

上海电子信息职业技术学院

人才培养方案

2024 级高本贯通适用

申安网络安全产业学院

教务处汇编

2024 年 7 月

目录

信息安全技术应用（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	10
八、主要课程介绍	10
九、实训资源配置	14
十、 附件	15
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	16

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 2-1 所示:

表 2-1 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 2-4 所示:

表 2-4 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	72.25	1012	256	1268	24%
专业基础课	40	544	192	736	14%
专业必修课	39	432	384	816	16%
专业选修课	12	368	288	656	13%
实践教学	54	0	1728	1728	33%
合计	217.25	2356	2848	5204	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、人工智能伦理与安全、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 2-5 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	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		1.5									
	军事理论及军事训练	考查	2	32	8	24	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		0.25									
	习近平新时代中国特色社会主义思想概论	考试	3	48	48		3									
	大学物理 1	考试	3	64	32	32		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		2								
	马克思主义基本原理概论	考查	2.5	48	32	16		2.5								
	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			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				2							
	体育（3）	考查	1.5	32	16	16			1.5							
	形势与政策	考查	0.25	4	4				0.25							
	大学英语 4	考试	4	64	64					4						
	大学语文 2	考试	1.5	24	24					1.5						

	大学生职业生涯规划与发展规划(1)	考查	0.25	4	4					0.25						
	体育(4)	考查	1.5	32	16	16				1.5						
	大学英语 5	考试	3.5	64	48	16					3.5					
	大学生职业生涯规划与发展规划(2)	考查	0.25	4	4						0.25					
	形势与政策	考查	0.25	4	4						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				
	大学生职业生涯规划与发展规划	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		66.25	1172	916	256	20.25	18.5	10.25	7.25	4	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							
	小计		6	96	96	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				2							
	离散数学	考试	3	48	48				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						3					
	计算机组成与结构	考试	3	48	48						3					
	线性代数	考试	4	64	64							4				

	人工智能	考查	2	32	32								2			
	编译原理	考试	1.5	32	16	16								1.5		
	小计		40	736	544	192	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							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			
	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	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									1		
	物联网安全	考查	1	16	16									1		
	数据分析与建模	考查	1.5	32	16	16								1.5		
	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									2		
	电子商务安全	考查	2	32	32									2		
	电磁泄漏与物理安全	考查	2	32	32									2		
	人工智能伦理与安全		2	32	32									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）		12	656	368	288			2	2				8		
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							
	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	1	0	1	2	2	16	2	2	12	16
全程总计			217.25	5204	2356	2848	27.75	23.5	24.75	20.75	21	16	28.5	20.5	12.5	16

（二）学年课程学时表

表 2- 6 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	1024	624	61%	400	39%
第三学年	984	296	30%	688	70%
第四学年	1352	752	56%	600	44%
第五学年	904	8	1%	896	99%
合 计	5204	2356	45%	2848	55%

（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 5204（217.25 学分），其中实践学时数为 2848，占 55%。
- （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 2-7 所示:

表 2-7 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 2-8 课程说明

模块	课 程	介 绍	学时
公共基础	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	256

模块	课 程	介 绍	学时
课		信息安全事件和最新的安全技术相对接。	
	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
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	48

模块	课 程	介 绍	学时
		子邮件协议 S / MIME、网络层安全协议 IPSec。	
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 design 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
应用开发与安全	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
	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	48

模块	课 程	介 绍	学时
		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。	
	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
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

模块	课 程	介 绍	学时
	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 2-9）。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 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 2-10）。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 2-9 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；	42

实训室名称	教学与训练	工位数
	● ZigBEE 安全实训； ● 物联网系统安全实训。	

表 2-10 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
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、附件

附件 1 信息安全技术应用专业人才需求与专业改革调研报告

附件 2 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（高本贯通）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，了解教育部批准的网络与信息安全相关的 1+X 证书试点情况；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。

围绕上海加快发展现代服务业和先进制造业、发展低炭和高附加值经济和重大经济建设项目的需要，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) 与信息安全工作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

序号	企业名称	所在省（市）	企业性质	主营业务
				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

2023年11月～2024年1月，进行走访企业现场调查，问卷调查。

2024年3月～2024年4月，受疫情影响，采用电话或者视频方式进行询问。

2024年5月，调研结果分析、完成调研总结报告。

二、专业人才需求调研

（一）相关行业发展现状

随着大数据、云计算、移动互联网、物联网的不断发展，网络的边界越来越模糊，安全形势也越来越复杂化，虚拟空间和实体空间结合的越来越紧密，网络安全的范畴发生了很大的变化。现目前对网络安全行业的发展主要是针对三个方面的发展，主要包括防火墙、身份认证、终端安全管理、安全管理平台等传统产品；云安全、大数据安全、工控安全等新兴产品；以及安全评估、安全咨询、安全集成为主的安全服务。

