上海电子信息职业技术学院

人才培养方案

2023级中高职贯通适用

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（中高职贯通）专业人才培养方案

一、专业名称及代码

中高职 名称代码	中职	高职
专业名称	计算机网络技术	信息安全技术应用
专业代码	710202	510207

二、入学要求

初中毕业或相当于初中毕业文化程度

三、修业年限

五年

四、职业面向

表1 本专业职业面向

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	计算机类 5102	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	华为认证工程师（HCIA-安全） 红帽认证工程师（RHCE） CISP-PTE 渗透测试工程师 网络安全运维（1+X 初级） 企业网络安全防护（1+X 初级） 企业网络安全防护（1+X 中级） 网络安全应急响应（1+X 中级）

五、培养目标与培养规格

（一）培养目标

本专业培养思想政治坚定，德技并修，德、智、体、美、劳全面发展，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，掌握本专业知识和主流的安全技术技能，有较强的就业能力和可持续发展能力，面向网络集成公司、网络设备厂商、安全设备厂商等互联网企业或者软件与信息服务企业，能够从事数据信息安全系统集成、网络安全运维、Web安全管理与评估、网络安全事件应急响应等工作的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，热爱社会主义祖国，在习近平新时代中国特色社会主义思想指引下，准确理解和把握社会主义核心价值观的深刻内涵和实践要求，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，具有正确的世界观、人生观、价值观；

（2）具有健康的体魄、心理和健全的人格，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，养成良好的健身与卫生习惯，以及良好的行为习惯，体能测试基本合格，提高自身心理健康水平，增强自我调适的能力，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）具有一定的审美、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）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，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）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；

（6）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，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。

（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）掌握必备通识性知识；

（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；

（6）掌握数据库方面知识；

（7）掌握DNS、DHCP和WEB服务器等常用服务器方面的知识；

（8）掌握交换机、路由器、防火墙的常用网络设备方面的知识；

（9）掌握网络安全设备的配置管理等方面的知识；

（10）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；

（11）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；

（12）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；

（13）熟悉信息安全管理体系、风险管理方法；

（14）了解常用WEB开发语言，中间件框架，JavaScript框架；

（15）了解应用开发的基本流程及关键点。

3．能力

（1）能设计、组建、维护与安全管理中小型企业网络；

（2）能使用网络操作系统、网络管理软件或工具、搭建服务器；

（3）能安装、配置、调试、维护路由器、交换机、无线设备等网络设备；

（4）能配置、调试、维护防火墙、VPN、入侵检测等网络安全设备；

（5）能检测、评估应用服务安全，加固安全服务；

（6）能集成、安全管理与维护信息系统；

（7）能撰写工程文件和渗透测试评估工作报告，查阅技术文献；

（8）能使用至少一种脚本语言（如python、perl、bash）进行开发；

（9）能使用至少一种开源的渗透测试工具；

（10）能分析网络数据；

（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）能进行探究学习、终身学习、从实践中分析问题和解决问题；

（13）能使用良好的语言、文字进行表达和沟通；

（14）能有效进行创业与学习、创新，快速适应岗位迁移。

六、课程设置及要求

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

公共基础必修课程有：中国特色社会主义、心理健康与职业生涯、哲学与人生、职业道德与法治、形势与政策、互联网+创业实践、思想道德与法治、毛泽东思想和中国特色社会主义理论体系概论、语文、数学、英语、物理、历史、军事理论与训练、信息技术基础、体育、应用文写作、心理健康教育、职业生涯规划与职业指导、大学生安全教育、劳动教育等。

2．公共基础选修课程

公共基础选修课程有：公共艺术选修课、公共通识选修课。

（二）专业课程

专业课程包括专业必修课程和专业选修课程。

专业必修课程

专业必修课程又分为专业基础课程和专业核心课程。

专业基础课程包括：计算机系统配置与维护、计算机网络技术、Web前端开发、数据库安全管理、Python程序设计基础、Linux操作系统基础、Web应用开发、Python网络编程、企业网络安全防护（初级）、网络攻防技术、网络安全应急响应等。

