上海电子信息职业技术学院

人才培养方案

2023 级三年制高职适用

申安网络安全产业学院

教务处汇编

2023 年 7 月

目录

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	所属专业类	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
电子与信息大类51	电子信息类5101	互联网及相关服务64 -互联网安全服务6440	网络与信息安全管理员（4-04-04-02）	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，具有良好的人文素养、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 优秀语言文化的意识。

2. 知识

（1）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；

（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。

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）具有初步创业与学习、创新、岗位迁移能力。

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

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	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、社会主义改革开放论等，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制度的最大优势。	32
2	思想道德与法治	**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
3	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
4	体育	**内容：**体育理论、身体素质、篮球、排球 **要求：**掌握各项目的动作技能、培养吃苦耐劳，顽强拼搏的意志品质。	64
5	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

序号	课程	主要教学内容与要求	参考学时
6	计算机应用基础	**内容：**计算机基础知识、Win7 操作系统、Word 软件、Excel 软件、PowerPoint 软件、多媒体、网络基础应用、网页制作 **要求：**能达到国家计算机一级考试大纲的要求	80
7	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。	192
8	习近平新时代中国 特色社会主义思想概论	**内容：**习近平新时代中国特色社会主义思想的主要内容是党的十九大报告概括的“八个明 确”和“十四个坚持”，它系统回答了新时代坚持和发展什么样的中国特色社会主 义、怎样坚持和发展中国特色社会主义的问题，体现了习近平新时代中国特色社会 主义思想理论与实际相结合、认识论与方法论相统一的鲜明特色。 **要求：**以马克思主义中国化最新成果为重点，全面把握中国特色社会主义进入新时 代，系统阐释习近平新时代中国特色社会主义思想的主要内容和历史地位，充分反 映实现全面建设社会主义现代化强国、中华民族伟大复兴中国梦的战略部署。	48
9	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

序号	课程	主要教学内容与要求	参考学时
10	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、 掌握两个重要极限、掌握函数在点 处的连续性、掌握导数的基本定义、 几何意义、掌握导数与连续的关系、掌握微分的基本定义、了解微分在 近似运算上的运用、掌握导数在函数单调性判定上的应用、、掌握原函 数和不定积分的定义、掌握不定积分的性质、熟练掌握基本积分公式、 掌握定积分的定义、性质、几何意义、在几何上的应用。	96
11	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
12	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
13	互联网+创业实践	**内容：**创业意识、创业环境认知与项目选择、模拟创业、创业项目运营，创业意识培养、找准创业项目、建立创业团队。 **要求：**引导学生通过体验性学习，培养创业意识，掌握创业技巧。	32
14	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

序号	课程	主要教学内容与要求	参考学时
15	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

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：包括计算机网络技术、信息安全基础、Python 程序设计、Windows 系统管理与应用等。

（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、Python 安全工具开发、渗透测试、WEB 应用安全、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、信息安全标准与法规、WEB 应用开发、安全运维技术、云安全技术与应用、数字取证技术等。

其中纯实践性教学课程为：网络安全应急响应、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 信息安全应用技术核心课程内容与要求

序号	课程名称	主要教学内容与要求
1	Python安全工具开发	**要求:**掌握python安全工具的编写。 **内容：**全端口扫描器，网络爬虫，渗透测试，文件清理恢复，元数据分析，无线网络渗透、明文协议渗透。
2	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

序号	课程名称	主要教学内容与要求
		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。 **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。 **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
3	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。
4	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。
5	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。
6	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。 **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。

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	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		
2	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扎实的基础。 **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		
3	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
4	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	
5	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		

（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、认识实习、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；认识实习、岗位实习可由学校组织在信息安全相关企业开展完成。实训实习主要包括项目实战，综合能力实训等类型，顶岗实习等应严格执行《职业学校学生实习管理规定》和《高等职业学校信息安全应用技术顶岗实习标准》。

（五）相关要求

学校应统筹安排各类课程设置，注重理论与实践一体化教学；应结合实际，开设安全教育、社会责任、绿色环保、管理等方面的选修课程、拓展课程或专题讲座（活动），并将有关内容融入专业课程教学；开设创新创业教育课程；自主开设其他特色课程；组织开展德育活动、志愿服务活动和其他实践活动。

七、教学进度总体安排

（一）学时安排

信息安全应用技术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	1		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	2		1		1	8	28
第五学期	0	0	10		8	1		1	4	24
第六学期	0	0			16	1		3	0	20
总计	1	0	74	5	24	6		10	28	148

（二）教学进度表

信息安全应用技术的专业教学进程表如表 6 所示。

表 6 信息安全技术应用教学进程表

课程类别	学院	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+2
公共基础必修	马院	思想道德与法治	3	48	考试	8	3					
	马院	形势与政策 1	0.5	8	考查	0	0.5					
	基础	体育 1	2	32	考查	30	2					
	基础	心理健康教育 1	1	16	考查	0	1					
	通信	计算机应用基础 1	2	32	考查	22	2					
	基础	应用数学 1	4	64	考试	0	4					
	外语	实用英语 1	4	64	考试	8	4					
	经管	职业生涯规划与职业指导	1	16	考查	8	1					
	基础	心理健康教育 2	1	16	考查	0			1			
	通信	计算机应用基础 2	2	32	考试	20		2				
	基础	大学生安全教育	2	38	考查	0	*	2	*		*	
	马院	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					
	马院	习近平新时代中国特色社会主义思想概论	3	48	考试	8		3				

课程类别	学院	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+2
	马院	形势与政策 2	0.5	8	考查	0		0.5				
	经管	互联网+创业实践	2	32	考查	16			2			
	通信	计算机应用基础 3	1	16	考查	16			1			
	马院	形势与政策 3	0.5	8	考查	0			0.5			
	基础	大学语文	2	32	考查	0				2		
	马院	形势与政策 4	0.5	8	考查	0				0.5		
	基础	体育 2	2	32	考查	30		2				
	基础	应用数学 2	2	32	考试	0		2				
	外语	实用英语 2	4	64	考试	8		4				
	基础	军事理论与训练	2	32	考查	16		2				
	外语	实用英语 3	2	32	考试	8			2			
	外语	实用英语 4	2	32	考试	8				2		
	学工	劳动教育	1	16	考查	16					1	
	小计		49	790		222	19.5	17.5	6.5	4.5	1	0
公共	基础	公共艺术选修	2	32	考查			2，任意一学期				

课程类别	学院	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+2
基础选修	基础	公共通识选修	4	64	考查			4，任意一学期				
	小计		6	96								
专业必修	申安	计算机网络技术	4	64	考试	32	4					
	申安	Python 程序设计	4	64	考试	32		4				
	申安	Windows 系统管理与应用	2	32	考查	16		2				
	申安	Windows 系统安全实训	1	30	考查	30		1				
	申安	★Linux 服务与安全管理	6	96	考试	48			6			
	申安	★网络设备安全配置	4	64	考试	32		4				
	申安	信息安全基础	3	48	考试	24			3			
	申安	★Python 安全工具开发	4	64	考查	32				4		
	申安	Linux 服务安全管理实训	1	30	考查	30			1			
	申安	★渗透测试	4	64	考试	32				4		
	申安	★WEB 应用安全	6	96	考试	48				6		
	申安	★数据库安全管理	4	64	考试	32			4			
	申	防火墙与 VPN 技术	1	30	考查	30				1		

课程类别	学院	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+2
	安	项目实战										
	申安	网络安全应急响应	4	64	考试	32				4		
	申安	网络安全应急响应项目实战	1	30	考查	30				1		
	申安	网络攻防项目实战	1	30	考查	30					1	
	申安	认识实习	2	60	考查	60					2 周	
	申安	岗位实习 1	8	240	考查	240					8 周	
	申安	岗位实习 2	14	420	考查	420						14 周
	小计		74	1590		1230	4	11	14	20	10	14
专业选修	经管	创新创业教育	2	32		0			2			
	申安	C 语言程序设计	4	64	考试	32	4					
	申安	Java 程序设计基础	4	64	考试	32						
	申安	计算机系统配置	1	30	考查	30	1					
	申安	《企业网络安全防护（中级）实训》	1	30	考查	30						
	申安	网络安全标准与法律法规	2	32	考查	16			2			
	申安	安全风险管理	2	32	考查	16						

