

上海电子信息职业技术学院

人才培养方案

2024 级五年一贯制适用

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（五年一贯制）专业人才培养方案	1
一、专业名称及代码	1
二、入学要求	1
三、修业年限	1
四、职业面向	1
五、培养目标与培养规格	1
六、课程设置及要求	3
七、教学进程总体安排	5
八、实施保障	13
九、毕业要求	17
十、附件	18
附件 1 信息安全技术应用专业人才需求与专业改革调研报告	19

信息安全技术应用（五年一贯制）专业人才培养方案

一、专业名称及代码

专业名称：信息安全技术应用

专业代码：510207

二、入学要求

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（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	网络安全应急响应(1+X 中级) 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)

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传统文化的意识。

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制、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；
- (16) 掌握专业文本的撰写规范，包括结构、语言、格式等方面的要求。

3. 能力

- (1) 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) 能分析网络数据；
- (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) 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；
- (11) 能进行探究学习、终身学习、从实践中分析问题和解决问题；
- (12) 能使用良好的语言、文字进行表达和沟通；
- (13) 能够准确理解专业文献、报告、合同等文本；
- (14) 能够撰写本专业领域的常见应用文本；
- (15) 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。

1. 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。

(1) 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。

(2) 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，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公钥基础设施基础知识，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。

2. 专业选修课程

专业选修课程：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服务与安全管理和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

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 2022 级信息安全技术应用专业（五年一贯）人才培养方案 5 年教学进度表

课程类别	课程分类	课程名称	学分	总学时	考试	实践学时	各学期周数、学分配									
							1	2	3	4	5	6	7	8	9	10
							18	18	18	18	18	18	16+2	16+2	10+8	16
公共基础必修	思想政治类	职业道德与法治	2	36	考试	0	2									
		中国特色社会主义	2	36	考试	0				2						
		心理健康与职业生涯	2	36	考试	0		2								
		历史 1	2	36	考试	0	2									
		历史 2	2	36	考试	0		2								
		哲学与人生	2	36	考试	0			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					
		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		
		思想道德与法治	3	48	考试	8								3		
		毛泽东思想和中国特色社会主义理论体系概论	2	32	考试	0								2		
		习近平新时代中国特色社会主义思想概论	3	48	考试	8							3			

课程类别	课程分类	课程名称	学分	总学时	考试	实践学时	各学期周数、学分配									
							1	2	3	4	5	6	7	8	9	10
							18	18	18	18	18	18	16+2	16+2	10+8	16
	身体素质类	体育与健康 1	2	36	考试	30	2									
		体育与健康 2	2	36	考试	30		2								
		体育与健康 3	2	36	考试	30			2							
		体育与健康 4	2	36	考试	30				2						
		体育与健康 5	2	36	考试	30					2					
		体育与健康 6	2	36	考试	30						2				
		体育与健康 7	2	32	考查	30							2			
		体育与健康 8	2	32	考查	30								2		
	综合素养类 (科学、人文素养)	数学 1	4	72	考试	0	4									
		数学 2	4	72	考试	0		4								
		数学 3	4	72	考试	0			4							
		数学 4	2	36	考试	0				2						
		数学 5	2	36	考试	0					2					
		数学 6	4	64	考试	0							4			
		物理 1	4	72	考试	0	4									
		物理 2	4	72	考试	0		4								
		物理 3	2	32	考试	0							2			
		语文 1	4	72	考试	0	4									
		语文 2	4	72	考试	0		4								
		语文 3	4	72	考试	0			4							
		语文 4	2	36	考查	0				2						
		语文 5	2	36	考查	0					2					
		语文 6	2	32	考查	0								2		
		中华优秀传统文化	2	32	考查	0							2			

课程类别	课程分类	课程名称	学分	总学时	考试	实践学时	各学期周数、学分分配									
							1	2	3	4	5	6	7	8	9	10
							18	18	18	18	18	18	16+2	16+2	10+8	16
		英语 1	4	72	考试	0	4									
		英语 2	4	72	考试	0		4								
		英语 3	4	72	考试	0			4							
		英语 4	4	72	考试	0				4						
		英语 5	2	36	考试	0					2					
		英语 6	2	36	考试	0						2				
		英语 7	2	32	考查	0							2			
		英语 8	2	32	考查	0								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	2	36	考试	32					2					
		信息技术基础 4	1	18	考查	18						1				
		人工智能（AGI）技术应用	2	32	考查	18							2			
		元宇宙技术与应用	2	32	考查	18								2		
		职业生涯规划与职业指导	1	16	考查	0							1			
		互联网+创业实践	2	36	考试	16						2				
		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	16							2			
		心理健康教育	1	16	考查	0							2			
		大学生安全教育	2	32	考查	0	*	*	*	*	*	*	*	2		
		劳动教育	1	16	考查	16									1	
		小计	135	2364		484	24.25	22.25	19.25	15.25	10.25	7.25	22.25	15.25	1	0

课程类别	课程分类	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
							18	18	18	18	18	18	16+2	16+2	10+8	16
公共基础选修	通识、艺术、传统文化类	公共艺术选修	2	36	考查					2						
		公共通识选修	4	68	考查					2			2			
		小计	6	104						2	2		2			
专业必修	专业基础课 30%-40% 10%-15%专业群课	工程数学	2	32	考查	0								2		
		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							
		Python 程序设计	3	54	考试	48				3						
		Linux 操作系统基础	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					
		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				
		渗透测试实训	1	30	考查	30						1 周				

课程类别	课程分类	课程名称	学分	总学时	考试	实践学时	各学期周数、学分配									
							1	2	3	4	5	6	7	8	9	10
							18	18	18	18	18	18	16+2	16+2	10+8	16
		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		
		网络安全标准与法律法规	2	32	考查	0								2		
		职业技能认证实训	2	60	考试	60									2周	
		合计	47	894		628	6	5	4	7	5	6	6	6	2	0
	专业核心课	*Linux 服务与安全管理	4	72	考试	48					4					
		*网络设备安全配置	4	72	考试	48					4					
		*渗透测试	4	72	考试	48						4				
		*WEB 服务安全	4	72	考试	32						4				
		信息安全技术	3	48	考试	32							3			
		*网络系统安全管理	4	64	考试	48							4			
		*应用服务器加固	4	64	考试	48								4		
		数据库安全管理	3	54	考试	36				3						
		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	54	1238		1056	0	0	0	3	8	8	7	4	8	16
专业选修	专业拓展	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	54			4							
		安全检测与评估	4	72	考试	54										
		网络设备配置与管理	4	72	考试	54			4							

课程类别	课程分类	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	
							18	18	18	18	18	18	16+2	16+2	10+8	16	
		网络安全运维技术	4	72	考试	54											
		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											
		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											
		网络安全方案设计	3	48	考查	32								3			
		信息安全管理	3	48	考查	32											
		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											
		Python 安全工具开发	3	48	考查	32										3	
		安全风险管 理	3	48	考查	32											
		小计		34	592		428	0	2	8	2	6	6	0	7	3	0
合计			276	5192		2600	29.25	29.25	31.25	29.25	31.25	27.25	35.25	34.25	14	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、附件

附件1信息安全技术应用专业人才需求与专业改革调研报告

附件2专业建设指导委员会审定意见

附件3 学术委员会审批意见

附件 1 信息安全技术应用专业人才需求与专业改革调研报告

信息安全技术应用专业

2024 年人才需求与专业改革调研报告

一、基本思路与方法

（一）调研思路

深入与专业联系较为紧密的典型企业、行业协会和职业培训鉴定机构，通过与企业人事部门的主管、工程技术人员、各层次管理骨干以及职业培训鉴定专家进行有效的沟通、访谈，了解行业的发展趋势、行业对中、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，分析信息安全技术应用专业人才培养的优势。

（二）调研方法

1. 调研内容

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

2. 调研方式

（1）文献查阅

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

（2）电话访谈

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

（3）网络调查

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

3. 调研范围

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

4. 调研对象

(1) 企业选择

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

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

表 1 调研企业一览表（部分企业）

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

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

（2）被调研人员选择

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

5. 调研过程

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

2024 年 3 月～2024 年 4 月，采用电话或者视频方式进行询问。

2024 年 5 月，调研结果分析、完成调研总结报告。

二、专业人才需求调研

（一）欧美等发达国家网络安全产业及人才发展概况

1. 欧美网络安全领域立法不断加强

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

欧洲议会成员就《网络弹性法案》（Cyber Resilience Act）中有关制造商的义务以及如何适用于开源软件的条款进行了讨论。英国信息专员办公室（ICO）发布了对拟议的《数据保护和数字信息法案》（Data Protection and Digital Information Bill）的意见。荷兰政府宣布将各分散的网络安全机构融并为一个单独的国家机构。新西兰内政部（DIA）公布了一项提案，呼吁建立一个新的全行业监管机构，以保护新西兰人免受社交媒体和其他数字平台上的有害内容的侵害。

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

2. 全球网络安全产业稳步增长

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

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

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

3. 全球网络安全人才缺口较大

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

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

据美国信息系统审计和控制协会（ISACA）的研究，网络安全的两个主要技能缺口是软技能和云计算知识。为了帮助建立网络安全劳动力职业路径并填补现今的空缺职位，需要来自各种不同背景的专业人员，把这些软技能带到网络安全前线。麦肯锡认为，企业可以拓宽

潜在应聘者的寻找范围，识别并保留背景更多样的候选人。另外，还应该培养网络安全团队领导人合作解决问题的能力，帮助其重新审视团队内的职业发展策略，消除传统的职业发展障碍，建立更具包容性的工作场所文化。为了更好防范安全威胁，企业除了引进软技能及云计算方面的技术人才外，还应加强全体员工的网络安全培训。一些安全事件往往由业务项目和网络钓鱼而起，通过改善各行业、各岗位的网络安全培训，企业可以推动建立安全第一的文化，让安全成为每个人的职责。例如，亚马逊正在帮助更多人认识到网络安全的重要性，联合美国国家网络安全防范联盟发起“保护和连接”网络安全意识宣传活动，并向全世界个人和企业免费提供网络安全意识培训。