专业核心课程

专业核心课程包括：Linux服务与安全管理、网络安全设备配置、渗透测试、WEB服务安全（两学期）、网络系统安全管理、应用服务器加固等。

表2 专业核心课程主要教学内容

序号	课程名称	主要教学内容与要求
1	网络安全设备配置	**主要教学内容：**防火墙一般配置、防火墙的多种工作模式应用，配置防火墙的高可用性、VPN技术分类，VPN产品配置与应用、入侵检测的工作原理，入侵检测类产品的配置与应用、物理隔离产品（网闸类）的配置与应用。 **教学要求：**学生能够掌握网络边界安全设备的安全配置要求，理解防火墙的工作原理及配置策略及各类VPN技术在不同应用场景的配置。
2	网络系统安全管理	**主要教学内容：**Windows Server系统的安装、 DNS、DHCP服务器的架设与管理、WEB服务器的搭建与配置、FTP的搭建与配置、邮件服务的安装、配置与管理、NTFS权限的应用、域用户和组的管理、磁盘管理，防火墙的基本配置等。 **教学要求：**学生能够比较熟练地运用Windows Server系统组建企业常用服务器，并进行日常管理、服务功能的配置、日常排错以及资源管理。
3	WEB服务安全	**主要教学内容：**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。 **教学要求：**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应用安全有较为完整的认识，较全面地掌握维护WEB应用安全的管理技能。
4	渗透测试	**主要教学内容：**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。 **教学要求：**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。
5	应用服务器加固	**主要教学内容：**WEB服务器,数据库服务器安全等要注意的核心问题；服务器加固的常用方法；系统的安全加固、IIS加固和系统应用程序加固。 **教学要求：**学生能够设计本地账户策略，目录权限，系统安全策略，协议栈加强，系统服务和访问控制，本地安全策略设置，IPSec端口过滤等来整体提高服务器的安全性。能有效的提高web站点的安全性，合理分配用户权限，配置相应的安全策略，有效的防止IIS用户溢出提权，

序号	课程名称	主要教学内容与要求
		针对应用需求配置应用层防火墙过滤应用程序层的攻击。能实施SQL的安全配置以及服务器应用软件的安全加固来提高应用程序的安全性。
6	Linux服务与安全管理	**主要教学内容：**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。 **教学要求：**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。

专业选修课程

为专业拓展课程：包含网页设计与制作、网站系统配置与维护、网络设备配置与管理、网络安全运维技术、JavaScript 程序设计基础、C 语言程序设计基础、安全控制技术、网络存储技术、信息安全等级保护、信息网络布线技术、网络安全方案设计、信息安全管理、云安全技术与应用、虚拟化云技术、Windows 系统管理与应用、防火墙与 VPN 技术、Python 安全工具开发、创业创新教育等。

其中纯实践性教学课程为：计算机网络技术综合实训、Windows 系统安全实训、Linux 服务安全管理实训、企业网络安全防护（初级）实训、渗透测试实训、企业网络安全防护（中级）实训。

（三）实践性教学环节

实践性教学环节主要包括实验、实训、专业实践、认识实习、岗位实习等。实验实训可在校内实验室、实训室以及校外实训基地等开展完成；专业实践、社会实践、跟岗实习、顶岗实习可由学校组织在网络集成公司、网络设备厂商、安全设备厂商等企业开展完成。跟岗实习、顶岗实习等应严格执行《职业学校学生实习管理规定》。

（四）相关要求

学校将统筹安排各类课程设置，注重 Linux 服务与安全管理、网络安全设备配置等专业课程理实一体化教学；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；将创新创业教育融入专业课程教学和相关实践性教学；自主开设信息安全管理、安全控制技术、信息安全等级保护等特色课程；组织开展德育活动、志愿服务活动和其他实践活动。

七、教学进程总体安排

（一）学时安排

信息安全技术应用专业的教学活动周进程安排表如下表所示。

表3 教学活动周进程安排表　　（单位：周）

分类 / 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	合计
第一学期	1	（1）	16	0	1	1	0	1	4	24
第二学期	0	0	16	1	1	1	0	1	8	28
第三学期	0	0	16	1	1	1	0	1	4	24
第四学期	0	0	16	0	1	1	0	2	8	28
第五学期	0	0	16	1	1	1	0	1	4	24
第六学期	0	0	16	2	1	1	0	0	8	28
第七学期	1	（1）	16	0	1	1	0	1	4	24
第八学期	0	0	16	2	1	1	0	0	8	28
第九学期	0	0	1	0	16	0	2	1	4	24
第十学期	0	0	0	0	16	0	4	0	0	20
总计	2	0	129	7	40	8	6	8	52	252