2019年，虽然我国在网络安全领域取得了新的成就，但全球网络空间的情况依旧纷繁复杂。人工智能、区块链、5G、量子通信等具有颠覆性的战略性新技术突飞猛进，大数据、

云计算、物联网等基础应用持续深化，数据泄露、高危漏洞、网络攻击以及相关的智能犯罪等网络安全问题随着新技术的发展呈现出新变化，严重危害国家关键基础设施安全、挑战人民群众隐私安全甚至危及社会稳定。

2019年，我国不仅持续优化了网络安全的政策环境和产业生态、在网络安全技术产品取得新成就，同时还不断强化网络安全人才队伍建设，以保障网络安全产业的强劲发展势头和向好的网络安全形势。虽然在多个方面取得了良好的成绩，但我国当前的网络安全形势仍然严峻，个人信息与重要商业数据依旧遭遇大规模泄露与违规利用，针对关键信息基础设施的恶意网络攻击在2019年频发，另外还有多个高危漏洞被曝出严重危害网络安全。

2020年，近年来，随着全球网络空间快速发展，高危漏洞、大流量DDoS攻击、数据泄露事件频发，各国逐步出台并实施网络安全合规要求。信息泄露、网络诈骗和网络骚扰是网络安全最突出的问题。77.31%的从业人员认为网络安全最突出或亟需治理的问题是信息泄露。网络诈骗、网络骚扰关注度达65.58%和62.01%。行业内遭受网络勒索病毒、木马等的入侵而导致经济上受损的时有发生，渗透率达到53.81%，情况比较严重。

2021年，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。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”。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。

网络安全问题和网络安全事件仍呈较高发生率，57.86%从业人员认为供应链安全威胁比较高和非常高。43.42%的从业人员常遇到安全隐患(硬件漏洞、代码漏洞等)，41.48%从业人员遇到恶意程序(勒索病毒、挖矿勒索等)。

当前，网络安全已成为事关国家安全的重大问题和世界各国面临的共同挑战，对于当前面临各类政治风险、经济风险和社会风险；对于不断为带领人民全面建成小康社会和为实现民族复兴不断努力的中国而言，网络安全更是我国在实现政治安全、保障人民安全、维持社会稳定、实现小康社会和谋求民族复兴道路上的重要保障。

从安全人才需求的月度指数变化来看，2018年下半年以来，11月份出现第一个高峰，2019年6月份则是第二个高峰。第一个高峰源自于2018年10月，公安部发布《公安机关互联网安全监督检查规定》，这一规定的出台客观上要求被检查单位必须建立常态化的安全队伍，切实建立安全保障体制机制；第二个高峰则是业界关注的“等保2.0”发布的时间段，网信办和工信部颁布的相关安全管理规定，呼应了社会对网络与信息安全的关注，同时也对互联网企业、安全厂商、各大政企单位提出更高的安全合规要求，而这些制度的落实都离不开安全责任人的人才储备。从人才需求特征来看，2019年度网络安全人才市场呈现需求进一步增长、用人单位的地域分布进一步下沉、人才需求更加多样化、基础化、体系化（常态化）等

特点。数据显示，北京、深圳、上海、成都、广州是网络安全人才需求量最大的城市，这五个城市对网络安全人才需求的总量占全国需求总量的48.8%。相较于2018年需求量前五的城市占全国的60.7%，2019年的需求占比总和降低了约16个百分点，这表明更多地区加大了对网络安全的投入，增加了对网络安全人才的需求。2020年，由于疫情的严重影响，2020年网络安全行业的人才需求和供给明显下降，人才需求增幅为-8.48%。2021年上半年，网络安全人才需求快速回暖，增幅达到39.87%，超过2019年的16.11%，网络安全在各行业的渗透率全面提高，在人才需求结构中的重要性显著上升。在网安人才需求持续升温的人才市场状态下，网络安全人才供给虽每年在稳步递增，但网安人才市场仍供小于求。逐步增加的招聘岗位数，愈发精确的安全岗位人才需求，亟需学校输送更多高质量人才进入市场。

目前，国内3000所高校仅120所开设相关专业，年培养1-2万人，加上10-20家社会机构，全国每年相关人才输送量也才约3万多人。如果随着国内“新基建”的不断发展，网安人才缺口势必将会越来越大。

校企合作加快培育安全人才，已经有近半数的高校开展校企合作育才实践，就本科学校而言，北航、北邮、哈工大等多所高校分别与360企业安全、绿盟、永信至诚、安恒等成立校企联合实验室；

全国各地加快网络安全产业布局，产业集聚效应初显。其中华东地区的杭州出台信息安全十三五规划。入驻杭州的企业包括杭州迪普、安恒信息、阿里等。华南地区的深圳成立网络安全创投中心，出台专项扶持政策。深圳企业包括华为、腾讯、深信服、国民技术、任子行等。华北地区的北京的国家网络安全产业园区采取“产业联盟+创新基地+产业基金”的运营方式。知名企业包括奇安信、启明星辰、绿盟、天融信、华为等。西部地区的成都打造国家信息安全成果产业化（西部）基地。另有国家西部信息安全产业园等。龙头企业包括中国网安、亚信安全、卫士通等。