课程类别	学院	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+2
	申安	WEB 应用开发	4	64	考查	32			4			
	申安	安全运维技术	4	64	考查	32						
	申安	云安全技术与应用	3	48	考查	32				3		
	申安	数字取证技术	3	48	考查	32						
	申安	信息安全管理	2	32	考查	16					2	
	申安	安全检测与评估	2	32	考查	16						
	小计		18	302		158	5	0	8	3	2	0
合计			147	2778		1610	28.5	28.5	28.5	27.5	11	14

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.专业教室基本条件

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

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，工位数 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、操作系统管理与应用、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
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.校外实训基地基本要求

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.学生实习基地基本要求

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

教师采用“任务驱动”教学方法，进行“任务引领式”教学，让学生通过执行完整的任务来锻炼综合职业能力，改变教师本位观念，让学生充分发挥主观能动性。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。

（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 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、行业对中、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）》、普陀区“上海市网络安全产业示范园”挂牌成立，以中以（上海）创新园、上海清华国际创新中心、海纳小镇等创新载体空间，推动国内外创新要素资源集聚。《2022 网络安全保险科技白皮书》和《2022 年度上海市网络安全产业创新攻关成果目录》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 9 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。

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 9 家企业，企业情况如表 1 所示：

表 1 调研企业一览表

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	上海信息安全测评认证中心	上海市	国企	提供信息系统的等保测评，安全检查服务，致力于漏洞感知系统和安全测评系统的研发
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	上海安酷网络安全技术有限公司	上海市	国企	信息安全硬件产品的研发，设计，生产制造，主要是网络安全设备如防火墙等
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	上海斗象科技有限公司	上海市	民营	运营信息安全的主流媒体 FREEBUF 和漏洞盒子平台，漏洞盒子提供给安全白帽子的渗透测试的众测平台，为企业提供安全检测和加固服务
7	上海高嘉信息科技有限公司	上海市	民营	提供电子商务基础建设产品、解决方案和服务，业务范围涵盖分销业务、系统业务、IT 服务及自有产品业务等多个领域
8	上海视岳计算机科技有限公司	上海市	民营	主营移动产品安全检测及 WEB 安全渗透测试服务

序号	企业名称	所在省（市）	企业性质	主营业务
9	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

（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

2022 年 11 月～2023 年 1 月，受疫情影响，采用电话或者视频方式进行询问。

2023 年 3 月～2023 年 4 月， 进行走访企业现场调查，问卷调查。

2023 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）相关行业发展现状

在当今信息化时代，互联网与信息技术的快速发展使得我们获得了前所未有的便捷，但与之同时伴随而来的是日益增多的信息安全威胁。因此，信息安全技术变得尤为重要。信息安全技术应用专业正是致力于培养网络安全、计算机安全、数据安全、网络攻防和信息安全管理等方面的技术人才，以适应不断升级的信息安全形势，保障社会各界信息安全。

全球网络空间局部冲突依旧不断，国家级网络攻击频次不断增加，攻击复杂性持续上升，全球网络安全风险正在不断增加。在 2022 年发生了很多网络安全事件，如图 1-1 所示。

2022 年部分网络安全事件

时间	事件	相关内容
2022 年 2 月	国际航港巨头遭勒索软件攻击	全球航港巨头瑞士空港披露了一起勒索软件攻击，因 IT 基础设施与服务受到影响，导致运营被干扰。苏黎世机场透露，这波网络攻击发生在 2 月 3 日，导致当天 22 架次航班发生轻微延误。
	英国外交部遭遇一起严重网络安全事	英国外交部承认了一起严重网络安全事件的目标。文件显示，外交和联邦事务部被迫叫来本国防务公司贝宜系统(BAE Systems)旗下的子公司应用智能(BAE Systems Applied Intelligence，主营咨询业务)来处理这一事件，它为这项工作支付了 46.7 万英镑(约 63.3 万美元，400 万元人民币)
2022 年 3 月	英伟达 1TB 内部敏感数据失窃后遭勒索	国际芯片制造巨头英伟达证实，在上周三(2 月 23 日)遭遇了一次网络攻击，入侵者成功访问到专有信息与员工登录数据。《每日电讯报》表示，该公司经历了一场毁灭性的网络攻击，完全摧毁了内部系统。
	乌克兰电信运营商遭遇最严重网络中断攻击	乌克兰重要电信运营商 Ukrtelecom 遭遇“强大的”网络攻击，导致全国服务中断。专注监测互联网状态的 NetBlocks 公司称，Ukrtelecom 可正常运行的服务“已跌至战前水平的 13%，这是自俄乌冲突以来出现的最严重的网络攻击。
2022 年 4月	汽车租赁巨头全球系统中断，业务陷入混乱	国际汽车租赁巨头 Sixt 遭到网络攻击，部分业务系统被迫中断，运营出现大量技术问题。由于系统故障，公司的客户服务中心和部分分支机构受影响较大，业务陷入混乱，大多数汽车预定都是通过笔和纸进行的。
2022 年 5 月	俄罗斯胜利日，电台系统被黑	俄罗斯总统普京在 “胜利日”阅兵式上发表讲话期间，黑客组织破坏了俄罗斯在线电视时间表页面，以显示反战信息。试图通过智能电视访问电视节目表的俄罗斯公民阅读了指责克里姆林宫的信息。俄罗斯主要电视频道、最大搜索网站Yandex、最大视频网站 RuTube 均受到网络攻击的影响。
	俄最大银行遭到最严重 DDoS 攻击	俄罗斯最大银行联邦储蓄银行披露，在 5 月 6 日成功击退了有史以来规模最大的DDoS 攻击，峰值流量高达 450 GB/秒。此次攻击联邦储蓄银行主要网站的恶意流量是由一个僵尸网络所生成，该网络包含来自美国、英国、日本和中国台湾的27000 台被感染设备。
2022 年6 月	美国医疗设备公司遭黑客攻击	美国医疗保健集团希尔兹就此前发生的一起网络攻击事件发表公开声明，称攻击已被遏制。此次网络攻击导致约 200 万患者的医疗信息被泄露，包括姓名、身份证号、住址、诊断结果、保险编号等。
2022 年7 月	朝鲜间谍使用 Chrome 扩展程序窃取电子邮件	美国网络安全公司 Volexity 发现的相关恶意扩展名为 SHARPEXT，支持 Chrome、Edge 和韩国 Naver Whale 等三种基于 Chromium 的浏览器，目的是窃取 Google 和AOL 的电子邮件。
2022 年8月	中欧天然气管道公司疑遭勒索攻击导致150GB 数据失窃	BlackCat 勒索软件组织声称，对上周中欧地区天然气管道与电力网络运营商Creos Luxembourg SA 遭受的网络攻击负责，并威胁要发布总计 150 GB 大小的 18万个被盗文件，具体涵盖合同、协议、护照、账单及电子邮件。Creos 的母公司 Encevo 目前正在调查攻击造成的损害程度。

图 1-1　2022 年部分网络安全事件

比特币等虚拟加密货币飙涨刺激，DDoS 勒索攻击抬头，攻击方式从大规模通用攻击转

变为更具针对性的攻击，运营模式升级为“三重勒索”。国家级网络攻击正与私营企业技术融合发展，网络攻击私有化趋势带动了网络雇佣军的快速扩张，数量众多的高素质、有组织的黑客团体受雇于国家或私人机构，对特定目标发动网络袭击。受政府实体、国防承包商、关键基础设施等组织机构已经成为勒索软件团伙的主要攻击目标。网络空间对抗趋势更加突出，大规模针对性网络攻击行为增加，安全漏洞、数据泄露、网络诈骗等风险增加。

如图 1-2 所示，根据观研报告网发布的《中国网络空间安全行业发展现状分析与投资前景研究报告（2022-2029 年）》显示，在整体网络安全形势不容乐观下，强化网络安全的需求日益增强。对此各国政府高度重视网络安全，以美国、欧盟、澳大利亚为代表的国家地区纵深推进网络安全政策举措，为产业发展创造良好环境。