（二）教学进度表

信息安全应用技术专业的专业指导性教学进程表如下所示。

表4 信息安全技术应用专业中高贯通人才培养方案5年教学进度表

课程类别	课程名称	学分	总学时	考试	实践学时	各学期周数、学分分配									
						1	2	3	4	5	6	7	8	9	10
						16	16	16	16	16	16	16	16	16	16
公共基础必修	中国特色社会主义	2	36	考试	8	2									
	心理健康与职业生涯	2	36	考试	8		2								
	哲学与人生	2	36	考试	8			2							
	职业道德与法治	2	36	考试	4				2						
	形势与政策 1	0.25	4	考查	0	0.25									
	形势与政策 2	0.25	4	考查	0		0.25								
	形势与政策 3	0.25	4	考查	0			0.25							
	形势与政策 4	0.25	4	考查	0				0.25						
	形势与政策 5	0.25	4	考查	0					0.25					

课程类别	课程名称	学分	总学时	考试	实践学时	各学期周数、学分分配									
						1	2	3	4	5	6	7	8	9	10
						16	16	16	16	16	16	16	16	16	16
	形势与政策 6	0.25	4	考查	0						0.25				
	形势与政策 7	0.25	4	考查	0							0.25			
	形势与政策 8	0.25	4	考查	0								0.25		
	互联网+创业实践	2	36	考试	16						2				
	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	4							2			
	习近平新时代中国特色社会主义思想概论	3	48	考试	4								3		
	语文 1	4	72	考试	8	4									
	语文 2	4	72	考试	8		4								
	语文 3	4	72	考试	8			4							

课程类别	课程名称	学分	总学时	考试	实践学时	各学期周数、学分分配									
						1	2	3	4	5	6	7	8	9	10
						16	16	16	16	16	16	16	16	16	16
	语文 4	2	36	考查	4				2						
	语文 5	2	36	考查	4					2					
	数学 1	4	72	考试	6	4									
	数学 2	4	72	考试	6		4								
	数学 3	4	72	考试	4			4							
	数学 4	2	36	考试	4				2						
	数学 5	2	36	考试	4					2					
	数学 6	4	64	考试	4							4			
	数学 7	2	32	考查	4								2		
	英语 1	4	72	考试	6	4									
	英语 2	4	72	考试	6		4								

课程类别	课程名称	学分	总学时	考试	实践学时	各学期周数、学分分配									
						1	2	3	4	5	6	7	8	9	10
						16	16	16	16	16	16	16	16	16	16
	英语 3	4	72	考试	6			4							
	英语 4	4	72	考试	6				4						
	英语 5	4	72	考试	6					4					
	英语 6	4	72	考试	6						4				
	英语 7	2	32	考试	6							2			
	英语 8	2	32	考试	6								2		
	历史 1	2	36	考试	6			2							
	历史 2	2	36	考试	6				2						
	物理 1	4	72	考试	16	4									
	物理 2	4	72	考试	16		4								

课程类别	课程名称	学分	总学时	考试	实践学时	各学期周数、学分分配									
						1	2	3	4	5	6	7	8	9	10
						16	16	16	16	16	16	16	16	16	16
	军事理论与训练 1	1	30	考查	30	1 周									
	军事理论与训练 2	2	32	考查	24							2			
	信息技术基础 1	3	54	考试	32	3									
	信息技术基础 2	3	54	考试	32		3								
	信息技术基础 3	3	54	考试	32				3						
	信息技术基础 4	1	18	考试	18					1					
	体育 1	2	36	考试	30	2									
	体育 2	2	36	考试	30		2								
	体育 3	2	36	考试	30			2							
	体育 4	2	36	考试	30				2						
	体育 5	2	36	考试	30					2					

课程类别	课程名称	学分	总学时	考试	实践学时	各学期周数、学分分配									
						1	2	3	4	5	6	7	8	9	10
						16	16	16	16	16	16	16	16	16	16
	体育 6	2	36	考试	30						2				
	体育 7	2	32	考查	30							2			
	体育 8	2	32	考查	30								2		
	应用文写作	2	36	考试	8						2				
	心理健康教育	1	16	考查	0							1			
	职业生涯规划与职业指导	1	16	考查	0								1		
	大学生安全教育	2	42	考查	8	*		*		*		*	2	*	
	劳动教育	1	16	考查	16									1	
	小计	**134**	**2372**		**656**	**23.25**	**23.25**	**18.25**	**17.25**	**11.25**	**10.25**	**16.25**	**12.25**	**1**	**0**
公共基础	公共艺术选修课 1	1	18	考查	8	1									
	公共艺术选修课 2	1	18	考查	8		1								