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

（二）我国网络安全产业及人才发展概况

1. 我国网络安全领域政策规定不断完善

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

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

2. 我国网络安全产业发展更加清晰明确

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

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

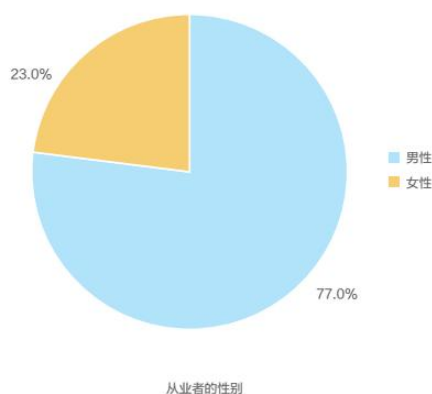
当前我国网络安全企业在学习国外先进技术的同时，国内需求侧对创新的驱动更为显著。数据安全在创新方面的比重已接近传统安全领域，我国网络安全重视攻防、安全运营、SOAR等更具实战化的赛道，工业安全、汽车安全、安全芯片等赛道符合我国新型行业对网络安全的需求。海外市场为我国网络安全企业带来新的机遇，网络安全国际市场、国家海外利益保护、中东/东南亚数字化加速带来的配套网络安全市场均是潜在增长点。

（三）网络安全人才从业现状

1. 我国网络安全从业人才画像

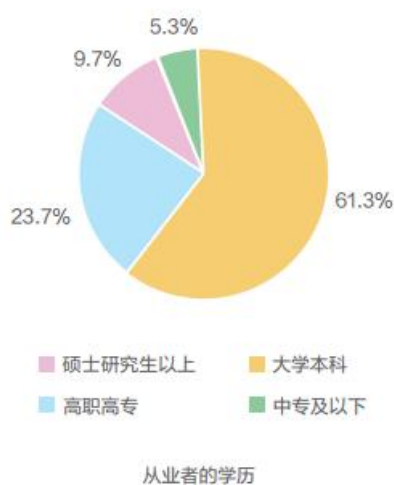
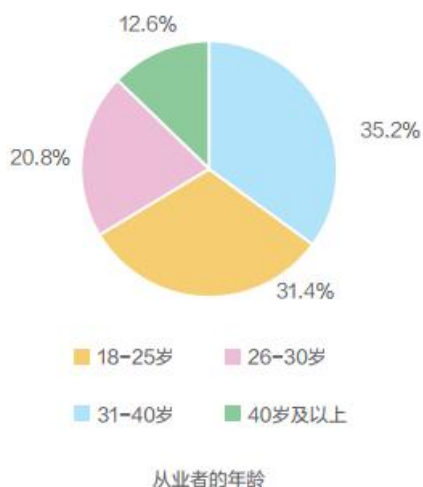
（1）男女比重为 77:23

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



（2）行业从业者逐渐年轻化

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



（3）本科毕业生占比超 6 成

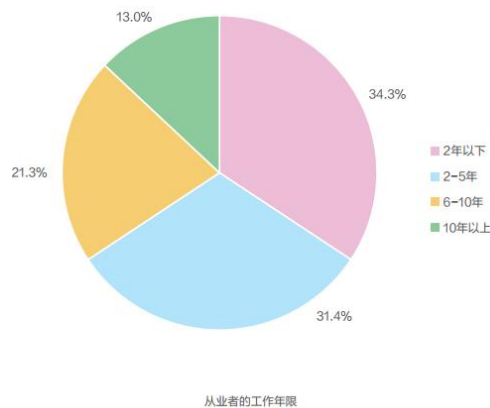
从学历来看，2023 年，本科毕业的网络安全从业者占比最高，达到 61.3%。其次是高职高专和硕士研究生以上学历的从业者，分别占比 23.7%、9.7%。本科学历从业者一直是网络安全领域的主要人才供给，在 2022 年、2021 年的调研数据中，分别占比 59.3%、63.9%。可见，网络安全从业者学历素质整体偏高。

（4）6 成以上网络安全从业者专业为计算机与网络

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

（5）5 年以下工作年限从业者占比超 6 成

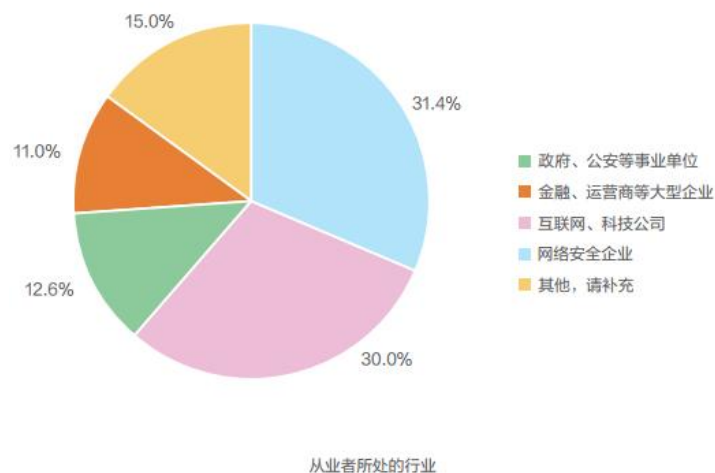
从工作年限来看，34.3%的受访者工作 2 年以下，占比最高。其次是 2-5 年、6-10 年工作者，占比分别为 31.4%、21.3%。由于网络安全产业兴起时间不长，目前处于稳步上升阶段，从业者整体上也处于探索和成长阶段，拥有较长工作经验的从业者占比较低。



2. 网络安全产业人才的从业现状

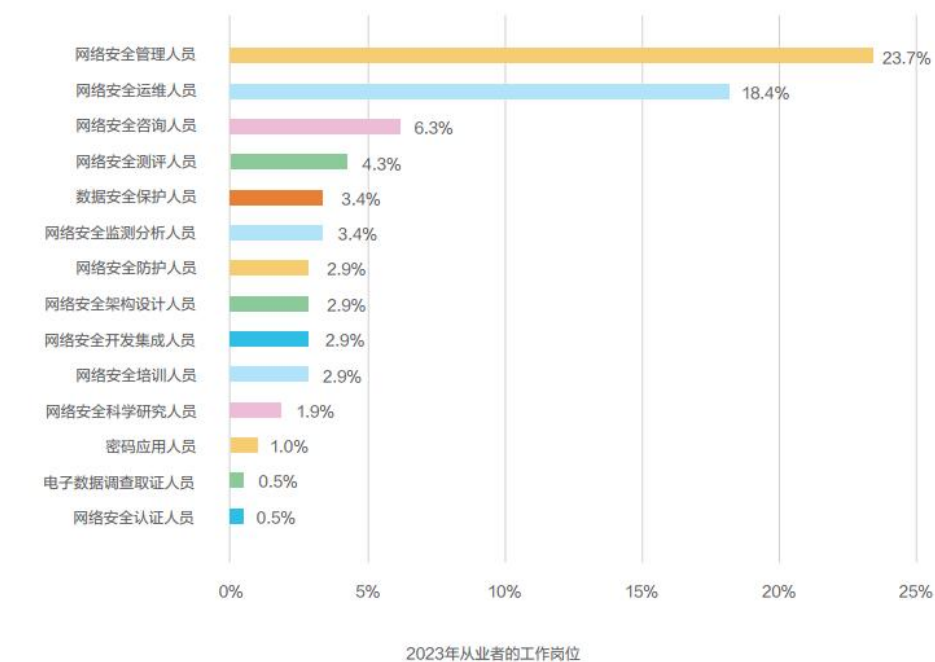
（1）网络安全企业和 IT 行业成产业人才汇聚地

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



(2) 安全管理和安全运维人员占比较高

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

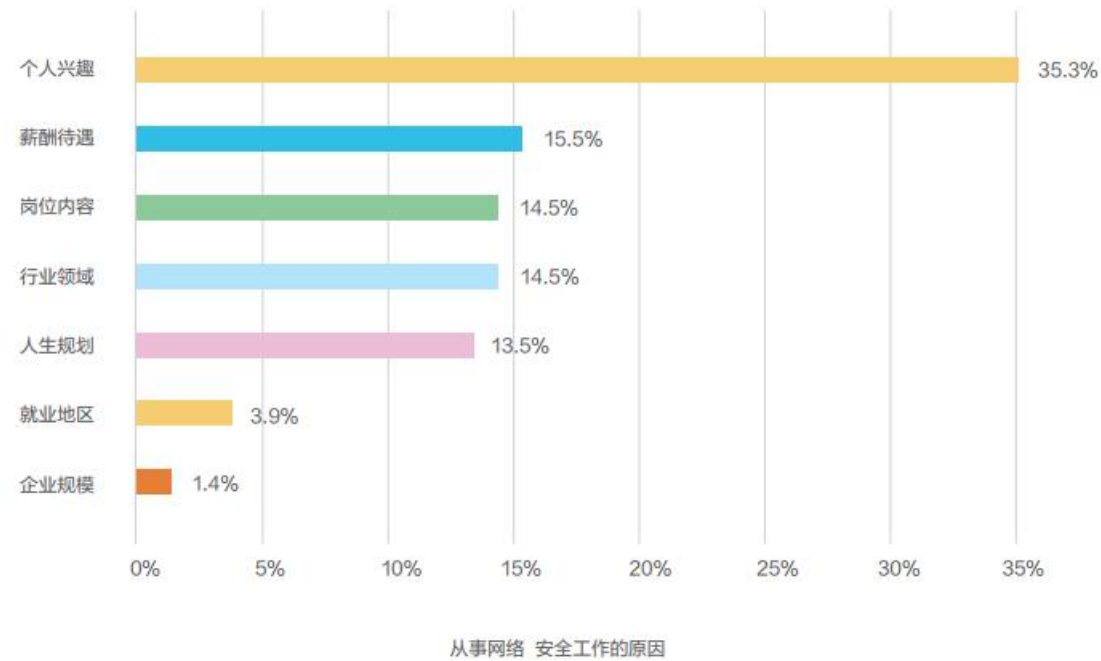


(3) 3 成以上人才因个人兴趣选择从事网络安全行业

调研数据显示, 在今年的受访者中, 35.3%表示因个人兴趣选择从事网络安全行业, 高于选择薪酬待遇的 15.5%, 也高于 2022 年选择个人兴趣而入行的 7.2%。

