上海电子信息职业技术学院

人才培养方案

2023级高本贯通适用

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（高本贯通）专业人才培养方案 1

一、专业名称及代码 1
二、招生对象及学制 1
三、培养目标 1
四、人才规格 1
五、课程体系 3
六、专业教学安排 5
七、企业实习 15
八、主要课程介绍 16
九、实训资源配置 20
十、附录 23
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 24
附件 2 学术委员会审批意见 40

信息安全技术应用（高本贯通）专业人才培养方案

一、专业名称及代码

计算机科学与技术（080901）（本）
信息安全技术应用（510207）（高）

二、招生对象及学制

招生对象：上海生源，高中应届毕业生
学　制：五年

三、培养目标

培养具备良好的职业道德和职业素养，具有创新精神和国际视野，系统掌握信息安全的基础理论与方法，在数据应用安全方面具备扎实的专业知识和综合应用能力，能够从事计算机、电子信息、电子商务、互联网金融、云计算与大数据、WEB 应用等领域的数据安全应用、开发、安全测试与评估等方面的一线高水平信息安全应用型人才。

具体培养目标：

目标 1：培养大学生具备良好的人文社会科学素养和高度的社会责任感。

目标 2：能胜任信息安全软件开发、项目管理、安全测试安全评估等工作。

目标 3：获得信息安全工程师、信息安全测评师基本训练，使学生具有专业的职业素养和宽阔的视野。

目标 4：具有终生学习、继续教育、国际视野意识以及适应发展的能力，能够解决信息安全工程领域复杂工程技术问题，成为一线应用型工程技术人才。

四、人才规格

（一）知识要求

- 具有扎实的数学和物理学等自然科学基础，较好的人文社会科学基础；
- 具备扎实的英语知识基础并达到所要求的考级水平；
- 掌握计算机与网络通信的基本理论和基本知识；
- 掌握网络安全的基础理论和基本方法；
- 掌握操作系统基本原理、系统服务配置与安全管理的基础知识；
- 掌握程序设计的基础知识、基本思路和方法；
- 掌握数据安全的基础知识、基本思路和方法；
- 了解物联网安全的基础知识；
- 了解云安全的基础知识；
- 掌握信息安全工程与基础设施建设、实施与管理的基本技术和方法；
- 掌握数据安全产品研发的基础知识；
- 熟悉信息安全政策、法律、法规和标准；

- 了解信息安全领域的最新发展动向与技术；
- 具有本专业先进的和面向现代人才市场需求所需要的科学知识。

（二）能力要求

- 具备运用辩证唯物主义的基本观点和方法去认识，分析和解决问题的能力；
- 具备较强的语言及文字表达能力；
- 具备优秀的思维习惯和良好的逆向思维能力；
- 具备运用英语进行简单会话，能够阅读本专业英语文献，并具有一定的听、说、读、 写、译能力；
- 具备较强的数学处理与应用能力；
- 具备文献检索、资料查询及应用现代信息技术获取相关信息的基本能力；
- 具备利用计算机常用应用软件进行文字及其他信息处理的能力；
- 具备撰写专业科技文档和软件文档写作的基本能力；
- 具有掌握新知识、新技术的自学和继续学习能力；
- 具有从事本专业相关职业活动所需要的方法能力、社会行为能力和创新能力；
- 具有较强的组织、协调能力；
- 具有自尊、自爱、自律、自强的优良品格和人际交往及管理能力；
- 具有计算机系统安装、配置、调试与维护的能力；
- 具备网络架构设计、网络组建与设备互联的能力；
- 具备网络安全产品的选型、安装与配置能力；
- 具备网络运维与故障排查能力；
- 具有应用服务器的配置与安全加固的能力；
- 具备 Web 应用开发能力；
- 具备对信息系统的安全检测、渗透测试和漏洞挖掘的能力；
- 具备数据安全审计的能力；
- 具备数据安全理论研究的能力；
- 具备数据安全存储架构设计及工程实施能力；
- 具备分析、设计和优化信息系统安全架构的能力；
- 能够独立完成用户需求分析与方案设计；
- 能够进行信息系统的工程实施；
- 职业技能达到国内职业资格高级认证和国际行业企业职业资格认证的要求。

（三）素质要求

- 具备良好的思想品德、行为规范以及职业道德；
- 具备良好的心理素质；
- 具备较强的法律、法规意识；
- 具备良好的服务意识、保密意识；
- 具备对信息安全事件的敏感性；
- 具备创新、实践、创业的专业技术开发素质；

- 具备竞争意识、合作精神、坚强毅力；
- 具有健康的体魄、良好的体能和适应本岗位工作的身体素质和心理素质。

（四）职业资格证书

学生可以根据未来的工作岗位有针对性地选择职业资格技能认证，实现毕业证与技能证双证毕业。在第五学期之前（含第五学期）要求获得国内行业企业高级资格证书，在第八学期之前（含第八学期）获得国际行业企业职业资格证书。与本专业对接的可供选择的认证如表 1 所示：