课程类别	课程名称	学分	总学时	考试	实践学时	各学期周数、学分分配									
						1	2	3	4	5	6	7	8	9	10
						16	16	16	16	16	16	16	16	16	16
选修	公共通识选修课 1	1	18	考查	8					1					
	公共通识选修课 2	1	18	考查	8						1				
	公共通识选修课 3	1	18	考查	8										
	公共通识选修课 4	2	32	考查	16							2			
	小计	7	122		56	1	1	0	0	1	1				
专业必修	计算机系统配置与维护	4	72	考试	48	4									
	计算机网络技术 1	2	36	考试	16	2									
	计算机网络技术 2	4	72	考试	48		4								
	计算机网络技术综合实训	1	30	考查	30		1 周								
	Web 前端开发	4	72	考试	48			4							
	Windows 系统安全实训	1	30	考查	30			1 周							

课程类别	课程名称	学分	总学时	考试	实践学时	各学期周数、学分分配									
						1	2	3	4	5	6	7	8	9	10
						16	16	16	16	16	16	16	16	16	16
	数据库安全管理	3	54	考试	32				3						
	Python 程序设计基础	3	54	考试	48				4						
	Linux 操作系统基础	4	72	考试	48				4						
	*Linux 服务与安全管理	4	72	考试	48					4					
	Linux 服务安全管理实训	1	30	考查	30					1 周					
	WEB 应用开发	4	72	考查	48					4					
	*网络安全设备配置	4	72	考试	48					4					
	企业网络安全防护基础	4	72	考试	48						4				
	企业网络安全防护基础实训	1	30	考查	30						1 周				
	*渗透测试	4	72	考试	48						4				
	渗透测试实训	1	30	考查	30						1 周				

课程类别	课程名称	学分	总学时	考试	实践学时	各学期周数、学分分配									
						1	2	3	4	5	6	7	8	9	10
						16	16	16	16	16	16	16	16	16	16
	*WEB 服务安全 1	4	72	考试	32						4				
	*WEB 服务安全 2	2	32	考试	24							2			
	*网络系统安全管理	4	64	考试	48							4			
	网络攻防技术	4	64	考试	48							4			
	网络安全应急响应	4	64	考试	48								4		
	*应用服务器加固	4	64	考试	48								4		
	职业技能认证实训	2	60	考试	60									2 周	
	认识实习	16	480	考查		1 周	1 周	1 周	1 周	1 周	1 周	1 周	1 周	8 周	
	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	113	2562		1706	6	4	4	11	12	12	10	8	18	16

课程类别	课程名称	学分	总学时	考试	实践学时	各学期周数、学分分配									
						1	2	3	4	5	6	7	8	9	10
						16	16	16	16	16	16	16	16	16	16
专业选修	创新创业教育	2	32	考查	0								2		
	网页设计与制作	2	36	考查	32		2								
	网站系统配置与维护	2	36	考查	32										
	Windows 系统管理与应用	4	72	考试	48			4							
	安全检测与评估	4	72	考试	48										
	网络设备配置与管理	4	72	考试	48			4							
	网络安全运维技术	4	72	考试	48										
	JavaScript 程序设计基础	2	36	考查	32				2						
	C 语言程序设计基础	2	36	考查	32										
	Python 网络编程	4	72	考试	48					4					
	Java 程序设计基础	4	72	考试	48										

课程类别	课程名称	学分	总学时	考试	实践学时	各学期周数、学分分配									
						1	2	3	4	5	6	7	8	9	10
						16	16	16	16	16	16	16	16	16	16
	安全控制技术	2	36	考查	32					2					
	网络存储技术	2	36	考查	32										
	防火墙与 VPN 技术	4	72	考试	32						4				
	路由与交换技术	4	72	考试	32										
	信息安全等级保护	2	36	考查	32						2				
	信息网络布线技术	2	36	考查	32										
	Python 安全工具开发	2	32	考查	24								2		
	安全风险管理	2	32	考查	24										
	云安全技术与应用	4	64	考查	48								4		
	虚拟化云技术	4	64	考查	48										
	网络安全方案设计	2	32	考查	16									2	

