

2019 级信息安全技术应用专业 人才培养方案

2019 级信息安全技术应用专业人才培养方案

修订说明

依据教育部关于印发《职业教育专业目录(2021 年)》的通知(教职成〔2021〕2 号)要求,信息安全与管理专业更名为信息安全技术应用,相应信息安全与管理专业代码(610211)调整为信息安全技术应用(510207)。

2019 级信息安全技术应用专业人才培养方案修订经过**电子信息职业技术学院学术委员会,审核并通过。

2020 年 8 月

目 录

修订说明.....	1
2019 级信息安全技术应用专业人才培养方案.....	4
一、专业名称及代码.....	4
二、入学要求.....	4
三、修业年限.....	4
四、职业面向.....	4
五、培养目标与培养规格.....	4
（一）培养目标.....	4
（二）培养规格.....	4
六、课程设置.....	6
（一）公共基础课程.....	6
（二）专业（技能）课程.....	6
七、学时安排.....	8
八、教学总体安排.....	8
（一）教学进度表.....	8
（二）实践教学安排表.....	10
九、实施保障.....	10
（一）师资队伍.....	10
（二）教学设施.....	10
（三）教学资源.....	12
（四）教学方法.....	12
（五）教学评价.....	12
（六）质量管理.....	13
十、毕业要求.....	13
附件 1：专业人才需求与专业改革调研报告.....	14
一、基本思路与方法.....	14
（一）调研思路.....	14
（二）调研方法.....	14
二、调研内容.....	15
（一）相关行业发展现状.....	15
（二）行业从业人员基本情况.....	20
三、专业现状调研.....	22
（一）专业点分布情况（113 所高职专科学校）.....	22
（二）专业招生与就业岗位分布情况.....	25
（三）专业教学情况及存在的主要问题.....	29
四、专业人才培养方案优化建议.....	30
（一）专业岗位优化建议.....	30
（二）专业课程内容优化建议.....	30
（三）专业教学改革建议.....	30
（四）专业师资与实训条件配置建议.....	31

附件 2：专业建设指导委员会审定意见.....	32
附件 3：学术委员会审定意见.....	33

2019 级信息安全技术应用专业人才培养方案

一、专业名称及代码

信息安全技术应用(510207)。

二、入学要求

普通高中毕业生、中职毕业生或同等学力人员。

三、修业年限

三年。

四、职业面向

信息安全技术应用专业的职业面向见表 1 所示。

表 1 职业面向表

所属专业大类	所属专业类	对应行业	主要职业类别	主要岗位类别(或技术领域)	职业资格证书或技能等级证书举例
电子信息大类 51	计算机类 5102	软件和信息技术服务业 65	网络与信息安全管理员	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	思科网络安全工程师 (CCNAS) 微软认证系统工程师 (MCSE) 红帽认证工程师 (RHCE) 信息安全防护(专项能力三级)

五、培养目标与培养规格

(一) 培养目标

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 and 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人才。

(二) 培养规格

1. 素质

(1)思想政治素质：热爱社会主义祖国，能够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，具有正确的世界观、人生观、价值观；

(2)身心素质：掌握常规体育与健康运动项目的基础知识和基本技能，掌握有关身体健康的知识和健身方法，体能测试基本合格，提高大学生心理健康水平，增强自我调适的能力；使学生能正确认识自我，热爱生命，善待他人，增强调控自我、承受挫折、适应环境的能力；