表 1 职业资格证书要求

序号	认证类型	证书名称	发证单位	备注
1	国内职业资格认证	互联网管理人员（三级）	上海市人力资源和社会保障局	三选一（第 5 学期考）
		网络安全防护		
		信息安全架构		
2	国际行业企业资格认证	CompTIA 认证	美国计算机行业协会	选考一（第 8 学期考）
		红帽认证工程师（RHCE）	Red Hat 公司	
		华为认证网络资深工程师(HCNP)	华为公司	
		思科网络安全专家（CCSP）	思科公司	
		红帽认证架构师(RHCA)	Red Hat 公司	
		红帽认证安全专家(RHCSS)	Red Hat 公司	
		华为认证互联网专家（HCIE）	华为公司	
		思科认证互联网专家（CCIE）	思科公司	
		云安全知识认证（CCSK）	云安全联盟	

备注：证书类型可选，对应 4 学分。

五、课程体系

（一）课程类型设置

本专业课程根据岗位实际需求和能力培养规律分成四大类型，根据课程的重要性，设置不同的学分。具体课程组成及比例如下表 2 所示：

表 2 教学学时分配表

类　　型	学分	学时数			
		理论	实践	总计	比例
公共基础课	68.25	852	256	1108	22%
专业基础课	40	544	192	736	15%
专业必修课	39	432	384	816	16%
专业选修课	10	336	288	624	12%
实践教学	54	0	1728	1728	34%
合计	211.25	2164	2848	5012	100%

（二）公共基础课程

公共基础课程主要包括：大学英语、大学语文、大学物理、　军事理论及军事训练、体育、思想道德修养与法律基础、马克思主义基本原理概论、毛泽东思想和中国特色社会主义理论体系概论、大学生职业生涯发展与规划等

（三）专业基础课

专业基础课主要包括：计算机导论、计算机信息技术基础、程序设计基础、信息安全数学基础、离散数学、面向对象程序设计 1、数据结构与算法、计算机网络原理、操作系统原理、面向对象程序设计 2、概率论与数理统计、计算机组成与结构、线性代数、人工智能、编译原理。

（四）专业必修课

专业必修课主要包括：信息安全基础、Windows 安全与管理、数据库原理及安全、LINUX 系统与安全管理、应用密码学、服务器安全检测与加固、Web 应用开发、JAVA 程序设计、嵌入式系统开发、恶意代码原理与分析、网络安全协议分析、数据隐私与取证、移动应用开发、渗透测试、网络安全监管与评测、大数据挖掘与安全技术等。

（五）专业选修课

专业选修课包括：路由与交换技术、网络安全配置、虚拟化技术、Python 程序设计、安全标准与法律法规、物联网安全、云计算与安全、数据分析与建模、信息安全等级保护、社会工程学、大数据处理、情报分析、电子商务安全、电磁泄漏与物理安全、数据存储安全、源码审计等。

（六）实践教学

实践教学主要包括：计算机组成与维护实训、Windows 安全与管理实训、数据库原理及安全实训、面向对象程序设计实训、Web 应用开发实训、内网入侵检测系统与配置、企业综合实训（一）、攻防对抗实训、安全方案设计与工程实施、渗透测试实训、网络安全综合实训、企业综合实训（二）、毕业设计/论文等

六、专业教学安排

（一）教学进程表

表 3 教学进度表

分类	课程名称	考核方式	总学分	总学时	讲课课时	实验课时	上机课时	按学期周课时分配									
								1	2	3	4	5	6	7	8	9	10
公共基础必修	大学英语 1	考试	3.5	64	48	16		3.5									
	大学语文 1	考试	1.5	24	24	0	0	1.5									
	军事理论及军事训练	考查	2	32	8	24	0	2									
	体育（1）	考查	1.5	32	16	16		1.5									
	高等数学（1）	考试	6	96	96			6									
	思想道德与法治	考试	2.5	48	32	16		2.5									
	形势与政策	考查	0.25	4	4	0		0.25									
	习近平新时代中国特色社会主义思想概论	考试	3	48	48	0		3									
	大学物理 1	考试	3	64	32	32	0		3								
	大学英语 2	考试	3.5	64	48	16			3.5								
	大学生安全教育	考查	2	32	32	0	0		2								
	马克思主义基本原理概论	考查	2.5	48	32	16	0		2.5								

分类	课程名称	考核方式	总学分	总学时	讲课课时	实验课时	上机课时	按学期周课时分配									
								1	2	3	4	5	6	7	8	9	10
	体育（2）	考查	1.5	32	16	16			1.5								
	高等数学（2）	考试	6	96	96				6								
	大学物理 2	考试	3	64	32	32	0			3							
	大学英语 3	考试	3.5	64	48	16				3.5							
	毛泽东思想和中国特色社会主义理论体系概论	考查	2	32	32	0	0			2							
	体育（3）	考查	1.5	32	16	16				1.5							
	形势与政策	考查	0.25	4	4	0				0.25							
	大学英语 4	考试	2	32	32						2						
	大学语文 2	考试	1.5	24	24	0	0				1.5						
	大学生职业生涯发展与规划（1）	考查	0.25	4	4	0					0.25						
	体育（4）	考查	1.5	32	16	16					1.5						
	大学英语 5	考试	1.5	32	16	16						1.5					

