职者占比较高，且呈上升趋势

从学历来看，2023 年本科学历的网络安全求职者占比最高，达到 61.1%，相比 2022 年的 57.8%，提升了 3.3 个百分点。其次是大专学历，求职者占比 30.2%，比 2022 年的 32.7% 下降了 2.5 个百分点。随着学历教育的普遍提升以及网络安全行业的知识密集特性，网络安全行业本科求职者在增多。

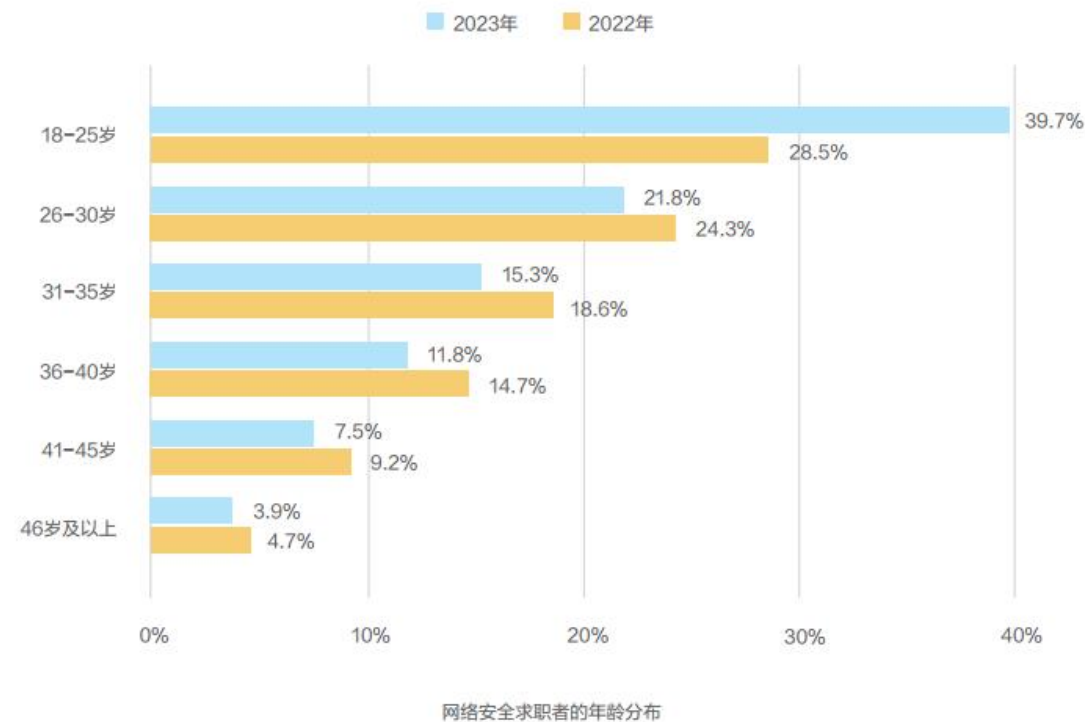


网络安全求职者的学历分布

（3）18-25 岁人才求职者占比排名第一

从年龄来看，2023 年，网络安全领域 18-25 岁人才求职者占比 39.7%，排名第一，而且相比 2022 年的 28.5%，提高了 11.2 个百分点。其次是 26-30 岁、31-35 岁求职者，占比分

别为 21.8%和 15.3%，但相比 2022 年均有所下降。可见年轻人普遍看好我国网络安全行业这一蓝海市场的发展前景，未来网络安全行业将受到更多求职者的青睐。



（4）计算机科学与技术专业求职者占比最高

从专业分布来看，2023 年，计算机科学与技术专业毕业的求职者占比最高达 11.8%，且高于 2022 年的 9.5%。其次是软件工程、计算机网络技术和工商管理，2023 年的占比分别为 4.3%、3.3%和 3.1%。计算机科学与技术专业学生具有较强的专业优势，网络安全产业的学科交叉特性也鼓励着具有专业优势的技术人才跨界求职。

排名	2023专业	占比	排名	2022专业	占比
1	计算机科学与技术	11.8%	1	计算机科学与技术	9.5%
2	软件工程	4.3%	2	工商管理	3.3%
3	计算机网络技术	3.3%	3	计算机网络技术	3.3%
4	工商管理	3.1%	4	软件工程	3.0%
5	网络工程	3.0%	5	网络工程	2.9%
6	计算机应用技术	3.0%	6	计算机应用技术	2.8%
7	通信工程	2.6%	7	通信工程	2.7%
8	电子信息工程	2.0%	8	电子信息工程	2.1%
9	信息管理与信息系统	1.6%	9	会计学	1.7%
10	软件技术	1.5%	10	信息管理与信息系统	1.7%
11	会计学	1.3%	11	市场营销	1.5%
12	土木工程	1.3%	12	电子信息科学与技术	1.3%
13	市场营销	1.2%	13	电气工程及其自动化	1.3%
14	物联网工程	1.2%	14	土木工程	1.1%
15	电气工程及其自动化	1.2%	15	软件技术	1.1%

网络安全求职者的专业TOP15

（5）MySQL 是网络安全求职者掌握最多的技能

从求职者具备的技能看，在各种针对研发人员的技能中，求职者具备的前三项技能分别是 MySQL、Java、Linux。其次是 SQL、SpringBoot、Python 等技能，求职者具备多元化技能，不同技术人才都希望在网络安全领域找到用武之地。对比求职者技能和职位所需技能，MySQL 是时下最流行的关系型数据库管理系统之一，学习者众多，因此这项技能的供给更加充足。

排名	技能
1	MySQL
2	Java
3	Linux
4	SQL
5	SpringBoot
6	Python
7	Windows
8	Vue
9	CAD
10	SpringCloud

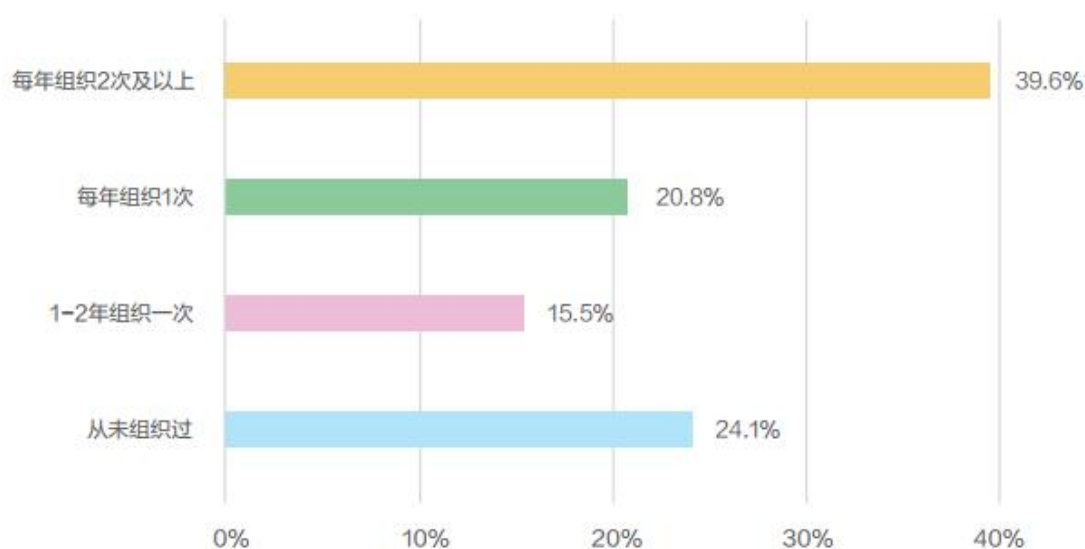
网络安全求职者具备的技能TOP10

（五）用人单位人才培养

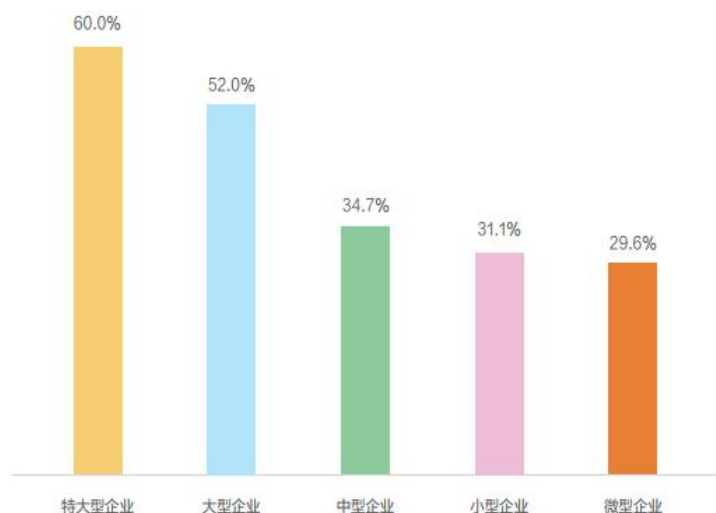
1. 用人单位人才能力建设

(1) 近四成从业者所在企业每年组织 2 次及以上网络安全培训

问卷调研结果显示，39.6%的网络安全从业者所在企业每年组织 2 次及以上培训，占比最高。其次是从未组织过培训的，占比 24.2%。每年组织 1 次培训的，占比 20.8%。可见，网络安全从业者所在企业组织培训呈现“两极分化”，培训频率较高和从未培训的企业同时存在。



从业者所在企业组织培训的频率



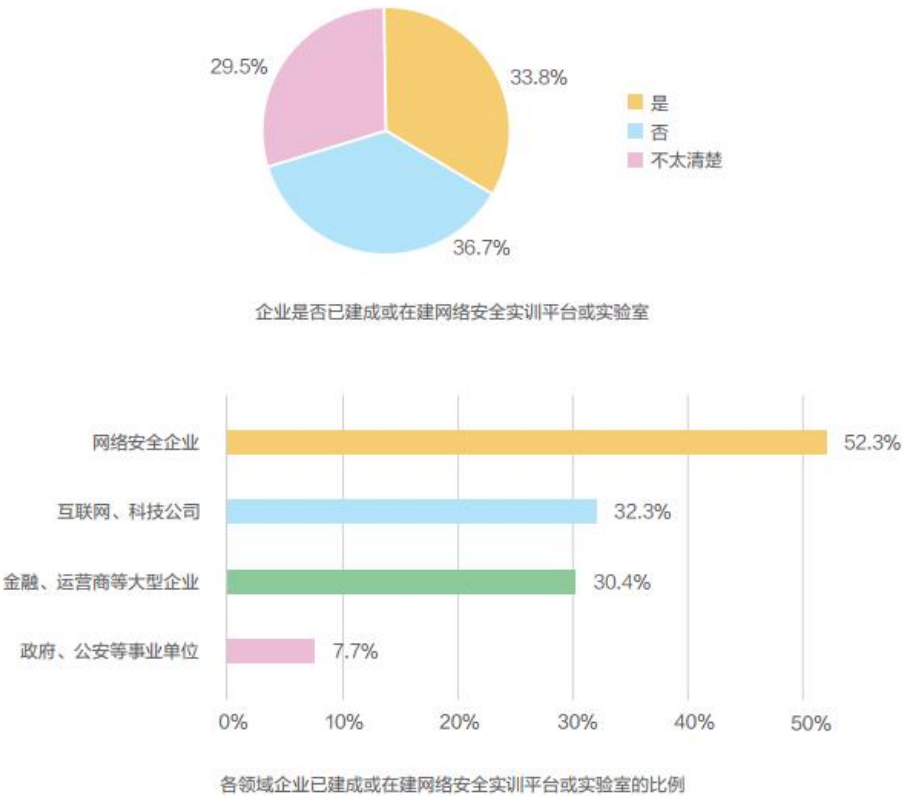
各规模企业每年组织2次及以上网络安全相关培训的比例

其中，每年组织 2 次以上培训的特大型企业占比 60%，高于大型企业的 52%、中型企业的 34.7%、小型企业的 31.1% 和微型企业的 29.6%。可见企业规模越大，对于培训就越重视，开展培训活动也更加频繁。微型企业受制于人手和经费所限，对网络安全相关培训的组织力

度相对更弱。

（2）过半网络安全企业已建成或在建网络安全实训平台

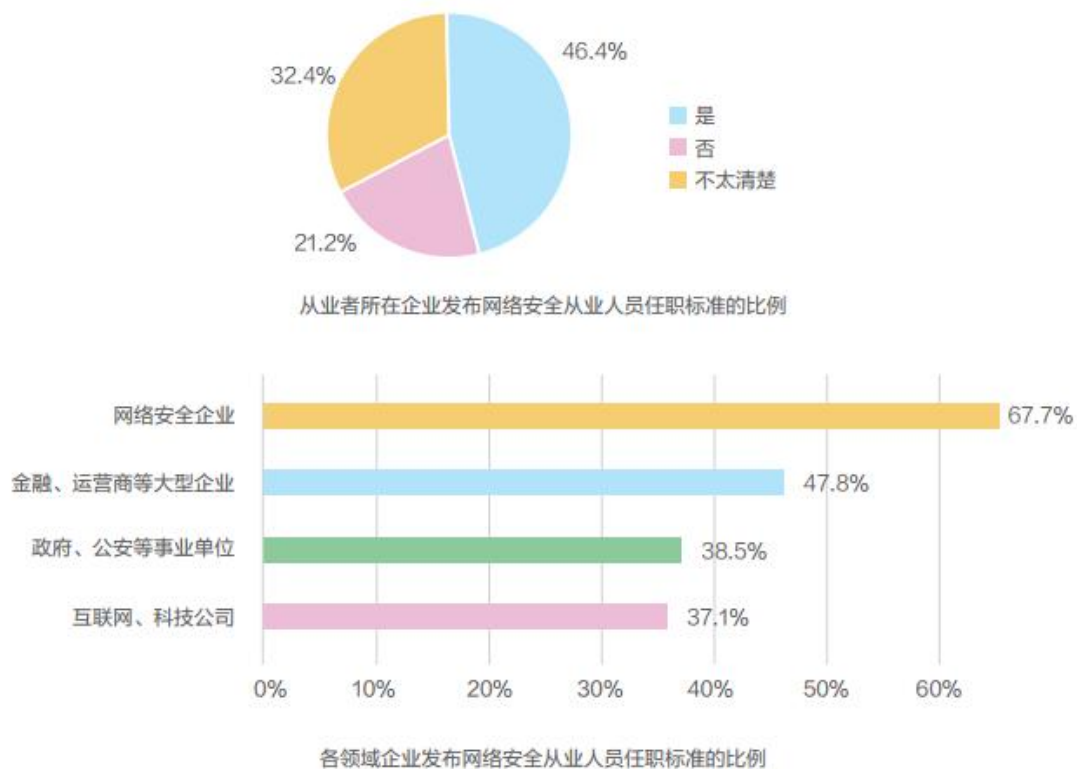
目前,33.8%的受访网络安全从业者所在企业已建成或在建网络安全实训平台或实验室,而未建成的占比高达 36.7%。从不同领域来看,已建成或在建网络安全实训平台或实验室的网络安全企业占比最高,达到 52.3%,超过互联网、科技公司,金融、运营商等大型企业,政府、公安等事业单位。



2. 用人单位人才体系建设

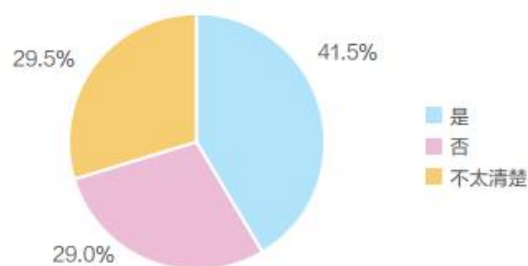
（1）近七成网络安全企业建立任职标准

从任职标准来看,46.4%的受访网络安全从业者所在企业发布了能力评价、等级认证等任职标准。不过,也有 21.2%的从业者所在企业未建立这项标准。具体来看,网络安全企业的从业者中,有 67.7%表示所在企业建立了任职标准,占比高于金融、运营商等大型企业(47.8%),政府、公安等事业单位(38.5%),以及互联网、科技等公司(37.1%)。

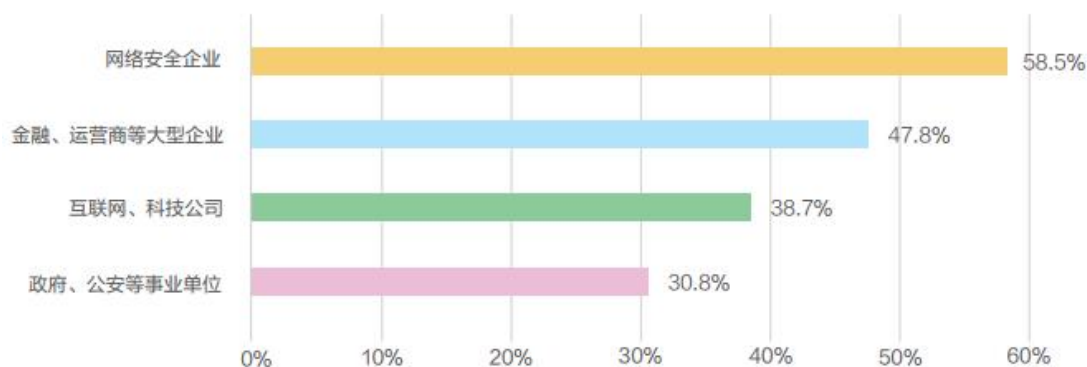


（2）四成从业者所在企业建立网络安全领域用人机制

专业人才的引入、选拔、培养对于网络安全领域专业人才至关重要，41.5%的受访从业者表示所在企业建立了网络安全领域用人机制。不过，也有 29%的从业者所在企业未建立这项机制。具体来看，网络安全企业的用人机制构建最为完善，有 58.5%的从业者所在企业建立了用人机制，超过金融、运营商等大型企业（47.8%），互联网、科技公司（38.7%），政府、公安等事业单位（30.8%）。