（二）行业从业人员基本情况

行业从业情况的数据主要是根据中国信息安全测评中心的调研报告得出。中国信息安全测评中心主办了“中国信息安全从业人员现状调研（2018-2019年度）”调研活动，该活动通过在线问卷调查、一线实地访谈、专家会商研讨等方式，从“调研对象、工作状况、流动配置、能力提升、制度环境、安全态势”六大维度深度调研信息安全从业人员及当前人才环境现状。

1、报告调研对象

报告首次对信息安全这一非传统领域的从业人员进行定义和分类，将调研对象明确为“以信息安全工作职责为主要社会劳动分工和生活来源的人员”，并把信息安全从业人员工作角色分为6个大类，14个子类。调研显示，当前承担安全运营（62.4%）和安全建设（32.4%）工作角色的信息安全从业人员数量最多；45.5%的从业人员在私营企业任职，其次为国有企业（19.3%）和政府机关事业单位（16.5%）；近四成（38.4%）从业人员都参加过实战类网络安全竞赛。

（1）根据工作角色

承担安全运营（62.4%）和安全建设（32.4%）工作角色的信息安全从业人员数量最多（见图2-2）。其中安全运营包括安全运维（22.2%）、审计与评估（17.5%）、应急响应（9.9%）、数据处置（9.0%）和安全态势分析（3.8%）；安全建设包括分析设计（14.8%）、开发与集成（17.6%）。其余工作角色类别依次是规划管理（26.9%）、科研教育（17.2%）、监管治理（16.7%）和内容安全。

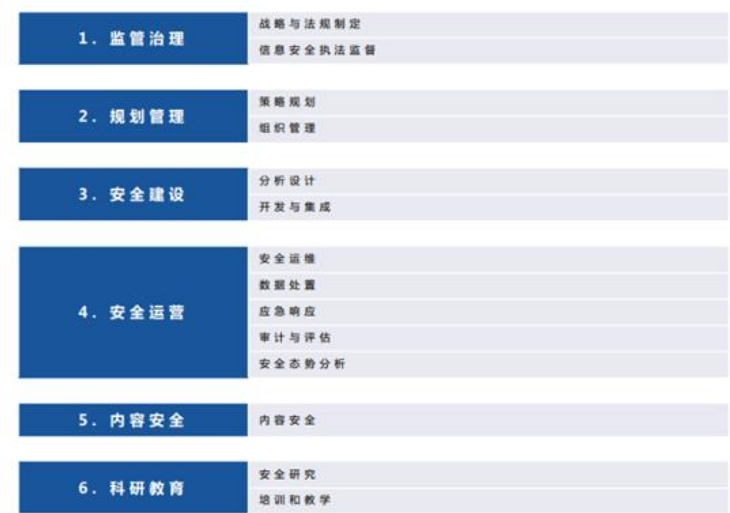


图1 调研首次提出的6个工作角色大类的划分

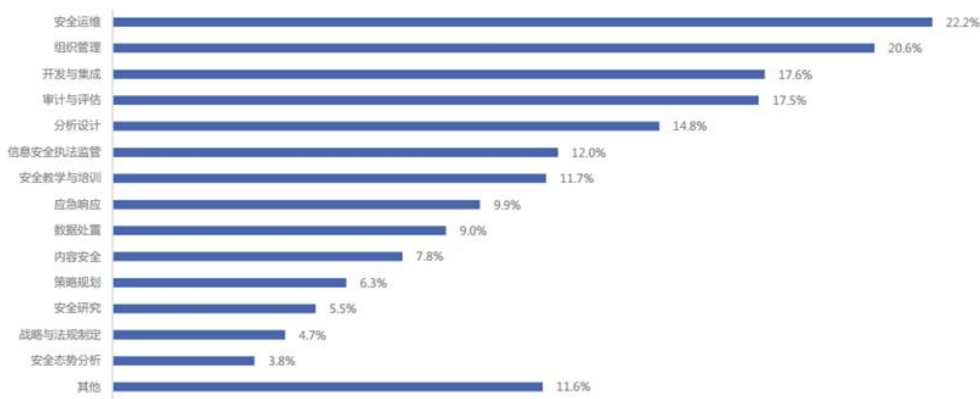


图2 受访者工作角色图（样本量 4349 人）

（2）根据从业年限

样本数据显示，目前我国信息安全从业人员从业年限大多在十年以下，其中拥有1-5年从业年限的人数占比最高，为45.5%；拥有6-10年从业经验的人数占比次之，为28.4%。10年以上工作年限从业人员占比为14.2%，同上一年度相比上涨了2.6个百分点（见图3）。