分类	课程名称	考核方式	总学分	总学时	讲课课时	实验课时	上机课时	按学期周课时分配									
								1	2	3	4	5	6	7	8	9	10
	大学生职业生涯发展与规划（2）	考查	0.25	4	4	0						0.25					
	形势与政策	考查	0.25	4	4	0						0.25					
	形势与政策	考查	0.5	8	8									0.5			
	中国近现代史纲要	考试	3	48	40	8								3			
	大学生职业生涯发展与规划	考查	1	16	16									1			
	形势与政策	考查	0.5	8	8										0.5		
	大学生体育测试（一）	考试	0.5	8	8										0.5		
	大学生体育测试（二）	考试	0.5	8	8											0.5	
	小计		62.25	1108	852	256	0	20.25	18.5	10.25	5.25	2	0	4.5	1	0.5	0
通识选修	通识教育选修（公共通识选修）		4	64	64				4								
	艺术教育限选（公共艺术选修）		2	32	32				2								

分类	课程名称	考核方式	总学分	总学时	讲课课时	实验课时	上机课时	按学期周课时分配									
								1	2	3	4	5	6	7	8	9	10
小计			6	96	96	0	0	0	0	0	0	0	0	0	0	0	0
专业基础	计算机导论	考试	3.5	64	48	16		3.5									
	计算机信息技术基础	考试	3	64	32	32		3									
	程序设计基础	考试	2.5	48	32	16			2.5								
	信息安全数学基础	考试	2	32	32	0				2							
	离散数学	考试	3	48	48	0				3							
	面向对象程序设计 1	考试	3	64	32	32				3							
	数据结构与算法	考试	2.5	48	32	16				2.5							
	计算机网络原理	考试	3	64	32	32					3						
	操作系统原理	考试	1.5	32	16	16					1.5						
	面向对象程序设计 2	考试	2.5	48	32	16					2.5						
	概率论与数理统计	考试	3	48	48	0						3					
	计算机组成与结构	考试	3	48	48	0						3					
	线性代数	考试	4	64	64									4			
	人工智能	考查	2	32	32	0								2			

分类	课程名称	考核方式	总学分	总学时	讲课课时	实验课时	上机课时	按学期周课时分配									
								1	2	3	4	5	6	7	8	9	10
	编译原理	考试	1.5	32	16	16									1.5		
	小计		40	736	544	192	0	6.5	2.5	10.5	7	6	0	6	1.5	0	0
专业必修	信息安全基础	考试	2.5	48	32	16			2.5								
	Windows 安全与管理	考查	3	64	32	32				3							
	数据库原理及安全	考试	2.5	48	32	16					2.5						
	LINUX 系统与安全管理	考查	2.5	48	32	16						2.5					
	应用密码学	考试	2.5	48	32	16						2.5					
	服务器安全检测与加固	考查	2	48	16	32						2					
	Web 应用开发	考查	3	64	32	32						0		3			
	JAVA 程序设计	考试	2	48	16	32								2			
	嵌入式系统开发	考查	2	48	16	32								2			
	恶意代码原理与分析	考查	1.5	32	16	16								1.5			
	网络安全协议分析	考试	2	48	16	32								2			

分类	课程名称	考核方式	总学分	总学时	讲课课时	实验课时	上机课时	按学期周课时分配									
								1	2	3	4	5	6	7	8	9	10
	数据隐私与取证	考试	2.5	48	32	16								2.5			
	移动应用开发	考查	3	64	32	32								3			
	渗透测试	考试	3	64	32	32									3		
	网络安全监管与评测	考试	2.5	48	32	16									2.5		
	大数据挖掘与安全技术	考试	2.5	48	32	16									2.5		
	小计	考查	39	816	432	384	0	0	2.5	3	2.5	7	0	16	8	0	0
专业选修	路由与交换技术	考查	2	48	16	32					2						
	虚拟化技术	考查	2	48	16	32					2						
	网络安全配置	考查	2	48	16	32						2					
	云计算与安全	考查	2	48	16	32						2					
	Python 程序设计	考查	2	48	16	32									2		
	安全标准与法律法规	考查	1	16	16	0									1		
	物联网安全	考查	1	16	16	0									1		
	数据分析与建模	考查	1.5	32	16	16									1.5		