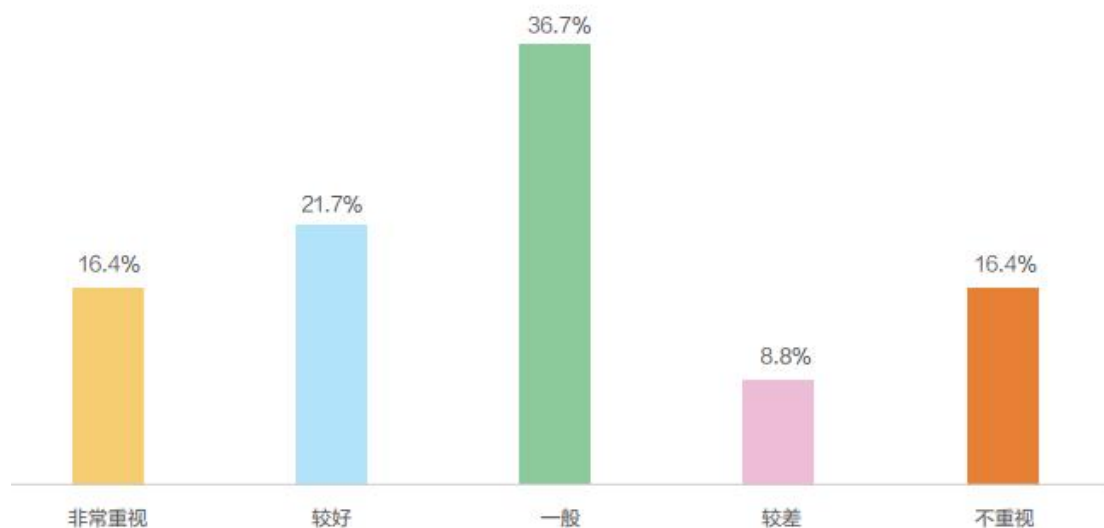
从业者所在企业建立网络安全专业人才用人机制的比例



各领域企业建立网络安全专业人才用人机制的比例

(3) 近四成从业者所属公司重视人才建设

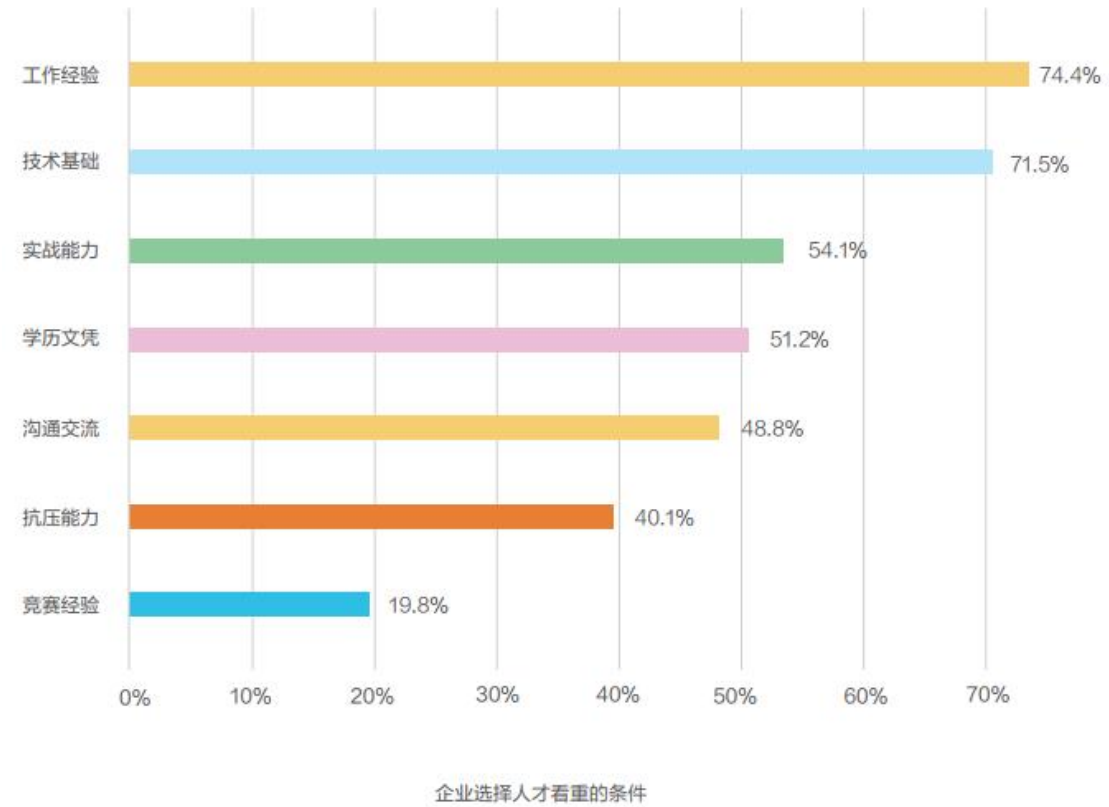
调研结果显示，分别有 16.4% 和 21.7% 的从业者所属企业对网络安全人才建设“非常重视”或“较好”。不过，36.7% 的从业者认为企业对人才建设的重视程度“一般”。可见，网络安全人才所在公司对人才建设的重视程度仍有待提高。



企业对网络安全人才建设的重视程度

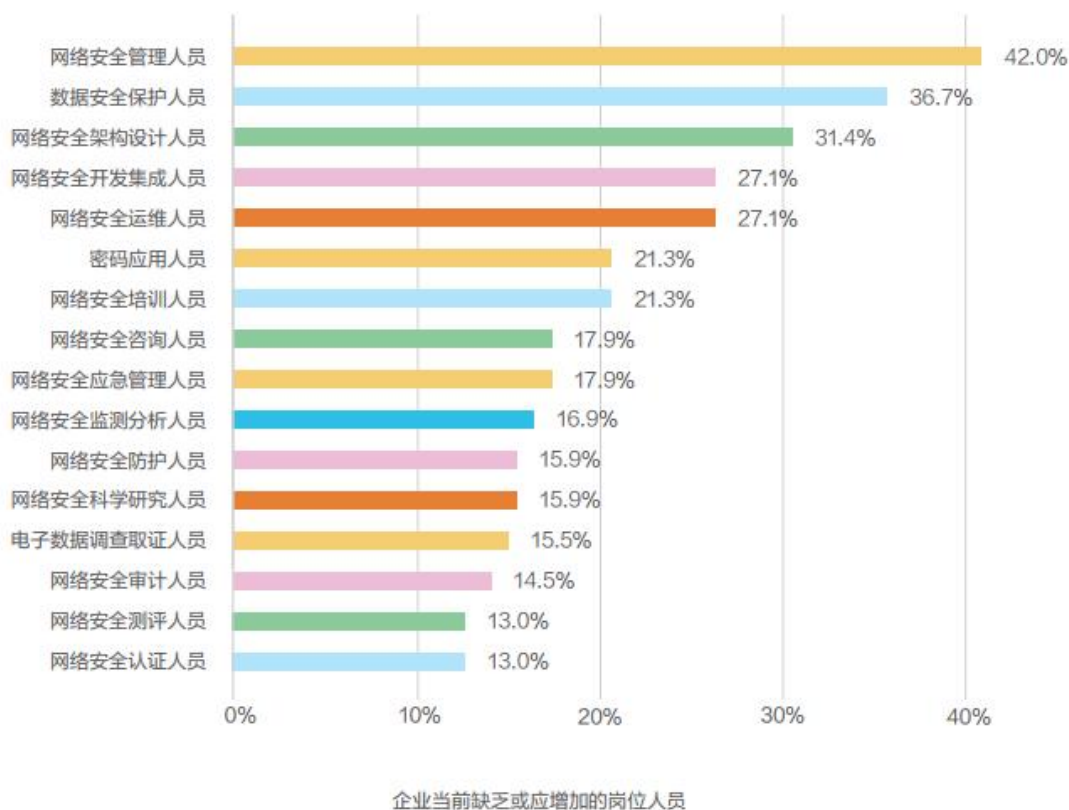
(4) 七成以上网络安全从业者所在用人单位重视工作经验

从用人单位在选才时注重的条件来看，74.4%的受访从业者表示所在企业重视工作经验，占比排名第一。其次是技术基础、实战能力、学历文凭，分别占比71.5%、54.1%、51.2%。可见，学历是网络安全人才选拔的关键一环，但不是唯一一环。工作经验和技术能力，才是用人单位更看重的因素。



（5）超四成从业者认为公司应当增加网络安全管理人才

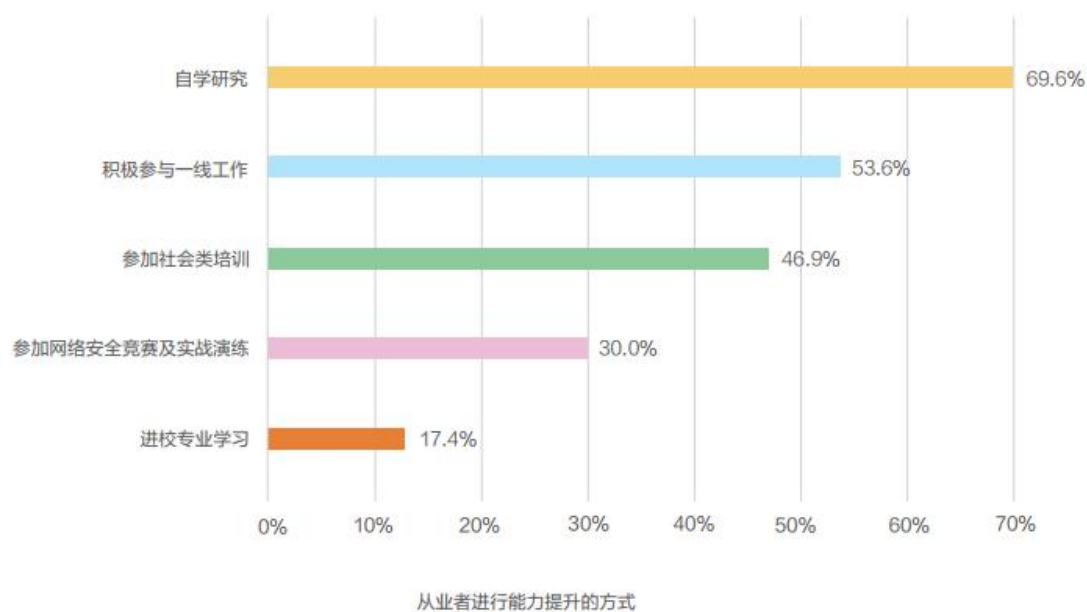
根据企业业务发展需求，42%的网络安全从业者认为，企业应当增加网络安全管理人员，其次是数据安全保护人员，占比36.7%，也有31.4%的从业者认为应当增加网络安全架构设计人员。此外，网络安全开发集成人员、网络安全运维人员、密码应用人员、网络安全培训人员的需求也排名前列。可见，管理人员和技术人员是目前行业较为缺乏人才的岗位。



3. 在岗人才能力提升

(1) 自学研究是从业者能力提升的主要方式

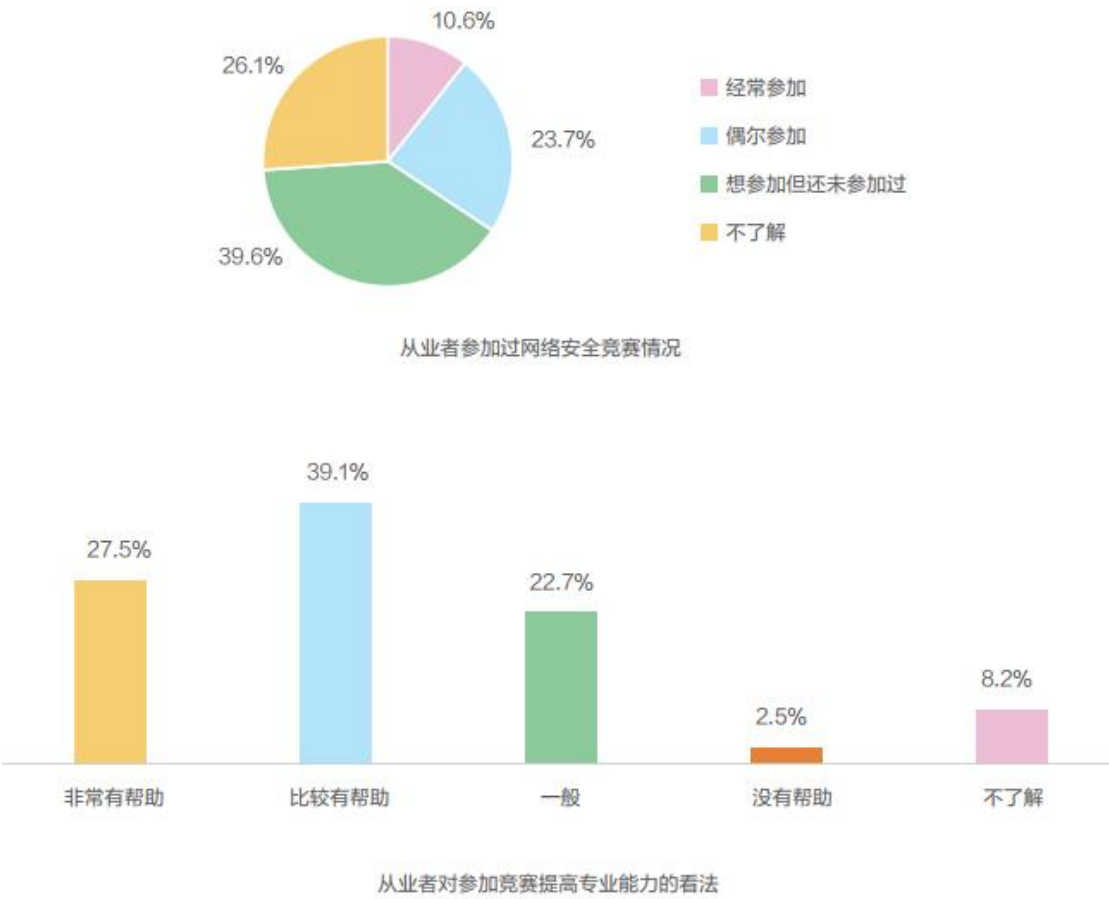
在提升能力的方法中，69.6%的网络安全从业者选择“自学研究”，其次是“积极参与一线工作”“参加社会类培训”，分别占比 53.6%、46.9%。此外，“参加网络安全竞赛及实战演练”“进校专业学习”，也是从业者提高网络安全领域能力的方式。



(2) 34%从业者参加过网络安全竞赛，六成以上认为有助于提高专业能力

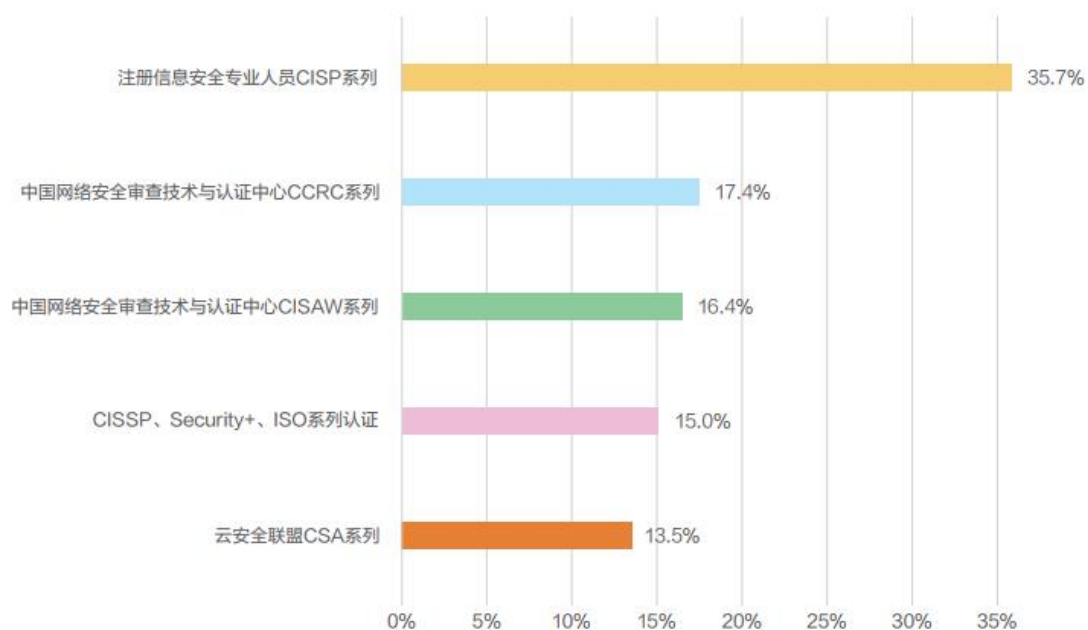
问卷调研显示，分别有 10.6%、23.7%的从业者经常参加和偶尔参加竞赛，39.6%的从业

者想参加但还未参加过网络安全竞赛。对于竞赛提高专业能力方面的作用，从业者普遍反映较好。其中，27.5%认为“非常有帮助”，39.1%认为“比较有帮助”，共计有66.6%的从业者认为有帮助。