（3）根据单位性质

本次调研样本数据显示我国私营企业任职的信息安全从业人员最多，占比45.5%（见图4，）

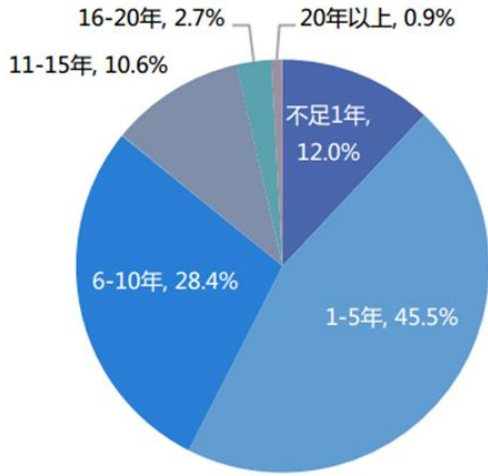


图3 受访者从业年限分布图

其次为国有企业（19.3%）和政府机关事业单位（16.5%）。

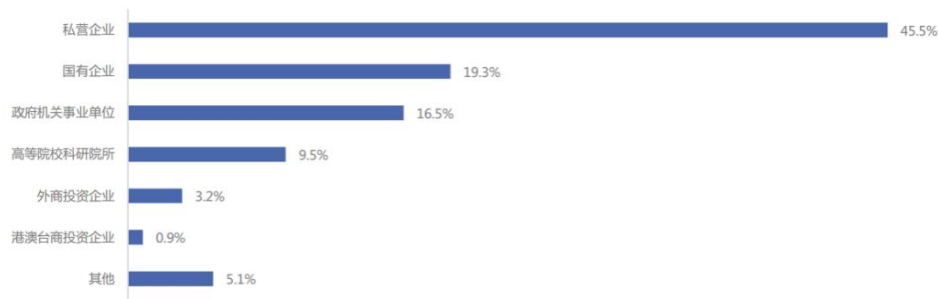


图4 受访者工作单位性质分布图（样本量 4349 人）

（4）根据所属行业

调研数据显示，我国信息安全从业人员最集中的是技术密集的信息技术|通信|互联网行业，占比 51.1%。其次为政府机关和事业单位（18.1%）、金融（7.7%）等行业（见图6）。

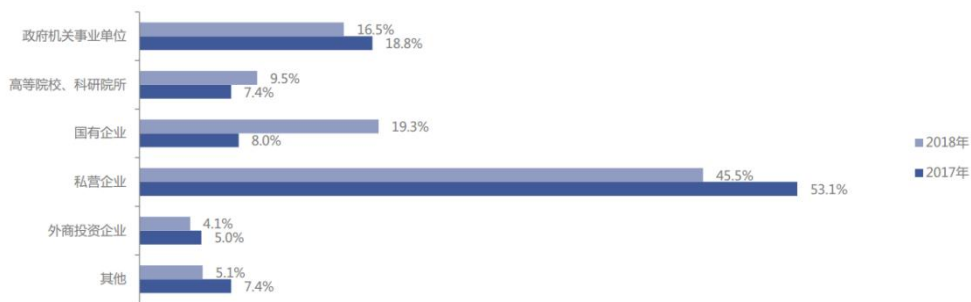


图 5 2017 年和 2018 年受访者工作单位性质分布对比图

(5) 根据单位规模

调研显示,我国大多数信息安全从业人员所在的工作单位为 300 人以下人员规模的中小

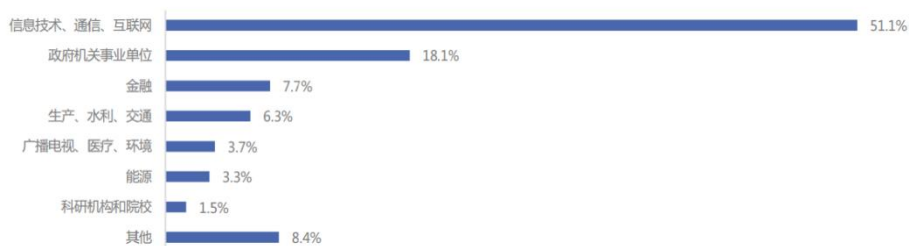


图 6 受访者行业分布图（样本量 4349 人）

型企业, 占比 55.1%（见图 7）。单位人员规模在 1000 人以上的从业人员占比 30.9%；单位人员规模在 20 人以下的人群占比最少, 仅为 7%。

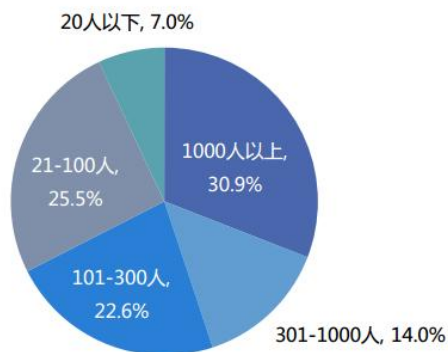


图 7 受访者工作单位人员规模分布图（样本量 4349 人）

(6) 根据竞赛经验

近年来,各类企事业单位、关键信息基础设施运营单位组织和参与网络安全攻防挑战赛、红蓝对抗、技能竞赛热度空前,实战演练在网络安全人才选拔和练兵等方面发挥了重要作用。调研发现,近四成(38.4%)从业人员表示参加过实战类网络安全竞赛,其中参加过面向国内从业人员的网络竞赛群体占比最高,为24.1%(见图8)。