我国国家层面网络安全政策梳理

发布时间	政策文件	部分内容
2015年7月	《国家安全法》	国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控；加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。
2017年6月	《网络安全法》	网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力 。
2020年1月	《密码法》	为规范密码应用和管理，促进密码事业发展，保障网络与信息安全，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益，提供有效法律支撑。通过立法提升密码管理科学化、规范化、法治化水平，促进我国密码事业的稳步健康发展。
2021年1月	《民法典》	自然人的个人信息受法律保护。任何组织或者个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。
2021年3月	《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》	第十八章提出，统筹数据开发利用、隐私保护和公共安全，加快建立数据资源产权、交易流通、跨境传输和安全保护等基础制度和标准规范。
2021年9月	《数据安全法》	第三条明确，数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。
2021年11月	《个人信息保护法》	第四条明确，个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

图 1-2 网络安全政策

美国白宫在 2021 年 3 月发布《国家安全战略临时指导方针》，将提升网络安全作为美国政府首要任务，鼓励私营部门与各级政府合作，保卫美国免受恶意网络活动侵害。随后 5 月，拜登签署《改进国家网络安全行政令》，提出预防、检测、评估和处路网络安全事件是国家和经济安全的重中之重。此外美国在新技术领域安全方面，将人工智能、能源、量子信息科学、通信和网络技术、半导体和太空技术作为关键和新兴技术，不断强化上述领域的网络安全治理。

澳大利亚在 2020 年 8 月发布《2020 年网络安全战略》，将投资 16.7 亿美元用于建立新的网络安全和执法能力，协助行业加强自我保护，并增强社区对保护在线安全的理解。随后在 2021 年 2 月，更新《在线安全法案 2021》，保护网络空间中澳大利亚公民，尤其是儿童的在线安全。2022 年 4 月，澳大利亚政府发布《国际网络和关键技术参与战略》，用于指导澳大利亚在网络和关键技术问题上的国际参与决策，帮助其拥抱巨大创新机会并减轻或避免相关风险。

我国先后发布相关政策。在 2017 年 6 月发布的《中华人民共和国网络安全法》，明确规定国家实行网络安全等级保护制度，并要求网络运营者应当按照网络安全等级保护制度要求，履行安全保护义务。2021 年 9 月发布的《数据安全法》，明确数据安全是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

在国家战略引导下，我国在国家安全、网络安全、数据安全、个人信息保护、关键信息基础设施、车联网等多个领域密集出台了多项法律法规和政策文件，有效促进了网络安全领域的技术创新和应用落地，为筑牢国家网络安全屏障、推进网络强国建设提供了有力支撑。保障关键信息基础设施的安全，对于维护国家网络安全、网络空间主权和国家安全、保障经济社会健康发展、维护公共利益和公民合法权益都具有十分重大的意义。

1.行业发展现状

如图 1-3 所示，近年来随着国内信息安全政策法规持续完善优化，网络安全市场规范性逐步提升，政府及企业客户在产品和服务上的投入稳步增长，我国国内网络安全市场规模不断扩大。根据相关数据，2021 年我国网络信息安全市场规模达到 926.8 亿元，年增长率达到 23.7%。预计 2022 年，我国网络信息安全市场规模将达到 1144.2 亿元，年增长率达到 23.5%。

图 1-3 网络安全市值

但对比美国来看，我国仍有较大的提升空间。从市场规模来看，根据信通院发布的《中国网络安全产业白皮书（2022 年）》，2020 年全球网络安全市场的规模为 1367 亿美元。其中我国市场规模为 82 亿美元，约占全球市场的 6.1%；而北美市场规模为 640 亿美元，占比为 46.8%，相比之下我国仍有 7 到 8 倍的上升空间。

从网安支出占比看，我国支出提升空间大。根据 IDC 数据，2021 年我国安全支出为 98 亿元，占 IT 总支出比重仅为 1.87%，而美国政府 2021 年 IT 总预算为 922 亿美元，其中网络安全领域总预算 188 亿美元，占 IT 预算的 20.4%。可见，我国网络安全支出占 IT 支出的比重不仅与美国相差十倍，也低于全球 3.74%的水平。

图 1-4 中美网络安全支出对比

2.网络安全人才岗位技能要素

虽然不同岗位的技能准则各不相同，但网络安全是个综合学科，综合能力、专业知识、技术技能和工程实践都是需要掌握的。战略性的人力资源管理核心在于把人看作重要的资产，通过教育培训等投入，持续提高其知识、技能和素质水平，更好地达成用人单位的业务目标。用人单位能否提供足够的培训、持续提升人才专业能力、帮助其完成自我价值实现，将在“引才”和“留才”中发挥越来越重要的作用。当前人员能力提升需求普遍难以得到满足，一是从业人员能力提升需求旺盛，新入职人员在学历教育之后普遍需要进行“二次培训”，已从业的人员也需要持续教育和终身学习。调研显示，受访者在专业知识和能力的各个细分方向均有能力提升需求，其中最希望提升的方是大数据安全、云安全、安全管理和渗透测试等方向的专业能力。二是从业人员期望获得专业资质，作为证明自己具备一定知识、能力和工作经验的凭证。超过六成（64.7%）的受访者持有不同类型的信息安全资质证书，其中持有注册信息安全专业人员（CISP）资质证书的占比最高（71.8%）。未来一年内，有 83.7%的从

业人员期望获得信息安全资质证书，其中希望获取 CISP 证书的人员占比最高，达到 68.9%。三是用人单位教育培训投入不够，对信息安全人员普遍存在“使用多、培养少”的情况，内训制度实施效果不佳，74.9%的从业人员所在单位建立了信息安全工作人员培训制度，但仅有 23.1%的受访者认为培训取得了良好效果；同时，用人单位资助从业人员接受职业培训的意愿和力度也不高，资助比例达到 50%以上的占比仅为 18.5%，33.5%的从业人员表示自己所在工作单位不提供任何资助。

3.网络安全产品

如图 1-5 示，随着国家对互联网安全、个人隐私安全等相关方面的政策出台，网络安全相关产业也随之强大起来，在保障国家、社会和个人的信息安全发挥重大作用的同时，亦推动了相关产业链的发展。从网络安全产业链看，上游为设备 / 系统等供应商，如芯片、内存、操作系统、引擎等；中游为网络安全产品和服务厂商，如网络安全设备领域的防火墙 / VPN，软件领域的安全性与漏洞管理以及服务领域的运维培训等；下游为应用领域，除个人消费者外，还包含政府、军工、金融等相关领域。

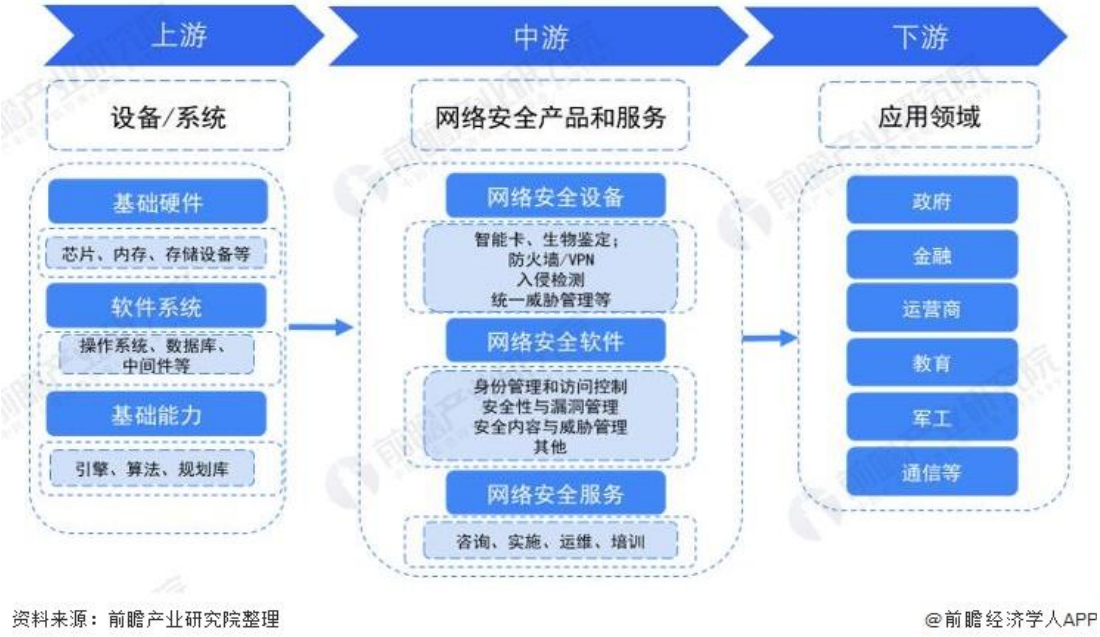

图 1-5 网络安全行业产品链

4.网络安全企业发展总体良好

如图 1-6 所示，在营收规模方面，企业营收规模总体呈稳定增长态势。10 家上市网络安全企业 2019 年平均营收规模为 16.82 亿元，较 2018 年的 13.23 亿元增长了 27.08%。其中，深信服凭借安全业务云化转型实现高速增长，2019 年营收规模首次突破 40 亿元，同比增速超过 40%。中孚信息整体收入快速增长 69%，主要受益于安全服务业务的快速推进。2017-2019 年我国上市网络安全企业营收情况。在营业收入构成方面，10 家上市网络安全企业的营业收入主要由网络安全软硬件产品及服务组成；其中，网络安全软硬件产品营收占比较高，平均占比达到企业营业收入的七成。部分网安企业在新兴安全领域的营收迅速增长。