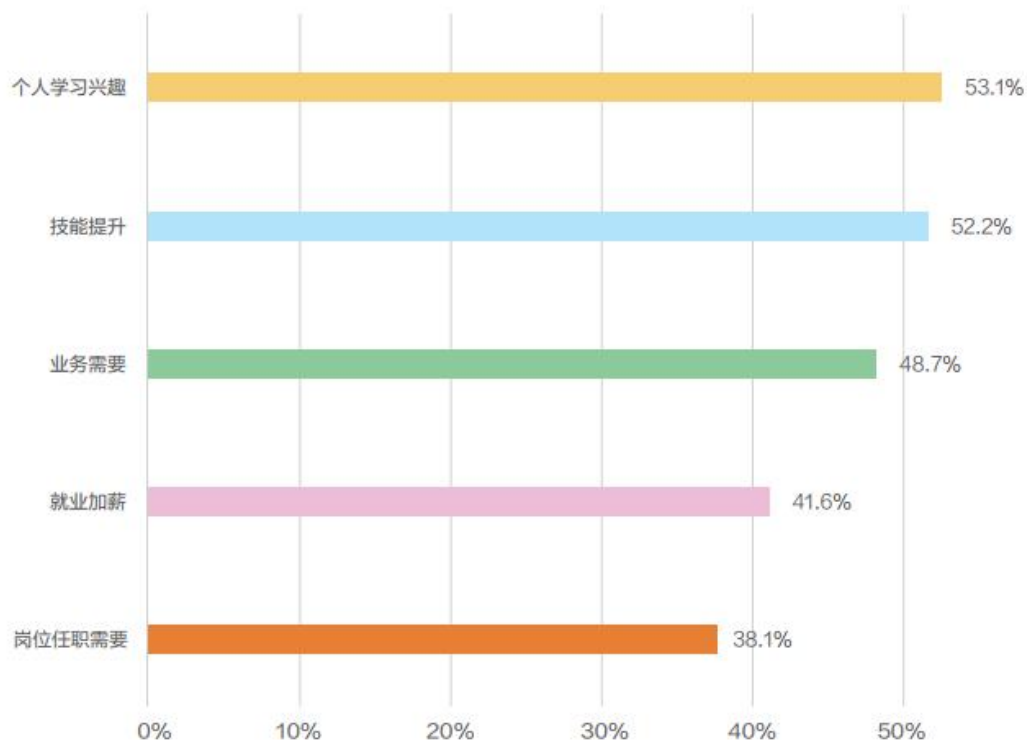
（3）兴趣、技能、业务是考证的主要驱动力

在认证方面，目前拥有注册信息安全专业人员 CISP 系列认证的从业者占比最高，达到 35.7%。其次是中国网络安全审查技术与认证中心 CCRC 系列，中国网络安全审查技术与认证中心 CISA 系列，CISSP、Security+、ISO 系列认证，占比均超过 15%。



从业者拥有的网络安全相关认证

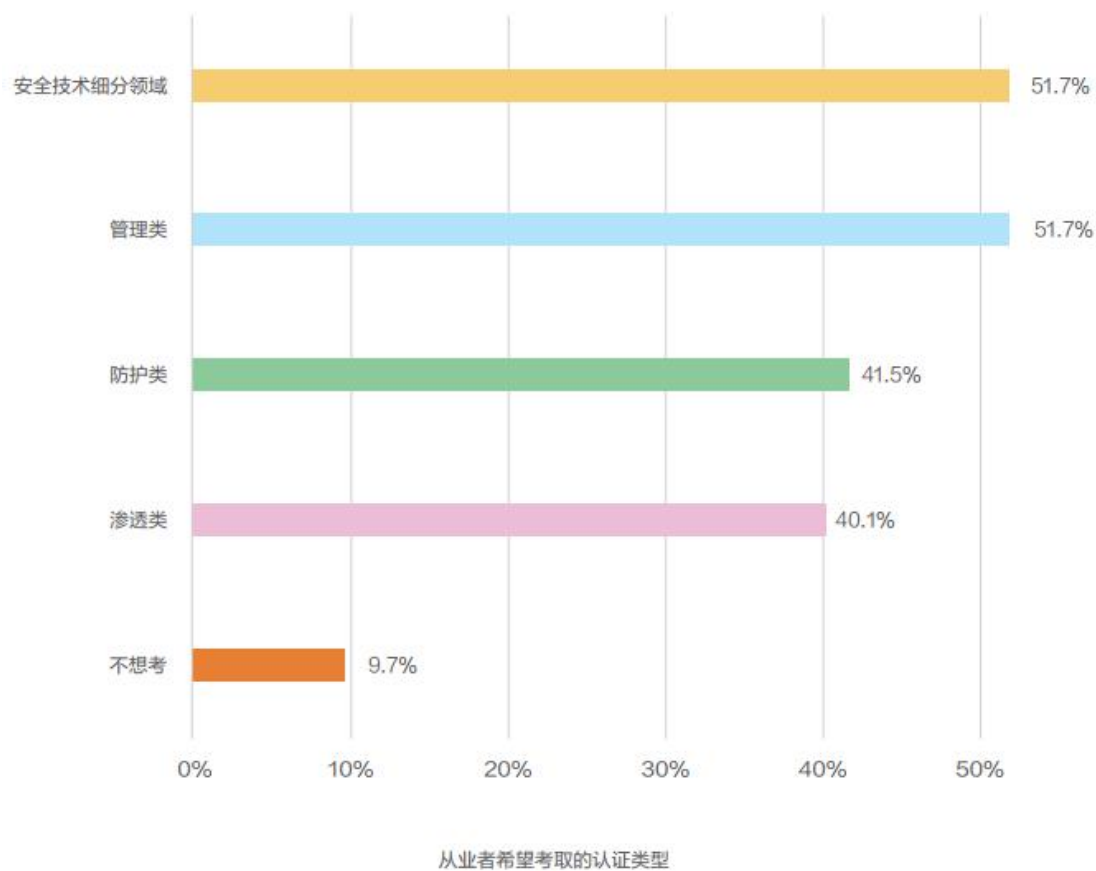
从考证驱动力来看，有 53.1%的从业者考证是出于个人学习兴趣，也有 52.2%和 48.7%的从业者因为技能提升和业务需要而考证。也有 41.6%的从业者奔着“就业加薪”目标，这些国家级或国际级认证，是从业者求职和升职加薪的重要“助攻”。



从业者考取认证的原因

从业者希望考取的认证类型中，安全技术细分领域、管理类为主要类别，占比均为 51.7%。

同时也有 41.5%、40.1%的从业者分别选择防护类、渗透类认证。



（六）专业招生与就业岗位分布情况

1. 安全与管理专业人才典型工作任务与职业能力调研

通过调研我们得知，目前信息安全技术应用行业的从业人员基本上呈两个层次：第一层次为信息安全软件及信息安全产品的研发，从业人员以高等院校相关专业的本科毕业生或博士为主。第二层次为网络安全产品的使用操作人员，主要从事网络安装调试、网络管理与运维、网络安全管理、信息安全保全、信息安全事件处置、网络架构维护、售后工程、网络安全产品销售与售后服务等技术工作。第二层次的人员因为涉及工作领域较广，因此需求量最大。在本次调研过程中我们发现，目前 python 程序设计语言的使用越来越普遍，市场需求旺盛，就业前景较好。现从业人员以高职和中职相关专业的毕业生为主，企业对各岗位群专业技能要求如表 2。

表2 信息安全岗位群技能要求分析表

序号	任务领域	典型工作任务	职业需求技能
1	信息安全工程师	1. 计算机软硬件、网络、应用相关领域从事安全系统设计，并完成相应报告； 2. 信息系统安全检测与审计等	1. 懂得并理解相关的信息运行与安全规范；如 ITIL、ISO20000、等级保护等相关知识； 2. 掌握 WINDOWS、LINUX 操作系统安全防护设置； 3. 熟悉无线局域网安全标准与防护方法；

序号	任务领域	典型工作任务	职业需求技能
		方面工作； 3. 熟悉渗透测试，熟练使用渗透测试工具，能通过工具对主机和应用系统进行有效的渗透； 4. 能够完成各种系统（主机、网络、数据库等系统）的安全评估和加固 5. 熟悉 web 相关网络原理、协议，熟悉多种 web 攻防技术和工具；能快速响应 Web 攻击事件； 6. 精通常见的 web 漏洞防范方法与安全审计； 7. 应用技术管理手段进行网络安全(如黑客攻击、病毒攻击、网络权限等)的防范与部署； 8. 熟悉信息安全相关理论知识，熟悉国内外信息安全相关重要法律法规、管理标准和技术标准，能指导进行风险评估； 9. 信息安全体系规划、ISMS 建设。	4. 掌握各种网络安全及管理软件使用（sniffer、ACL 配置、各种检测命令等）方法； 5. 掌握各类网络安全和防攻击技术，具有一定的系统与网络的攻防对抗能力；、 6. 能进行内外网分段安全测试； 7. 熟悉数据安全与行为安全；熟悉数据备份与远程容灾； 8. 精通 WINDOWS、LINUX 平台下的各类网络 WEB 应用； 9. 掌握 WEB 开发与网络数据库管理技术，并且有相应的安全防护知识； 10. 懂得基本的网络程序设计语言； 11. 能够制定简单的被评估对象的核查列表； 12. 可以结合重要性和发现的脆弱性进行系统综合风险分析； 13. 能够利用相关安全评估扫描工具对测评对象进行扫描； 14. 能够利用应用渗透评估扫描工具对测评对象； 15. 能够利用网络截包工具对网络数据进行分析； 16. 能够发现渗透对象可能存在的漏洞； 17. 能够利用渗透工具对漏洞进行验证； 18. 能够根据应用需求，对主流厂商的网络设备和安全产品的功能、参数、安全特性进行合理选型； 19. 能够根据应用需求，制订及实施网络安全解决方案； 20. 能够对网络安全方案进行实施与检测。
2	信息安全评测工程师	1. 从事信息安全风险评估、等级保护、检测评估等工作；包括利用各种工具对网络、系统、数据库等进行安全漏洞检测； 2. 为客户信息系统提供安全咨询和解决方案； 3. 为客户提供安全规划和设计整改方案； 4. 遵照规范出具信息安全相关报告。	1. 掌握企业基本安全生产管理制度； 2. 懂得并理解相关的信息运行与安全规范；如 ITIL、ISO20000、等级保护等相关知识； 3. 能进行内外网分段安全测试； 4. 熟悉市场上的各类型主流安全产品特性及功能应用情况； 5. 学会基本的应用功能测试与分析； 6. 能够制定信息系统安全分析评估工作计划； 7. 能够根据系统特征对被评估对象重要性进行划分； 8. 能够制定简单的被评估对象的核查列表； 9. 能够对被评估对象进行脆弱性分析；

序号	任务领域	典型工作任务	职业需求技能
			10. 可以结合重要性和发现的脆弱性进行系统综合风险分析； 11. 可以撰写风险评估报告； 12. 能够利用相关安全评估扫描工具对测评对象进行扫描； 13. 能够利用应用渗透评估扫描工具对测评对象； 14. 能够利用网络截包工具对网络数据进行分析； 15. 能够发现渗透对象可能存在的漏洞； 16. 能够利用渗透工具对漏洞进行验证； 17. 能够充分利用网络资源查找了解相关渗透性攻击方法和工具； 18. 能够利用工具对信息系统进行初步的安全评估。
3	安全渗透测试工程师	1. 参与安全测评项目、安全服务项目的具体实施； 2. 实施主机、网络和 Web 安全渗透测试； 3. 信息安全渗透测试、风险评估与加固工作的组织实施； 4. 构建 WEB 内容安全体系，评估上线业务安全问题，指导安全测试，跟踪解决内容安全问题； 5. 了解信息安全技术应用趋势，及时掌握新的安全技术、安全攻击及防御技术； 6. 在出现网络攻击或安全事件时，配合提供应急响应的技术支持，帮助用户恢复系统及调查取证。	1. 掌握 WINDOWS、LINUX 操作系统安全防护设置； 2. 掌握路由与交换技术； 3. 掌握各类网络安全和防攻击技术，具有一定的系统与网络的攻防对抗能力； 4. 能进行内外网分段安全测试； 5. 熟悉数据安全与行为安全；熟悉数据备份与远程容灾； 6. 能够制定简单的被评估对象的核查列表； 7. 能够对被评估对象进行脆弱性分析； 8. 可以结合重要性和发现的脆弱性进行系统综合风险分析； 9. 能够利用相关安全评估扫描工具对测评对象进行扫描； 10. 能够利用应用渗透评估扫描工具对测评对象； 11. 能够利用网络截包工具对网络数据进行分析； 12. 能够发现渗透对象可能存在的漏洞； 13. 能够利用渗透工具对漏洞进行验证； 14. 能够充分利用网络资源查找了解相关渗透性攻击方法和工具； 15. 能够对网络安全方案进行实施与检测。
4	信息安全评估员	1. 负责对信息安全(网络、系统、数据安全等)策略规划及协调部署； 2. 信息安全审计（包括操作系	1. 信系统安全分析评估工作计划能够根据系统特征对被评估对象重要性进行赋值； 2. 制定简单的被评估对象的核查列表； 3. 对被评估对象进行脆弱性分析；

序号	任务领域	典型工作任务	职业需求技能
		统、数据库、应用系统和网络，及信息安全体系）； 3. 负责信息安全政策、流程及管理制度建设和完善； 4. 负责定期完成信息安全自查工作，撰写自查报告并提出整改措施； 5. 信息安全监控和预警； 6. 安全系统的维护。	4. 结合重要性和发现的脆弱性进行系统综合风险分析； 5. 撰写风险评估报告； 6. 能够利用相关安全评估扫描工具对测评对象进行扫描； 7. 能够利用应用渗透评估扫描工具对测评对象； 8. 能够利用网络截包工具对网络数据进行分析； 9. 能够发现渗透对象可能存在的漏洞； 10. 能够利用渗透工具对漏洞进行验证； 11. 能够充分利用网络资源查找了解相关渗透性攻击方法和工具。
5	网络运维安全管理员	1. 能熟练配置 Windows、Linux 下的各类服务器及相关软件； 2. 能对服务器的安全进行评估； 3. 对系统安全 BUG 进行评估和测试； 4. 了解服务器性能，能架设高性能服务器(负载均衡，双机热备)； 5. 熟练掌握服务器架设、局域网架设及维护； 6. 对服务器的数据进行日常备案和灾难性恢复； 7. 熟悉 web 系统的安全管理和优化，熟悉网络知识，掌握网络安全维护知识，对 web 安全熟悉； 8. 熟悉各种黑客防范措施，熟悉开源软件的安装配置以及功能方面的应用； 9. 任职资格负责公司网络终端的安全管理维护； 10. 负责公司网络安全体系建设、系统安全评估与加固。	1. 具备选择适当技术的规划设计能力； 2. 掌握 WINDOWS、LINUX 操作系统的管理与应用； 3. 掌握 WINDOWS、LINUX 操作系统安全防护设置； 4. 掌握路由与交换技术； 5. 具有 ISP 选择与管理能力； 6. 能够根据应用需求，制订及实施网络安全解决方案； 7. 能够根据应用需求，对主流厂商的网络设备和安全产品的功能、参数、安全特性进行合理选型； 8. 能够对网络安全方案进行实施与检测； 9. 能够按应用需求，进行安全角色与权限的划分与管理； 10. 能够利用工具对信息系统进行初步的安全评估； 11. 熟悉主要操作系统平台的安全管理方法； 12. 具有分析网络结构、排查网络线路故障能力； 13. 掌握故障诊断、分析、隔离、排除的一般方法、流程 14. 熟练使用安全测试、网络抓包工具、协议分析工具 15. 熟练操作主流网管工具； 16. 能够对操作系统平台、网络应用服务进行渗透检测； 17. 能够对主要的应用服务进行加固处理； 18. 能够进行关键业务数据安全维护。
6	安全	1. 安全设备的集成、上架测试	1. 掌握路由与交换技术；

序号	任务领域	典型工作任务	职业需求技能
	设备运维（调试）工程师	等； 2. 安全设备日常维护和安全分析，制定和实施安全措施； 3. 对安全事件进行备案记录； 4. 对系统作安全合规审计，形成运维报告； 5. 建立安全设备运维文档、完成安全运维报告。	2. 能进行内外网分段安全测试； 3. 熟悉市场上的各类型主流安全产品特性及功能应用情况； 4. 会调试防火墙、UTM、VPN、IDS、审计认证等安全设备； 5. 了解安全产品中 IPV6 技术； 6. 熟悉安全产品的高级配置与部署，如分布式出口部署、高可用性 HA 部署等； 7. 熟悉安防系统功能和构成，如监控、门禁、防盗等系统的配置使用； 8. 学会基本的的功能测试与分析； 9. 具备选择适当技术的规划设计能力； 10. 够按应用需求，进行安全角色与权限的划分与管理。

2. 培养目标分析

信息安全与管理人才应具备的能力来看，企业最看重的信息安全技术应用专业毕业生的三项综合能力，依次为专业核心能力、职业技术能力和职业拓展能力。信息安全技术应用从业人员必须具备这些综合能力才能适应现代企业的要求。

通过对调研情况分析，我们归纳出适应上海经济社会发展需要的信息安全技术应用专业人才规格应为：

●素质要求：坚定的政治立场，拥护党的领导和社会主义制度；崇高的道德品质，崇尚宪法、遵法守纪，具有社会责任感与参与意识；强烈的职业素养，崇德向善、诚实守信，爱岗敬业，精益求精；全面的实践能力，尊重并热爱劳动，勇于奋斗、乐观向上；良好的团队协作精神，勇于探索和创新，具备健康的体魄和健全的人格。

●能力要求：具备网络安全设备的配置与维护能力，网络系统信息安全管理能力，信息安全系统的集成和维护能力，网络安全防护能力等专业核心能力；具备中小型企业网络组建与维护能力，测试设备、测试工具的使用能力，网络数据分析能力，网络线路故障的排查能力，应用服务安全检测、评估和加固能力，网络安全产品销售与服务能力，专业英语能力等职业技术能力；具备沟通合作能力，快速跟踪网络新技术能力，信息收集与吸收能力，可持续发展的终身学习能力等职业拓展能力。

●知识要求：具备安全检测知识，渗透测试知识，网络攻防技术，应用服务器加固知识，信息安全法律法规知识等安全检测与评估模块知识；具备计算机系统知识，组网知识，路由与交换技术，无线网络技术，网络安全设备知识等网络设备安全管理模块知识；具备网络管理知识，信息系统安全管理知识，WEB 服务安全，网络安全防护技术，网络安全方案设计知识等网络服务安全管理模块知识；具备网页制作技术，数据库安全知识，WEB 应用开发，网