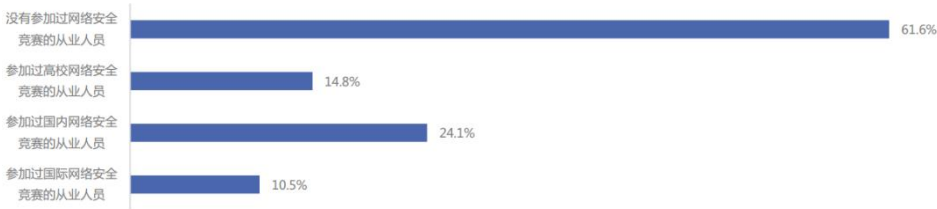


图8 受访者参加实战类竞赛情况分布图(样本量4349人)

2、工作状况

调研数据显示,除信息安全专业服务企业、特大型企业集团,以及大型互联网企业建立有较大规模的信息安全人才梯队外,50%的政企单位信息安全团队人员规模在20人以下;近六成信息安全从业人员需要承担非信息安全内容的工作,政府机关事业单位信息安全工作人员“身兼数职”现象最显著;各种类型的人才均存在短缺现象,其中承担安全建设和规划管理类工作角色的人才相对更加紧缺。

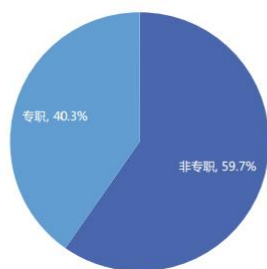


图9 信息安全行业受访者专职和非专职占比分布图（样本量4349人）

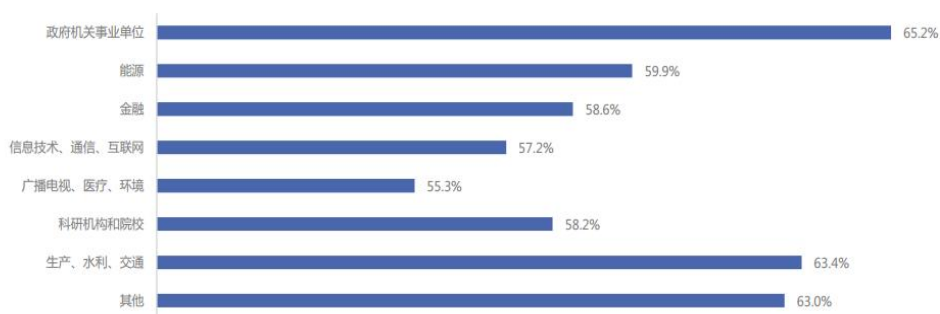


图10 不同行业非专职信息安全从业人员占比分布图（样本量 2596 人）

调研数据显示，除信息安全专业服务企业、特大型企业集团，以及大型互联网企业建立有较大规模的信息安全人才梯队外，50%的政企单位信息安全团队人员规模在 20 人以下；近六成信息安全从业人员需要承担非信息安全内容的工作，政府机关事业单位信息安全工作人员“身兼数职”现象最显著；各种类型的人才均存在短缺现象，其中承担安全建设和规划管理类工作角色的人才相对更加紧缺。

受访者认为当前各类型的信息安全工作角色均存在短缺现象，其中最为紧缺的工作角色主要包括“安全建设”类中的分析设计（35.9%）和开发与集成（30.5%）两个子类，“规划管理”类中的策略规划（27.6%）和组织管理（33.5%）两个子类，以及“监管治理”类中的战略与法规制定（25.3%）和信息安全执法监管（24.6%）两个子类（见图 11）。