2019 年，启明星辰以云安全和工业互联网安全为代表的新安全业务收入约占总收入的 20%，同比增长 200%。

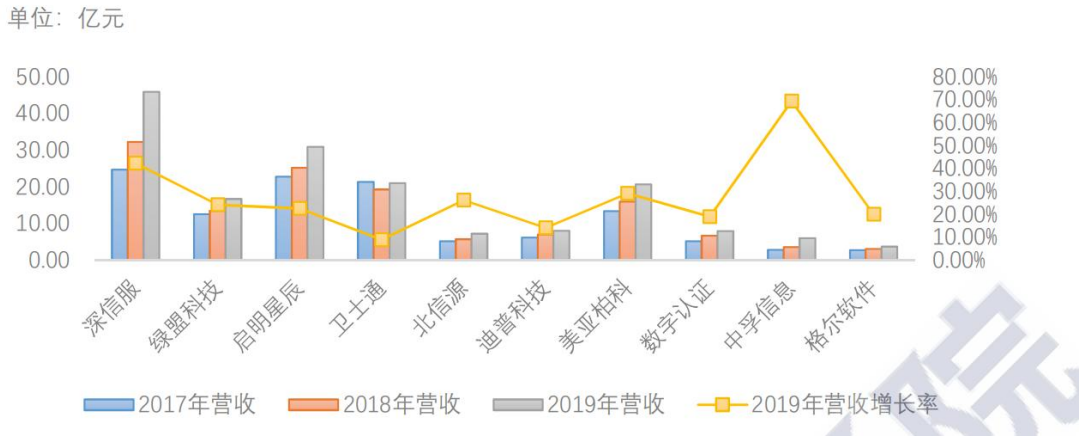

图 1-6 网络安全企业营收

三、专业现状调研

（一）专业点分布情况

信息安全专业在我国的高校中普及较晚，但近年来得到了快速发展。目前，国内的大部分高校都开设了信息安全相关专业，包括网络安全、信息保密、信息安全等专业。这些专业的设置也逐渐从少数的重点高校扩散到了大部分高校，特别是近几年名称“网络空间安全”的专业越来越受到重视，成为高校开设的重点专业之一。具体来说，像北京邮电大学、哈尔滨工业大学、上海交通大学、华中科技大学等一批著名高校在信息安全领域有着丰富的教学研究经验和较高的招生录取水平。此外，像国防科技大学、南京理工大学、电子科技大学等高校也有着相对较强的信息安全专业。

全国现有 119 所高职院校开设有信息安全技术应用专业，其中华东地区（包括山东省、江苏省、江西省、浙江省、安徽省、福建省、上海市）共有 39 所学校；华南地区（包括广东、广西）共有 7 所；华中地区（包括湖北、湖南、河南）共有 19 所；华北地区（包括北京、天津、河北、山西、内蒙古）共有 20 所，其中北京政法职业学院侦查类（涉外安全信息分析与管理），该学校设立了特殊的专业方向；西南地区（包括四川、云南、贵州、西藏、重庆），除了西藏和云南两省未有学校开设本专业以外，重庆、四川和云南三省共有 18 所院校开设有信息安全技术应用专业；西北地区（包括宁夏、新疆、青海、陕西、甘肃、内蒙古）仅有陕西交通职业技术学院与陕西工商职业学院开设了信息安全技术应用专业；东北地区（包括辽宁、吉林、黑龙江、内蒙古）仅吉林省的 2 所院校开设有本专业。

（二）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二个层次：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；	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； 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；

序号	任务领域	典型工作任务	职业需求技能
		9．信息安全体系规划、ISMS 建设。	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； 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；

序号	任务领域	典型工作任务	职业需求技能
			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	1．负责对信息安全（网络、系统、数据安全等）策略规划及协	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；

序号	任务领域	典型工作任务	职业需求技能
	评估员	调部署； 2．信息安全审计（包括操作系统、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。	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； 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；	1．具备选择适当技术的规划设计能力来； 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；

序号	任务领域	典型工作任务	职业需求技能
		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。	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管理。
6	安全设备运维（调试）工程师	1．安全设备的集成、上架测试等； 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。	1．掌握路由与交换技术； 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．学会基本的应用功能测试与分析； 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：爱党爱国、立场坚定、爱岗敬业、遵纪守法、严谨细致、吃苦耐劳、精诚合作、健康体魄、心理健全。

●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；具备英语应用能力 A 级，计算机应用上海市一级等通识教育模块知识。

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型人才。 然而，由于本专业课程涉及到计算机技术、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,学生只能被接收知识,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具，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其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》内容融入到《网络设备安全配置》，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》、《Python 安全工具开发》、《渗透测试》和《数据库安全管理》专业核心课程，制定课程标准，并着力打造精品课程资源。《信息安全基础》和《信息安全管理》两门课程的重复内容较多，可考虑融合。《信息安全基础》的基础内容

上，加入风险评估内容的学习，其次，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。

另外增加《数字取证技术》课程，作为选修课，数字取证技术是计算机学科与法学等学科的交叉研究与应用，作为网络空间安全治理中必不可少的技术支持，发挥了至关重要的作用。课程的主要内容包括：数字取证模型、磁盘取证技术、网络证据获取技术、网络证据分析技术、物理内存取证技术、即时通信取证技术、云计算取证等。

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，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、下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质证书，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 专业大类	所属 专业类	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 网络与信息安全管理员职业资格等级证书 1+X 商用密码应用与维护职业技能等级证书

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，面向信息处理和存储支持服务行业的密码技术应用员、商用密码应用安全性评估工程师、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、安全保密、安全审计工作的高素质劳动者和高素质技术技能人才。

（二）培养规格

1. 素质

(1) 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。

(2)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。

(3)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。

(4)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。

(5)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。

(6)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。

(7)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 优秀语言文化的意识。

2.知识

(1)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。

(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；

(6)熟悉密码体系架构、技术标准、规范及相关法律法规。

(7)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。

(8)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、认证授权和安全管理等安全技术及产品。

(9)熟悉调研计划流程，掌握用户调研问卷设计方法，掌握调研方案编写方法，同时熟悉密码模块应用规范。

(10)掌握项目管理工作要点、密码故障管理要求相关知识，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、测试报告规范，同时掌握基本故障处理方法。

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

(12)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。

3.能力

(1)具有独立思考、逻辑推理、信息加工能力。

(2)具有语言表达和文字写作能力。

(3)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。

(4)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。

(5)具备组建局域网和实现网络资源共享的能力。

(6)具备专业软件应用、程序编码和调试能力。

(7)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。

(8)具备 SSL、VPN 等安全加密技术产品使用与配置能力。

(9)具备基本的密码应用规划中的需求分析和密码应用方案设计能力。具备密码应用建设模块中，实施保障方案设计、应用部署、密码应用联调测试和系统交付模块应用能力；能按照密码应用方案进行密码产品选型并核验密码产品安装的正确性、部署密码产品以及完成项目经费概算。