从年龄看, 18-25 岁受访者因个人兴趣而入行的占比最高, 为 46.2%, 其次是 26-30 岁、40 岁以上和 31-40 岁的从业者, 选择该项的占比分别为 34.9%、34.6%和 26%。新一代年轻人更倾向于以热爱为激励, 把个人兴趣与职业相结合。随着越来越多年轻人加入网络安

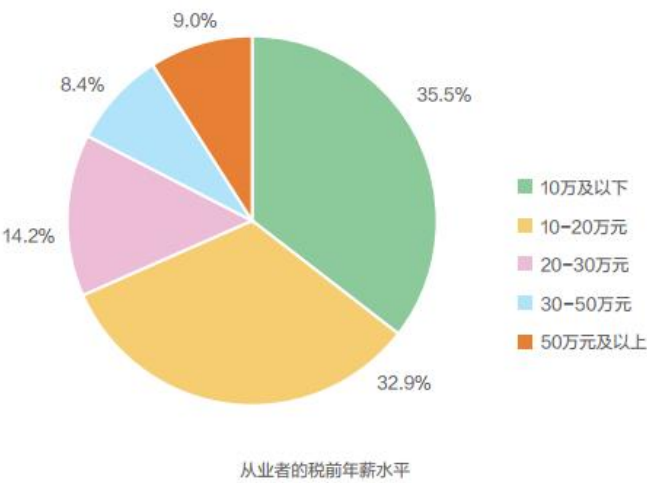
全行业，与薪酬待遇等“身外物”相比，因“真爱”而入行网络安全也显得更为普遍。



3. 网络安全产业人才的薪酬及福利待遇

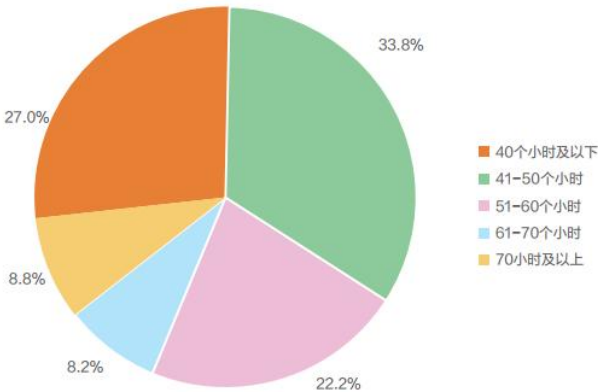
(1) 近 2 成从业者税前年薪 30 万元以上

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



(2) 超 7 成从业者每周工作时长 40 小时以上

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



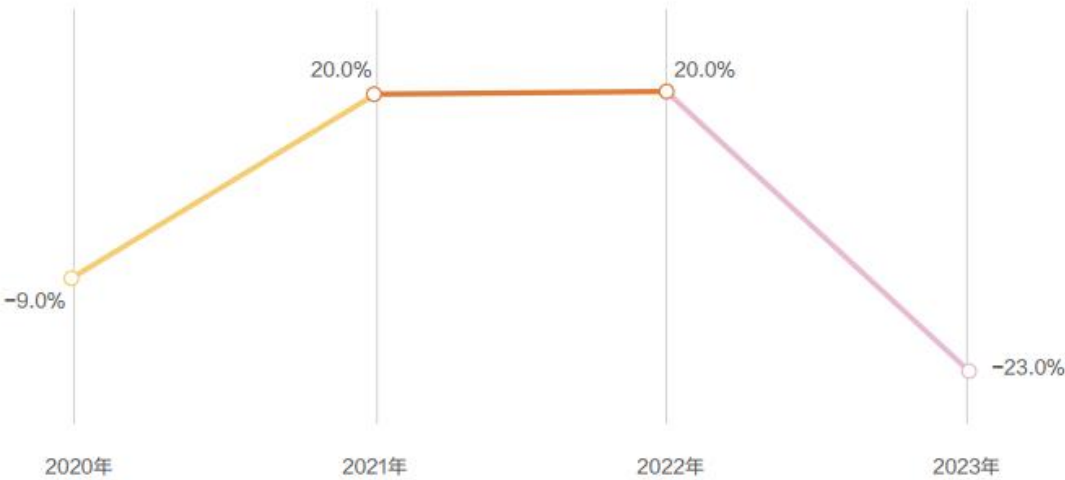
从业者的每周工作时长

（四）网络安全产业人才供需分析

1. 网络安全产业人才需求

（1）网络安全产业招聘职位数呈现波动

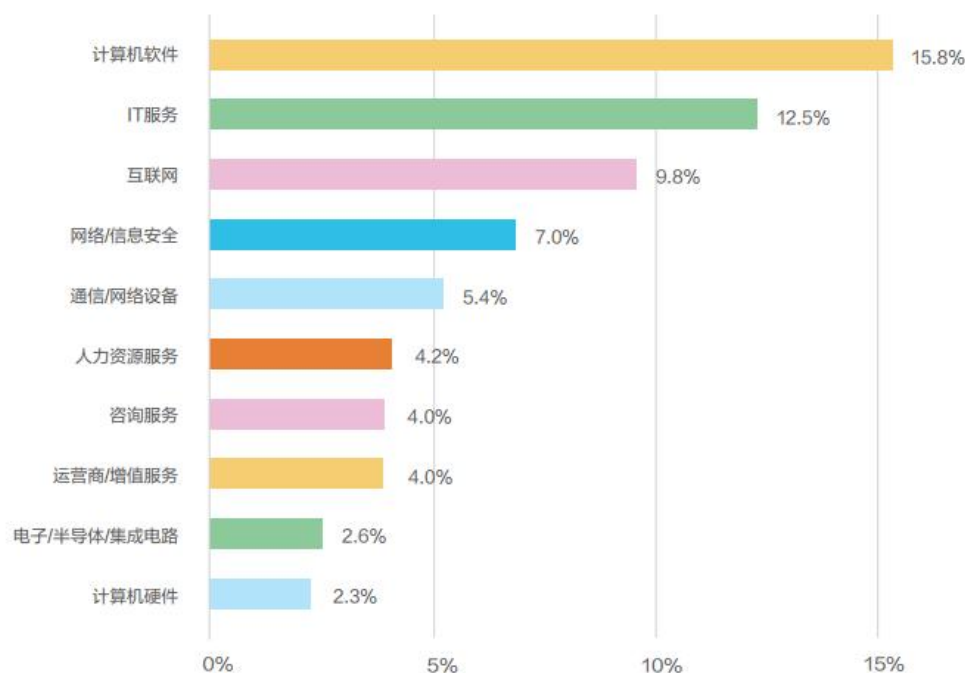
从网络安全人才需求来看，该产业招聘职位数呈现波动趋势。智联招聘平台数据显示，2021 和 2022 年网络安全相关岗位招聘数量分别同比增长 20.0%，2023 年则有所下降。考虑到每年平台数据统计周期为上一年 7 月至今年 6 月，而 2022 年下半年疫情较严重，同时受国内外经济波动影响，部分行业在投资、拓展业务等方面有所收缩，企业人员增速放缓，同时内部推荐选才比例有所上升，因而网络安全产业招聘职位需求呈现出波动状态。



网络安全人才需求同比增速

（2）计算机软件、IT 服务、互联网招聘需求排名前三

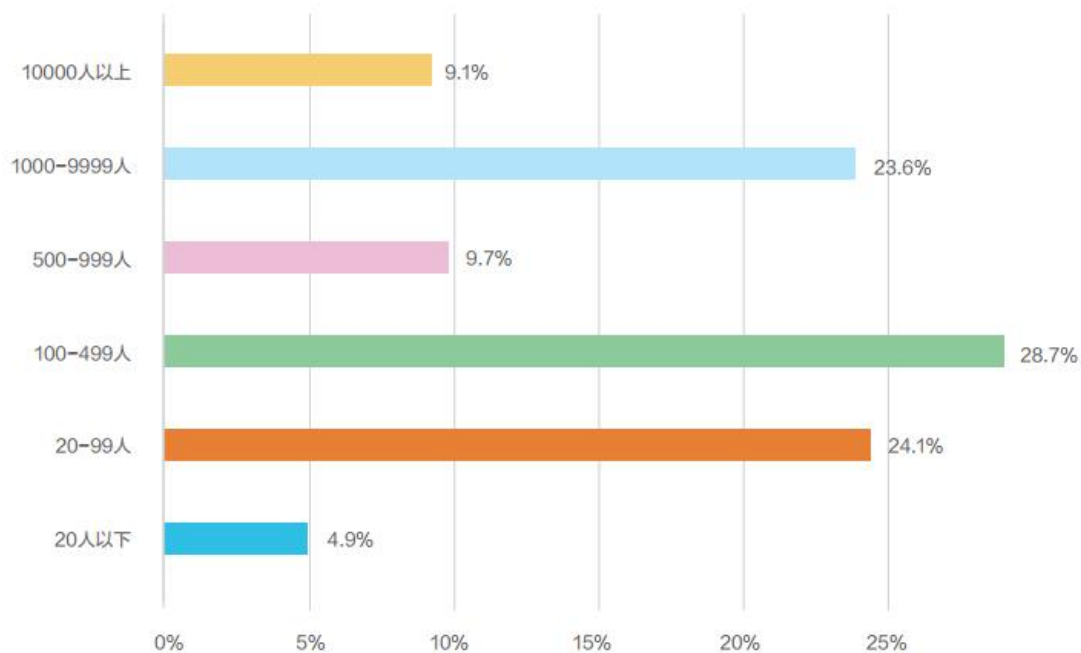
从招聘职位所在行业分布来看，2023 年招聘网络安全岗位数量最多的是计算机软件行业，占比 15.8%。其次是 IT 服务和互联网行业，招聘职位数占比分别为 12.5%和 9.8%。此外，网络/信息安全、通信/网络设备、人力资源服务、咨询服务等行业，也对网络安全人才有较大需求。