站维护知识等 WEB 应用开发模块知识。

信息安全技术应用人才的需求规格,信息安全技术应用人才的培养目标应确定为:培养适应上海经济结构调整、产业结构提升、发展方式转变、智慧城市建设推进需要的,德、技、智、体、美全面发展的,具备良好的职业道德和职业素养,具有良好的综合素质和创新能力,熟悉安全等级保护和国家信息安全相关法律法规,具有扎实的网络技术和信息安全技术应用专业基础,掌握网络安全管理技能,有很强的实际操作能力、有较强的英语功底的,“能组网布线、能管理维护、能检测评估、能攻防加固、能开发设计、能沟通合作、能持续发展”的“七能”型应用性信息安全技术应用高级技能人才。

(三) 教学情况及存在的主要问题

本专业培养思想政治坚定、德技并修、全面发展,具有一定的科学文化水平、良好的职业道德和工匠精神,熟悉安全等级保护和国家信息安全相关法律法规,掌握主流的安全技术、具备熟练操作网络安全管理工具、会进行信息系统安全设计和组建、会安全配置应用系统平台、配置网络安全设备、能对信息系统进行日常安全检测、渗透测试和安全运维等专业技术技能。在企业和事业单位、网络集成公司、网络设备厂商、安全设备厂商处从事信息系统安全测评、信息系统安全规划实施、信息系统安全运维管理等工作的高素质技术技能人才。然而,由于本专业课程涉及计算机技术、通信技术、网络技术、信息安全技术、数学、法律、密码学、管理等多门学科,理论与实际又联系紧密,新概念、新方法、新技术以及新问题层出不穷,所以在教学中存在着如下问题。

1、教学方面

教学方法存在局限性,传统的教学方式采用以教师讲授为主。这种重课堂教学,轻实验和实践教学的方式,学生只能被接受知识,无法参与其中,因此学生对课程知识难以理解和掌握,无法融会贯通,从而缺乏学习的积极性。这种教学方法与现代教育教学手段不相适应,不利于培养学生的独立思考能力和创新力。

2、教学模式方面

以网络安全原理为主的理论教学,这是大多数网络安全技术教材的编写风格。但是,这种“从概念到概念”的传统教学模式不适用于学生对网络安全技术课程知识的理解和掌握。

3、实验环节

一方面局限于学校实验室缺乏网络安全技术实验教学环境,缺乏为学生提供模拟真实攻防环境的实验平台,另一方面是部分教师缺乏网络安全实践经验。因此课程大部分实验均以演示为主,学生亲自动手实践少。这就使得许多新技术、新方法、新工具无法通过实验验证,不利于学生提高对新技术、新方法、新工具的认知、体验和掌握。

4、考核方面

以往的考核方式主要由卷面成绩和平时成绩两部分组成,所以容易给学生一种错觉认为只要考试时记住课本的概念、技术、原理和方法等理论知识就行。所以,学得好的学生在考试中不一定及格或取得高分,相反,那些平时并不上课或上课时不听教师讲课的学生有可能

取得高分。因此,传统的考核方法无法全面地反映出学生的学习水平和动手能力。

四、专业人才培养方案优化建议

（一）专业岗位优化建议

根据调研中对信息安全技术应用专业的深入了解,将本专业第一培养岗位基本定位于 Web 安全工程师,网络安全系统集成工程师等。Web 安全工程师是信息安全领域的重要职位,它负责对公司网站、业务系统进行安全评估测试;对公司各类系统进行安全加固;对公司安全事件进行响应,清理后门,根据日志分析攻击途径;安全技术研究,包括安全防范技术,黑客技术等;跟踪最新漏洞信息,进行业务产品的安全检查。通过用人单位反馈,高职学生在这个安全服务岗位的胜任度最高。

网络安全是万物互联时代的基石。近些年,国家非常重视网络安全人才的培养,《网络安全法》第二十条要求:“国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训,采取多种方式培养网络安全人才,促进网络安全人才交流。”根据对现有专业人才岗位需求的了解,本专业将第二岗位地位于网络安全系统集成工程师,具备扎实的计算机与网络原理知识,熟悉各类网络与安全设备(路由、交换、防火墙、VPN、漏洞扫描);对网络数据包具备分析实践能力,熟练使用数据包分析工具;熟悉常见网络通信协议(TCP/IP、交换路由协议、VPN 协议等);熟悉防火墙原理,能够熟练配置防火墙策略;熟悉主流网络与安全厂商产品(思科/华为)。

对专业人才的培养上,专业人才岗位还可以增加 web 安全等级保护测评师相关岗位培养,本岗位的要求是了解主流网络设备、安全设备、操作系统、数据库的安装与调试;熟悉防火墙、VPN、CA、入侵检测、网络攻击、系统加固、黑客攻防等安全技术;熟悉国内外网络、安全界发展现状;了解各类网络、安全产品、各主流厂家产品的技术优劣势;熟悉信息安全等级保护、27001 信息安全体系、ITIL 等相关标准、法律法规等;掌握各类开源的安全漏洞检测扫描、安全防范、安全渗透测试、安全审计及信息管理工作,熟悉主流的 Web 安全技术,熟悉常见攻击和防御办法,自行进行 web 渗透测试,恶意代码监测和分析;具有 CCIE、CISP 或者 CISSP 资质等。

数据安全工程技术人员:该职业与数据安全人才新需求较为匹配,建议在原有基本类安全运维管理的基础上增加数据安全分级分类及合规流程管理类的内容。近年,由国家网信部门牵头管理并推行数据安全分级分类及评估认证工作,对于用人企业来说相应的用人需求逐步显现在可选增信息安全相关的资质证书考试考证,如 CCRC,1+X 网络安全运维职业技能等级证书,人社部信息测试安全员证书等。

通过调研发现,工控安全领域为信息安全领域的子分支,是信息安全的新兴领域。工控安全领域的安全工程师,不但需要理解工控协议以及工业流程,还需要理解传统信息安全的攻防技术。课程体系应重点面向工控安全领域,向信息安全周边范围进行扩散。工控安全领域的安全工程师,不但需要理解工控协议以及工业流程,还需要理解传统信息安全的攻防技术,对工程师要求非常高。课程力求做到设计一个体系框架,从工控安全入门到精通,都需

要全部进行涉猎。从理论到实践，再到真实环境的实战渗透，循序渐进，培养一个合格的工控安全工程师。

（二）专业课程内容优化建议

根据高职高专应用型人才的培养目标，实施以基础理论知识的应用和实践能力培养的原则，以应用为目的，以“必需、够用”为度，加强针对性和实用性。高职高专学生毕业后主要从事运维等应用型岗位，将《防火墙与VPN技术》内容融入《网络安全产品配置》，针对此类岗位必须具备的职业技能，在CISAW下的网络安全运维包含了比较广的内容，能够让学生了解更多的安全运维相关的整体工作内容，建立安全运维知识方面的体系。

（三）专业教学改革建议

信息安全技术涉及技术领域广泛，新技术发展迅速，新应用领域层出不穷。信息安全技术专业教学团队为培养适应市场需要的信息安全技术人才，结合上海市情，将网络安全、平台安全、WEB应用安全和移动安全作为信息安全技术发展的重点应用领域，提炼信息安全相关岗位的典型工作任务，能力分析，依托网络安全、平台安全、WEB应用安全和移动安全等典型综合性项目，将原来的5门核心课程重构为现在的6门《网络设备安全配置》《Linux服务与安全管理》《WEB应用安全》《网络安全应急响应》《渗透测试》和《数据安全与安全管理》专业核心课程，制定课程标准，强化网络安全产品教学，加强网络安全产品相关课程设置，考虑增加态势感知等内容，并着力打造精品课程资源。《信息安全技术》和《信息安全管理》两门课程的重叠内容较多，可考虑融合。数据安全、网络安全等级保护都有风险评估的技术思维，各个安全方向都通用。

另外强化网络安全产品教学，加强网络安全产品相关课程设置，考虑增加态势感知等内容。部分课程内容相关性较高，考虑做适当合并，优化课时设置。课程开设时间调整：部分专业课程的开设时间，建议根据教学需求，做适当调整。

对现行过程化考核模式存在的问题与不足，可以加大平时成绩的比重在实际教学过程中，要更加注重学生的日常学习和思考、考核方式要激发学生学习的积极性和主动性等。可以采用过程化的考核方式，考核元素可以更加多元化。如：学生的出勤率、课堂提问、平时课堂的积极参与情况、作业等加入考核。考核内容要以实际问题为导向防止学生只停留在对课程知识点的死记硬背上，同时也利于教师能采用更多更灵活的考核方式。

（四）专业师资与实训条件配置建议

信息技术应用创新发展是目前的一项国家战略，也是当今形势下国家经济发展的新动能。发展信创是为了解决本质安全的问题。信创产业发展已经成为经济数字化转型、提升产业链发展的关键，从技术体系引进、强化产业基础、加强保障能力等方面着手，促进信创产业在本地落地生根，带动传统IT信息产业转型升级，构建区域级产业聚集集群。信创实验室的建设很有必要。可将一些专业核心课程《Linux服务与安全管理》《网络设备安全配置》融合进去，让学生提前掌握一下信创的操作系统等知识。

信息安全人才被要求攻防兼备，非常考验人才的实操技术。近二十年来，各大高职院校

均在致力提高“双师型”教师的比例和教学水平,不断改善实验实训室条件。“双师型”教师兼备了扎实的专业理论知识和卓越的专业实践能力。根据高职教师不同的发展需求,通过学历学位提升、专业技术培训、科技创新与技术平台服务、企业参与实际项目等方式,鼓励专业教师开展合作开发、参与技术革新,提升教师的专业实践能力。在培养“双师型”教师队伍的基础上,鼓励教师参与指导“1+X 网络安全应急响应”;为加强“产、学、研”交流,开拓教师的实践空间,鼓励教师开展与企业生产一线相关的技术研发和工艺改进,鼓励教师参与行业技术职务的评审。要求任课教师必须具有相关资格证书,鼓励教师考取相关职业资格证书,提高教师的实践和理论水平。为了培养符合企业需求的技能型人才,加强校企合作的深度与广度,积极引导企业参与职业院校的教育教学改革。在企业内建设校外实践教学基地,在校内共建实训室或工作室,将企业岗位技能要求提炼出知识点,企业行业专家参与学校的专业规划、课程设置和教学内容的开发,校企共同开发教材及其他教学资源,每年安排教师下企业参与工程实践,将企业岗位的技能需求融入人才培养环节。

密码技术应用专业人才培养方案

一、专业名称及代码

专业名称：密码技术应用

专业代码：510216

二、入学要求

普通高中毕业生、中等职业学校毕业生或具备同等学力人员。

三、修业年限

三年

四、职业面向

密码技术应用专业的职业面向见表 1 所示。

表 1 职业面向表

所属 专业大	所属 专业	对应 行业	主要 职业类别	主要岗位类别 (或技术领域)	职业资格证书或 技能等级证书举例
电子信息 大类 51	计算 机类 5102	软件和 信息技 术服务 业 65	密码技术应用员 (4-07-05-06) 网络与信息安全 管理员 (4-04-04-02)	密码产品部署 与运维 商用密码应用 安全性评估 网络与信息安 全管理 渗透测试	密码技术应用员职业资格等级证书 密码测评工程师 1+X 网络安全应急响应职业技能等 级证书 网络与信息安全管理员职业资格等 级证书 华为 HCIA-安全

五、培养目标与培养规格

(一) 培养目标

本专业培养理想信念坚定，德、智、体、美、劳全面发展，具有一定的科学文化水平，良好的人文素养、职业道德和创新意识，精益求精的工匠精神，较强的就业能力和可持续发展的能力；掌握本专业知识和技术技能，面向互联网和信息服务业的密码技术应用员、网络与信息安全管理员，能够从事密码产品部署与运维、密码管理、密码测评、渗透测试等工作的高素质技术技能人才。

(二) 培养规格

1. 素质

坚定拥护中国共产党领导和我国社会主义制度，在习近平新时代中国特色社会主义思想指引下，践行社会主义核心价值观，具有深厚的爱国情感和中华民族自豪感。

崇尚宪法、遵法守纪、崇德向善、诚实守信、尊重生命、热爱劳动，履行道德准则和行为规范，具有社会责任感和社会参与意识。

具有质量意识、环保意识、安全意识、信息素养、工匠精神、创新思维。

勇于奋斗、乐观向上，具有自我管理能力、职业生涯规划的意识，有较强的集体意识和团队合作精神。

具有健康的体魄、心理和健全的人格，掌握基本运动知识和 1-2 项运动技能，养成良好的健身与卫生习惯，以及良好的行为习惯。

具有一定的审美和人文素养，能够形成 1-2 项艺术特长或爱好。

具有语言文字应用能力和自觉规范使用国家通用语言文字的意识、自觉传承弘扬中华优秀传统文化的意识，具备一定的文本写作能力。

2. 知识

掌握必备的思想政治理论、科学文化基础知识和中华优秀传统文化知识；

达到英语应用能力 A 级水平、计算机应用达到计算机等级考试一级水平；

熟悉信息安全相关法律法规和标准；

掌握计算机系统、信息系统架构、网络拓扑、信息安全理论与安全技术、网络协议的基础知识；

掌握常用关系型数据库系统的创建、修改、删除、设置、备份、恢复等基本知识；

熟悉密码体系架构、技术标准、规范及相关法律法规；

运用密码技术，从事信息系统安全密码保障的架构设计、系统集成、检测评估、运维管理、密码咨询等相关密码服务的人员；

熟悉当前国内外各种主流的 PKI、防火墙、UTM、VPN、加解密、签名、身份管理、认证授权等安全技术及产品；

了解项目管理工作要点、掌握密码产品部署方法、密码产品安装技术规范相关内容，了解测试基础概念、测试方法、测试工具使用方法、具备一定的报告撰写能力。

初步掌握方案评估技术规范，初步掌握信息系统密码应用调研问卷设计方法，了解测评工具使用方法以及密码设备配置方法，了解测评结果分析方法。

了解密钥管理保障规范、日志审计规范，掌握管理工具安装和设置方法和系统日志管理方法，掌握安全事件处理方法以及执行报告编写方法。

掌握专业文本的撰写规范，包括结构、语言、格式等方面的要求。

3. 能力

具有独立思考、逻辑推理、信息加工能力。

具有语言表达和文字写作能力。

具有终身学习的意识和能力、自我管理能力、与他人合作的能力。

具有创新思维和创新创造能力，动手实践和解决实际问题的能力。

具备组建局域网和实现网络资源共享的能力。

具备对网络操作系统、服务器搭建等工具的使用能力。

具备对网络设备如路由器、交换机的安装、配置和运维的能力。

具备对密码等网络安全产品与设备，如防火墙、VPN、安全网关、密码机等，部署实施和管理运维的能力。

具备微软 Windows 数字身份认证、Kerberos 数字身份认证、PKI 数字身份认证等商用密码认证系统的配置能力。

初步具备依据国家密码相关标准与法规，开展信息系统密码应用安全性评估工作的能力。

初步具备数据管理能力，初步具备能根据应用需求，大数据管理平台和区块链平台搭建和运维能力。

初步具备渗透测试和网络攻防、应急响应的能力。

能够准确理解专业文献、报告、合同等文本。

能够撰写本专业领域的常见应用文本。

六、课程设置

本专业课程主要包括公共基础课程和专业课程。

(一)公共基础课程

公共基础课程包括公共基础必修课程和公共基础选修课程。

1. 公共基础必修课程

公共基础必修课程主要包括：毛泽东思想和中国特色社会主义理论体系概论、思想道德与法治、形势与政策、体育、心理健康教育、计算机应用基础、实用英语、职业生涯规划与职业指导、应用数学、大学生安全教育、军事理论与训练、习近平新时代中国特色社会主义思想概论、互联网+创业实践、大学语文、劳动教育。

表 2 公共基础必修课程介绍

序号	课程	课程学院	主要教学内容与要求	参考学时
1	毛泽东思想和中国特色社会主义理论体系概论	马克思主义学院	内容： 内容：毛泽东思想及其历史地位、新民主主义革命理论、社会主义改造理论、社会主义建设道路初步探索的理论成果、“三个代表”重要思想、习近平新时代中国特色社会主义思想及其历史地位。 要求： 全面认识我国革命、建设和改革的基本国情，了解马克思主义中国化的历史进程和理论成果，理解社会主义本质论、社会主义初级阶段论、社会主义市场经济论等，深入认识和理解中国共产党领导是中国特色社会主义最本质的特征和中国特色社会主义制度的最大优势。	32
2	习近平新时代中国特色社会主义思想	马克思主义学院	内容： 历史方位、鲜明主题、奋斗目标、发展方式、总体布局、战略布局、发展动力、发展保障、安全保障、外部环境、政治保证、	48

	特色社会主义思想概论	院	治国理政世界观方法论、价值观等	
			要求: 教育学生认识中国特色社会主义的新理论形态, 养成严密理论新逻辑。	
3	思想道德修养与法律基础	马克思主义学院	内容: 坚定理想信念、弘扬中国精神、践行社会主义核心价值观、明大德守公德严私德。 要求: 教育学生加强思想道德修养, 继承和弘扬中华传统美德和中国革命道德, 树立为人民服务的思想, 弘扬集体主义精神, 培养良好的道德品质和高尚的道德人格。	48
4	应用数学	公共基础学院	内容: 函数、导数的概念、导数的运算、微分函数的单调性与极值不定积分的概念、不定积分的计算、定积分的概念、定积分的计算、定积分的应用 要求: 熟练掌握函数的基本概念和基本特性、掌握极限的四则运算法则、导数在函数单调性判定上的应用、基本积分公式的应用。注重实用性和职场意识, 培养学生创新能力和自主学习能力。	64
5	实用英语	外语学院	内容: 课堂交流; 介绍、问候、感谢、致谦、道别、指路等日常交际; 阅读与翻译科普、人物、政治、商贸等一般题材的文字材料。 要求: 培养学生实际应用英语的能力, 侧重培养职场环境下语言交际能力, 使学生逐步提高用英语进行交流与沟通的能力, 掌握有效的英语学习方法和策略, 培养学生的英语学习兴趣和自主学习能力, 提高学生的综合文化素养和跨文化交际意识, 为提升学生的就业竞争力及未来的可持续发展打下必要的基础。	128
6	体育与健康	公共基础学院	内容: 体育理论、身体素质、篮球、排球。 要求: 掌握各项动作技能、培养吃苦耐劳, 顽强拼搏的意志品质。	108
7	军事理论与训练	公共基础学院	内容: 中国国防、军事思想、信息化战争、战略环境 要求: 了解我国国防历史和国防建设的现状及其发展趋势, 熟悉国防法规和国防政策的基本内容, 明确我军的性质、任务和军队建设的指导思想, 了解信息化战争的形成、发展趋势和与国防建设的关系, 熟悉信息化战争的特征, 树立打赢信息化战争的信心。了解国际战略格局的现状、特点和发展趋势, 正确认识我国的周边安全环境, 现状和安全策略, 增强国家安全意识。	32
8	职业生涯规划与就业指导	经济与管理学院	内容: 掌握职业生涯设计、职业道德、职场法律、职业礼仪、职业精神、求职申请与面试准备、求职面试技巧、创业规划和实施。 要求: 培养学生通用的职业意识, 提高其可雇用能力。	16
9	大学生安全教育	公共基础学院	内容: 饮食安全、学习安全、交通安全、人身安全、财产安全、网络安全、心理安全、社会实践安全、消防安全、国家安全以及救护知识等。 要求: 养成良好的安全习惯, 提高安全意识, 掌握安全知识和防范技能, 增强自我防范能力。	38
10	形势与政策	马克思主义学院	内容: 根据教育部每学期发布的最新形势与政策课教学要点, 结合学校实际灵活选择相应主题开展教学。 要求: 帮助学生认清国内外形势, 增强学生的爱国主义责任感和使	32