分类	课程名称	考核方式	总学分	总学时	讲课课时	实验课时	上机课时	按学期周课时分配									
								1	2	3	4	5	6	7	8	9	10
	信息安全等级保护	考查	1.5	32	16	16									1.5		
	社会工程学	考查	1.5	32	16	16									1.5		
	大数据处理	考查	1.5	32	16	16									1.5		
	情报分析	考查	2	32	32	0									2		
	电子商务安全	考查	2	32	32	0									2		
	电磁泄漏与物理安全	考查	2	32	32	0									2		
	数据存储安全	考查	3	64	32	32									3		
	源码审计	考查	3	64	32	32									3		
	小计（选修 15 学分）		10	624	336	288	0				2	2			6		
实践教学	计算机组成与维护实训	考查	1	32	0	32		1									
	Windows 安全与管理实训	考查	1	32	0	32				1							
	数据库原理及安全实训	考查	1	32	0	32					1						

分类	课程名称	考核方式	总学分	总学时	讲课课时	实验课时	上机课时	按学期周课时分配									
								1	2	3	4	5	6	7	8	9	10
	面向对象程序设计实训	考查	1	32	0	32					1						
	Web 应用开发实训	考查	1	32	0	32						1					
	内网入侵检测系统与配置	考查	1	32	0	32						1					
	企业综合实训（一）	考查	16	512	0	512							16				
	攻防对抗实训	考查	1	32	0	32								1			
	安全方案设计与工程实施	考查	1	32	0	32								1			
	渗透测试实训	考查	1	32	0	32									1		
	网络安全综合实训	考查	1	32	0	32									1		
	企业综合实训（二）	考查	12	384	0	384										12	
	毕业设计/论文	考查	16	512	0	512											16
	小计		54	1728	0	1728	0	1	0	1	2	2	16	2	2	12	16
全程总计			211.25	5108	2260	2848	0	27.75	23.5	24.75	18.75	19	16	28.5	18.5	12.5	16

（二）学年课程学时表

表 4 学年课程学时表

学　年	总学时数	理论		实践	
		学时数	占比	学时数	占比
第一学年	940	676	72%	264	28%
第二学年	928	528	57%	400	43%
第三学年	952	232	24%	720	76%
第四学年	1288	720	56%	568	44%
第五学年	904	8	1%	896	99%
合 计	5012	2164	43%	2848	57%

（三）教学安排相关说明

1.师资要求

（1）专任专业教师具备硕士学位以上或副教授职称以上。

（2）本专业专任专业教师“双师”资格（具备相关专业职业资格证书或企业经历）的比例要达到 50%以上。

（3）专任教师需具备高等学校教师资格证。

2.实训实践教学要求

实训实践教学要求实践教学包括实验、实训、企业实习等项目。实训课时一般不低于该课程总课时的 50%。实训课时缺课超过 1/2 或实训成绩不及格者，原则上不得参加相应课程的考试。本计划实训教学体系的设计，按照基础、提高、综合三个层次和基本实训、单项技能训练、综合技能训练、综合在岗/企业实习等模块构建实践能力培养体系。

3.实施安排

（1）本方案规定的总学时数为 5012（211.25 学分），其中实践学时数为 2848，占 57%。

（2）本方案的实训、实践环节体现在各门课程的实践课时、实践周及企业实习中。

（3）本方案在实施过程中，课程开设顺序与周课时安排可根据实际情况进行微调。

4.教学评价

（1）理论性较强的课程以笔试考核为主，能力考核以过程性考核为主，可以根据不同课程的特点和要求采用笔试、口试、实操等多种方式进行考核，操作技能考核以目标性考核为主，可以根据不同课程的特点和要求采用作品展示、成果汇报、职业资格证书等多种方式进行考核。

（2）各门课程应该根据课程的特点和要求，对采用不同方式、对各个方面的考核结果，通过一定的加权系数评定课程最终成绩，具体每门课程的考核要点权重由课程教学方案负责制定。

说明：形成性评价是在教学过程中对学生的学习态度和各类作业情况进行的评价；目标性评价是在教学模块结束时，对学生完成设定课程目标所需的某项职业能力的评价。若模块考评同时采用形成性评价和目标性评价时，建议采用 5：5 的方式评分。课程按百分制考评，60 分以上（含 60 分）为合格。

七、企业实习

企业实习是教学过程中的一个重要组成部分，是检验学生的实际动手能力和技能熟练程度的必要过程，也是学生从学校走向社会的必要环节。根据信息安全行业快速发展，实习采用更为灵活的机制，服务学生，服务社会，促进教学，形成教学----实习----反馈----改进教学的良性循环。

通过建立学校与企业联合培养机制，充分发挥企业在人才培养上的优势，使学生的课堂学习与工作实践有机结合起来，做到企业人才培养前移和学生的职业认知前移，从而实现企业、学校和学生的共赢。

学生在企业实习期间应该遵守企业各项规章制度，不迟到不早退，积极主动完成企业分配的任务，与同事和谐相处；认真总结实习工作中遇到的问题和收获体会，撰写实习记录；及时与学校的指导老师联系并接受指导老师的指导；实习结束后提交企业实习报告。各学期企业实习具体安排如表 5 所示：