课程类别	课程名称	学分	总学时	考试	实践学时	各学期周数、学分分配									
						1	2	3	4	5	6	7	8	9	10
						16	16	16	16	16	16	16	16	16	16
	信息安全管理	2	32	考查	32										
	小计	34	592		400	0	2	8	2	6	6	0	8	2	0
合计		288	5648		2818	30.25	30.25	30.25	30.25	30.25	29.25	26.25	28.25	21	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．实训环境

职业教育要有效培养学生的职业能力，就必须强化实训、实践环节，加强职业教育与工作体系、工作过程的关联度。学生在实训实践中掌握相应的专业技能，提高适应职业岗位要求的能力，缩短从学校教育到实际工作岗位的距离。作为两校共享的实训基地，上海市行政管理学校具有功能完善的计算机信息技术实训中心，上海电子信息职业技术学院具有专业的信息安全专业实训室。

（1）上海市行政管理学校计算机信息技术实训中心实训室

表5 计算机信息技术实训中心实训室表

实训室名称	实训内容	工位数
网络安全管理实训室（H3C 设备）	网络设备的基础配置（接口，地址，网关，设备名称，设备基本信息） 基础路由协议的配置（静态路由、RIP 路由协议，ospf 路由协议） 配置交换机 VLAN,生成树配置 无线控制器配置（瘦 AP、胖 AP、无线加密协议配置）	48
综合布线实训室	各种电缆、光纤测试分析，对新安装的布线系统和网络系统进行验收认证测试 光纤、光缆尾纤连接方法训练 各种管线的安装、布线训练	48
计算机组装与维护实训室	Windows 系统加固 网络系统检测 系统检测报告的撰写	48
计算机应用实训室	软件的应用（office 软件、编程、平面设计类）	48
虚拟化实训室	部署云计算网络、云计算存储 部署云计算服务器、云计算虚拟化平台 部署云资源、管理虚拟机、部署 EVB 部署高可用性环境、部署网络管理平台 管理云服务、维护云计算系统	48

（2）上海电子信息职业技术学院信息安全专业实训室

信息安全技术应用专业目前建有，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。实训室主要功能见下表：

表6 校内实训室一览表

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 Linux 服务与安全管理、WEB 服务安全、渗透测试、防火墙与 VPN 技术、网络设备安全配置、网络攻防技术等特色鲜明、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，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

1．制度保障

在“信息安全技术应用专业建设指导委员会”指导下，成立“教学质量监控工作小组”和教学督导组，构建人才培养质量监控与保障体系。

为使人才培养方案实施制度化、科学化和规范化，保证教学工作有序进行、教学质量的不断提高，建立了管理规范体系：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》等，使整个人才培养过程做到有章可循、规范有序。

制定《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。

2．质量监控

为确保人才培养质量，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。通过行业、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。建立教材招标工作组，采用教材三级审核制。

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，完成规定的教学活动，德育合格，体育达标，所有课程全部考核合格，完成一年的认识实习和岗位实习，实习成绩考核合格，方可准许毕业。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。与本专业对接的可供选择的职业技能等级证书见下表。

表7 职业技能等级证书一览表

序号	职业技能等级证书名称	颁证单位	要求
1	华为HCIA-安全（A级）	华为技术有限公司	选考其中一个或多个
2	红帽认证工程师（RHCE）	红帽linux公司	
3	CISP-PTE渗透测试工程师	中国信息安全测评中心	
4	企业网络安全防护（1+X初级）	公安部第三研究所	
5	企业网络安全防护（1+X中级）	公安部第三研究所	
6	网络安全应急响应（1+X中级）	奇安信科技集团股份有限公司	

十、附录

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（中高职贯通）专业人才需求与专业改革调研报告

信息安全技术应用（中高职贯通）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

序号	企业名称	所在省（市）	企业性质	主营业务
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
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。