			命感。	
1 1	心理健康 教育	公共基 础学院	内容： 心理保健知识。 要求： 培养创造性思维，训练坚强意志，优化心理品质，培养健全人格，开发心理潜能，促进全面人才。	32
1 2	大学语文	公共基 础学院	内容： 优秀经典文学赏析、职场应用文写作和语言交流表达。 要求： 学语用文，培养学生的高尚审美情操；注重实用性和职场意识，培养学生创新能力和自主学习能力。	32
1 3	劳动教育	学工部	内容： 劳动观点、劳动习惯。 要求： 树立学生正确的劳动观点，培养学生热爱劳动和劳动人民的情感，养成劳动的习惯。	16
1 4	中华优秀 传统文化	公共基 础学院	内容： 涵盖中华优秀思想、文学、艺术、科技、民俗等。通过讲授和体悟中国传统文化，提高学生人文素养，传承中国民族精神，弘扬优秀传统文化。 要求： 讲授中国传统文化，提高学生人文素养，传承中国民族精神，弘扬优秀传统文化。	32
1 5	人工智能 (AGI)技 术应用	通信与 信息工 程学院	内容： 大语言模型原理、现有主流大语言模型平台介绍，大语言模型应用案例 要求： 会用现在主流大语言模型生成相关内容和应用程序。	32
1 6	元宇宙技 术与应用	设计与 艺术学 院	内容： 元宇宙基本概念和发展历程，相关基本技术知识和应用场景 要求： 了解元宇宙的内涵，熟悉基本技术知识及其应用，掌握元宇宙的发展趋势，启发学生关于元宇宙的思考和探索。	32
1 7	信息技术	通信与 信息工 程学院	内容： 课程主要介绍人工智能相关概念，通过各种学习工具讲解机器学习等相关知识，结合大量的案例讲解人工智能技术在现实生活中的应用，通过对人工智能现状的深入剖析，展望人工智能的发展方向与未来。包括人工智能发展历史、人工智能基本概念、机器学习、计算机视觉、自然语言处理、人工智能应用、人工智能未来发展。 要求： 理解人工智能的基本概念和原理；掌握人工智能的关键技术并了解它们在各个领域的应用；关注人工智能在法律、伦理和道德方面的问题，培养批判性思维能力；了解我国在人工智能领域的成就和贡献，树立文化自信。	32
1 8	互联网+ 创业实践	经济与 管理学 院	内容： 创新创业、互联网+创业本质、互联网+商业模式、创业机会识别与开发、互联网创业团队、产品设计与开发、市场运营、互联网创业企业的股权结构设计、互联网创业企业融资、创业孵化、商业计划书撰写和路演、中国国际大学生创新大赛等内容。 要求： 学生具备互联网创业的基本素养，了解互联网创业的流程等相关知识，掌握互联网创业的方法，为学生未来的创业之路提供有力的支持。	32

2. 公共基础选修课程

公共基础选修课程主要包括公共艺术选修课和公共通识选修课，具体课程按照学校实际情况实施。

(二) 专业课程

专业课程包括专业必修课程和专业选修课程。

1. 专业必修课程

包含专业基础课程和专业核心课程。

(1) 专业基础课程：包含计算机网络技术、C 语言程序设计、计算机系统配置、工程数学、密码学数学基础、Python 程序设计、Linux 服务安全管理实训、参观讲座、信息安全技术、网络安全防护项目实训、商用密码产品及其部署运维、网络安全标准与法律法规、职业技能考证。

(2) 专业核心课程：包含 Linux 服务与安全管理、网络设备安全配置、密码技术、大数据安全技术应用、数字身份认证、区块链技术应用、岗位实习 1、岗位实习 2 等。课程名前带有★标识。

2. 专业选修课

专业选修课程包括数据库安全管理、大数据平台安全管理、Web 应用开发、大数据安全与隐私保护、渗透测试、Web 应用安全、商用密码应用安全性评估、安全检测与评估。其中数据库安全管理、大数据平台安全管理为二选一，Web 应用开发、大数据安全与隐私保护为二选一，渗透测试、Web 应用安全为二选一，商用密码应用安全性评估、安全检测与评估为二选一。

其中纯实践性教学课程为：计算机系统配置、Linux 服务安全管理实训、网络安全防护项目实训、职业技能考证培训、岗位实习等。

(三) 专业必修课程主要教学内容

1. 主要专业必修课程教学内容如表 3 所示。

表 3 专业必修课程内容

序号	课程名称	主要教学内容与要求	参考学时
1	工程数学	内容：(1) 线性代数：矩阵的概念及其基本性质、矩阵运算、能用矩阵乘法表示线性方程组；了解矩阵行列式的定义，会计算二阶和三阶矩阵的行列式、逆矩阵、矩阵的初等行变换，求解线性方程组。(2) 微分方程的概念，可分离变量的一阶微分方程和一阶线性微分方程、二阶常系数齐次线性微分方程。 要求：理解矩阵的概念，了解零矩阵、单位矩阵、对角矩阵、三角矩阵、对称矩阵及其基本性质。掌握矩阵的运算、能用矩阵乘法表示线性方程组；会计算二阶和三阶矩阵的行列式。掌握矩阵的初等行变换，会求矩阵的秩，了解矩阵可逆的充要条件；能够运用矩阵初等行变换求解线性方程组。理解微分方程的概念，了解微分方程的阶、解、通解、初始条件和特解等概念。掌握可分离变量的一阶微分方程和一阶线性微分方程的解法。 掌握二阶常系数齐次线性微分方程的解法。会建立微分方程模型解决简单的实际问题。	32

序号	课程名称	主要教学内容与要求	参考学时
2	网络安全标准与法律法规	内容: 结合典型案例, 国内外信息安全标准和法律法规的背景知识、发展状况, 讲授网络安全法律法规的基本知识, 帮助学生树立信息安全法律意识, 从而在今后实际工作中加以遵守和运用。 要求: 通过该课程的学习, 使学生具有基本的信息安全常识和安全理念, 提高信息安全意识, 对国内外信息安全标准及法律法规有一个较为全面的了解, 掌握信息法律法规的基本知识, 在今后从事信息安全管理等实际工作中加以遵守和运用。	32
3	计算机网络技术	内容: 计算机网络和互联网、家庭网络 (SOHO) 的组建、小型办公室局域网的组建、网络的互联、IP 编址、对 IP 网络划分子网、传输层、应用层、无线网络和移动网络、广域网与宽带接入技术、中小型网络安全攻防。 要求: 通过课程学习, 目的在于使学生了解计算机网络概述、数据通信基础、物理层、数据链路层、计算机局域网、网络层、传输层、应用层及网络规划设计等相关知识, 具备相应实践的理论基础。	64
4	C 语言程序设计	内容: C 语言概述、数据类型、运算符和表达式、数据的输入和输出、选择结构、循环结构、数组、函数、指针、结构体、共用体、枚举与链表, 以及文件操作。 要求: 通过课程学习, 目的在于使学生了解 C 语言程序设计的一些常规算法和功能程序设计方法, 掌握使用 C 语言进行系统程序设计的相关知识和程序设计技巧, 以及通过 C 语言让学生掌握计算机系统程序设计基本原理。	64
5	密码学数学基础	内容: 介绍现代密码学相关的数学基本概念, 主要是数论和有限域理论, 包括整除、同余、同余式、平方剩余、原根与指数、群环域。 要求: 通过课程学习, 目的在于使学生了解现代密码学, 尤其是公钥密码涉及的基础理论和实用算法, 如 RSA、ElGamma 等算法数学理论基础。	48
6	Linux 服务与安全管理★	要求: 学生能够进行日常企业工作中的 Linux 系统安全防护管理工作。对系统安全有一个整体的认识, 全方位、立体化的综合掌握系统平台安全管理知识。 内容: 服务器的安全管理、保障数据传输安全、架设 CA 服务器; 能对 Web、FTP 服务器进行安全维护, 架设 SSL 网站; PKI 公钥基础架构基础知识, 申请与签发证书; 邮件的数字签名与加密; 使用网络管理工具等。	64
7	Python 程序设计	内容: Python 开发环境、Python 变量类型运算符与表达式、Python 程序控制结构、列表与元组、字典与集合、函数定义使用、Python 数据分析基础、Python 数据可视化等。 要求: 让学生通过课程学习掌握 Python 语言基础, 程序流程控制, 常用内置数据类型, 组合数据类型, 输入、输出和文件, 错误和异常处理, 函数和函	64

序号	课程名称	主要教学内容与要求	参考学时
		数式编程，面向对象的程序设计，模块和 模块化程序设计，数据结构与算法基础，图形用户界面，图形绘制和数据可视化，数值日期和时间处理，字符串和文本处理，数据库访问，网络编程和通信，并行计算，系统管理以及 Python 计算生态。	
8	网络设备安全配置★	要求:使学生能够熟练运用各种网络安全技术,掌握各种网络设备的安全配置方法, 并能根据实际应用需求进行网络安全策略的设计, 实施和检测。 内容: 网络风险分析、网络设备的管理安全、AAA 认证授权审计、二层交换安全、IOS 防火墙技术、IPS、加密技术和 IPSEC VPN 技术。将华为安全认证的内容融入课程。	64
9	密码技术★	内容: 密码学基础、古典密码、对称密码体制、非对称密码体制、HASH 函数和消息认证、数字签名、流密码以及密码学的新进展。初步掌握密码管理、密码测评技术等。 要求: 通过课程学习, 要求学生掌握密码技术相关的古典密码、对称密码、非对称密码等加密算法; 掌握认证等典型的算法, 熟悉几种典型的数字签名方案等。了解现有的商用密码技术等, 着重培养现代密码学方面的工程应用技能。	64
10	信息安全技术	内容: 信息安全的基本概念、物理安全与风险评估、黑客攻击与防范、加密技术及其应用、网络安全、系统安全、应用安全的解决方案等。 要求: 了解信息安全技术基本概念、发展现状及趋势, 掌握企事业单位信息安全安全管理的主要内容、技术、方法等, 初步掌握加密技术、黑客攻击与防范的技术、网络安全设备等。	48
11	数字身份证书★	内容: 数字身份认证的概念和相关密码学基础, 数字身份认证在网络安全、隐私保护及信任建立中的作用, 数字身份认证的主要类型(如密码认证、生物识别、公钥基础设施等)以及认证技术的原理、方法和应用场景, 数字身份认证协议的基本原理(如挑战-响应协议、零知识证明等), 数字身份认证系统所提供的服务功能(如身份验证、访问控制、数据完整性保护等), 不同场景下数字身份认证体系的选择、应用和实践案例。 要求: 通过课程学习, 使学生全面了解数字身份认证的概念、原理和技术方法。掌握数字身份认证的主要技术和应用场景, 能够根据实际需求选择合适的数字身份认证方案。理解数字身份认证的安全性和隐私保护问题, 具备分析数字身份认证体系安全性的能力。培养学生的实践能力和创新能力, 能够运用所学知识解决实际问题 and 设计新的数字身份认证方案。提高学生的团队协作和沟通能力, 能够在团队中有效地进行数字身份认证系统的设计、开发和维护工作。	64
12	大数据安全技术应	内容: 搭建网络流量大数据平台、网络流量数据采集、网络流量数据预处理、	

序号	课程名称	主要教学内容与要求	参考学时
	用★	网络流量威胁主要类型、网络流量威胁大数据检测模型、网络流量威胁大数据分析实例、网络流量威胁可视化等 7 个模块。 要求：掌握大数据处理技术在网络威胁流量分析中的应用步骤和方法，拓展学生大数据技术综合应用的能力。	64
13	区块链技术应用★	内容：区块链的概念、知识体系、应用场景及典型区块链技术架构。 要求：通过课程学习要求学生掌握区块链技术的基本概念与专业术语；区块链的形成的基本原理；区块链现有技术应用领域等。	64
14	数据库安全管理	内容：数据库技术基础，数据库、表的创建与使用，SQL 查询，SQL 编程 基础，视图和索引，存储过程与触发器，数据库的权限管理与安全保护，数据库的备份与恢复。 要求：使学生了解数据库原理，掌握常用的数据库对象及其使用方法，掌握常用 SQL 命令，掌握数据库安全管理的方法。培养学生运用数据库分析和解决实际问题能力，使学生具有一定的数据库编程能力和相当的管理数据库系统的能力。	64
15	商用密码产品及其部署运维	内容：涵盖市场主流国产商用密码产品原理与使用，包括安全网关、加密机、身份验签服务器、时间戳服务器等。 要求：熟悉常用的商用密码产品，根据商用密码应用方案的要求，完成设备的采购、部署、安装、配置、测试和维护等工作；能够处理常见的运维问题和安全事件等。	32

2. 主要纯实践性教学课程教学内容，如表 4 所示。

表 4 纯实践教学课程安排表

序号	课程名称	内容、要求	学期	周数	场地	备注
1	计算机系统配置	内容：从处理器、存储系统、I/O 系统和并行处理系统 4 个方面，介绍了计算机系统结构的概念和计算机系统性能的定量分析和测试方法，提高处理器性能的指令系统优化编码方法、流水线技术和向量处理机，I/O 系统及提高其性能的技术以及存储系统及提高其性能的各种技术。 要求：通过课程学习，要求学生明确计算机系统在实际应用系统中的地位和作用，提出计算机系统配置设计任务说明书。其中包括应用范围、工作负载特征和吞吐量、信息流分析和其他要求。	1	0.5	计算机系统配置实训室	

序号	课程名称	内容、要求	学期	周数	场地	备注
2	linux 服务安全管理实训	内容:网络操作系统中的系统基础管理命令、远程连接服务、DHCP 服务、SAMBA 服务、NFS 服务、DNS 服务、Web 服务、磁盘配额、FTP 服务、邮件服务、MYSQL 数据库、Iptables 与 NAT 服务。 要求: 通过本课程的学习, 使得学生了解并掌握 Linux 桌面应用、Linux 系统管理和服务器管理与维护等工作中的应用技能, 包括 Linux 操作系统的安装、登录及删除, 图形用户界面, 字符界面与文本编辑器, 用户与组群管理, 文件系统与文件管理, Linux 应用程序, 网络配置, 网络服务器配置等。	2	1	开放型信创应用实训室、网络安全虚实结合实训室	
3	网络安全防护项目实训	内容: 防火墙基础配置和安全策略配置, NAT 策略配置, 华为安全认证体系、安全 CIA 模型、分析攻击行为、二层交换安全、三层路由安全、AAA 认证、实施三层的 IPSEC VPN 技术等。 要求: 使学生理解防火墙的工作原理, 掌握防火墙的安全策略配置、NAT 策略配置及 VPN 技术配置、二层交换安全、IPS、加密技术和 IPSEC VPN 技术。使学生获得有关安全问题及挑战和解决方案的知识, 能够对二层和三层的交换和路由等网络设备进行安全特性的配置, 并能进行故障排除, 以保护小型分支机构网络。	3	1	计算机网络互联实训室 (Cisco设备)、密码技术应用实训室	
4	职业技能考证培训	内容: 1+x 网络安全应急响应 (中级、高级) 内容或网络与信息安全管理员、密码技术应用员等人社证书要求内容。 要求: 参考对应证书 (四级) 要求。	4	1	Web应用安全实训室、密码技术应用实训室	
5	岗位实习 1、2	内容: 企业岗位实习 要求: 在企业岗位进行技能训练	5、6	24	校外实践基地	
总计				27.5		

七、教学进度总体安排

(一) 学时安排

密码技术应用专业的教学活动周进程安排表如表 5 所示。

表 5 教学活动周进程安排表

单位：周

学期	入学教育	军训	课堂教学	实训(实验)	实习	考试	毕业设计	机动	假期	总计
第一学期	1	(1)	16	0.5		1		1	4	24
第二学期	0	0	16	1		1		2	8	28
第三学期	0	0	16	1		1		2	4	24
第四学期	0	0	16	1		1		1	8	28
第五学期	0	0	8		8			1	4	24
第六学期	0	0			16			2		20
总计	1	0	74	3.5	24	4	0	9	28	148