表 5 企业实习安排表

	时间安排	实习内容	实习目标
第六学期	12 周	●任务 1：针对实习岗位撰写实习计划书； ●任务 2：掌握软件开发流程知识； ●任务 3：以实际所做的项目为例说明项目过程中所需要掌握的基础知识、工具、步骤与方法。	锻炼学生软件设计及代码编写的能力，锻炼学生发现问题和解决问题的能力。
第九学期	12 周	●任务 1：针对实习岗位撰写实习计划书； ●任务 2：完成漏洞挖掘与分析的学习； ●任务 3：以实际的项目为例分析网络安全方案设计所需要的知识，设计的步骤、方法、技术等； ●任务 4：完成小型商务网站的安全维护项目。	在企业老师的指导下完成漏洞挖掘与分析课程的学习；深化对课程知识的理解，培养学生项目管理的能力和源码审计的能力。
第十学期	20 周	●任务 1：针对实习岗位撰写实习计划书； ●任务 2：毕业设计的选题； ●任务 3：完成毕业设计。	培养学生信息安全技术的综合应用能力、方案设计能力和工程实施能力。

八、主要课程介绍

表 6 课程说明

模块	课 程	介 绍	学时
公共基础课	大学英语	本课程打破传统公共英语+专业英语模式，根据信息安全岗位对英语的需求培养学生英语听、说、读、写能力，鉴于本课程对信息安全学生学习能力培养具有重要的作用，故分为 5 个学期不间断学习和训练，并在第六学期之前通过大学英语四级考试。同时教学内容与国际信息安全事件和最新的安全技术相对接。	256
	大学数学	本课程对信息安全学生能否学好信息安全技术及应用至关重要，所以本课程分为 6 个学期不间断学习和训练。 教学内容服务专业课程对数学的要求，以够用为准，以实用为主，对传统大学数学课程体系根据专业课的需要打散与重构，主要讲授函数、极限、一元微积分、二元微积分、一元微分方程、线性微分方程、微分方程应用、逻辑思维训练、关系划分与应用、图、树、矩阵计算、线性变换、线性方程组、代数系统、群、环、域、优化算法、智能计算、随机事件与概率、随机变量与分布、数学特征与极限定理等。	320

模块	课　程	介　绍	学时
计算机基础	计算机信息技术基础	本课程是为计算机专业学生开设的一门计算机基础课，属计算机方面的入门级课程。内容涉及计算机的基本知识、微机操作系统、常用的文字处理软件、多媒体技术、INTERNET 基础知识和使用、网页设计等。	64
	计算机组成与结构	通过本课程教学，使学生了解计算机的组织结构和工作原理，能够系统地掌握微型计算机的结构、微处理器和指令系统、微机系统的接口电路设计等、掌握微型计算机汇编语言程序设计方法。 课程的主要内容包括：计算机的基础知识、汇编语言、计算机的各子系统（包括运算器、存储器、控制器、外部设备和输入输出子系统等）的基本组成原理、设计方法、相互关系以及各子系统互相连接构成整机系统的技术。	64
网络安全	计算机网络原理	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 协议工程和 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基础。 本课程的主要内容包括：网络体系结构、网络编址、网络寻址、局域网组建、网络传输控制、网络服务、广域网接入等。	64
	信息安全基础	通过课程学习，学生将具备计算机安全防御的技能，并能够依据实际需求，设计和部署计算机安全组件，增强计算机系统与网络的安全防范能力。通过本课程的学习，使学生对信息安全领域有一个较为全面的了解，初步了解和掌握计算机安全学、系统与网络安全的基本理论、体系、方法与技能。 本课程的主要内容包括：信息与信息安全认识、物理安全与信息安全风险评估、经典信息加密方法、信息加密应用、信息隐藏与数字水印操作、黑客与系统嗅探、病毒防治等。	48
	网络安全监管与评测	本课程是为计算机科学与技术专业数据应用安全方向学生开设的专业必修课。课程可安排在第八学期。通过本课程的学习，使学生了解网络安全管理、计算机信息网络国际联网安全管理、互联网用户的用网行为安全规范、互联网单位用户的安全管理、互联网上网服务营业场所安全管理、信息系统安全等级保护制度、计算机病毒防护、计算机信息系统安全专用产品安全管理以及网络安全标准与评测等，为学生今后进行网络管理、维护以及安全技术服务奠定基础。	64
	网络安全协议分析	通过本课程的学习，学生将学习 6 种常见的安全协议，了解它们在 OSI 七层模型中的层次，并理解这些安全协议能够提供的安全服务，加密和认证机制、工作原理及应用领域等。 本课程的主要内容有：网络认证协议 Kerberos、安全电子交易协议 SET、安全套接层协议 SSL、安全超文本传输协议 HTTPS、安全电子邮件协议 S / MIME、网络层安全协议 IPSec。	48