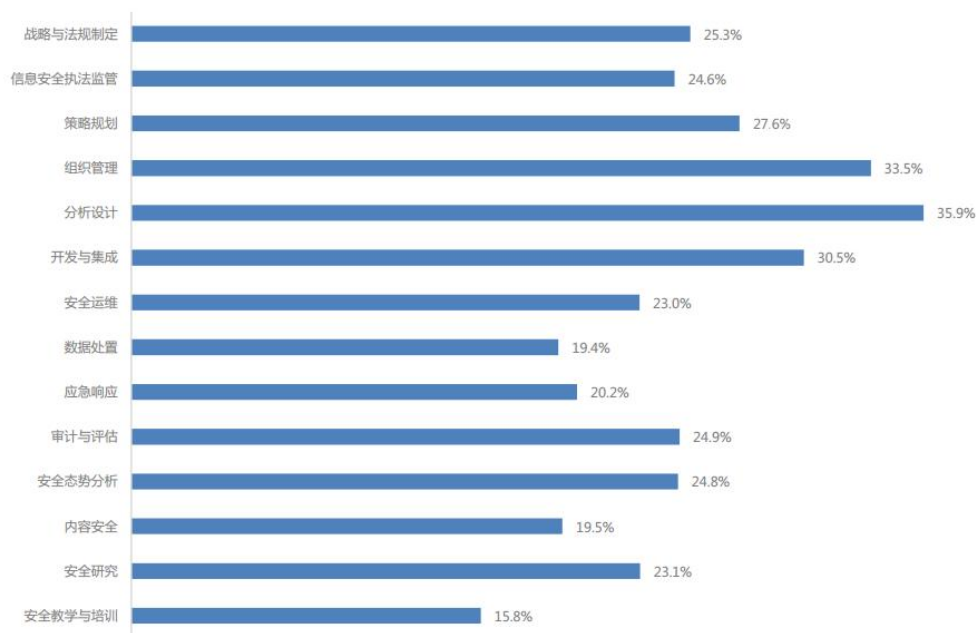


图 11 信息安全人才缺乏类型分布图（样本量 4349 人）

3、流动配置

信息安全从业人员平均年薪约为 15.3 万元，同 2018 年度相比薪酬继续上涨，但增幅有所缩减；42.9%的信息安全从业人员工作压力感受明显，但对职业发展前景多持乐观态度；过去三年人才流动速度放缓，影响职业流动的原因依次是“薪酬”、“晋升空间”、“工作氛围”和“自我价值实现”，显示从业人员对工作的福利性因素和发展性因素均十分看重。

（1）关联分析信息安全从业人员参赛经验和薪酬情况发现，参加过国内网络安全竞赛的从业人员平均年薪（17.0 万元）显著高于没有竞赛经验的人员（14.8 万元）（见图 12）。

（2）从单位质上看，除其他未分类工作单位外，受访者中超过一半人员认为用人单



图 12 参加不同类型网络安全竞赛从业人员的平均年薪分布（样本量 4347 人）

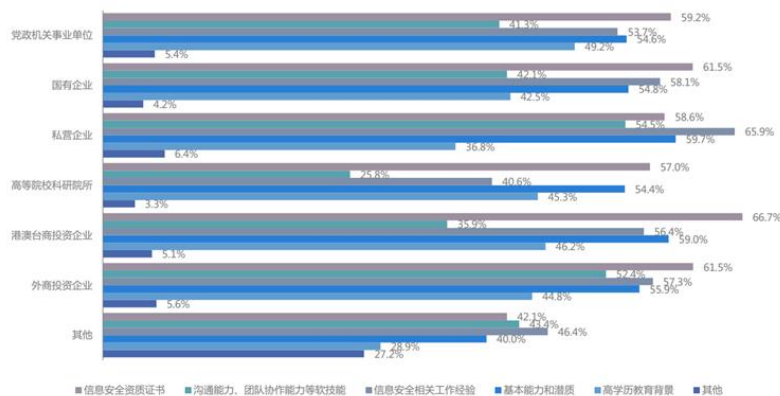


图 13 不同性质工作单位看重的人才资质条件分布（样本量 4349 人）

位最看重人才的信息安全专业资质证书持有情况。其中，国企、科研院所、党政机关事业单位、外商投资企业和港澳台投资企业的受访者对于信息安全专业资质证书的认可度最高。大部分私营企业受访者认为用人单位对人才的信息安全相关工作经验（65.9%）要求较高，其次是基本能力和发展潜质（59.7%）以及信息安全专业资质证书持有情况（58.6%）（见图 13）。

4、能力提升

从业人员在各细分方向均存在能力提升需求，排名靠前的依次是大数据安全、云安全、安全管理和渗透测试；在各类信息安全证书中，从业人员持有最多（71.8%）、最希望获取（68.9%）注册信息安全专业人员（CISP）资质证书。

对图 11 数据进行分析，目前对于最为紧缺的工作角色主要包括“安全建设”类中的分析设计（35.9%）、开发与集成（30.5%）；“规划管理”类中的策略规划（27.6%）和组织管理（33.5%）两个子类，以及“监管治理”类中的战略与法规制定（25.3%）和信息安全执法监管（24.6%）两个子类。从上述数据可以看出，除去开发与集成这个子类是属于技术类，其他子类大多偏向管理子类，充分说明目前的市场对于信息安全管理类方面的人才还是比较紧缺的。

根据图 12 数据得出，拥有竞赛经验以及持有专业资质证书的求职者是人才需求方比较青睐的，对于专业的人才培养方案修订者来说，该数据充分说明可以借助信息安全各项大赛用以培养学生动手能力以及思维辩证能力；