(二) 教学进程表

密码技术应用专业的专业教学进程表如表 6 所示。

表 6 专业教学进程表

课程类别	课程分类	课程名称	学分	总学时	考试(考查)	实践学时	各学期周数、学分分配					
							1	2	3	4	5	6
							16	16+2	16+2	16+2	10+8	16
公共基础必修	思想政治类	思想道德与法治	3	48	考试	8		3				
		毛泽东思想和中国特色社会主义理论体系概论	2	32	考试	0		2				
		习近平新时代中国特色社会主义思想概论	3	48	考试	8	3					
		形势与政策 1	0.5	8	考查	0	0.5					
		形势与政策 2	0.5	8	考查	0		0.5				
		形势与政策 3	0.5	8	考查	0			0.5			
		形势与政策 4	0.5	8	考查	0				0.5		
	身体素质类	体育与健康 1	2	32	考查	30	2					
		体育与健康 2	2	32	考查	30		2				
		体育与健康 3	1	22	考查	16			1			
		体育与健康 4	1	22	考查	16				1		
	综合素养类(科学、人文素养)	应用数学	4	64	考试	0	4					
		实用英语 1	3	48	考试	0	3					
		实用英语 2	3	48	考试	0		3				
		实用英语 3	2	32	考试	0			2			
		大学语文	2	32	考查	0		2				

课程类别	课程分类	课程名称	学分	总学时	考试(考查)	实践学时	各学期周数、学分分配					
							1	2	3	4	5	6
							16	16+2	16+2	16+2	10+8	16
		中华优秀传统文化	2	32	考查	0	2					
		信息技术(人工智能基础)	2	32	考查	18		2				
		人工智能(AGI)技术应用	2	32	考查	18	2					
		元宇宙技术与应用	2	32	考查	18		2				
	综合能力类	职业生涯规划与职业指导	1	16	考查	0	1					
		互联网+创业实践	2	32	考查	16	2					
		心理健康教育	2	32	考查	0	2					
		大学生安全教育	2	32	考查	0	*	*	*	2		
		军事理论与训练	2	32	考查	16		2				
		劳动教育	1	16	考查	16					1	
	总计		48	780		210	21.5	18.5	3.5	3.5	1	0
公共基础选修	通识、艺术、传统文化类	公共艺术选修	2	32	考查	0		2, 3, 4				
		公共通识选修	4	64	考查	0		2, 3, 4				
		小计	6	96								
专业必修	专业基础	计算机网络技术	4	64	考试	32	4					
		c 语言程序设计	4	64	考试	32	4					
		计算机系统配置	0.5	16	考查	16	0.5					
		工程数学	2	32	考试	0		2				
		密码学数学基础	3	48	考查	0		3				
		python 程序设计	4	64	考试	32		4				
		linux 服务安全管理实训	1	30	考查	30		1				
		参观讲座	0.5	8	考查	8			0.5			
		信息安全技术	3	48	考查	32			3			
		网络安全防护项目实训	1	30	考查	30			1			
		商用密码产品及其部署运维	2	32	考查	16				2		
		网络安全标准与法律法规	2	32	考查	0				2		

课程类别	课程分类	课程名称	学分	总学时	考试(考查)	实践学时	各学期周数、学分分配					
							1	2	3	4	5	6
							16	16+2	16+2	16+2	10+8	16
		职业技能考证	1	30	考查	30				1		
		小计	28	498	0	178	8.5	10	4.5	5	0	0
	专业核心	linux 服务与安全管理	4	64	考试	32		4				
		网络设备安全配置	4	64	考试	32			4			
		密码技术	4	64	考试	16			4			
		区块链技术应用	4	64	考试	32			4			
		大数据安全技术应用	4	64	考试	32				4		
		数字身份认证	4	64	考试	32				4		
		岗位实习 1	8	240	考查	240					8 周	
		岗位实习 2	16	480	考查	480						16 周
		小计	48	1104		896	0	4	12	8	8	16
专业选修	专业拓展	数据库安全管理	4	64	考查	32			4			
		大数据平台安全管理	4	64	考查	32						
		Web 应用开发	3	48	考查	32			3			
		大数据安全与隐私保护	3	48	考查	32						
		渗透测试	4	64	考查	32			4			
		Web 应用安全	4	64	考查	32						
		商用密码应用安全性评估	3	48	考查	16				3		
		安全检测与评估	3	48	考查	16						
		小计	14	224		112	0	0	7	4	3	0
		合计	144	2702		1396	30	32.5	27	20.5	12	16

八、实施保障

(一) 师资队伍

1. 队伍结构

目前专业专任教师 5 人，高级职称 2 人，中级职称 3 人；博士 2 人，硕士学位及以上 5 人，双师素质教师占比 100%。

2. 专任教师

专任教师应具有高校教师资格；有理想信念、有道德情操、有扎实学识、有仁爱之心；

具有计算机科学与技术、信息安全与管理、密码学、数学等相关专业本科及以上学历；具有扎实的本专业相关理论功底和实践能力；具有较强信息化教学能力，能够开展课程教学改革和科学研究；有每 5 年累计不少于 6 个月的企业实践经历。

3. 专业带头人

校企双专业带头人，1 名校内专业带头人，1 名企业专业带头人。校内专业带头人原则上应具有副高及以上职称，能够较好地把握密码、信息安全行业等领域的专业发展，能广泛联系行业企业，了解行业企业对本专业人才的需求实际，教学设计、专业研究能力强，组织开展教科研工作能力强，在本区域或本领域具有一定的专业影响力。

4. 兼职教师

兼职教师主要从本专业相关的行业企业聘任，具备良好的思想政治素质、职业道德和工匠精神，具有扎实的专业知识和丰富的实际工作经验，具有中级及以上相关专业职称，能担专业课程教学、实习实训指导和学生职业发展规划指导等教学任务。

（二）教学设施

1. 校内实训基地

教学设施能满足本专业人才培养实施需要，其中有关实训条件达到有关专业实训教学条件建设标准（仪器设备配备规范）要求。信息化条件保障能满足专业建设、教学管理、信息化教学、使用数字化教学资源、学生自主学习等的需要，主要实训室如表 7 所示。

表 7 校内主要实训教学条件配置表

序号	实训室名称	主要设备	开设课程
1	网络安全虚实结合实训室	信息安全实训系统、入侵防御课程资源包、日志审计课程资源包、VPN 课程资源包、漏洞扫描课程资源包、终端安全课程资源包、上网行为管理课程资源包 SDN 交换机、二层接入交换机、网络机柜	linux 服务与安全管理、linux 服务安全管理实训、网络安全设备配置、渗透测试、网络安全防护项目实训
2	密码技术应用实训室	密码技术课程资源包、数字身份认证课程资源包、密码实训接入服务器密码机 CRY-001、密码实训密钥管理系统、IPSEC VPN、SSL VPN、签名验签服务器、智能密码钥匙、证书认证系统、时间戳服务器	密码技术、数字身份认证、商用密码产品及其部署运维、商用密码应用安全性评估
3	Web 应用安全实训室	台式计算机、存储设备、服务器、教学实训系统、机柜	数据库安全管理、信息安全技术、计算机网络技术、Web 应用开发、渗透测试、Web 应用安全
4	开放型信创应用实训室	国产计算机、国产服务器服务器 实训室的软件，包括国产办公软件、国产桌面操作系统、国产服务器操作系统、国产数据库等安全专用软件	linux 服务与安全管理、linux 服务安全管理实训、C 语言程序设计、Python 程序设计、职业技能考证培训

序号	实训室名称	主要设备	开设课程
5	计算机网络 互联实训室 (Cisco 设备)	台式计算机、交换机、企业级接入层交换机、企业级汇聚层交换机、企业级核心层交换机、企业级网关、防火墙、网络课程资源系统	网络安全设备配置 网络安全防护项目实训
6	计算机系统 配置实训室	台式计算机	计算机系统配置

2. 校外实习基地

在专业层面，与相关企业建立合作关系，为学生提供充足的校外实习场所。校外实习基地原则上为教师提供企业实践岗位，为学生提供真实企业环境，满足认知性实践、岗位实习和应用与创新三个实践环节的教学需要。主要校外实践基地见表 8。

表 8 主要校外实践基地一览表

序号	实践基地名称	在专业教学中的作用
1	格尔软件股份有限公司	合作建设密码技术应用产教融合实践基地 为认知学习提供参观场所 为学生提供岗位实习岗位； 为专任教师提供企业践习平台
2	上海奇安信科技集团股份有限公司	依托“多主体”的产业学院，在专业建设、人才培养、实习实训等方面产学研深度融合 为学生提供岗位实习岗位； 为认知学习提供参观场所 为专任教师提供企业践习平台
3	智巡密码（上海）检测技术有限公司	为认知学习提供参观场所； 为专任教师提供企业践习平台。
4	上海观源科技有限公司	为认知学习提供参观场所； 为学生提供岗位实习岗位； 为专任教师提供企业践习平台。
5	上海馥欣信息科技有限公司	为认知学习提供参观场所 为学生提供岗位实习岗位； 为专任教师提供企业践习平台。
6	上海豌豆信息技术有限公司	为认知学习提供参观场所； 为学生提供岗位实习岗位；

序号	实践基地名称	在专业教学中的作用
		为专任教师提供企业见习平台。
7	上海仪电物联技术股份有限公司	为认知学习提供参观场所； 为专任教师提供企业见习平台。
8	上海三零卫士信息安全有限公司	为认知学习提供参观场所； 为学生提供岗位实习岗位； 为专任教师提供企业见习平台。
9	上海飒智智能科技有限公司	为认知学习提供参观场所； 为专任教师提供企业见习平台。

（三）教学资源

1. 教材选用基本要求

按照国家规定选用优质教材，禁止不合格的教材进入课堂。学校建立专业教师、行业专家和教研人员等参与的教材选用机构，完善教材选用制度，经过规范程序择优选用教材。

2. 图书文献配备基本要求

图书文献配备满足人才培养、专业建设、教科研等工作的需要，方便师生查询、借阅。专业类图书文献主要包括：密码及网络安全政策法规、行业标准、国家标准、技术规范等；密码技术与引用专业技术类图书和实务案例类图书；3种以上密码技术类专业学术期刊。

3. 数字教学资源配置基本要求

建设、配备与本专业有关的音视频素材、教学课件、数字化教学案例库、数字教材等专业教学资源库，应种类丰富、形式多样、使用便捷、动态更新，能满足教学要求。

（四）教学方法

教师依据专业培养目标、课程教学要求、学生学习基础、教学资源等，采用理实一体化教学、案例教学、项目教学等方法，以达成预期教学目标。坚持学中做、做中学，倡导因材施教、因需施教，鼓励创新教学方法和策略。鼓励信息化技术在教育教学中的应用，改进教学方式。具体要求如下：

贯彻任务引领的教学理念，密切联系密码管理、密码测评工作实际，采用项目教学，注重学生实际操作能力培养，提高学生的学习积极性。

创设与密码技术应用等工作实际贴近的工作情景，以完成工作任务为主线，以学生为主体，以教师为主导，做中学，做中练，充分发挥学生的主观能动性。

通过校企合作，让学生参加到实际的项目开发中，为步入职场做好铺垫。

技能训练围绕职业功能与综合职业能力展开，在以职业功能为模块，开展项目式教学的同时，开展综合实践训练，强化岗位技能与综合职业能力。

充分利用实物、投影仪、多媒体课件等多种教学手段进行辅助教学，帮助学生理解相关

理论知识。

（五）学习评价

1. 以企业用人标准为主要评价标准，包括用人单位对毕业生的综合评价，行业企业对实习顶岗学生的知、能、素评价，社会对专业的认可度评价，学生专业技能认证水平和职业资格通过率的评价等。辅助以兼职教师对学生实践能力的评价，教学督导对教学过程组织实施的评价，教师对教学效果的评价，学生对教学团队教学能力的评价，专业技能竞赛参赛成绩的评价等。

2. 建立多元评价机制，除了教师评价、小组互评、自评外，增加企业评价。

3. 评价内容可包括学生学习态度和职业道德素养、理论知识和实践动手能力、分析解决问题和团队协作能力等综合评价。

4. 评价方式书面与口头相结合、课内与课外相结合、结果与过程相结合，形成终结性评价为主，形成性评价为辅的评价体系。

5. 注重课程评价与职业资格鉴定的衔接。

（六）质量管理

建立健全校院两级，全员、全过程、全方位的质量保障体系。以保障和提高教学质量为目标，运用系统方法，依靠必要的组织结构，统筹考虑影响教学质量的各主要因素，结合教学诊断与改进、质量年报等职业院校自主保证人才培养质量的工作，统筹管理学校各部门、各环节的教学质量管理活动，形成任务、职责、权限明确，相互协调、相互促进的质量管理有机整体。

1. 制度保障

建立健全校院两级，全员、全过程、全方位的质量保障体系。以保障和提高教学质量为目标，运用系统方法，依靠必要的组织结构。修订和完善学校和二级学院的相关管理规范体系：制订（修订）了《教学督导工作规程》、《教学管理规范》、《专业人才培养方案制订（修订）工作规程》、《课程标准制订（修订）指导性意见》、《校本教材建设的若干意见》、《教师教学工作规范》、《教学质量标准》、《教学质量评价实施办法》、《教师工作室管理办法》、《兼职教师对接工作要求（暂行）》、《教学检查制度》、《教师听课制度》、《教学质量信息反馈制度》、《毕业生跟踪调查制度》等。通过上述方方面面的规章制度体系来监管保障教学活动地正规化执行。

2. 质量监控

为确保人才培养质量，学院建立质量监控体系。质量监控包括人才培养目标监控、人才培养方案和教学大纲监控、教学过程监控、学生信息反馈、教材质量监控。

人才培养目标监控。结合行业调研评估，实时调整优化人才培养模式，保障专业人才培养目标顺应时代发展变化。

（2）人才培养方案和教学大纲制订与执行监控。人才培养方案和教学大纲是组织和实施人才培养工作的核心教学文件，也是开展教学工作和对教学工作监控与评估的重要依据。

（3）教学过程监控。通过听课、教学检查、教学督导、学生评教、教师评学、考试等措施进行教学监控。

（4）学生信息反馈。以班级/课程为单位指定信息收集员并建立学生教学信息员制度，并定期召开院系两级学生教学信息交流会议。

（5）教材质量监控。学院建立教材招标工作组，采用教材三级审核制：教研室申报、教学单位审核、教务处审定。

九、毕业要求

学生通过规定年限的学习，修满人才培养方案规定的全部学分准予毕业。

十、附件

附件 1 密码技术应用专业人才需求与专业改革调研报告

附件 2 专业建设指导委员会审定意见

附件 3 学术委员会审批意见

密码技术应用专业人才需求与专业改革调研报告

一、基本思路与方法

（一）调研思路

通过对专业设置背景、密码与网络空间安全产业发展研究调研、论证分析过程，主要从国家战略导向、上海地区战略发展导向、人才培养体系的局限性等方面进行分析，最终得出集中于专业发展方向的改革调研报告。

现代密码学作为保护信息安全的最有效手段和关键技术，随着信息和信息技术的发展逐渐兴起。过去，密码的研制、生产、使用和管理都在封闭的环境中进行。自七十年代以来，随着计算机、通信和信息技术的发展，密码领域发生了新的变化——密码应用范围不断扩大，社会对密码的需求更加迫切，密码研究领域不断拓宽，密码技术得到了前所未有的发展。密码技术不仅具备保护信息机密性的信息加密功能，还具备数字签名、身份验证、秘密分存、系统安全等功能。因此，使用密码技术不仅可以确保信息的机密性，还可以确保信息的完整性和确证性，防止信息被篡改、伪造和假冒。选择一个强壮的加密算法至关重要。此外，安全系统的结构、算法的实现以及通信协议也会影响系统的安全性。

密码技术是保障网络安全的核心技术，密码算法和密码产品的自主可控是确保我国信息安全的重中之重。基础信息网络、重要信息系统、重要工业控制系统和政务信息系统等重要领域的密码应用持续深化，密码技术积极护航 5G、云计算、物联网等新基建的安全发展，商用密码产业发展迅猛。国家“十四五”规划指出：“发展数字经济，推进数字产业化和产业数字化，推动数字经济和实体经济深度融合”，密码作为数字经济的“安全基因”，将迎来全新的发展机遇和挑战。密码技术应用专业方面的人才需求不断增加，能够熟练掌握密码相关技术的专业人才缺口巨大。

（二）调研方法

1. 调研对象

学院走访了上海地区具有代表性的行业企业和省内外高职院校，了解专业建设的需求与内涵。主要选择有代表性的企业、行业组织从事密码技术服务及相关领域的负责人、业务主管、工程技术人员作为走访和调研对象，调研范围涵盖了北京、深圳、重庆、成都以及上海本地的 10 多家企事业单位和 10 余所高校。

2. 调研形式

- ①通过电子邮件、QQ 共享平台等以网络社交方式发送设计好的调研问卷；
- ②通过我院招聘就业平台收集信息；
- ③调研团队成员参加国内外会议了解信息；
- ④组织研讨会、专题交流，邀请行业专家进行访谈；
- ⑤采用问卷调查、电话访谈等方式调查用人单位、从业人员对专业建设的意见建议；

⑥通过网络收集资料，收集行业发展资料、兄弟院校相关专业调研报告等；

⑦查阅行业资讯报告，例如，上海市产业现状分析报告等，密码技术行业报告等。

通过行业调研，我们主要了解了行业现状及未来发展趋势、行业政策与规划、不同层次人才的现状及特点、行业人才需求变化趋势、行业从业人员的职业技能、职业道德和职业素养等方面的信息。

通过企业调研，我们主要了解了企业基本情况、人才需求、校企合作情况、人才培养建议、用工岗位需求、通用能力与职业素养、岗位职业能力与素质要求、职业资格证书和职业技能等级证书等情况。

通过学校调研，我们了解了学校基本情况、师资队伍情况、专业招生情况、专业建设情况、课程设置情况、实验实训条件建设情况、人才培养建议以及校企合作情况等。

通过研究评价机构调研，我们主要了解了发达国家相关专业建设和专业教学设计情况、典型案例、职业教育教学、教法、教改最新研究成果、职业教育人才培养国际比较研究成果以及教学标准与国际接轨的建议等。

通过以上方式获取的各种调查资料进行归类、整理和分析，我们总结形成了如下报告。

二、专业人才需求调研

（一）相关行业发展现状

1. 国家战略导向

根据中国网络安全产业联盟（CCIA）发布的《2023 年中国网络安全市场与企业竞争力分析报告》，网络安全行业在国家层面的发展现状呈现出一系列积极态势和显著特点。以下是对该报告所揭示的网络安全行业国家发展现状的详细分析：