2023年招聘网络安全岗位数占比TOP10行业

（3）中小型企业对网络安全人才招聘需求更高

从企业规模看，2023 年，招聘网络安全岗位数量最多的是 100-499 人企业，招聘职位数占比达 28.7%。其次是 20-99 人企业、1000-9999 人企业，分别占比 24.1%、23.6%。在全球网络安全人才短缺的背景下，中小型企业普遍进入数字化转型阶段，网络安全业务处于成长期，因而网络安全人才需求相对更加旺盛，有志于在网络安全领域发展的求职者可以重点投递中小型企业，积累经验迅速成长。

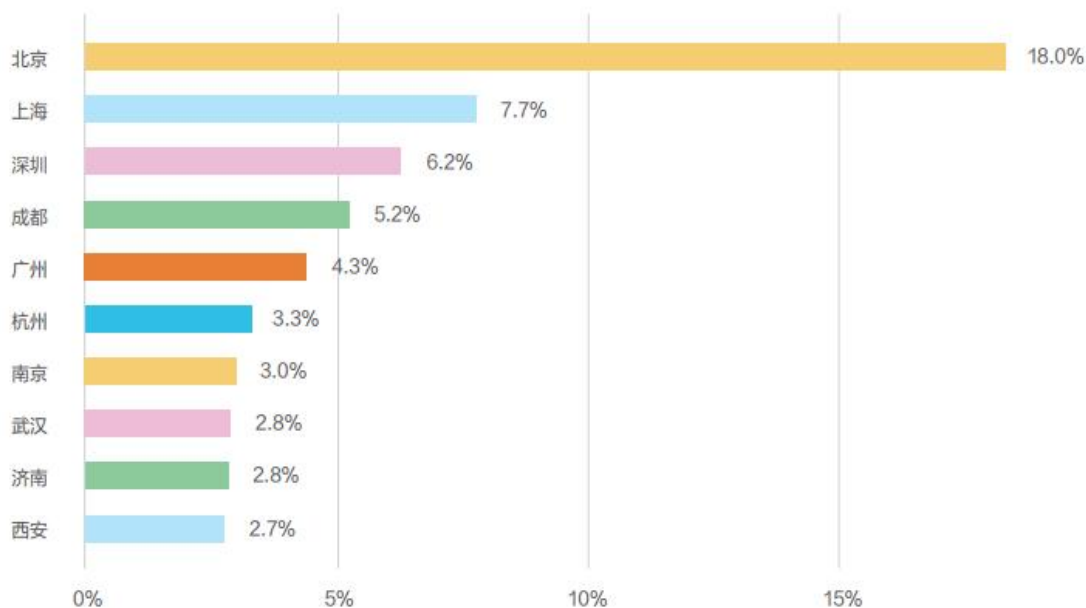


2023年不同规模企业招聘网络安全岗位数量占比

（4）一线城市对网络安全人才招聘需求大

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

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



2023年招聘网络安全岗位数量占比TOP10城市

(5) 网络安全运营岗位招聘职位数占比 29%

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

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

一级职能	二级职能	典型职位	招聘职位数占比
网络安全审计和 评估 (8.8%)	网络安全分析	渗透测试/漏洞挖掘工程师	5.90%
	网络安全评估	网络安全评估师	2.50%
	网络安全认证	安全认证工程师	0.4

(6) Linux、Java、Windows 等技能需求大

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

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

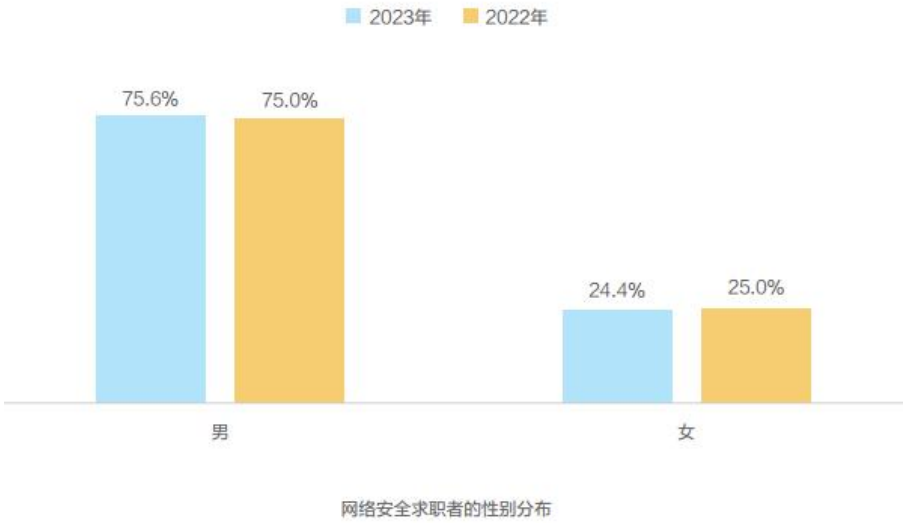
2023年网络安全岗位需求的专业技能TOP10

2. 网络安全产业人才供给

(1) 男性求职者占比超 7 成

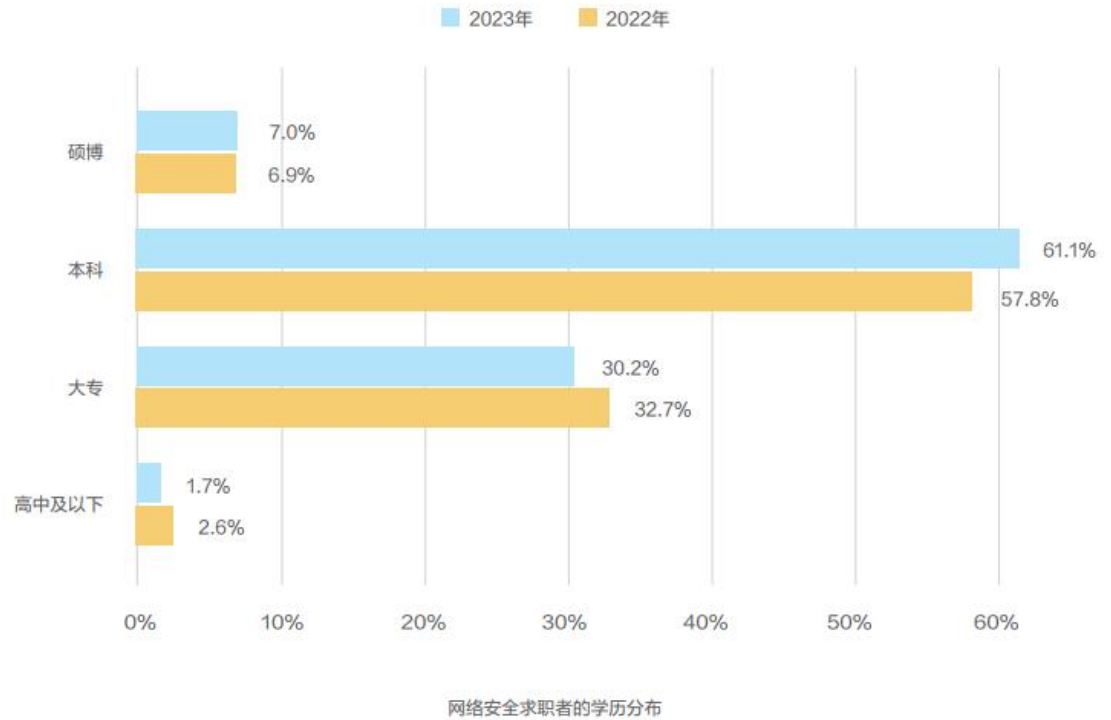
智联招聘平台数据显示，2023 年向网络安全岗位求职的人才中，男性占比 75.6%，女性占比 24.4%。2022 年，男性占比 75%，女性占比 25%。性别结构较为稳定。由于网络安全属于理工科，就读相关专业的男性更多，而该工作对技术升级迭代、工作时间的要求较高，

需要持续学习和加班工作，相比之下男性更适应这样的工作要求，因此男性求职者比重持续处于高位，属于绝对的求职主体。



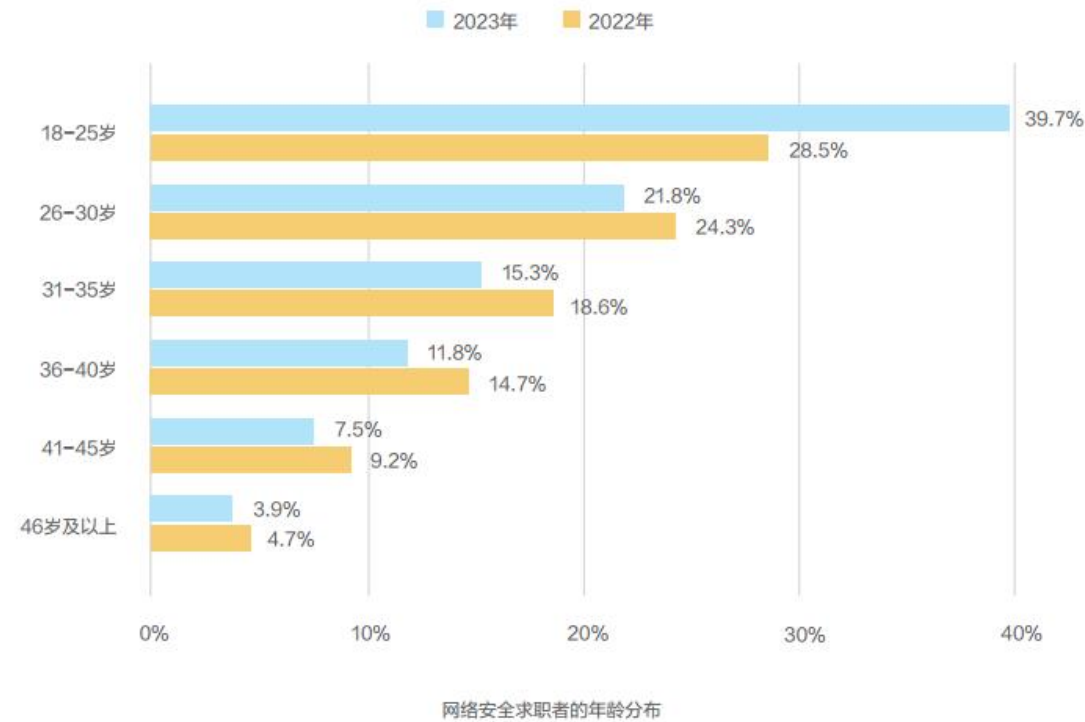
(2) 本科学历求职者占比较高，且呈上升趋势

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



(3) 18-25 岁人才求职者占比排名第一

从年龄来看，2023 年，网络安全领域 18-25 岁人才求职者占比 39.7%，排名第一，而且相比 2022 年的 28.5%，提高了 11.2 个百分点。其次是 26-30 岁、31-35 岁求职者，占比分别为 21.8%和 15.3%，但相比 2022 年均有所下降。可见年轻人普遍看好我国网络安全行业这一蓝海市场的发展前景，未来网络安全行业将受到更多求职者的青睐。