模块	课　程	介　绍	学时
系统安全	Windows 安全与管理	通过本课程教学，使学生具备运用 Windows Server 及 Linux 系统组建企业常用服务器、系统管理网络资源的能力，掌握 Windows 服务器系统的日常管理、服务功能的配置、日常排错以及资源管理的方法。 课程的主要内容包括：网络的分类、拓扑结构、网络操作系统的安装、常用的网络命令、系统基本配置、共享文件的应用、用户和组的管理、域与活动目录、NTFS 权限的应用、磁盘管理、DNS、DHCP、WEB、FTP、邮件服务的基本配置和维护、远程管理与终端服务、防火墙的基本配置等。	64
	操作系统原理	通过本课程教学，使学生具备掌握操作系统的基本工作原理和设计方法，把所学原理贯穿到具体的 Windows 系统中，增强平台管理能力。 课程的主要内容包括：操作系统的概述、进程管理、设备管理、文件系统、操作系统安全，并行与分布式操作系统、操作系统的前沿技术。	32
	LINUX 系统与安全管理	通过本课程的教学，要求学生能够进行日常企业工作中的常见网络系统安全防护管理工作。对网络系统安全有一个整体的认识，全方位、立体化的综合掌握网络系统的安全管理知识。本课程分别在第四和第五学期实施。 课程的主要内容包括：服务器的安全管理、保障数据传输安全、架设 CA 服务器，具有申请与签发证书的能力；能对 WEB、FTP 服务器进行安全维护，架设 SSL 网站；具有 PKI 公钥基础架构基础知识，能架设独立的 CA，申请与签发相应的证书；邮件的数字签名与加密使用网络管理工具等。	96
	服务器安全检测与加固	通过本课程教学，使学生具备对服务器漏洞的检测、漏洞的修补及加固的能力、熟练掌握常用的检测及加固工具，对服务器进行多维防护。 课程的主要内容包括：服务器漏洞的检测修补加固、HIPS-主机入侵防护系统的应用、对拒绝攻击的防范、从系统内核入手的防范四个方面。	48
应用开发与安	数据结构与算法	通过本课程的教学，培养学生逻辑思维能力、程序编码能力和解决实际问题能力，对学生毕业后从事软件编码以及其它分析力较强的岗位工作的职业能力培养和职业素养起着重要的支撑作用。 课程的主要内容：描述数据结构的概念，各种存储表示方法，顺序表的查找、插入和删除，单链表的查找、插入和删除操作等。	48

模块	课　程	介　绍	学时
全	程序设计基础	通过本课程的教学，学生掌握结构化程序设计思想，具有一定的简单代码编写能力，能看懂程序流程图。 本课程的主要内容：C 语言数据类型、变量、控制语句、数组、函数定义与调用、指针、文件读写	64
	数据库原理与应用	通过本课程的教学，学生能够掌握数据库的基本原理、基本操作和数据库系统设计开发的基本方法，使学生有现代信息管理的科学素质，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。 课程的主要内容包括：数据库的安装、环境的搭建和数据库的基本概念、数据库（表）的创建和使用、数据库数据的查询、数据库程序的设计与使用、游标的设计与使用、视图的使用、创建和管理存储过程、创建和管理触发器、数据库的安全保护机制、备份和恢复数据库。	48
	面向对象程序设计	通过本课程的教学，学生能够理解掌握面向对象程序开发思想，并能从面向对象的角度设计开发中小型的桌面应用程序。本课程分别在第三和第四学期实施。 本课程的主要内容包括：类、继承、多态、接口的概念、常用类的使用、IO 流、异常、线程、GUI、网络编程等。	112
	JAVA 程序设计		48
	移动应用开发	通过本课程的教学要求：学生能够根据产品需求分析，运用 Android 各种视图控件和相应的 API 实现 Android 产品的设计、实现、测试及维护。本课程分别在第六和第七学期实施。 本课程主要内容：java 程序设计基础、android 环境的搭建、UI、四大组件、数据存储、线程、网络编程等内容。	128
	Web 应用开发	通过本课程的学习，学生掌握 web 应用程序的工作原理，能利用主流 web 应用开发工具编写简单的 web 应用后台服务程序。 本课程的主要内容：前台表单数据与后台程序交互、后台程序访问数据库、Session 与 Cookie 技术、Ajax 技术、文件上传与下载。角色分配与权限管理技术、利用框架或模板进行快速开发。	64
	应用密码学	通过本课程的学习，学生将能够在密码分析和加密技术两方面加强，能够独立研究密码变化的客观规律，用于编制密码并保守通信秘密的，并且能应用密码学的原理去破译密码以获取通信内容。 本课程的主要内容有两部分：一是加密技术，分为：古典密钥 、对称加密、公钥体系、序列密码、量子密码。 二是分析技术，针对加密技术的种种攻击手段进行分析，同时按密码体系分析密钥分配、密码协议、密码算法、密钥共享、身份认证等。	48