(10)具备密码应用安全性评估模块中，密码应用方案审查、密码测评准备、现场测评以及测评总结相关工作流程知识技能，能审查密码应用方案合规性并撰写合规性审查意见等。

(11)具备密码应用运行模块中，具备基本密码资产管理、系统维护和应急处置相关知识技能。

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	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、社会主义改革开放论等，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制度的最大优势。	32
2	思想道德与法治	**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
3	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
4	体育	**内容：**体育理论、身体素质、篮球、排球 **要求：**掌握各项目的动作技能、培养吃苦耐劳，顽强拼搏的意志品质。	64
5	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
6	计算机应用基础	**内容：**计算机基础知识、Win7 操作系统、Word 软件、Excel 软件、PowerPoint 软件、多媒体、网络基础应用、网页制作 **要求：**能达到国家计算机一级考试大纲的要求	80

序号	课程	主要教学内容与要求	参考学时
7	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。	192
8	习近平新时代中国 特色社会主义思想概论	**内容：**习近平新时代中国特色社会主义思想的主要内容是党的十九大报告概括的“八个明 确”和“十四个坚持”，它系统回答了新时代坚持和发展什么样的中国特色社会主 义、怎样坚持和发展中国特色社会主义的问题，体现了习近平新时代中国特色社会 主义思想理论与实际相结合、认识论与方法论相统一的鲜明特色。 **要求：**以马克思主义中国化最新成果为重点，全面把握中国特色社会主义进入新时 代，系统阐释习近平新时代中国特色社会主义思想的主要内容和历史地位，充分反 映实现全面建设社会主义现代化强国、中华民族伟大复兴中国梦的战略部署。	48
9	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

序号	课程	主要教学内容与要求	参考学时
10	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、 掌握两个重要极限、掌握函数在点 处的连续性、掌握导数的基本定义、 几何意义、掌握导数与连续的关系、掌握微分的基本定义、了解微分在 近似运算上的运用、掌握导数在函数单调性判定上的应用、、掌握原函 数和不定积分的定义、掌握不定积分的性质、熟练掌握基本积分公式、 掌握定积分的定义、性质、几何意义、在几何上的应用。	96
11	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
12	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
13	互联网+创业实践	**内容：**创业意识、创业环境认知与项目选择、模拟创业、创业项目运营，创业意识培养、找准创业项目、建立创业团队。 **要求：**引导学生通过体验性学习，培养创业意识，掌握创业技巧。	32
14	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

序号	课程	主要教学内容与要求	参考学时
15	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

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：包含专业讲座、计算机网络技术、密码学数学基础、C 语言程序设计、计算机系统配置、linux 服务与安全管理项目实训、Python 程序设计、信息安全基础、商用密码应用安全性评估、密码产品部署与运维项目实践等。

（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、密码技术、大数据安全技术应用、公钥基础设施应用、区块链技术应用等，课程名前带有★标识。

2.专业选修课程

为专业拓展课程：包含网络安全标准与法规（限选）。网络安全方向：数据库安全管理、网络安全防护项目实训、Web 应用开发、渗透测试。大数据安全方向：大数据安全与隐私保护、大数据平台安全管理、大数据应用技术实训、数据分析应用。

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、密码产品部署与运维项目实践、网络安全防护项目实训、大数据应用技术实训、认识实习以及岗位实习等。

（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	专业讲座	**要求:**密码是网络空间安全的基础，是保障数据与通信安全，构建各类安全协议、安全机制与安全系统的核心技术。从密码面临的现实需求和威胁出发，探讨密码技术在网络空间安全中的前沿应用以及未来的发展趋势。 **内容：**密码是网络空间安全的基础，是保障数据与通信安全，构建各类安全协议、安全机制与安全系统的核心技术。从密码面临的现实需求和威胁出发，	16

序号	课程名称	主要教学内容与要求	参考学时
		探讨密码技术在网络空间安全中的前沿应用以及未来的发展趋势。	
2	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**
3	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**
4	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，同时介绍流密码、分组密码、公钥密码、密钥分配与密钥管理、消息认证和哈希函数、数字签名和认证协议、密码协议、可证明安全、网络加密与认证、区块链。 **要求：**通过课程学习，目的在于使学生了解现代密码学涉及的基础理论和实用算法，同时也涵盖了现代密码学的数学基础相关研究成果，力求使学生了解本学科的发展方向。	**48**
5	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。	**96**
6	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。	

序号	课程名称	主要教学内容与要求	参考学时
		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。	64
7	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
8	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
9	信息安全基础	**内容：**数论和代数基础知识、经典密码、对称密码、公钥密码、数字签名等信息安全知识的内容,还包括课内实验以及实验参考程序（包含用 Java、MATLAB、Maple 实现部分密码系统等）。 **要求：**通过课程学习，让学生掌握信息安全概述、物理安全、密码学基础与应用、网络攻击与防范、网络安全技术、信息系统安全、信息内容安全、云计算与云安全、信息安全管理相关知识。	48
10	公钥基础设施应用★	**内容：**PKI 的概念、PKI 的主要内容、PKI 的理论基础、PKI 体系及其所提供的服务功能，重点论述 PKI 在各种领域的应用，如电子商务和电子政务、网上银行、网上证券和网上税务，以及企业内部的信息安全管理等。 要求：通过课程学习，目的在于使学生理解公钥基础设施（PKI）体系、认证机构 CA、PKI 标准化活动等概念和功能。理解并掌握 CA 的分层结构，以及 CA 的安全体系。	24
11	大数据安全技术应用★	**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、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。	

序号	课程名称	主要教学内容与要求	参考学时
		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
12	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
13	商用密码应用安全性评估	**内容**：采用商用密码技术、产品和服务集成建设的网络和信息系统中，对其密码应用的合规性、正确性和有效性进行评估的方法，为有效控制安全风险，关键信息基础设施的运营者应当在规划、建设等必要阶段进行评估，系统投入运行后，还应当定期开展评估。 **要求**：通过课程学习，让学生掌握对于基础信息网络、涉及国计民生和基础信息资源的重要信息系统、重要工业控制系统、面向社会服务的政务信息系统，以及关键信息基础设施、网络安全等级保护第三级及以上的信息系统的商用密码应用安全性评估原理和方法。	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
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	1	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
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	网络安全虚实结合实训室
3	密码产品部署与运维项目实践	内容：终端侧的密码产品部署主要涵盖三种形式：安装软件密码模块、内嵌硬件密码模块以及外接安全网关。对于PC、手机、高性能嵌入式设备，我们可以部署软件密码模块，借助CPU的强大运算能力，实现高性能的密码运算，无需额外增加硬件成本。 要求：借助云化、虚拟化的思想将密码能力服务化，按需提供密码资源，不同应用系统只需通过服务调用的方式即可安全地获取密码能力，从而快速实现密码应用改造。	4	1	密码技术应用实训室
4	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	3、4	2	校内外实践基地
5	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				27	

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	1		1			4	24
第二学期	0	0	16	1		1			8	28
第三学期	0	0	16	1	1	1			4	24
第四学期	0	0	16	1	1	1			8	28
第五学期	0	0	10		8	1			4	24
第六学期	0	0			16				0	20
总计	1	0	74	4	26	5	0	0	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 密码技术应用专业教学进程表

课程类别	学院	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+2
公共基础必修	马院	思想道德与法治	3	48	考试	8	3					
	马院	形势与政策 1	0.5	8	考查	0	0.5					
	基础	体育 1	2	32	考查	30	2					
	基础	心理健康教育 1	1	16	考查	0	1					
	通信	计算机应用基础 1	2	32	考查	22	2					

课程类别	学院	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+2
	基础	应用数学 1	4	64	考试	0	4					
	外语	实用英语 1	4	64	考试	8	4					
	经管	职业生涯规划与职业指导	1	16	考查	8	1					
	基础	心理健康教育 2	1	16	考查	0			1			
	通信	计算机应用基础 2	2	32	考试	20		2				
	基础	大学生安全教育	2	38	考查	0	*	2	*		*	
	马院	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					
	马院	习近平新时代中国特色社会主义思想概论	3	48	考试	8		3				
	马院	形势与政策 2	0.5	8	考查	0		0.5				
	经管	互联网+创业实践	2	32	考查	16			2			
	通信	计算机应用基础 3	1	16	考查	16			1			
	马院	形势与政策 3	0.5	8	考查	0			0.5			