根据图 13 数据，对于求职者来说，信息安全专业资质证书是职业生涯里面比较重要的一类证书。

三、专业现状调研

（一）专业点分布情况

全国现有 108 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。

在这 108 所院校中，仅有 25 所高职院校将信息安全技术应用专业划为重点专业发展，其中重庆市的 7 所院校都将该专业设为了重点专业。

（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

职业 岗位	典型工作 任务分析	职业能力分析	
		职业能力要求	相关知识
数据安全 测评 工程师	信息安全测评	● 能够制定简单的被测对象的核查列表； ● 能进行内外网分段安全测试； ● 能够利用网络截包工具对网络数据进行分析； ● 能够利用相关安全扫描工具对	● 掌握计算机网络的基础知识； ● 熟悉无线局域网安全标准； ● 熟悉 Windows、Linux 等操作系统的使用； ● 熟悉应用服务器的配置与管理； ● 熟悉 Web 应用开发与安全防护

职业 岗位	典型工作 任务分析	职业能力分析	
		职业能力要求	相关知识
		测评对象进行检测； ● 能够利用渗透工具对漏洞进行验证； ● 能够结合重要性和发现的脆弱性进行系统综合风险分析。	的知识； ● 掌握软件测试的方式与流程； ● 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； ● 熟悉常用的安全检测软件； ● 掌握网络攻防技术。
	信息安全加固	● 能够根据测评结果结合用户需求，制订网络安全解决方案； ● 能够实施信息系统的安全加固方案。	● 熟悉 Windows、Linux 操作系统安全防护设置； ● 熟悉常见数据库的安全配置和管理； ● 熟悉数据备份与远程容灾； ● 熟悉无线局域网防护方法； ● 熟悉 TCP/IP 协议，精通思科、华为等交换、路由设备的管理和配置； ● 熟悉防火墙、IDS、IPS、WAF 的配置与管理； ● 熟悉网络程序设计语言； ● 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； ● 精通 Windows、Linux 平台下的各类网络 WEB 应用； ● 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； ● 熟悉常用的信息安全测评相关标准； ● 计算机基础应用知识； ● 熟悉信息安全的常见体系架构。
渗透测试工程师	渗透测试	● 能够制定渗透测试的计划； ● 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； ● 能够对操作系统平台、网络应用服务进行渗透检测； ● 能够对 Web 应用系统进行渗透检测； ● 能够对移动环境进行渗透检测； ● 能够利用渗透工具对漏洞进行验证；	● 熟悉渗透测试的步骤、方法、流程； ● 熟悉 TCP/IP 协议，熟悉网络设备（路由器、交换机）的配置及安全特性； ● 熟悉防火墙、IDS、IPS、WAF 安全特性； ● 熟悉无线局域网安全标准与防护方法； ● 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；

职业岗位	典型工作任务分析	职业能力分析	
		职业能力要求	相关知识
		● 能自行开发渗透测试的脚本或工具软件； ● 能够分析和检测恶意代码； ● 能够进行源码审计； ● 能够进行漏洞的挖掘与分析。	● 熟悉 Windows、Linux 及移动操作系统常见的漏洞与危害； ● 掌握主流数据库结构以及安全特性； ● 熟练掌握各种渗透测试工具； ● 熟悉网络程序设计语言； ● 熟悉 Web 开发语言； ● 熟悉软件测试流程与技术； ● 熟练掌握 SQL 注入/XSS/CSRF/文件上传/文件包含/命令执行等漏洞利用方法，熟悉 OWASP TOP 10 漏洞； ● 熟悉移动应用的开发技术； ● 掌握一门以上的脚本语言； ● 熟悉漏洞挖掘的理论与方法； ● 熟悉社会工程学常用的攻击方法。
	撰写渗透测试报告	● 具备文档撰写能力，能出具渗透测试评估报告； ● 能够针对渗透测试结果提出相应的整改方案； ● 能够对网络安全方案进行实施与检测。	● 计算机基础应用知识； ● 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； ● 熟悉常用的信息安全测评相关标准； ● 熟悉信息安全的常见体系架构。
数据安全运维与管理工程师	网络安全运维与管理	● 能够分析计算机和网络设备常见的硬件故障； ● 具有分析网络结构、排查网络线路故障能力； ● 能够利用网络截包工具对网络数据进行分析； ● 能够对操作系统平台、应用服务平台进行安全检测； ● 能够分析网络协议存在的漏洞； ● 能够利用工具对信息系统进行初步的安全评估； ● 能够规划并实施广域网安全方案； ● 能够根据应用需求，制订及实施网络安全解决方案； ● 能够连接网络互联和安全控制设备； ● 能够要求安装网络操作系统配	● 掌握计算机网络基本原理； ● 熟悉 PC、服务器硬件等设备； ● 熟悉 Windows、Linux 等操作系统的使用； ● 熟悉无线局域网安全标准； ● 熟悉各种网络安全协议； ● 掌握渗透测试的流程、方法； ● 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； ● 熟悉常用的安全检测软件； ● 熟悉虚拟化技术； ● 熟悉云计算技术的基本架构； ● 熟悉云计算的安全技术； ● 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； ● 了解相关的信息运行与安全规范，如 ITIL、ISO20000、等级保