模块	课　程	介　绍	学时
信息安全综合实践	渗透测试	通过本课程的学习，学生能够在信息系统的不同位置（比如从内网、从外网等位置）利用各种手段对某个特定网络和应用系统进行测试，以发现和挖掘系统中存在的漏洞，然后输出渗透测试报告，并提交。 本课程的主要内容有：漏洞扫描，权限提升、密码攻击、社会工程学、无线网络攻击、渗透测试工具使用等。	64
	大数据挖掘与安全技术	通过本课程的学识可以理解理解大数据安全的基本内容、核心技术、使用机制，掌握大数据安全的关键技术和应用实践。 本课程的主要内容：大数据与云计算、大数据安全威胁、大数据安全、大数据安全保障技术、大数据安全保障实践、大数据安全应用技术、大数据安全应用实践、大数据安全趋势与应对策略。	48
	攻防对抗实训	通过本课程的学习可以使学生能够解决不同的网络应用环境中遇到的信息安全问题，成为具备基本安全知识和技能的安全应用型人才。能正确配置网络安全产品、实施应用安全技术、熟练掌握各类安全工具的使用方法，并能规划不同应用网络环境中的安全方案及应急响应策略。 本课程的主要内容包括：个人主机的攻防、办公网络攻防、企业网络的攻防等。	48
	安全方案设计与工程实施	通过本课程的教学，培养学生能按照网络安全设计和等级保护理念，规范、准确、熟练地完成网络方案设计任务的人才。 课程主要内容包括：网络方案整体设计、网络安全规划设计、网络方案的实施等方面。	32

九、实训资源配置

作为两校共享的实训基地上海应用技术大学和上海电子信息职业技术学院具有专业的信息安全实训室。上海应用技术大学现有“网络原理实训室”、“信息安全实训室”、“Web开发实训室”等专业实训室并计划增建云安全实训室和物联网安全实训室（见表1-8）。实训内容侧重与让学生理解网络通信的工作原理、加密解密的工作原理和实现、网络协议的分析、网络攻防技术的研究等深层次的信息安全实验。（见表7）。上海电子信息职业技术学院信息安全技术应用专业目前已建成，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）、计算机网络安全实训室、无线网络安全管理实训室、综合布线实训室、程序设计实训室等7个专业实训室，工位数294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（见表8）。实训室的条件可以支撑

学生进行网络综合布线、网络互联、网络设备配置、网络服务管理等侧重于培养学生的技能项目。两校实训室从硬件设备到实训功能上均形成了互补，各自可以发挥自己的优势对学生不同层次的实践能力加以重点的训练。

表 7 上海应用技术大学实训室表

实训室名称	教学与训练	工位数
网络原理实训室	● 交换机基本使用实训； ● 路由器基本使用实训； ● 交换机带内访问实训 ； ● 路由协议配置实训； ● 网络边界安全实训。	42
信息安全实训室	● 经典密码算法； ● 现代密码算法； ● 网络攻防实训一； ● 网络攻防实训二； ● 网络攻防实训三； ● 部署构建 VPN 实训； ● 计算机病毒攻防实训。	42
Web 开发实训室	● Web 服务器配置实训； ● Web 应用开发实训一（小型商务网站）； ● Web 应用开发实训二（中型商务网站）； ● Web 安全实训；	42
云安全实训室	● 虚拟化平台搭建实训； ● 云计算平台搭建实训； ● 大数据处理。	42
物联网安全实训室	● 通信安全实训； ● RFID 安全实训； ● ZigBEE 安全实训； ● 物联网系统安全实训。	42

表 8 上海电子信息职业技术学院实训室表

实训室名称	教学与训练	工位数

实训室名称	教学与训练	工位数
计算机网络管理实训室	● 网络系统的基础设置（域目录管理，WEB 应用服务，DNS 网络服务，DHCP 网络服务）； ● Linux 系统配置（网络系统基础配置，web 服务配置，DNS 服务配置，DHCP 服务系统配置）； ● 网页设计与制作、数据库安全管理、WEB 应用开发、网站系统配置与维护实训。	42
计算机网络互联实训室（Cisco 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，EIGRP 路由协议）； ● 配置交换机 VLAN，生成树配置，VTP 配置； ● 接口安全配置，802.1X 协议配置。	42
计算机网络互联实训室（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。	42
无线网络安全管理实训室	● 无线控制器配置（瘦 AP、胖 AP、无线加密协议配置）； ● Windows、Linux 系统渗透； ● 网站跨站攻击； ● 系统暴力破解。	42
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。	42
计算机网络安全实训室	● Windows 系统加固； ● 网络系统检测； ● 系统检测报告的撰写。	42
程序设计实训室	● C 语言程序设计实训； ● C#语言程序设计实训； ● Java 程序设计实训； ● Android 程序设计实训； ● 数据库应用系统设计实训； ● 网站开发实训。	42

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：学术委员会审定意见

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
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。