课程类别	学院	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+2
	基础	大学语文	2	32	考查	0				2		
	马院	形势与政策4	0.5	8	考查	0				0.5		
	基础	体育 2	2	32	考查	30		2				
	基础	应用数学 2	2	32	考试	0		2				
	外语	实用英语 2	4	64	考试	8		4				
	基础	军事理论与训练	2	32	考查	16		2				
	外语	实用英语 3	2	32	考试	8			2			
	外语	实用英语 4	2	32	考试	8				2		
	学工	劳动教育	1	16	考查	16					1	
	小计		49	790		222	19.5	17.5	6.5	4.5	1	0
公共基础选	公共艺术选修		2	32	考查					2，任意一学期		
	公共通识选修		4	64	考查					4，任意一学期		

课程类别	学院	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+2
修	小计		6	96								
专业必修	申安	专业讲座	1	16	考查	16	0.25	0.25	0.25	0.25		
	申安	计算机系统配置	1	30	考查	30	1					
	申安	计算机网络技术	4	64	考试	32	4					
	申安	C 语言程序设计	4	64	考试	32	4					
	申安	密码学数学基础	3	48	考查	0		3				
	申安	★linux 服务与安全管理	6	96	考试	48		6				
	申安	linux 服务安全管理实训	1	30	考查	30		1				
	申安	Python 程序设计	4	64	考试	32		4				
	申安	★网络设备安全配置	4	64	考试	32			4			
	申安	★密码技术	4	64	考试	16			4			
	申安	信息安全基础	3	48	考查	24			3			

课程类别	学院		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+2
	申安		★大数据安全技术应用	4	64	考试	32				4		
	申安		★公钥基础设施应用	2	32	考试	16				2		
	申安		★区块链技术应用	4	64	考试	32				4		
	申安		密码产品部署与运维项目实践	1	30	考查	30				1		
	申安		商用密码应用安全性评估	2	32	考查	12					2	
	申安		认识实习	2	60	考查	60			1 周	1 周		
	申安		岗位实习 1	8	240	考查	240					8 周	
	申安		岗位实习 2	14	420	考查	420						14 周
	小计			72	1530		1134	9.25	14.25	12.25	12.25	10	14
专业选修	申安	网络安全方向	数据库安全管理	4	64	考查	32			4			
			Web 应用开发	4	64	考查	32			4			
			网络安全防护项目实训	1	30	考查	30			1			
			渗透测试	4	64	考查	32				4		

课程类别	学院		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+2
	申安	大数据安全	大数据安全与隐私保护	4	64	考查	32			4			
			大数据平台安全管理	4	64	考查	32			4			
			大数据应用技术实训	1	30	考查	30			1			
			数据分析应用	4	64	考查	32				4		
	申安		网络安全标准与法律法规	2	32	考查	16				2		
	经管		创新创业教育	2	32	考查	0				2		
	小计			17	286		142	0	0	9	8	0	0
合计				144	2702		1498	28.75	31.75	26.75	24.75	11	14

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 1 人，中级职称 3 人；博士 1 人，硕士学位及以上 4 人。双师素质教师占比 80%。

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 操作系统、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 公钥基础设施应用课程资源包 密码工程应用课程资源包 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、公钥基础设施应用、大数据安全与隐私保护、密码产品部署与运维项目实践、商用密码应用安全性评估

序号	实训室名称	主要设备	开设课程
3	程序设计开发实训室	台式计算机 存储设备 服务器 教学实训系统 机柜	C 语言程序设计、Python 程序设计、大数据应用技术、大数据平台安全管理、大数据安全与隐私保护、数据分析应用
4	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、信息安全基础、计算机网络技术、Web 应用开发、渗透测试
5	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、顶岗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 ●为学生提供顶岗实习岗位； ●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深度融合 ●为学生提供顶岗实习岗位； ●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	上海馥欣信息科技有限公司	●为认知学习提供参观场所

序号	实践基地名称	在专业教学中的作用
		●为学生提供顶岗实习岗位； ●为专任教师提供企业践习平台。
4	上海驭胜信息技术有限公司	●为认知学习提供参观场所； ●为专任教师提供企业践习平台。
5	上海观安信息技术股份有限公司	●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； ●为学生提供顶岗实习岗位； ●为专任教师提供企业践习平台。
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践习平台。
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； ●为学生提供顶岗实习岗位； ●为专任教师提供企业践习平台。
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践习平台。

（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。

（1）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、附录

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

附件1 密码技术应用专业人才需求与专业改革调研报告

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。

随着信息和信息技术发展起来的现代密码学，是保护信息安全的最有效的手段，也是保护信息安全的关键技术。过去密码的研制、生产、使用和管理都是在封闭的环境下进行的。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——密码应用范围日益扩大，社会对密码的需求更加迫切，密码研究领域不断拓宽，密码科研也从专用机构走向社会和民间，密码技术得到了空前发展。密码技术不仅具有保证信息机密性的信息加密功能，而且具有数字签名、身份验证、秘密分存、系统安全等功能。所以，使用密码技术不仅可以保证信息的机密性，而且可以保证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是至关重要的。此外，安全系统的结构和算法的实现以及通信协议也会影响到系统的安全性。

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、物联网等新基建安全发展，商用密码产业发展极速前进。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”，密码产业将迎来全新发展机遇，也面临着新挑战。密码技术应用专业方面的专业人才需求不断增加，能熟练掌握密码相关技术的专业人才缺口很大。

（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，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，包含了 10 多家分属于北京、深圳、重庆、成都以及上海本地企事业单位和 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，我们主要了解行业现状及未来发展趋势情况、行业政策与规划情况、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、职业素养等。

通过企业调研，我们主要了解企业基本情况、人才需求情况、校企合作情况、人才培养建议、用工岗位需求情况、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情况等。

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、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，典型案例等；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，教学标准与国际接轨建议等。

通过以上方式对获取的各种调查资料归类、整理、分析，我们总结形成了如下的报告。

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

据中国网络安全产业联盟（CCIA）《2022 年中国网络安全市场与企业竞争力分析》报告统计，2021 年我国网络安全市场规模约为 614 亿元，同比增长率为 15.4%。近三年我国网络安全行业总体保持增长态势。尽管受疫情影响，行业增速出现一定波动，但随着网络安全相关立法继续向体系化、纵深化发展，各行业数字化转型加速升级，网络安全政策法规红利释放，网络安全需求不断提升，预计未来三年增速仍将保持在 15%以上，到 2024 年市场规模预计将超过 1000 亿元。

截至 2022 年 6 月，我国共有 3256 家公司开展网络安全业务，相比上一年减少 31%。其中，产品型公司 1379 家，同比增长 8%；服务型公司 2155 家，同比减少 44%。其中，受新冠肺炎疫情影响，服务型安全公司数量下降较多，也导致网络安全企业总数量减少。

2022 年，在《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的同时，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给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。

2022 年，国际形势变相环生，世界经济增长放缓态势明显。国内疫情多发散发，对经济稳定运行造成了严重冲击，我国经济面临着预期转弱、需求收缩和供给冲击三重压力，复杂性、严峻性和不确定性上升。但是，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是对宏观经济形势的折射，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）》中提出要通过 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，争取到 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。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。打造形成包括网络信息安全人才培育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》等法律法规的渐次出台，在顶层设计上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深度融合，催生出更加广泛的业务模式和应用场景，这些也使得密码应用需求日趋多样化和个性化——再这样的背景下，开设密码技术应用专业（高职），培养大批具有密码应用技术能力，为各单位的信息安全提供了技术保障、岗位规范和专业化人才，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。我们也需要为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，迫切需要发展自主可控的信息安全技术。商用密码正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，也是商用密码实现持续健康快速发展的动力源泉。密码应用既是保安全的有力支撑，也是促发展的有效手段，在实现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度发展转向高质量发展的双

重挑战，尤其在我国信息产业缺少自主核心技术的局面没有根本改变的情况下，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。

在国外技术、标注和行业准入等客观情况存在的前提下，将有更多的国内标准、国内技术和行业标准建立并持续发挥影响力，从之前的国外知识产权向国内逐步过渡，未来国内的商用密码产业将引领潮流。