（4）计算机科学与技术专业求职者占比最高

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

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

网络安全求职者的专业TOP15

(5) MySQL 是网络安全求职者掌握最多的技能

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

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

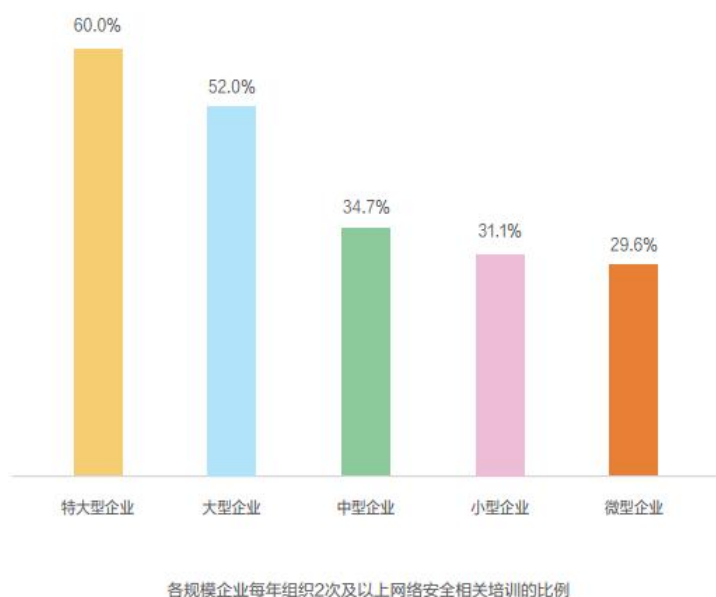
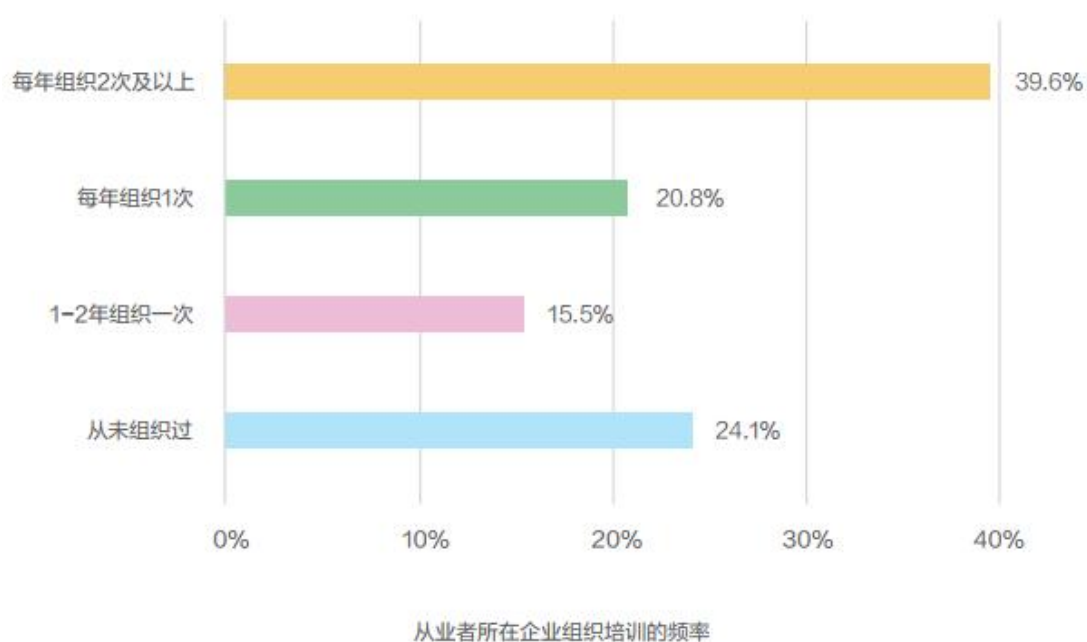
网络安全求职者具备的技能TOP10

（五）用人单位人才培养

1. 用人单位人才能力建设

（1）近 4 成从业者所在企业每年组织 2 次及以上网络安全培训

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

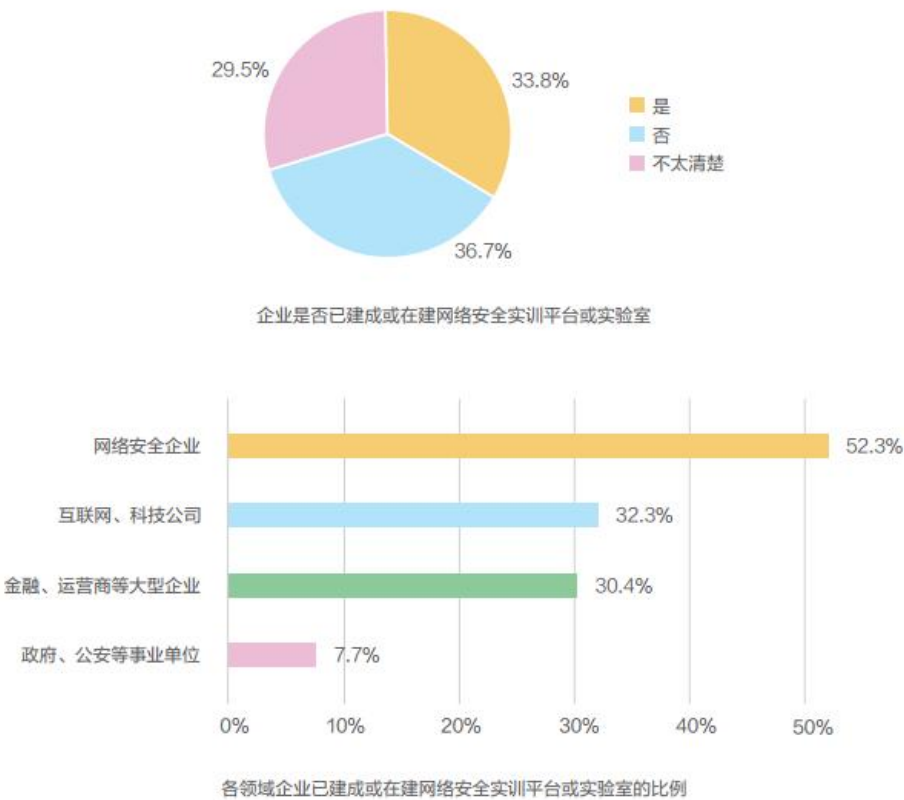


其中，每年组织 2 次以上培训的特大型企业占比 60%，高于大型企业的 52%、中型企业

的 34.7%、小型企业的 31.1%和微型企业的 29.6%。可见企业规模越大，对于培训就越重视，开展培训活动也更加频繁。微型企业受制于人手和经费所限，对网络安全相关培训的组织力度相对更弱。

（2）过半网络安全企业已建成或在建网络安全实训平台

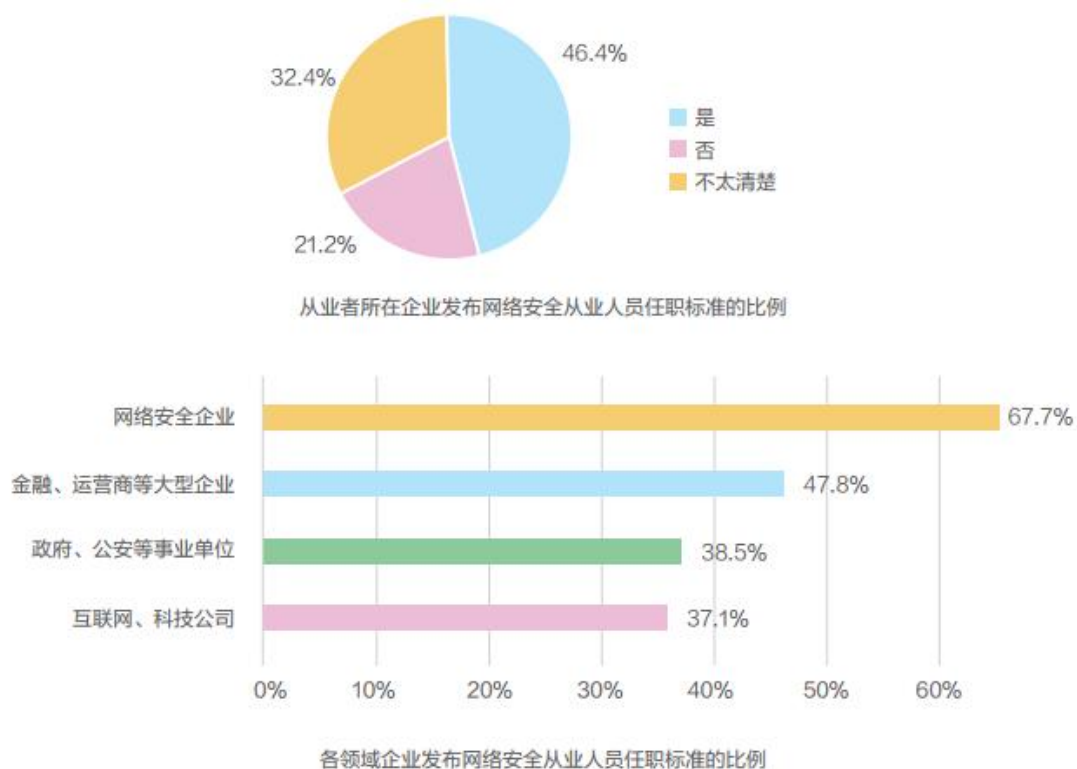
目前，33.8%的受访网络安全从业者所在企业已建成或在建网络安全实训平台或实验室，而未建成的占比高达 36.7%。从不同领域来看，已建成或在建网络安全实训平台或实验室的网络安全企业占比最高，达到 52.3%，超过互联网、科技公司，金融、运营商等大型企业，政府、公安等事业单位。