(3)文化素质：提升大学生的人文素养和文化底蕴，培养沟通交流、阅读理解、应用写作、文学鉴赏，促进学生的专业学习和综合素质提升；

(4)职业素质：树立正确的职业价值观、良好的职业精神、遵守职业法规、坚守职业理想；

(5)基本通用能力：提升通用基础能力，包括自我学习管理能力、数字运用能力、信息处理能力和中文外语能力；

(6)关键社会能力：促进有效参与社会实践、提升社会担当意识，包括沟通交流、团队合作、社会责任和社会认知能力；

(7)创新创业能力：培养良好的创新精神、创造性思维，促进参与创业实践，提升复合型能力和综合素质。

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；掌握数据库方面知识；

(6)掌握 DNS、DHCP 和 WEB 服务器等常用服务器方面的知识；

(7)掌握交换机、路由器、防火墙的常用网络设备方面的知识；

(8)网络安全设备的配置管理等方面的知识；

(9)掌握系统安全架构、信息系统日常检测与维护、网络系统集成、信息系统安全管理知识；

(10)初步掌握信息系统安全测评、渗透测试、应用服务安全加固等方面的知识；

(11)熟悉信息安全管理体系、风险管理方法；

(12)了解常用 WEB 开发语言，中间件框架，JavaScript 框架；

(13)了解应用开发的基本流程及关键点。

3. 能力

(1)具有设计、组建、维护与安全管理中小型企业网络能力；

(2)具有对网络操作系统、服务器搭建、网络管理软件或工具的使用能力；

(3)具有对网络设备如路由器、交换机、无线设备安装、配置、调试、维护的基本能力，对网络设备安全特性的配置与调试能力；

(4)具有对网络安全设备如防火墙、VPN、入侵检测等硬件设备配置、调试、维护的基本能力；

(5)初步具有应用服务安全检测、评估和安全服务加固能力；

(6)具有信息系统集成、安全管理与维护能力；

(7)能撰写工程文件和渗透测试评估工作报告，会查阅技术文献；

(8)具有至少一种脚本语言（如 python、perl、bash）开发能力；

- (9)具有至少一种开源的渗透测试工具的使用能力；
 (10)具有网络数据分析能力；
 (11)具有初步创业与学习、创新、岗位迁移能力。

六、课程设置

（一）公共基础课程

信息安全技术应用专业的公共基础课程主要包括毛泽东思想和中国特色社会主义理论体系概论、思想道德修养与法律基础、军事理论与训练、职业生涯规划与职业指导、心理健康教育、形势与政策、大学语文、应用数学、实用英语、计算机数学、 计算机应用基础、体育与健康、创业意识与创业技巧、大学生安全教育以及公共基础教育选修课。

（二）专业（技能）课程

信息安全技术应用专业专业（技能）课程见表 2 所示。

表 2 信息安全技术应用专业（技能）课程内容

序号	课程名称	主要教学内容与要求
1	Windows 系统管理与应用	要求: 使学生具备运用 Windows Server 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。 内容: 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。
2	Python 程序设计基础	要求: 学生能够掌握脚本语言的开发方法,课程分为三个学期实施,内容从基础到网络编程和安全工具开发,培养学生自动化运维,安全工具编写能力。 内容: 基本数据结构,函数,模块,包,程序的控制逻辑,面向对象程序设计,多线程技术,界面设计实现,正则表达式
3	Python 网络编程	要求: 掌握 python 网络编程库的使用方法及应用。 内容: Python 网络编程: Socket 库, requests 库, 实现 TCP、UDP 客户端服务端, FTP, SMTP 的客户端, HTTP 客户端认证
4	Python 安全工具开发	要求: 掌握 python 安全工具的编写。 内容: Python 安全工具开发: 全端口扫描器, 网络爬虫, 渗透测试, 文件清理恢复, 元数据分析, 无线网络渗透、明文协议渗透。
5	数据库安全管理	要求: 使学生能够系统、全面地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,使学生具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。 内容: 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。

序号	课程名称	主要教学内容与要求
6	WEB 应用开发	<p>要求:使学生能够进行小型的 WEB 应用项目开发, 能够系统地掌握项目开发流程规律, 掌握开发流程中的安全技术手段, 培养项目开发管理素养, 实现较完整的项目开发能力。</p> <p>内容: UI 界面设计, 开发环境搭建, 业务逻辑绘制, 功能模块编写, UI 代码改善, 项目上线调试。</p>
7	Windows 系统安全实训	<p>要求:使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。</p> <p>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。</p>
8	防火墙与 VPN 技术	<p>要求:使学生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。</p> <p>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。</p>
9	网络设备安全配置	<p>要求:使学生能够熟练运用各种网络安全技术, 掌握各种网络设备的安全配置方法, 并能根据实际应用需求进行网络安全策略的设计, 实施和检测。</p> <p>内容: 网络风险分析、网络设备的管理安全、AAA 认证授权审计、二层交换安全、IOS 防火墙技术、IPS、加密技术和 IPSEC VPN 技术。将思科安全认证的内容融入课程。</p>
10	Linux 服务与安全管理	<p>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。</p> <p>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; 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。</p>
11	Linux 服务安全管理实训	<p>要求:学生能够了解 Linux 系统安全机制, 会查看安全日志, 理解系统的审计功能, 会设置 Linux 防火墙, 熟练掌握 Linux 平台的扫描工具使用, 脚本工具的使用与脚本程序的编制。</p> <p>内容: Linux 系统的安全策略, PAM, 加密文件系统, 安全审计, 强制访问控制和防火墙。扫描工具 NMAP 的使用和 BASH 编写脚本用于 Linux 系统的安全运维。</p>
12	WEB 应用安全	<p>要求:使学生能够担负起中小型 WEB 服务器的安全管理工作。熟悉 WEB 应用中常见的安全漏洞, 对 WEB 服务安全有较为完整的认识, 较全面地掌握维护 WEB 服务安全的管理技能。</p> <p>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。</p>