（1）商用密码法律法规体系基本形成

我国现已初步形成了以《网络安全法》《密码法》《数据安全法》为核心组成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域式发展。从《密码法》对商用密码的法定化管理，到《信息安全技术网络安全等级保护基本要求》（即等保 2.0） 对商用密码的升级化保护，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，进一步规范商用密码的使用和管理，引导商用密码产业健康有序发展。

（2）商用密码标准体系基本完善

商用密码标准化是实现商用密码技术自主创新、促进商用密码产业发展、构建商用密码应用体系的重要支撑。《密码法》明确商用密码标准体系包括商用密码国家标准、行业标准、团体标准和企业标准。

商用密码国家标准、行业标准属于政府主导制定的标准,商用密码团体标准、企业标准属于市场主体自主制定的标准。其中,商用密码国家标准由国家标准化管理委员会组织制定,代号为 GB。商用密码行业标准由国家密码管理局组织制定,报国家标准化管理委员会备案,代号为 GM。商用密码团体标准由商用密码领域的学会、协会等社会团体制定,商用密码企业标准由商用密码企业制定或者企业联合制定。

（3）商用密码产业初具规模

《中华人民共和国密码法》明确我国密码分为核心密码、普通密码和商用密码三大类。其中，核心密码、普通密码用于保护国家秘密信息。商用密码是指对不属于国家秘密内容的信息进行加密保护、安全认证所使用的密码技术、密码产品和密码服务。

商用密码产品，是指采用密码技术对不涉及国家秘密内容的信息进行加密保护或安全认证的产品，即承载密码技术、实现密码功能的实体。商用密码服务，是指基于密码专业技术、技能和设施，为用户提供集成、运营、监理等商用密码支持和保障的服务活动，即基于密码技术和产品，实现密码功能，提供密码保障的服务行为。商用密码产品目前按形态划分为六类：密码软件、密码芯片、密码模块、密码板卡、密码整机、密码系统。

近年来，我国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。随着信息技术产业的持续发展和完善，密码产品也随之迭代丰富，现有商用密码产品达到 3000 余款，其中 2200 余款产品取得商用密码产品认证证书，品类涵盖了密码芯片、密码板卡、密码整机、密码系统等全产业链条，形成了完整的商用密

码产品体系。

（4）商用密码应用领域基本实现全覆盖

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、新模式的广泛应用，密码技术积极护航新基建安全发展，商用密码应用程度不断加深。在金融领域，累计发行应用国密算法的银行卡超过 10 亿张；在能源领域，部署支持商用密码的智能电表超 5 亿只；在惠民领域，已换发采用商用密码技术的二代身份证和港澳台居民居住证超过 19 亿张；在广播电视领域，基于商用密码技术的数字版权保护技术应用于移动智能终端 2700 万台；在政务领域 10 个省（区、市）完成商用密码技术支撑的政府云试点建设覆盖服务用户超过 5000 万。

同时，商用密码国产化进程高速发展——随着密码法的实施以及国家对国产化的支持，底层芯片、卡、装置性能要求将不断提高，引导产业技术和产品出现了较大幅度的性能升级。国家密码局发布了完全自主设计的 SM 系列算法的相关标准与规范，标志着我国密码算法标准体系已初步成型，全面采用国产密码算法的条件和时机日趋成熟。从产业基础上看，国产密码算法的推广已经具备一定基础，除了软件层的算法，更重要的是硬件层的密码芯片和通用芯片的自主可控，预计随着国产芯片性能提升和生态成熟，国产密码算法的逐步推广和标准的逐步完善，密码行业有望迎来国产化的机遇。

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）公安部第三研究所

主要从事网络安全与智慧警务科研创新与技术支撑，在警务信息智能感知、警务数据安全共享、违法犯罪监测预警等优势研究领域有着长期的积累，在网络攻防、网络侦察、技术侦察、国产密码、电子取证、等级保护、大数据分析、智能安防、毒品检测等领域提供核心关键技术支撑与系统解决方案。业务涵盖公共安全产品研发、检测评估、系统集成多领域，核心业务部门包括：六个全资（控股）公司：上海国际技贸联合有限公司、上海辰锐信息科技公司、上海网盾智能科技发展有限公司、上海海盾安全技术培训中心、上海公共安全器材厂、北京锐安科技有限公司。

2）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。上海 CA 共取

得软件著作权 42 项、软件产品登记 26 项；累计申请获得专利 11 项；拥有 2 项高新技术成果、6 项科学技术成果、4 项市科技进步奖；主持和参与编写行业国家标准 18 项、地方标准 5 项。

3）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。

4）上海豌豆信息技术有限公司

从事计算机技术、通信技术领域内的技术开发、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。

5）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。

6）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。

7）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”。

（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：

具备分析信息系统业务应用场景密码应用需求的能力；

具备依据业务需求，合理选择密码技术及产品的能力；

具备对信息系统的密码资源进行融合部署实施的能力；

具备对信息系统密码资源及应用进行运维管理的能力；

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；

具备应急处置密码应用安全突发事件的能力；

具备开展密码应用技术咨询、密码科普等相关服务的能力；

具备信息技术和数字技术的应用能力；

以及具有探究学习、终身学习和可持续发展的能力。

（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 62.57%，大专及以下占比为 17.51%，硕士占比有所提高，为 17.71%。

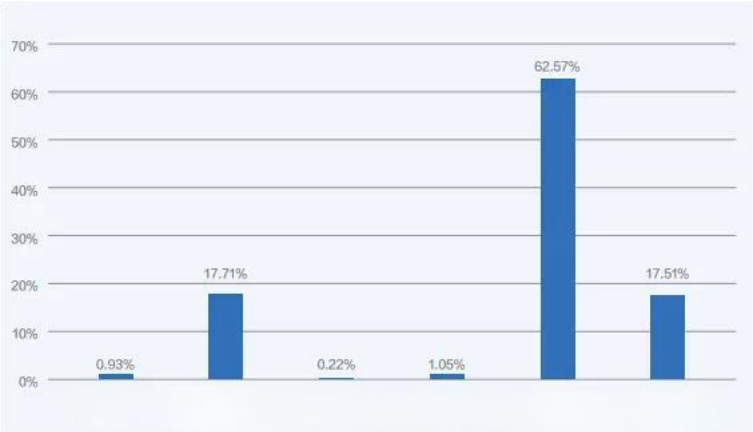

图 1 受访者最高学历分布

（2）网络安全从业人员毕业院校：根据猎聘网和安恒信息提供的数据来看，从业人员中，毕业于北京邮电大学、西安电子科技大学、上海交通大学、电子科技大学、北京航空航天大学的人才比例排名前五，最多的是北京邮电大学，占总数的 2.26%。今年，浙江工业大学和南阳理工学院也加入了 top50 的行列。

（3）网络安全从业人员从业年限：调查显示，网络安全人才中 5-8 年从业经验的人数占比最大，为 19.66%，其次是 10-15 年从业人员，占比为 19.47%。十五年以上的占比最少，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。

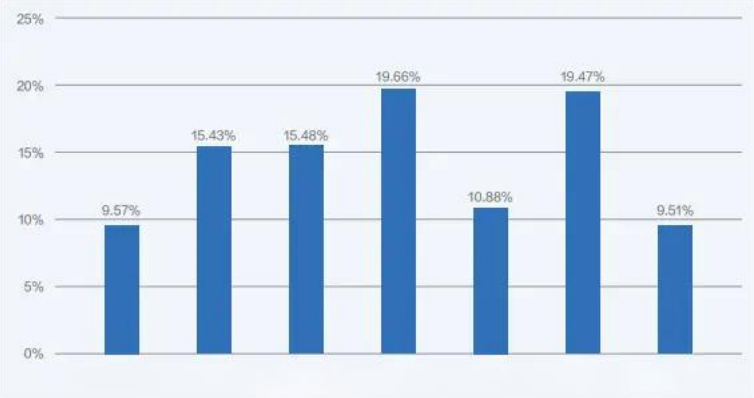

图 2 受访者从业年限分布图

2．网络安全从业人员从事行业分布

经调查，在通信和电子行业从业的网络安全人员较多，占比 33.14%，其次是 IT 和互联网行业，占比 27.46%。制造业占比 22.49%，较去年有所提升，这和工业企业的数字化转型升级有关。