首先，市场规模与增长态势。报告显示，2022 年我国网络安全市场规模约为 633 亿元，同比增长率为 3.1%。近三年行业总体保持增长态势，这反映出网络安全行业在国家政策支持和市场需求双重推动下，呈现出稳健的发展势头。预计未来三年，网络安全市场的增长率将持续超过 10%，到 2025 年市场规模预计将超过 800 亿元。这表明网络安全行业具有巨大的市场潜力和广阔的发展空间。

第二，政策环境与顶层设计。网络安全行业的发展离不开政策环境的支持和顶层设计的完善。近年来，国家陆续出台了多项政策，推动网络安全行业的发展。这些政策包括加强网络安全保障体系和能力建设、开发网络安全技术及相关产品、提升网络安全自主防御能力等方面。这些政策的出台为网络安全行业的发展提供了良好的发展环境和政策保障，推动了行业的快速发展。

第三，头部企业竞争力与市场份额。报告指出，当前我国网络安全市场进入稳健增长阶段，头部企业规模和资源优势进一步凸显，从而获得更大市场份额。一些具有领先技术实力和市场表现的企业在竞争中脱颖而出，成为行业的领军企业。这些企业不仅拥有强大的研发能力和技术实力，还在市场拓展、品牌建设等方面取得了显著成绩，为行业的健康发展起到了积极的推动作用。

第四，行业趋势与发展方向。报告还揭示了网络安全行业的六大发展趋势，包括数字经济、人工智能、数据安全、合规先行、信创加速和服务化转型。这些趋势反映了网络安全行业未来的发展方向和重点。随着数字经济的快速发展和数字化转型的深入推进，网络安全行业将面临更多的机遇和挑战。同时，人工智能、大数据等新技术的应用也将为网络安全行业的发展带来新的动力和可能性。

截止至 2023 年 12 月，我国开展网络安全业务的公司数量呈现显著增长趋势，业务范围也日趋广泛。这主要得益于我国对网络安全的重视程度不断提升，以及数字化、信息化进程的加速推进。在数量方面，我国网络安全企业数量已达到数千家，这些企业涵盖了网络安全设备提供商、安全服务提供商、安全软件开发商等多个领域。这些企业不仅为政府、金融、电信、能源等关键信息基础设施提供了重要的安全保障，还为各行各业的数字化转型提供了有力的支持。

2022 年，《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》等一系列法律法规加速落地，网络安全相关立法继续向体系化、纵深化发展。《网络安全审查办法》《互联网信息服务算法推荐管理规定》《数据出境安全评估办法》颁布实施，在坚定维护网络空间安全的同时，也刺激了网络安全产业的加速发展。同时，人工智能、自动驾驶、元宇宙等新概念、新技术、新业态的兴起与推广对网络安全法律体系建设提出了更高要求，细分领域的立法仍处于“进行时”。

2021 年以来，网络安全领域的执法检查活动更加频繁，执法更加严厉，典型网络安全司法判例和执法案例不断涌现。网络安全审查已逐渐成为我国网络安全生态治理的常态化内容，相关执法实践也越来越成熟。网络安全与数据保护逐渐成为企业必须正视的重大合规问题，刺激了数据合规、安全合规等服务需求，成为网络安全产业新的增长点。

近年来，国际形势变幻莫测，世界经济增长放缓态势明显。但我国经济韧性强、潜力大，长期向好的基本特点没有变。随着一揽子稳增长政策措施落地见效，经济运行有望逐步改善。网络安全产业的整体表现既反映了宏观经济形势，也受到宏观经济环境的影响，需要政府和行业共同努力，探索一条可持续发展之路。

2. 上海地区战略发展导向

《上海市建设网络安全产业创新高地行动计划（2021-2023 年）》提出，通过 3 年培育，基本建成具有全国影响力的网络安全产业创新高地。目标是到 2023 年，上海市网络安全产业规模从 120 亿元提升至 250 亿元，占全国 10%以上，带动相关产业增长 2500 亿元，培育 10 家行业龙头企业。该计划围绕下一代通信、智能治理等前沿领域，可信计算、零信任等新型架构以及云计算、人工智能等新技术与网络安全技术融合，打造包括网络信息安全人才培养和网络安全开放创新在内的五大高地。

“当前我国密码产业前景广阔、大有作为，正处于欣欣向荣的‘蓝海’阶段。”随着《网络安全法》《数据安全法》《个人信息保护法》《中华人民共和国密码法》等法律法规的相继出台，顶层设计激活了国内密码市场的潜力，为密码产业发展增添了关键动力，有效推动

了密码市场的加速形成。

同时，随着密码技术与大数据、人工智能、云计算、物联网等新一代信息技术的深度融合，催生出更加广泛的业务模式和应用场景，使得密码应用需求日趋多样化和个性化。在这样的背景下，开设密码技术应用专业（高职），培养大量具有密码应用技术能力的人才，为各单位的信息安全提供技术保障、岗位规范 and 专业化人才，从根本上解决信息安全整体专业技术水平跟不上国家发展战略需求的问题，从而提高各单位密码应用技术的综合实力已迫在眉睫。

我们需要团结上海及长三角地区从事商用密码业务的企事业单位、研究机构以及专家学者，积极推动商用密码产业发展，不断提升信息安全服务水平，为构建网络空间命运共同体贡献智慧和方案，提供人才储备。

3. 密码与网络空间安全产业发展分析

近年来我国信息产业发展迅速，但缺少自主核心技术的局面没有根本改变。在基础协议和技术标准、操作系统、高性能芯片等方面，尚未掌握产业链和供应链安全的主导权，许多重要领域的核心软硬件产品长期依赖进口。为此，发展自主可控的信息安全技术显得尤为迫切。商用密码是我国自主网络安全技术的典型代表，自主创新历来是商用密码事业发展的灵魂，也是其实现持续健康快速发展的动力源泉。

商用密码在保障网络和信息系统的真实性、机密性、完整性和不可否认性方面发挥着不可替代的重要作用。面对国内外安全环境的深刻变化和经济由高速发展转向高质量发展的双重挑战，尤其在信息产业缺少自主核心技术的条件下，亟需以密码应用为突破口实现“弯道超车”，构建以密码为基石的网络安全与信任体系，维护网络安全新秩序。

商用密码法律法规体系已经基本形成。以《网络安全法》《密码法》《数据安全法》为核心的新时期国家安全法律制度体系，积极推动密码工作在网络强国、数字中国建设中实现跨越式发展。国家在政策法规层面逐步完善现行商用密码管理制度，促进商用密码应用改造，引导商用密码产业健康有序发展。

商用密码标准体系也基本完善。《密码法》明确商用密码标准体系包括国家标准、行业标准、团体标准和企业标准。国家标准由国家标准化管理委员会组织制定，代号为 GB；行业标准由国家密码管理局组织制定，代号为 GM；团体标准由社会团体制定，企业标准由企业制定或企业联合制定。

商用密码产业初具规模，形成了完整的商用密码产品体系。近年来，商用密码产品自主创新能力持续增强，产业支撑能力不断提升，部分产品性能指标已达到国际先进水平。目前，商用密码产品包括密码软件、密码芯片、密码模块、密码板卡、密码整机和密码系统，现有商用密码产品达到 3000 余款，其中 2200 余款取得了商用密码产品认证证书。

商用密码应用领域也基本实现全覆盖。随着云计算、大数据、区块链、数字货币、物联网、车联网、人工智能等新技术的广泛应用，密码技术积极护航新基建安全发展。在金融、能源、惠民、广播电视、政务等多个领域，商用密码技术已得到广泛应用。

此外，上海市在《上海市建设网络安全产业创新高地行动计划（2021-2023 年）》中提出，通过 3 年培育，基本建成具有全国影响力的网络安全产业创新高地。到 2023 年，上海市网络安全产业规模从 120 亿元提升至 250 亿元，占全国 10%以上，带动相关产业增长 2500 亿元，培育 10 家行业龙头企业。行动计划围绕下一代通信、智能治理等前沿领域，推动可信计算、零信任等新型架构以及云计算、人工智能等新技术与网络安全技术融合，打造网络信息安全人才培育和网络安全开放创新等五大高地。

上海高度重视区块链为代表的数字经济发展，推进区块链技术和密码应用的高度融合，激发行业龙头企业对区块链技术的潜在需求，不断释放创新应用新的场景。密码与网络空间安全产业链条的主要企事业单位情况如下：

1) 格尔软件股份有限公司

是中国较早研制和推出公钥基础设施 PKI (Public Key Infrastructure) 平台的厂商之一，是国内首批商用密码产品定点生产与销售单位之一，是国家保密局批准认定的涉及国家秘密的计算机信息系统集成甲级资质单位，是全国信息安全标准化技术委员会的核心成员单位；公司是国家“863”计划信息安全示范工程金融子项目的责任承担单位，是国家科技支撑计划商用密码基础设施（ECC）项目的牵头单位之一；公司两次荣获国家科技进步二等奖，荣获国家密码科技进步奖和上海市科技进步奖；

格尔软件已经拥有一大批技术专利和自主知识产权产品，公司拥有全系列信息安全产品、安全服务和解决方案的提供能力，产品包括：“安全认证网关”、“可信边界安全网关”、“无线安全网关”、“电子签章系统”、“安全电子邮件系统”、“安全即时通系统”、“网络保险箱”、“终端保密系统”、“签名验证服务系统”、“局域网接入认证系统”、“打印管控系统”、“移动安全管理平台”、“云安全服务平台系统”、“移动介质管理系统等产品”。

2) 智巡密码（上海）检测技术有限公司

智巡承担上海市第三方商用密码检测机构培育工作的建设，具备国家商用密码产品检测资质的机构资质和商用密码应用安全性评估试点资质，是 G60 商用密码产业和应用示范基地的核心功能平台，也是上海市商用密码行业协会和长三角 G60 科创走廊智慧安防产业联盟的发起单位。

3) 观源科技是观源（上海）科技有限

观源科技是以密码技术为核心的数据安全产品及解决方案提供商。公司聚焦商用密码、隐私计算、区块链等技术在芯片安全、移动安全、应用安全、数据安全、云安全、安全管理等方面的创新应用，致力于以“密码创新，推动安全数字未来”。公司先后参与并完成了国家 973 课题、国家自然科学基金、国家重大专项课题、国家发改委专项、工信部专项和上海市科技创新计划等多个纵向科研任务，并荣获 2017 年国家科技进步二等奖。

4) 上海信息安全测评认证中心

上海市信息安全测评认证中心是专门从事信息技术产品、信息系统安全测评的第三方专

业机构，是国内最早开展信息安全测评的机构之一。上海测评中心创建了国内独有的“一个测评平台、资源共享、多方授权、服务各方”的上海测评模式，是最早通过中国合格评定国家认可委员会（CNAS）的检测实验室认可（L0754）及检查机构认可（IB0039）的机构之一，并获得了国家保密局涉密信息系统安全保密测评中心等部门的业务授权，是国家认监委对13种信息安全产品强制性认证的全国首批七家指定检测实验室之一。同时，上海测评中心是上海唯一一家公共信息系统安全测评机构；是经公安部能力评估、上海市公安局（市等保办）指定的本地信息系统等级保护测评机构；是上海市密码管理局指定的本地商用密码系统安全检测机构。

5) 上海市数字证书认证中心有限公司

1998年，上海市数字证书认证中心有限公司（简称上海CA）由中央密码工作领导小组批准试点，上海市政府批准成立。上海市数字证书认证中心有限公司率先通过国际Web Trust认证，并实现主流操作系统和浏览器根信任、Adobe根信任，先后通过CMMI3认证、ISO9001认证、ISO27001认证。作为依法设立的第三方电子认证服务机构，上海CA遵照《中华人民共和国电子签名法》的要求和相关政策法规，为政府、企事业单位、个人等提供第三方电子认证服务、数字身份相关产品和集成实施服务，客户涉及政府公共服务、招投标、医疗卫生、金融、电信、电子商务、房地产、制造业、物流业、流通业等83个细分行业。

6) 上海馥欣信息科技有限公司

从事密码技术服务、技术开发、技术咨询、技术交流、技术转让、技术推广；信息系统集成服务；信息咨询服务（不含许可类信息咨询服务）；大数据服务；互联网数据服务；计算机软硬件及辅助设备批发；软件开发；会议及展览服务；企业管理咨询。

7) 上海豌豆信息技术有限公司

从事计算机技术、通信技术领域的技术开发、技术转让、技术咨询、技术服务，网络科技，网络工程，计算机系统集成，电子商务（不得从事金融业务），计算机硬件及辅助设备、电子产品、通信设备及相关产品、数码产品的销售，自有设备租赁，商务信息咨询，计算机软件开发、制作、销售。

8) 上海三零卫士信息技术有限公司

是中国电子科技网络信息安全有限公司旗下专业从事网络安全服务的高新技术企业，总部设在上海，在北京、成都、广州、杭州、武汉等地设有分支机构。公司重点聚焦党政机关、医卫、教育、能源、军工、金融、交通等行业，为客户提供基于信息系统全生命周期的网络信息安全服务，形成了网络安全服务、工业互联网安全、信用与大数据、互联网情报四大核心业务，已成为国内网络空间安全领鲜明域具有特色的综合性网络安全服务提供商。

（二）行业从业人员基本情况

1. 工作岗位

密码应用技术专业人才就业领域主要面向密码技术应用、密码应用安全测评、信息安全工程管理等技术领域。主要工作能力需求如下：

(1) 分析信息系统业务应用场景密码应用需求的能力：能够根据业务场景的具体需求，准确分析和识别需要使用密码技术的地方，确保信息系统的安全性。

(2) 依据业务需求合理选择密码技术及产品的能力：根据实际业务需求，选择适合的信息系统的密码技术和产品，确保密码技术与业务需求的匹配。

(3) 对信息系统的密码资源进行融合部署实施的能力：具备将不同的密码资源进行有效融合和部署的能力，确保信息系统中密码资源的高效应用。

(4) 对信息系统密码资源及应用进行运维管理的能力：能够对已部署的密码资源进行日常运维和管理，确保系统持续、安全、稳定运行。

(5) 依据国家密码相关标准与法规开展信息系统密码应用安全性评估工作的能力：熟悉并能依据国家相关标准与法规，对信息系统中的密码应用进行安全性评估，确保符合国家规范。

(6) 应急处置密码应用安全突发事件的能力：具备处理和应对密码应用过程中可能出现的安全突发事件的能力，保障信息系统的安全。

(7) 开展密码应用技术咨询、密码科普等相关服务的能力：能够提供专业的密码应用技术咨询和培训服务，并能进行相关的科普教育，提高公众的密码应用意识和知识水平。

(8) 信息技术和数字技术的应用能力：掌握并能够应用信息技术和数字技术，支持密码技术的有效实施。

(9) 探究学习、终身学习和可持续发展的能力：具有持续学习和发展的意识和能力，能够不断更新知识，适应技术的发展和变化。

通过这些能力的培养，毕业生能够在密码技术应用、信息安全管理等领域获得广泛的就业机会，满足行业对高素质密码技术应用人才的需求。

(1) 网络安全从业人员最高学历：国内网络安全人才培养的主要途径是学历教育，包括高等院校的网络空间安全相关专业及职业院校的信息安全管理专业及其他 IT 相关专业。从网络安全人才的学历情况统计结果看，本科学历最多，占比为 40%，大专及以下占比为 15%，硕士以上占比有所提高，为 45%。

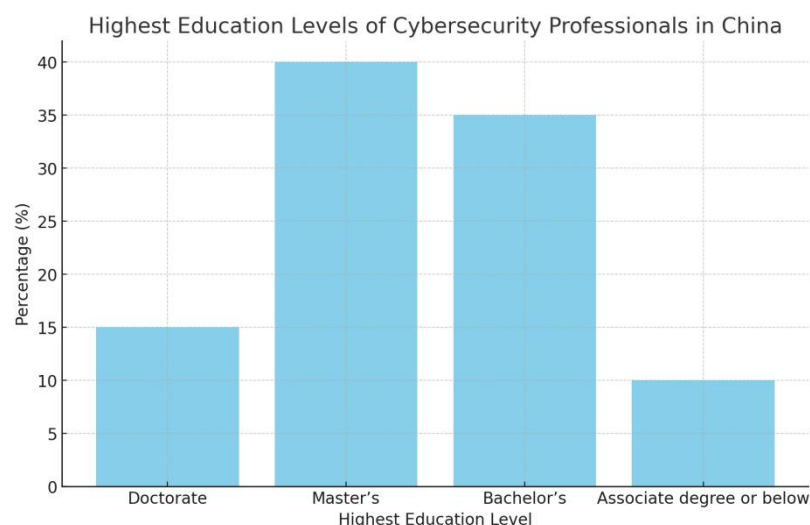


图 1 受访者最高学历分布

(2) 根据猎聘网和安恒信息提供的数据来看，网络安全从业人员中，毕业于以下高校的人才比例排名前五：

- 1) 北京邮电大学，占总数的 2.26%
- 2) 西安电子科技大学
- 3) 上海交通大学
- 4) 电子科技大学
- 5) 北京航空航天大学

今年，浙江工业大学和南阳理工学院也加入了前 50 名的行列。

(3) 网络安全从业人员从业年限：调查显示，工龄五年以下的占比最高，达到了 40%，而十五年以上的从业人员比例最少，为 9.51%。另外，工龄五年以下的共占比四成以上，这足以说明网络安全行业的新人正在逐渐增多，和最近几年国家的重视、行业的发展呈正相关。