2. 用人单位人才体系建设

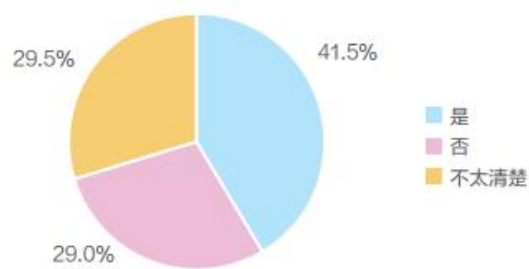
（1）近 7 成网络安全企业建立任职标准

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

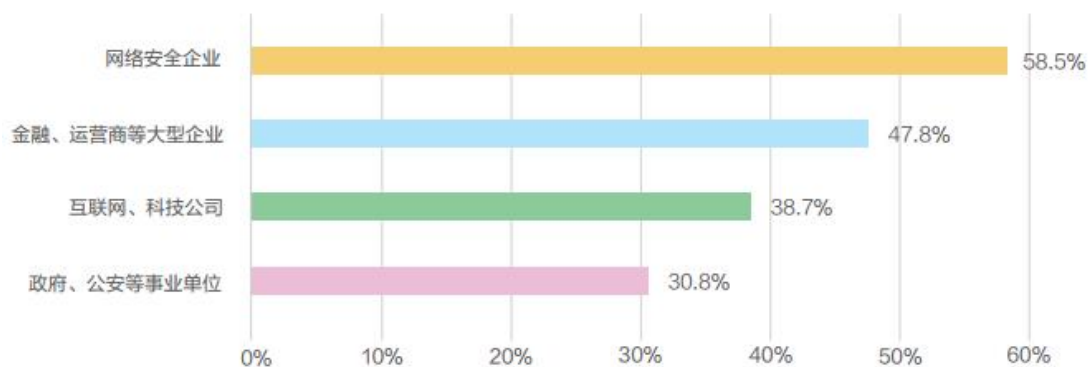


（2）4 成从业者所在企业建立网络安全领域用人机制

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



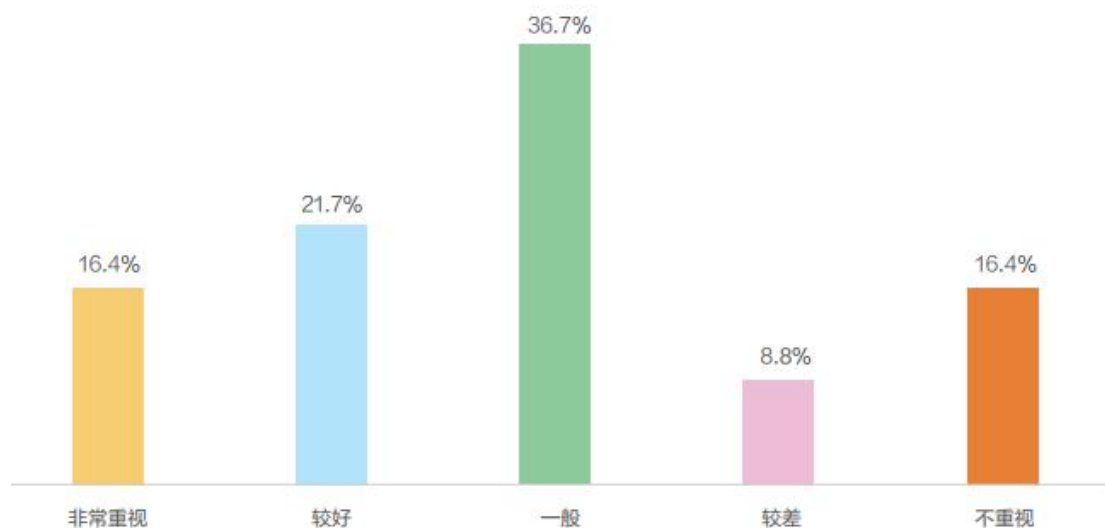
从业者所在企业建立网络安全专业人才用人机制的比例



各领域企业建立网络安全专业人才用人机制的比例

(3) 近 4 成从业者所属公司重视人才建设

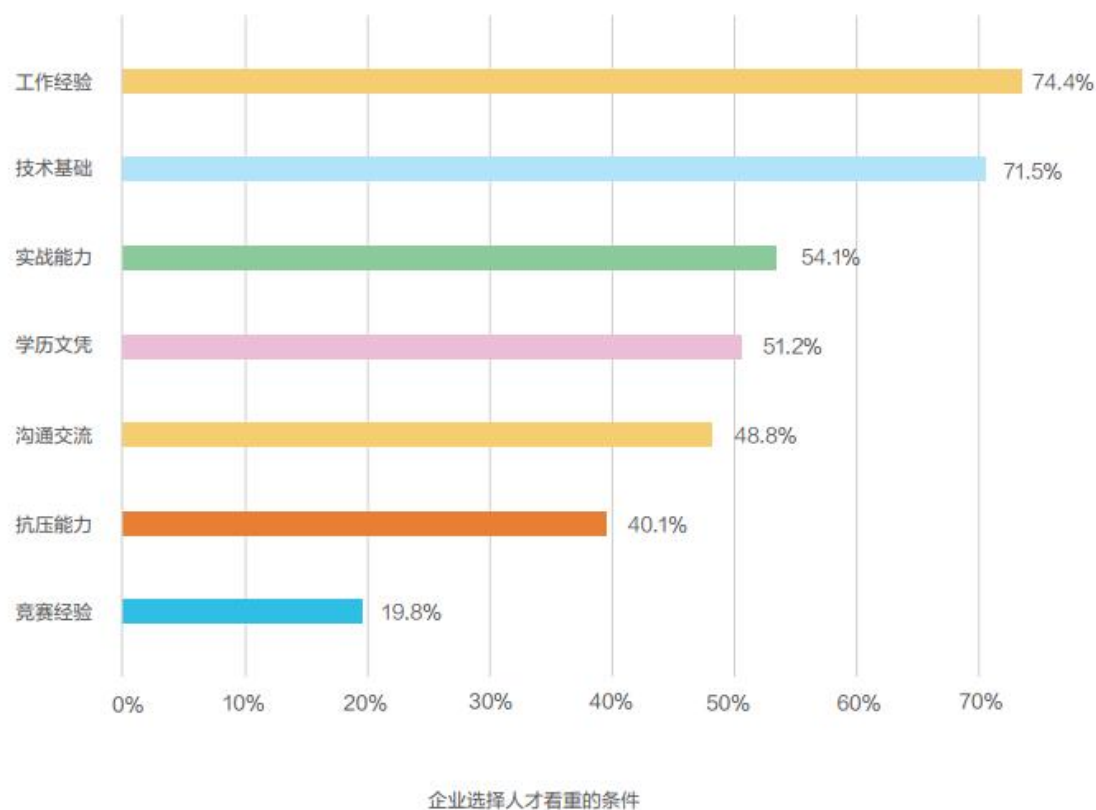
调研结果显示，分别有 16.4% 和 21.7% 的从业者所属企业对网络安全人才建设“非常重视”或“较好”。不过，36.7% 的从业者认为企业对人才建设的重视程度“一般”。可见，网络安全人才所在公司对人才建设的重视程度仍有待提高。