职业 岗位	典型工作 任务分析	职业能力分析	
		职业能力要求	相关知识
		置基础服务； ● 能够使用常用的网络管理工具； ● 能够对主要的应用服务进行加固处理； ● 能够进行关键业务数据安全的管理； ● 能够开发网络应用程序； ● 能够优化网络体系结构； ● 能够制定并实施网络安全管理制度； ● 能够撰写网络运维报告。	护等相关知识； ● 熟悉计算机的组装与配置； ● 掌握 Windows、Linux 操作系统的管理与应用； ● 掌握 Windows、Linux 操作系统安全防护设置； ● 掌握计算机网络基本原理； ● 掌握路由与交换技术； ● 掌握路由器、交换机、防火墙、IDS、IPS、WAF 等网络设备的配置； ● 熟悉无线局域网基本原理； ● 熟悉无线局域网安全标准与防护方法； ● 熟悉广域网接入方式； ● 掌握广域网的常见协议及配置； ● 掌握各种 VPN 的配置； ● 熟练操作主流网管工具； ● 掌握故障诊断、分析、隔离、排除的一般方法、流程； ● 熟悉常见数据库的安全配置和管理； ● 掌握数据的加密技术； ● 掌握数据备份与恢复的技术； ● 掌握基本的程序开发技术； ● 掌握 Web 应用服务器的安全管理配置。
	数据安全与管理	● 能够分析设计数据安全架构； ● 能够实施数据的安全存储、加密、备份和恢复 ● 能够做好数据中心的日常安全管理； ● 具备较高的文档方案编制能力，以及优秀的语言表达能力。	● 熟悉安全大数据分析，了解主流分布式计算框架； ● 熟悉备份软件的实施部署； ● 熟悉服务器，存储安装实施，有关实施经验； ● 掌握统计分析基础知识，熟练掌握各项函数操作，并能根据业务需求独立制作各类报表模版； ● 熟悉数据分析和挖掘理论； ● 精通主流的数据库技术； ● 熟练掌握数据分析模型的设计。

职业 岗位	典型工作 任务分析	职业能力分析	
		职业能力要求	相关知识
数据安全 设备集成工 程师	方案设计	● 能够独立完成需求分析； ● 能够选择适当规划设计技术； ● 具备信息安全整改业务方案设计、产品选型及预算制作能力； ● 能够根据安全需求选择合适网络安全设备； ● 具备安全服务业务项目组织实施能力（如安全评估咨询项目实施、信息安全等级测评项目实施、安全整改集成项目实施、安全加固服务实施，安全管理咨询服务实施）。	● 掌握等级保护的政策、标准、流程、指标要求； ● 熟悉国家相关部门的信息安全保护标准； ● 了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； ● 熟悉市场上的各类型主流安全产品特性及功能应用情况。
	设备集成	● 能够完成服务器、网络设备、存储设备的安全及配置； ● 能够安装、配置和管理数据库系统，能对数据进行后台的更新备份等操作； ● 能够部署云计算与大数据服务平台； ● 能够检测并修复安全设备故障。	● 掌握综合布线技术； ● 掌握路由与交换技术； ● 熟练掌握各种网络设备（防火墙、UTM、VPN、IDS、IPS、WAF 等）配置； ● 了解各种网络协议； ● 掌握 Windows、Linux 操作系统的管理与应用； ● 掌握应用服务器的配置； ● 掌握存储设备的安装与配置； ● 熟悉主流的数据库的安装与配置； ● 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； ● 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； ● 熟悉虚拟化技术； ● 熟悉云计算技术的基本架构； ● 熟悉云计算的安全技术。
	安全产品维护	● 能够进行简单的安全软硬件产品开发； ● 能够检测并修复安全设备故障。	● 熟悉电工与电子技术的相关知识； ● 掌握微机原理的基础知识； ● 掌握硬件编程的基础知识； ● 熟悉 ARM、MIPS 或网络处理器； ● 了解计算机系统架构，熟悉 LPC 总线。

（2）格与培养目标分析

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的能力；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。

●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。

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、安全设备厂商从事信息系统安全测评、信息系统安全规划实施、信息系统安全运维管理等工作的高素质技术技能人才。然而,由于本专业课程涉及到计算机技术、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,为提高学生英语四级通过率,并根据外语学院的建议,将大学英语4、5由原来

32学生增加为64学时。根据人工智能技术发展的趋势，建议在专业选修课中增加人工智能伦理与安全的课程。

（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。