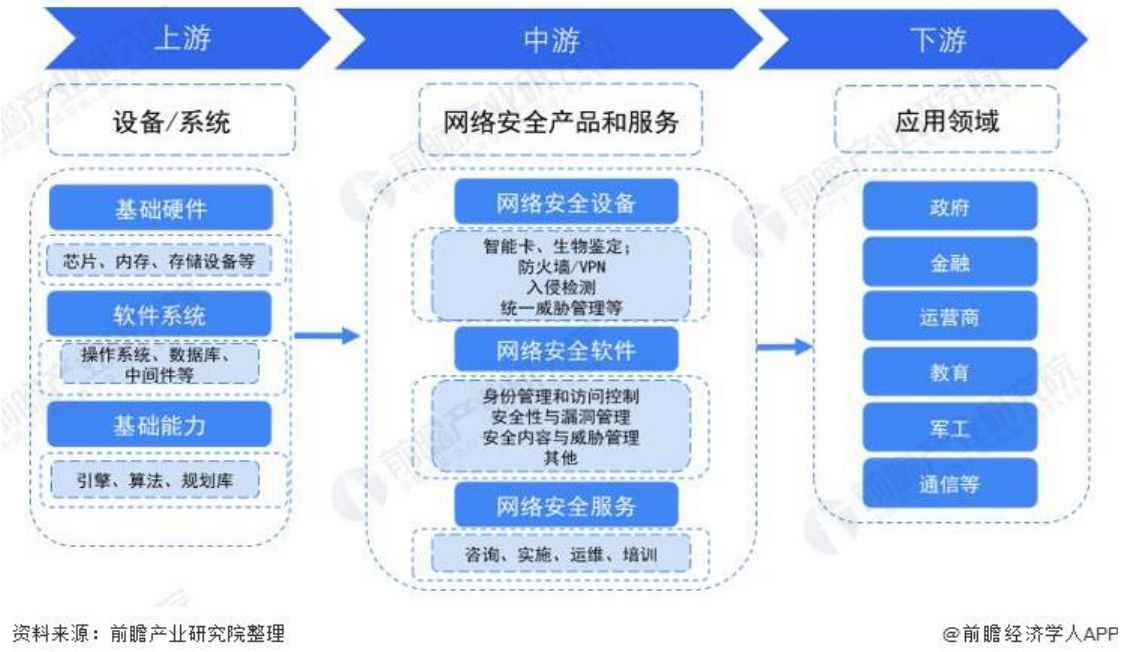

图1-5 网络安全行业产品链

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%。

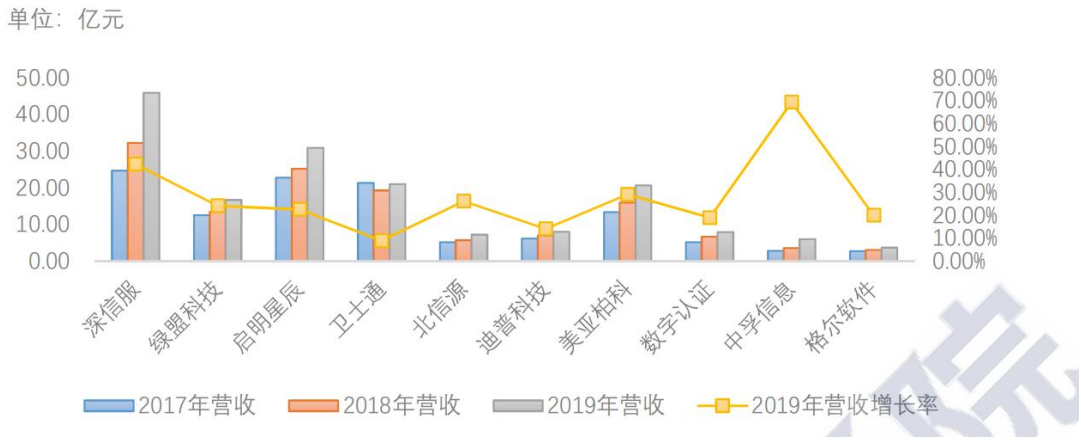

图1-6 网络安全企业营收

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；	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

序号	任务领域	典型工作任务	职业需求技能
		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。	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； 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

序号	任务领域	典型工作任务	职业需求技能
			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

序号	任务领域	典型工作任务	职业需求技能
			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。	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； 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	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；

序号	任务领域	典型工作任务	职业需求技能
		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。	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：

1）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。

2）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。

3）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, 这导致学生的实践能力和创新精神得不到充分锻炼和提高。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。

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

根据中高职贯通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 ，课程具有针对性，有取舍，真正的做到聚焦就业岗位。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《安全风险管理》替换为《信息安全管理》，介绍测评服务，包括等级保护、风险评估等。因为改课程综合性较强，建议放在第 5 学期。

（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。

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。