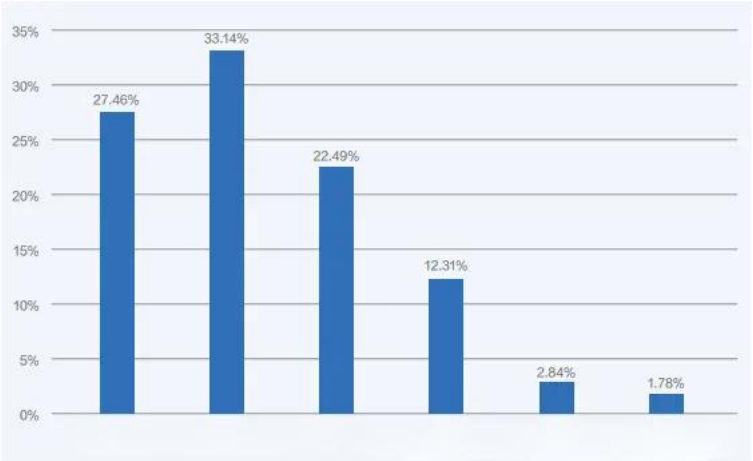

图 3 网络安全从业人员从事行业分布

3．网络安全从业人员择业首要因素

在选择行业时，从业人员表示专业对口对择业影响最大，人数占比为 28%，其次是薪资

待遇，占比 26%。而根据以往的数据来看，兴趣对专业选择有极大影响，因此，整体行业中因为兴趣驱动而择业的占比较高。

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

据统计分析，从业人员在浏览网络安全相关资讯时，最关注的模块是最新活动和竞赛，平均综合评分达到了 4.98（根据频率，权重以及样本数量计算（下同）），其次是安全新闻，得分 4.82，技术问答和技术分享模块受到的关注度相似，得分都为 4.66，再其次是招聘新闻和在线课程，得分分别为 4.11 和 4.09。安全工具受到的关注度最低，得分仅为 2.88。其中，超过半数的本科及以下学历人员首选关注技术分享，而半数以上本科以上学历人员首选关注最新活动和竞赛。

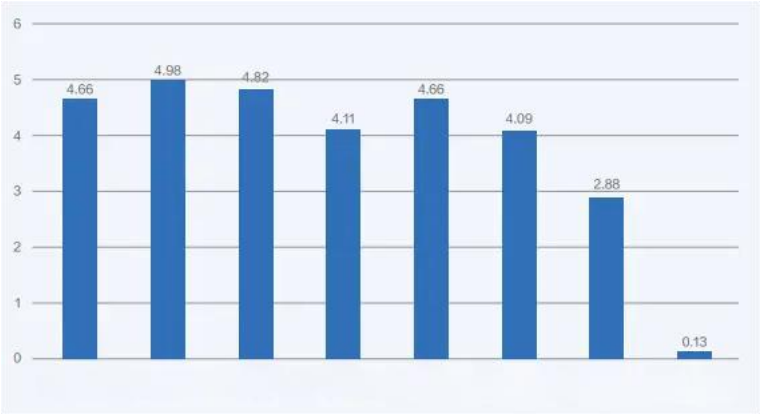

图 5　国内网络安全从业人员关注的模块

5.人才培养存在的问题

我国密码人才需求旺盛，呈现快速增长的态势。2020 年 3 月 1 日，“密码科学与技术”专业被列入普通高等学校本科专业目录；2021 年，人社部发布“密码技术应用员”新职业，这些举措为培养密码专业人才起到了重要促进作用。但根据媒体公开报道显示，现阶段我国密码人才需求人数约为 30 万，实际缺口达 20 万，随着 5G、新基建、东数西算等数据工程的建设提速，到 2025 年我国密码人需求将达 110 万左右。密码管理部门和商用密码企业对

密码从业人员状况的调研结果表明：未来3-5年内商用密码人才需求平均增长率为30%-60%。因此，在做好密码人才培养的顶层设计的同时，应加强推进校企合作培育，加强多层次、多场景的密码应用人才培养，推动产业的建设发展，这也是中国密码事业的百年大计。

从人才就业角度看，专业安全人员的价值真正受到重视，逐步独立、并列于IT信息化人才，而不再是像过去，保障信息安全或网络安全仅是IT开发运维人员的兼职而已。这让网络安全相关专业求职者在人才市场地位显著提升。结合当前我国在网络安全领域的立法和监管力度、深度，持续增加，广大政企单位招聘使用网络安全人才，不仅仅是自身的需要，更是国家和政府的要求。随着法律制度进一步完善，安全团队逐步成为政企单位组织的标配。政企机构必将更加重视和更多招用安全人才，按照国家相关合规标准与要求，逐步提升技术和管理手段，建立完善网络安全专门的机构职能体系。

密码学是一门综合性学科，与数学、物理、计算机、微电子、通信、网络等有着广泛而密切的联系。突破核心技术需要人才，打造安全产品需要人才，发展安全产业更需要人才。在目前的教育和培训体系下，面临着人才需求和人才提供非常不匹配的状况，如果人才培养的思路不跟上战略形势的发展，网络安全事业必将面临更大的困难。

三、专业现状调研

（一）专业点分布情况

密码技术应用专业于2021年列入《职业教育专业目录》。全国开设密码技术应用专业的大学有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、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、山东商业职业技术学院、聊城职业技术学院、深圳职业技术学院、重庆电子工程职业学院、陕西职业技术学院等。目前上海高职院校只有上海电子信息职业技术学院1家学校。全国开始密码相关专业的本科院校有北京理工大学、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、战略支援部队信息工程大学等。

（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。目前在校生共52人。

2.就业岗位情况分析

密码技术应用专业2021年开始招生，目前尚未有毕业生。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、密码测评工程师、网络安全与管理员、安全测评工程师等。

（三）专业教学情况及存在的主要问题

在现有学科和安全产业体系下，密码人才培养具有一定的局限性。突出表现为计算机学科背景下人才强于网络和系统安全，但对密码学及其之上的信息安全原理了解不够；而密码学出身人才的系统安全知识都相对缺乏。网络空间安全需要的是具有综合安全能力和素质的

人才，是具有从全面的视角来发现、分析和解决安全问题能力的人才。针对此类问题，经过大量研讨和论证，此次人才陪养方案调整方针为加强网络安全基础，突出密码特色。

四、专业人才培养方案优化建议

（一）专业岗位优化建议

信息技术应用创新已经成为当前形势下中国经济新动能，在外部严峻的形势背景与国内各项政策推动下，信创系统及大量国产设备在各行业推广部署。商用密码产品就属于我国信创产品。另外随着我国商用密码检测认证制度逐步建立，密评过程中不合格以及需进一步提高的环节，需要对其进行密码改造，增设密码改造产品，如服务器密码机、安全网关等，商用密码产品及部署运维人才急缺。此岗位与高职培养人才定位相符。因此，专业岗位增加商用密码部署与运维岗位。

（二）专业课程内容优化建议

1．扎实网络安全基础

专业课程中，《网络安全设备配置》建议改为专业必修，渗透测试增加前导课程《Web应用开发》。实训课程中可增设《linux服务与安全管理项目实训》、《网络安全防护项目实训》。

2．突出密码特色

根据岗位需求，增加《密码产品部署与运维项目实践》。《密码测评项目实战》是理实一体课程，名称建议更改为《商用密码应用安全性评估》。

（三）专业教学改革建议

1.教学资源

教学资源对于密码技术应用专业来说尤其重要。市面上有关密码技术教材多是本科教材，偏理论，需要建设符合职校教材。通过加强校企合作，引入企业资源，与企业联合方式开发工作式、活页式新型教材、实训类教材。

2.教学过程

教学过程宜采用轻理论，重应用，增设密码应用场景及密码服务实现功能，让学生理解密码的四大安全属性基础上，初步掌握密码理论与技术。

（四）专业师资与实训条件配置建议

加大对教师的培训，使教师能够尽快适应专业教学的需要。通过企业实践、项目实战等方式提高老师的技术技能水平，积极引进企业具有实际项目经验的企业教师，不断加强双师型教师队伍建设。建设配套实训室，如增加密码安全性评估的系统模拟仿真环境，提高实训教学效果。