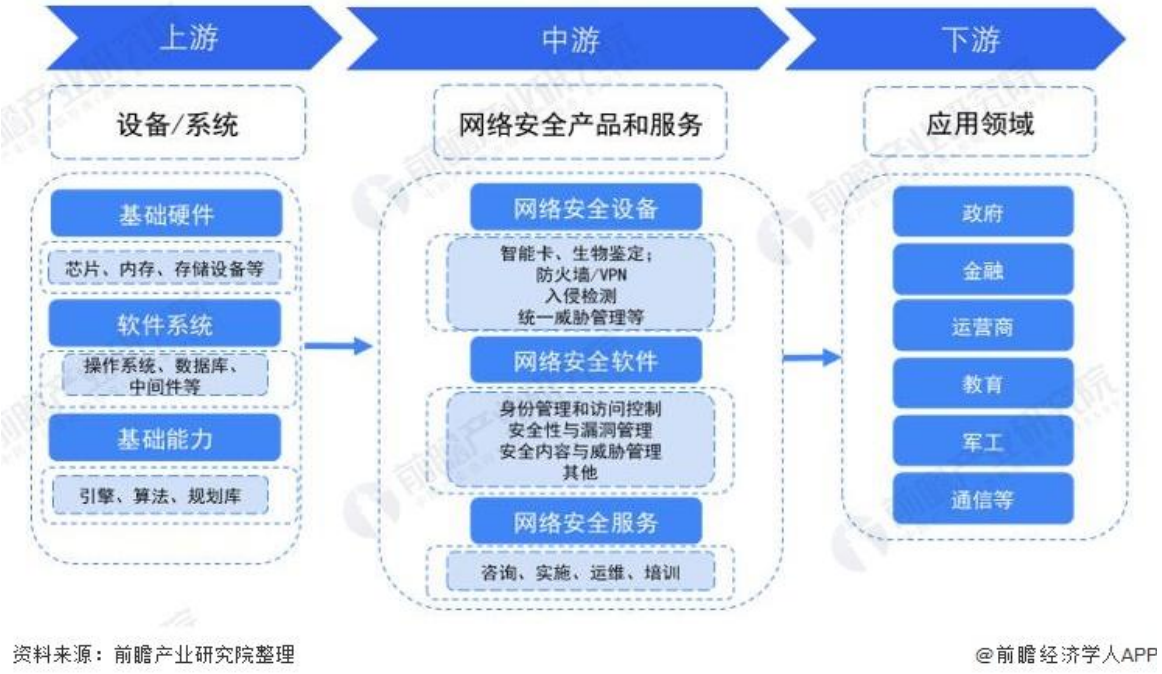

图 1-5 网络安全行业产品链

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%。

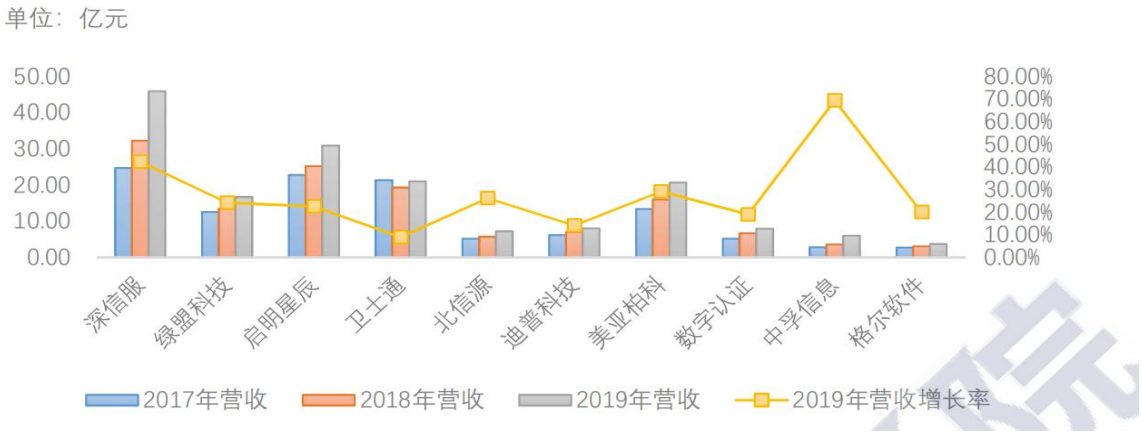

图 1-6 网络安全企业营收

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 信息安全岗位群专业技能要求分析表

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； 9．信息安全体系规划、ISMS 建设。	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； 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；

序号	任务领域	典型工作任务	职业需求技能
			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； 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；	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；

序号	任务领域	典型工作任务	职业需求技能
		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。	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	1．能熟练配置 Windows、Linux 下	1．具备选择适当技术的规划设计能力来；

序号	任务领域	典型工作任务	职业需求技能
	安全管理员	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。	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

序号	任务领域	典型工作任务	职业需求技能
			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）专业课程内容优化建议

从专业课程设置来看基本满足本专业人才培养的需要，建议保持稳定，不做修改。公共基础课，根据公共基础学院的要求，将原有的《毛泽东思想和中国特色社会主义理论体系概论 1》和《毛泽东思想和中国特色社会主义理论体系概论 2》合并为《毛泽东思想和中国特色社会主义理论体系概论》。

（二）专业教学改革建议

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。

（三）专业师资与实训条件配置建议

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。