企业对网络安全人才建设的重视程度

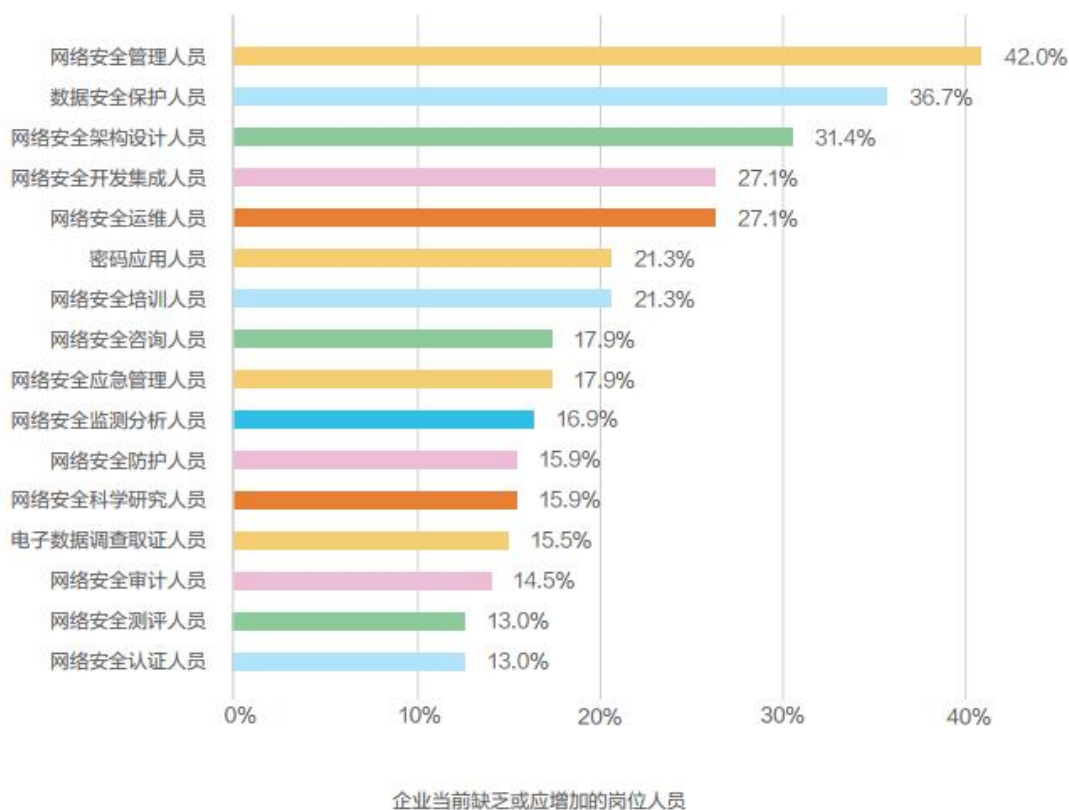
（4）7 成以上网络安全从业者所在用人单位重视工作经验

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



（5）超 4 成从业者认为公司应当增加网络安全管理人才

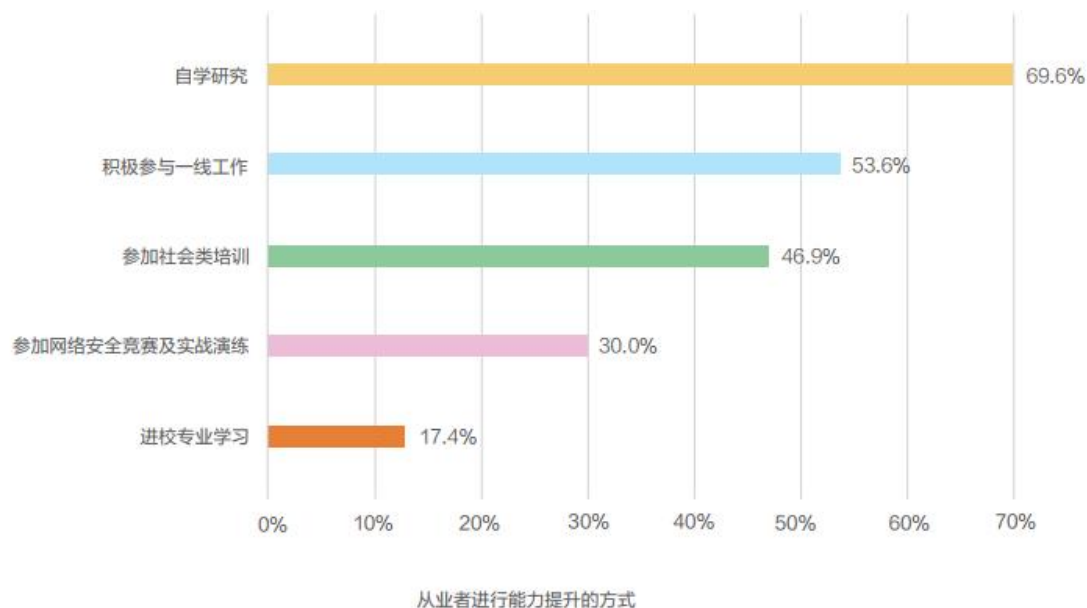
根据企业业务发展需求，42%的网络安全从业者认为，企业应当增加网络安全管理人员，其次是数据安全保护人员，占比 36.7%，也有 31.4%的从业者认为应当增加网络安全架构设计人员。此外，网络安全开发集成人员、网络安全运维人员、密码应用人员、网络安全培训人员的需求也排名前列。可见，管理人员和技术人员是目前行业较为缺乏人才的岗位。



3. 在岗人才能力提升

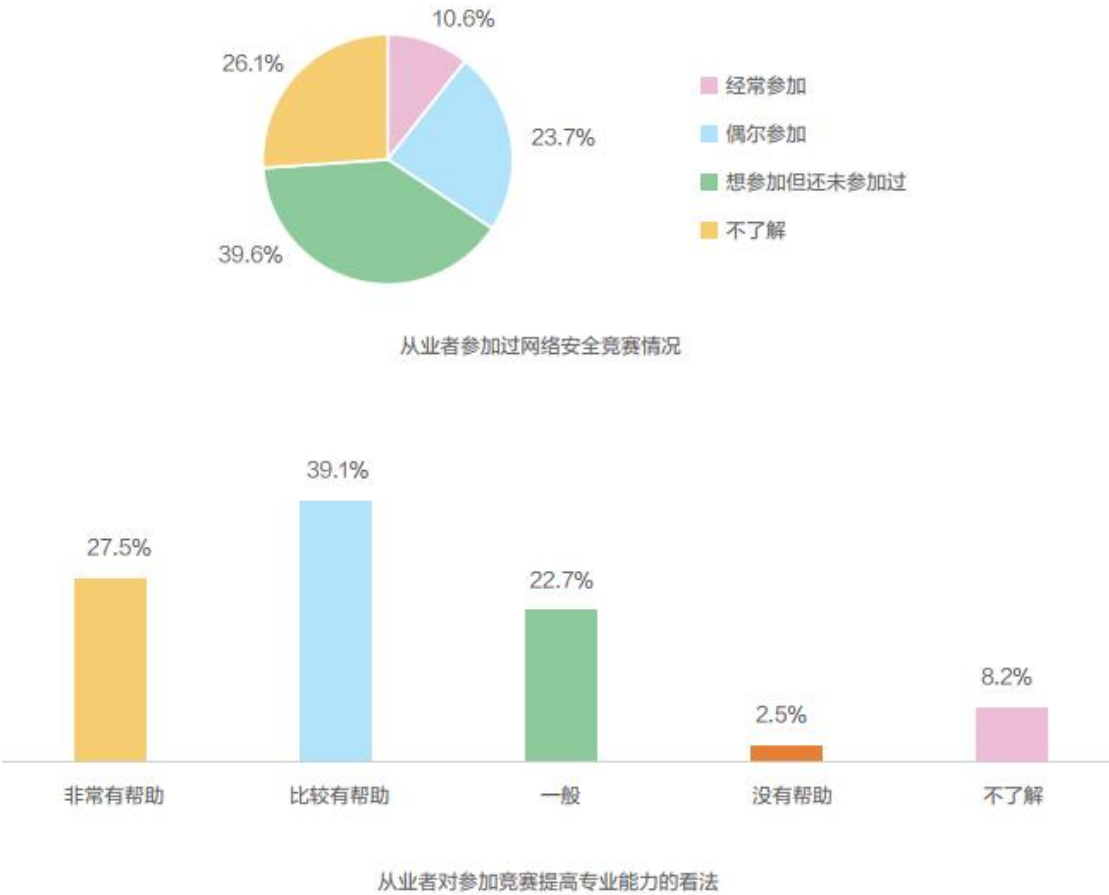
(1) 自学研究是从业者能力提升的主要方式

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



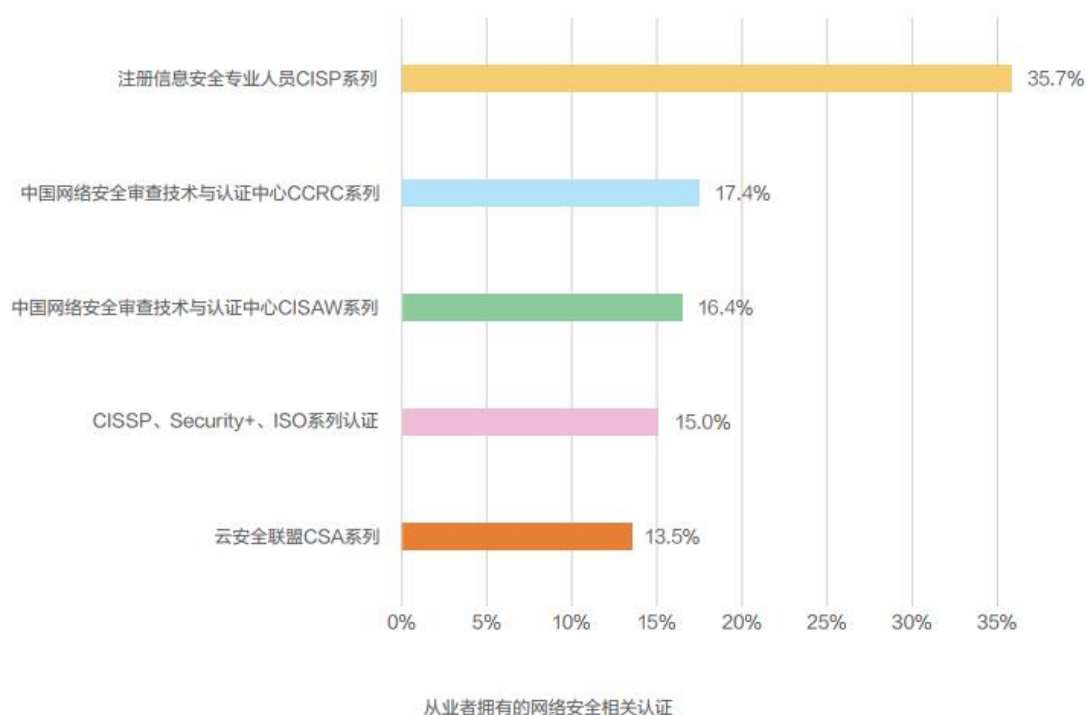
(2) 34%从业者参加过网络安全竞赛，6 成以上认为有助于提高专业能力

问卷调研显示，分别有 10.6%、23.7%的从业者经常参加和偶尔参加竞赛，39.6%的从业者想参加但还未参加过网络安全竞赛。对于竞赛提高专业能力方面的作用，从业者普遍反映较好。其中，27.5%认为“非常有帮助”，39.1%认为“比较有帮助”，共计有 66.6%的从业者认为有帮助。