序号	课程名称	主要教学内容与要求
13	安全检测与评估	要求: 学生能够对企业信息安全产品进行需求分析、风险评估项目立项、风险评估实施、风险评估验收及安全评估文档书写等专业能力。 内容: 数据传输安全,网络结构安全与设备安全等低层的安全检测知识,更侧重按照安全等级保护的标准进行于应用 WEB 服务安全的检测与评估。
14	渗透测试	要求: 学生能按照信息安全渗透测试基本操作流程,依据渗透测试的四步模型法,能够规范、准确、熟练地完成渗透测试全部流程。 内容: 渗透测试的定义与漏洞检测的区别、WEB 应用架构分析、owasp top 10、渗透测试的信息收集,漏洞检查,漏洞利用,访问维持及漏洞测试报告的书写规范等。
15	网络攻防实训	要求: 学生能够了解网络攻防的基础知识,具备网络安全管理的工作能力,能胜任系统管理、网络管理、网络安全工程师等一线岗位。 内容: 网络信息收集与扫描工具使用、网络攻击技术、网络防御技术及服务加固等。
16	云安全技术与应用	要求: 学生对云平台架构有较深入理解,从而能对云安全有更准确的认知,并将相关技术及理念应用到相关的云计算实践中去。 内容: 云安全的基本概念、云计算面临的安全威胁、云计算应用安全防护技术、安全云技术,云计算安全实践和应用案例分析。

七、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表 3 所示。

表 3：教学活动周进程安排表

单位：周

分类 学期	理实一体教学	实践教学	入学教育	军训	顶岗实习	考试	机动	假期	合计
第一学期	15	1	1			1	2	4	24
第二学期	16	1		1		1	1	8	28
第三学期	16	1				1	2	4	24
第四学期	16	2				1	1	8	28
第五学期	9				8	1	2	4	24
第六学期					16				16
总计	72	5	1	1	24	5	8	28	144

八、教学总体安排

(一) 教学进度表

信息安全技术应用专业的专业教学进程表如表 4 所示。

表 4 信息安全技术应用专业教学进程表

课程类别	课程名称	学分	总学时	按学分分配					
				1	2	3	4	5	6
				16+1	16+4	16+4	16+4	12+8	16
公共基础课程	毛泽东思想和中国特色社会主义理论体系概论	4	64	2	2				
	思想道德修养与法律基础	3	48	1.5	1.5				
	形势与政策	1	16	0.25	0.25	0.25	0.25		
	体育与健康	8	128	2	2	2	2		
	心理健康教育	4	64	1	1	2			
	计算机应用基础	6	96	2	3	1			
	应用数学	6	96	4	2				
	大学语文	2	32	2					
	实用英语	12	192	4	4	2	2		
	职业生涯规划与职业指导	2	32	1			1		
	大学生安全教育	2	36	*	2	*		*	
	军事理论与训练	2	32		2				
	创业意识与创业技巧	2	32		2				
	劳动教育	1	16					1	
小计		55	884	19.75	21.75	7.25	5.25	1	0
选修	艺术教育限选	2	32	2					
	通识教育选修	4	64	4					
小计		6	96	6					
专业（技能）课程	计算机网络技术	4	64	4					
	Python 程序设计基础	4	64	4					
	计算机系统配置	1	24	1					
	Windows 系统管理与应用	2	32		2				
	Python 网络编程	4	64		4				
	Windows 系统安全实训	1	24		1				
	★Linux 服务与安全管理	6	96			6			
	★网络设备安全配置	4	64			4			
	数据库安全管理	4	64			4			
	信息安全基础	4	64			4			
	Python 安全工具开发	8	128			4	4		
	Linux 服务安全管理实训	1	24			1			
	安全考证综合实训	1	24				1		
	★WEB 应用安全	6	96				6		
	WEB 应用开发	6	96				6		
	网络攻防实训	1	24				1		
	★防火墙与 VPN 技术	4	64				4		
	★渗透测试	4	64					4	
毕业顶岗实习		24	576					8	16
小计		89	1656	9	7	23	22	12	16