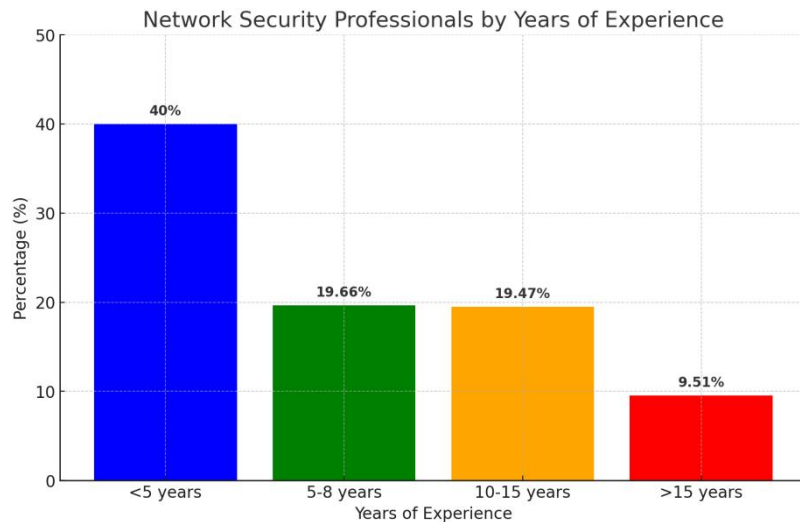


图 2 受访者从业年限分布图

2. 网络安全从业人员从事行业分布

数据显示，在通信和电子行业从业的网络安全人员占比最高，为 33.14%；其次是 IT 和互联网行业，占比 27.46%；制造业占比 22.49%。这些比例反映了网络安全从业人员在各个行业中的分布情况，以及工业企业数字化转型升级对制造业网络安全需求的推动。

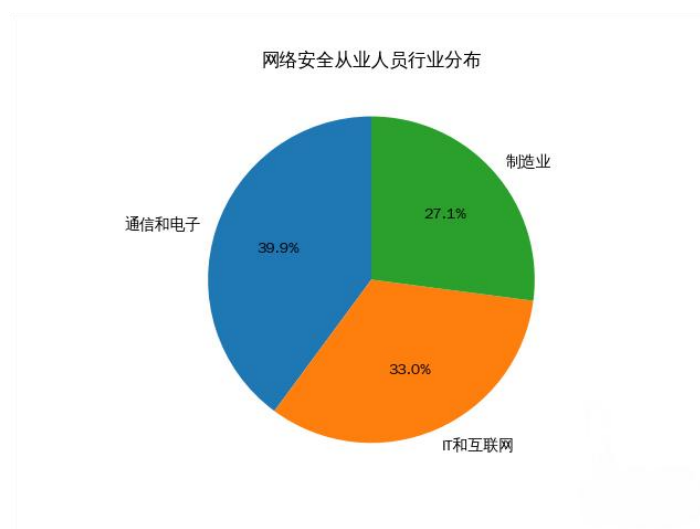


图 3 网络安全从业人员从事行业分布

3. 网络安全从业人员择业首要因素

网络安全从业人员择业的首要因素主要包括以下几点：

专业对口：在选择行业时，从业人员往往更倾向于选择与自己所学专业对口的岗位。这不仅有利于发挥他们的专业知识和技能，也有助于他们更快地适应工作环境和提升工作效率。根据最新的调研数据，专业对口在择业影响因素中占比较大，约为 30.3%。

薪资待遇：薪资待遇是网络安全从业人员择业时考虑的另一个重要因素。良好的薪资待遇可以激励员工更积极地投入工作，并提升他们的工作满意度。在调研中，有 28.17%的从业人员表示薪资待遇对他们的择业选择有重要影响。

兴趣驱动：尽管兴趣并未直接体现在调研数据中，但根据以往经验，兴趣对专业选择有着极大的影响。许多网络安全从业人员选择这个行业，是因为他们对网络安全领域有着浓厚的兴趣。这种兴趣驱动他们在工作中持续学习、不断进步，从而在这个快速发展的领域中保持竞争力。

综上所述，网络安全从业人员在择业时，会综合考虑专业对口、薪资待遇和个人兴趣等多个因素。这些因素共同影响着他们的职业选择和发展路径。同时，值得注意的是，随着网络安全行业的不断发展和变化，从业人员也需要不断更新自己的知识和技能，以适应行业的最新需求。

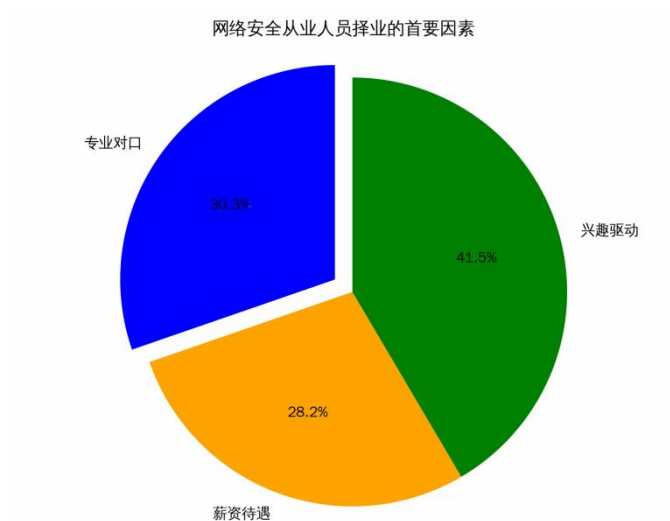


图 4 网络安全从业人员择业首要因素

4. 国内网络安全从业人员关注的模块主要包括以下几个方面：

最新活动和竞赛：这是从业人员最关注的模块，平均综合评分高达 4.98。从业人员对行业的最新动态和各类竞赛保持高度关注，这有助于他们了解行业趋势，提升专业技能，以及拓展职业发展的机会。

安全新闻：安全新闻模块也备受关注，得分为 4.82。从业人员通过关注安全新闻，能够及时了解行业内发生的安全事件、漏洞披露、政策变化等信息，从而保持对行业环境的敏锐感知。

技术问答和技术分享：这两个模块的关注度相似，得分都为 4.66。技术问答为从业人员提供了一个交流和解决技术问题的平台，而技术分享则能够让他们学习到更多的专业知识和实践经验。

招聘新闻和在线课程：招聘新闻得分为 4.11，在线课程得分为 4.09。这两个模块对于从业人员的职业发展具有重要意义。招聘新闻能够帮助他们了解市场动态和就业机会，而在线课程则提供了便捷的学习途径，有助于他们不断提升自身能力。

安全工具：相比之下，安全工具受到的关注度最低，得分仅为 2.88。这可能与从业人员更倾向于关注理论知识和实践经验，而对于具体工具的使用和选择则相对较为次要有关。

此外，不同学历背景的从业人员在关注重点上也存在一定的差异。超过半数的本科及以上学历人员首选关注技术分享，这可能与他们更注重实际操作和技能提升有关。而半数以上本科以上学历人员首选关注最新活动和竞赛，这可能反映了他们对于行业前沿动态和专业挑战的更高追求。

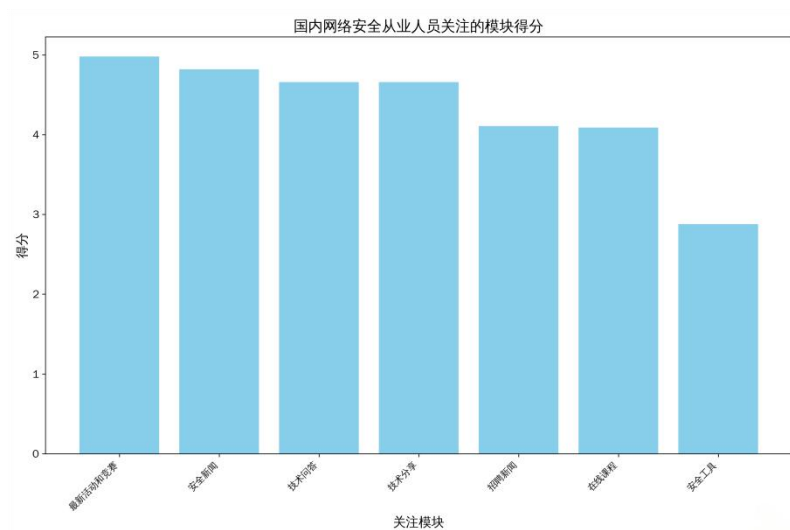


图5 国内网络安全从业人员关注的模块

5. 密码应用技术专业发展现状

随着 5G、新基建、东数西算等数据工程的建设不断提速，预计到 2025 年，我国的密码人才需求将达到惊人的 110 万左右。这一预测进一步凸显了密码人才培养的紧迫性和重要性。同时，商用密码企业对密码从业人员的调研结果也显示，未来 3-5 年内，商用密码人才的需求平均增长率将达到 30%-60%。这无疑为密码人才的培养 and 市场需求提供了有力的数据支持。

网络安全人才地位提升：随着网络安全问题的日益突出，专业安全人员的价值逐渐受到重视。他们不再仅仅是 IT 开发运维人员的兼职角色，而是逐步独立、并列于 IT 信息化人才的重要力量。这一变化使得网络安全相关专业的求职者在人才市场上的地位显著提升。

立法和监管推动人才需求：当前我国在网络安全领域的立法和监管力度持续增加，政企单位招聘使用网络安全人才不仅是自身的需要，更是国家和政府的要求。随着法律制度的进一步完善，安全团队将逐步成为政企单位的标配，从而进一步推动网络安全人才的需求增长。

学科交叉与核心技术突破：密码学作为一门综合性学科，与多个领域有着广泛的联系。突破核心技术、打造安全产品以及发展安全产业都离不开人才的支持。然而，目前的教育和培训体系面临着人才需求和供给不匹配的问题。因此，跟上战略形势的发展，加强人才培养的思路和创新显得尤为重要。

综上所述，为了适应这一形势的发展，我们需要加强密码人才的培养力度，推动校企合作培育模式的发展，以及加强多层次、多场景的密码应用人才培养。同时，我们也需要关注网络安全领域的立法和监管动态，以及学科交叉与核心技术突破对人才需求的影响。

三、专业现状调研

（一）专业点分布情况

1) 专科（高职）院校开设情况

密码技术应用专业于 2021 年被列入《职业教育专业目录》。

全国开设密码技术应用专业的专科（高职）院校包括但不限于以下几所：

- 河北软件职业技术学院
- 黑龙江商业职业学院
- 上海电子信息职业技术学院（目前上海唯一开设此专业的高职院校）
- 常州信息职业技术学院
- 浙江警官职业学院
- 安徽林业职业技术学院
- 重庆电子工程职业学院

院校开设专业情况可能会有变动，请以学校最新公布的名单为准。

2) 本科院校开设情况

全国开设密码相关专业的本科院校包括但不限于以下几所：

- 北京理工大学
- 北京电子科技学院
- 南开大学
- 华中科技大学
- 海南大学
- 西安电子科技大学

这些本科院校中，有的开设的是“密码科学与技术”专业，与专科（高职）的“密码技术应用”专业在培养目标和课程设置上可能有所不同，但都是围绕密码学和网络安全领域展开。

总的来说，随着网络安全问题的日益突出，密码技术应用和密码科学与技术专业的重要性不断提升。这些专业旨在培养具备密码学和网络安全知识与技能的专业人才，以应对网络安全挑战和维护国家网络安全。

（二）专业招生与就业岗位分布情况

1. 专业招生情况

2021 年密码技术应用专业计划招生 30 人，实际招生 29 人。2022 年密码技术应用专业计划招生 30 人，实际招生 23 人。2023 年密码技术应用专业计划招生 60 人，实际招生 54 人。目前在校生共 106 人。

2. 学生学情分析

根据前两届密码技术应用专业高职学生学情分析显示，学生普遍具备数学、计算机和英语基础，但存在个体差异。大部分学生对专业有较高兴趣，但部分学生学习动力不足。学习能力方面，学生能自主完成任务，但在应对复杂问题时存在挑战。实践能力上，学生重视实践，具备创新精神，但需加强独立思考能力。教学中，教师应因材施教，注重综合素质和创新能力的培养，加强与企业的合作，以更好地满足行业需求。

密码技术应用专业学生在学习过程中可能会面临多种问题,这些问题可能源自不同的方面,包括学习内容的复杂性、学习方法的不足、实践机会的限制等。

为了解决这些问题,学生可以采取以下措施:一是加强基础知识的学习,掌握密码学所需的数学和计算机科学理论知识;二是改进学习方法,注重实践和创新能力的培养;三是积极寻找实践机会,如参加科研项目、竞赛等;四是关注最新研究动态,了解密码学技术的发展趋势;五是培养学习兴趣和动力,将密码学知识与实际应用相结合,激发学习热情。

同时,学校和教师也应积极采取措施,如优化课程设置、更新教材、提供实践平台等,以帮助学生更好地学习和掌握密码学技术。

3. 就业岗位情况分析

密码技术应用专业 2021 年开始招生,目前有一届毕业生。据市场分析,密码技术应用专业学生就业岗位有密码技术应用员、密码产品部署与运维、密码测评工程师、网络安全与管理员等。

(三) 专业教学情况及存在的主要问题

针对现有学科和安全产业体系下密码人才培养的局限性,经过深入研讨和论证,此次人才培养方案调整的重点是在原有培养方案课程体系基础上,深入挖掘应用场景,提高技术技能水平。

首先,加强网络安全基础教育

在课程体系中网络安全基础课程非常重要,需要学生对网络安全相关标准与法规熟悉,提高法律意识。对网络安全的基本概念、原理和方法有深入的理解。强化实践操作能力:通过实验、实训和网络安全竞赛等多种形式,提高学生的网络安全实践操作能力,培养他们从实际问题中分析和解决安全问题的能力。

第二,突出密码技术应用

轻理论,重应用,淡化密码学理论教学:加强密码应用,将密码学与网络安全实际应用场景相结合,通过案例分析、项目实践等方式,使学生更好地理解密码学在网络安全中的应用。

第三,加强实训,提高技术技能

拓宽知识面:鼓励学生跨学科学习,提升创新能力:通过竞赛、校内实践与企业实践,培养学生的技术技能,使他们在实践中锻炼和提高自己的安全技能和综合素质,以适应网络安全领域的快速发展。

第四,加强校企合作

建立校企合作机制:与网络安全企业建立紧密的合作关系,共同制定人才培养方案,确保教育内容与行业需求紧密对接。

通过以上调整方针的实施,我们期望能够培养出更多具有综合安全能力和素质的人才,以满足网络空间安全领域对人才的需求。

四、专业人才培养方案优化建议

（一）专业岗位优化建议

根据最新的网络数据，商用密码部署与运维岗位的市场需求持续增长，预计未来几年内这一趋势将继续保持。这与高等职业教育培养技术技能型人才的定位高度契合，此岗位作为重点培养方向。高等职业教育机构应密切关注行业动态，调整专业设置和课程体系，加强与企业的合作，共同培养出更多符合市场需求的人才，比如熟悉各类密码产品、能根据密评密改设计密码产品方案，及商用密码部署与运维人才。

随着我国商用密码检测认证体系的逐步完善，对密码产品的评估和改造变得尤为重要。在密评过程中，针对不合格或需要改进的环节，必须进行相应的密码改造，如增设服务器密码机、安全网关等密码产品。这一改造过程不仅提升了信息系统的安全等级，也带来了对相关技术人才的需求。因此密码安全应用评估从业人员岗位需求明显，可根据岗位需求设置课程。

（二）专业课程内容优化建议

1. 聚焦网络安全产品部署及运维实训

培养目标对标密码产品运维部署岗位，对 VPN、安全网关等基础网络安全产品部署运维有较高要求，建议相关实训课程聚焦防火墙、路由、VPN 等基础网络安全产品部署及运维，以及特色密码设备，如安全网关、密码机、签名验签服务器等产品部署及运维。

2. 部分课程更改类型

网络安全不仅关乎技术层面，更涉及法律、管理等多个领域，随着网络安全行业的快速发展，国家对网络安全相关的法律法规的制定和发布也有着明显加快的趋势，网络安全从业人员要熟读相关网络安全标准与法律法规。提高法律意识，规范职业道德养成。《网络安全标准与法律法规》课程重要，应该从专业限选改为专业必修。

（三）专业教学改革建议

1. 教学资源

加快开发更适合职业学校学生的教材。加强校企合作显得尤为重要，这样我们可以引入企业的实际案例和前沿技术，使教材内容更贴近实际应用。我们计划与企业联手，共同开发工作手册式、活页式的新型教材以及实训教材，确保教材内容既有理论深度，又具备实践指导意义。《密码技术》、《商用密码产品及其部署运维》、《商用密码应用安全性评估》现有资源并不多，建议加强建设。

2. 教学过程

在密码技术的教学过程中，采用轻理论，重应用教学策略，不过于深究复杂的理论细节，而是将重点放在如何应用密码技术上。现阶段通过与奇安信科技集团联合建设的实训平台，在教学中增加密码应用场景的模拟，并展示密码服务的实际功能。通过优化以上教学内容和方法，我们期望学生能够更直观地理解密码技术的实际应用，并提升他们的实践能力。

（四）专业师资与实训条件配置建议

为了进一步提升教师的教学能力，以满足专业教学的需求，我们将采取以下措施：

1. 加大教师培训力度：增加对教师的专业培训投入，通过组织多样化的培训活动，如企业实践、项目实战等，切实提升教师的技术技能水平。目前已经有 2 位老师考取了密码技术应用员（四级）证书。1 人考取区块链应用技术（三级）证书。

2. 引进企业实战经验教师：我们将积极引进具有丰富实战经验的企业教师，他们不仅能为学校带来新的教学理念和方法，还能为学生提供更贴近实际的工作经验分享。这一举措将有助于加强双师型教师队伍建设，提升整体教学质量。目前奇安信定期派驻企业兼职教师对师生集中培训。

3. 加强实训室建设：为了增强密码产品部署运维等技术技能，我们充分利用现有密码产品，创设实训场景，开展教学。这些实训室将为学生提供更多动手实践的机会，帮助他们更好地理解 and 掌握所学知识，从而提高实训教学效果。目前已经完成信创实验室的建设，并着手区块链技术应用实训室建设。

综上所述，我们将通过加大教师培训、引进企业教师和加强实训室建设等多方面的举措，不断优化教学环境，提升教师的教学水平，以满足专业教学的需要，培养出更多具备实战能力的优秀人才。