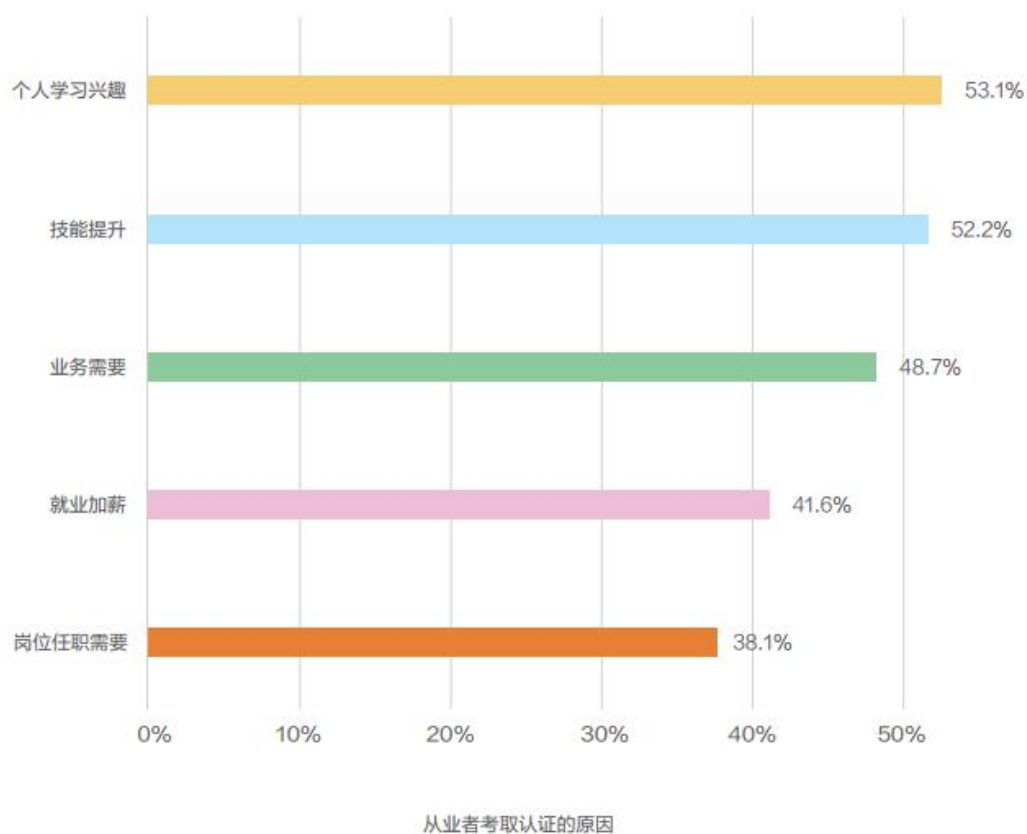


（3）兴趣、技能、业务是考证的主要驱动力

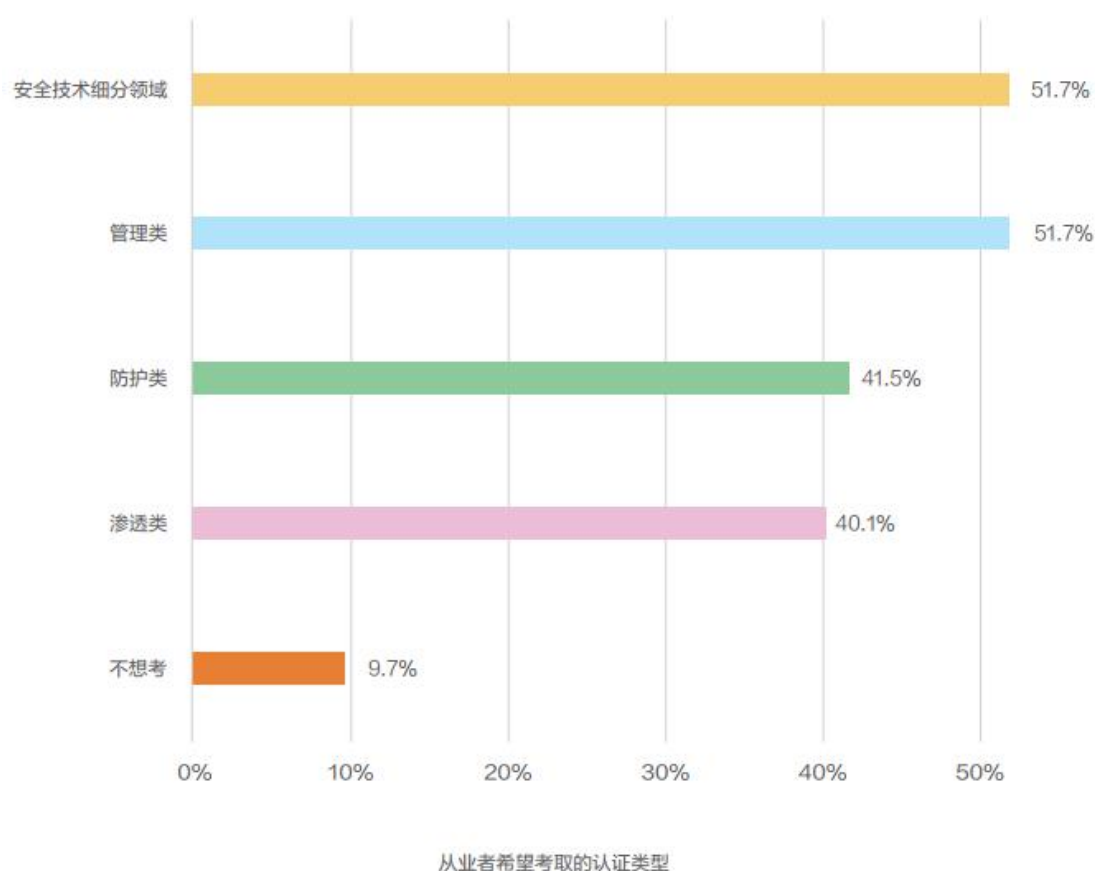
在认证方面，目前拥有注册信息安全专业人员 CISP 系列认证的从业者占比最高，达到 35.7%。其次是中国网络安全审查技术与认证中心 CCRC 系列，中国网络安全审查技术与认证中心 CISA 系列，CISSP、Security+、ISO 系列认证，占比均超过 15%。



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



从业者希望考取认证类型中，安全技术细分领域、管理类为主要类别，占比均为 51.7%。同时也有 41.5%、40.1%的从业者分别选择防护类、渗透类认证。



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。

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

对于企业而言，当前网络安全业务份额越来越重，但是招到匹配和适合的网络安全技术人才却并不容易。从人才培养角度来看，深耕研究的定向人才十分缺乏，实战人才也处于

供不应求的状态。日益增加的网络安全招聘岗位数，愈发精确地面向专业人才。

（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分析； 13. 能够利用相关安全评估扫描工具对测评对象进行

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。	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. 学会基本的的功能测试与分析; 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。

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

序号	任务领域	典型工作任务	职业需求技能
			11. 能够充分利用网络资源查找了解相关渗透性攻击方法和工具。
5	网络运维安全管理员	1. 能熟练配置 Windows、Linux 下的各类服务器及相关软件； 2. 能对服务器的安全进行评估； 3. 对系统安全 BUG 进行评估和测试； 4. 了解服务器性能，能架设高性能服务器(负载均衡，双机热备)； 5. 熟练掌握服务器架设、局域网架设及维护； 6. 对服务器的数据进行日常备案和灾难性恢复； 7. 熟悉 web 系统的安全管理和优化，熟悉网络知识，掌握网络安全维护知识，对 web 安全熟悉； 8. 熟悉各种黑客防范措施，熟悉开源软件的安装配置以及功能方面的应用； 9. 任职资格负责公司网络终端的安全管理维护； 10. 负责公司网络安全体系建设、系统安全评估与加固。	1. 具备选择适当技术的规划设计能力来； 2. 掌握 WINDOWS、LINUX 操作系统的管理与应用； 3. 掌握 WINDOWS、LINUX 操作系统安全防护设置； 4. 掌握路由与交换技术； 5. 具有 ISP 选择与管理能力； 6. 能够根据应用需求，制订及实施网络安全解决方案； 7. 能够根据应用需求，对主流厂商的网络设备和安全产品的功能、参数、安全特性进行合理选型； 8. 能够对网络安全方案进行实施与检测； 9. 能够按应用需求，进行安全角色与权限的划分与管理； 10. 能够利用工具对信息系统进行初步的安全评估； 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。
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；	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；

序号	任务领域	典型工作任务	职业需求技能
		5. 建立安全设备运维文档、完成安全运维报告。	6. 熟悉安全产品的高级配置与部署，如分布式出口部署、高可用性 HA 部署等； 7. 熟悉安防系统功能和构成，如监控、门禁、防盗等系统的配置使用； 8. 学会基本的的功能测试与分析； 9. 具备选择适当技术的规划设计能力； 10. 够按应用需求，进行安全角色与权限的划分与管理。

(2) 培养目标分析

从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。

根据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：本专业培养理想信念坚定，德、智、体、美、劳全面发展，具有一定的科学文化水平，具有良好的人文素养、职业道德和创新意识，精益求精的工匠精神，较强的就业能力和可持续发展能力，掌握本专业知识和技术技能，面向互联网和相关服务、软件和信息服务业，能够从

事信息安全系统集成、网络安全运维、Web 安全管理与评估、网络安全应急响应、数据安全、企业网络等保测评等工作的高素质技术技能人才。

（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，本专业将第二岗位定位于网络安全系统集成工程师，具备扎实的计算机与网络原理知识，熟悉各类网络与安全设备（路由、交换、防火墙、VPN、漏洞扫描）；对网络数据包具备分析实践能力，熟练使用数据包分析工具；熟悉常见网络通信协议（TCP/IP、交换路由协议、VPN 协议等）；熟悉防火墙原理，能够熟练配置防火墙策略；熟悉主流网络与安全厂商产品（思科/华为）。

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

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

（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《web 服务安全》《渗透测试》和《应用服务器加固》课程内容调整，避免重复；《渗透测试实训》放入拓展课中；在第一学年的基础课中增加《网络安全标准与法律法规》；并将基础课程中的《计算机系统配置与维护》的课时修改为 2 课时；并且 5、6 学期课时总数较多，调整到 30 以内。在《数据库安全管理》中增加一些数据库权限管理、日志管理等内容。

（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 6 门核心课程重构为现在的 7 门《网络安全设备配置》、《Linux 服务与安全管理》、《WEB 服务安全》、《渗透测试》《数据库安全管理》《应用服务器加固》和《网络系统安全管理》专业核心课程，制定课程标准，并着力打造精品课程资源。

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

（四）专业师资与实训条件配置建议

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

信息安全人才被要求攻防兼备，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格证书，提高教师的实践和理论水平为了培养符合企业需求的技能型人才，加强校企合作的深度与广度，积极引导企业参与职业院校的教育教学改革。在企业内建设校外实践教学基地，在校内共建实训室或工作室，将企业岗位技能要求提炼出知识点，企业行业专家参与学校的专业规划、课程设置和教学内容的开发，校企共同开发教材及其他教学资源，每年安排教师下企业参与项目实践，将企业岗位的技能需求融入人才培养环节。