拓展 选修	创新创业教育（限选）	2	32			2			
	云安全技术与应用	4	64					4	
	安全检测与评估	4	64					4	
	校外专家讲座（限选）	1	16	0.25	0.25	0.25	0.25		
小计		7	112	0.25	0.25	2.25	0.25	4	0
总计		157	2748	29	29	32.5	27.5	23	16

（二）实践教学安排表

实践教学安排如表 5 所示。

表 5 实践教学安排表

单位：周

序号	项目名称	总周数	第一学年		第二学年		第三学年		备注
			1	2	3	4	5	6	
1	入学教育	1	1						
2	计算机系统配置	1	1						
3	Windows 系统安全实训	1		1					
4	安全考证综合实训	1				1			
5	Linux 服务安全管理实训	1			1				
6	网络攻防实训	1				1			
7	毕业顶岗实习	24					8	16	
总计		36	1	1	1	3	14	16	

九、实施保障

（一）师资队伍

通过外引（聘）内培的方式，与合作企业共建一支具有双专业带头人的双师结构教学团队。专业教师中包括专业带头人、骨干教师、青年教师、兼职教师，师生配比为 1:16，专兼配比为 2:1。全部具有大学本科以上学历。

双师素质比例 80%；有国外培训或 1 年以上的企业实践经历更好。

校内专任教师要求熟悉 1 门外语，具备一定程度的双语教学能力。

企业兼职教师应拥有国内知名或外资企业相关岗位 5 年以上工作经历。

（二）教学设施

信息安全技术应用专业实训室配置：计算机网络管理实训室、计算机网络互联实训室、计算机网络互联实训室、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 280 个，能够承担包括日常教学、认证培训和社会服务等多种任务。校内实训室主要功能如表 6 所示。（设备配置需要表述）

表 6 校内主要实训教学条件配置表

实训室名称	教学与训练	工位数量
计算机网络管理实训室	<p>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）</p> <p>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）</p> <p>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</p>	40
计算机网络互联实训室	<p>网络设备的安全接入配置（SSH、双因子认证，AAA 本地和服务器认证）</p> <p>防火墙基本配置（接口、路由）、模块化的策略架构配置、透明模式配置、A/S 配置、Failover 配置、防火墙的 SSL VPN 配置</p> <p>在 ISR 产品上配置 site-to-site VPN、MPLS VPN、GRE over IPSEC 和 DMVPN 等多种类型 VPN 功能</p> <p>在交换机设备上配置接口安全配置、实施 802.1X 协议配置</p>	40
计算机网络互联实训室	<p>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）</p> <p>基础路由协议的配置（静态路由、RIP 路由协议，ospf 路由协议）</p> <p>配置交换机 VLAN、生成树配置</p> <p>接口安全配置，802.1X 协议配置</p>	40
无线网络安全管理实训室	<p>无线控制器配置（瘦 AP、胖 AP、无线加密协议分析与配置）</p> <p>Windows 与 linux 系统渗透、Windows 与 linux 系统加固、网络系统检测、加密算法、内容隐藏、暴力（字典）破解、PKI 体系、证书服务器的搭建</p>	40
综合布线实训室	<p>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</p> <p>光纤、光缆尾纤连接方法训练</p> <p>各种管线的安装、布线训练</p>	40
软件安全实训室	<p>WEB 服务安全：WEB 常见安全漏洞检测，漏洞利用方法，漏洞防御措施，代码安全审计</p> <p>移动安全：漏洞成因分析（权限控制不当、组件保护不当、数据在传输和存储过程中泄漏、WebView 组件安全、源代码保护等），安卓组件安全，敏感数据存储与传输安全，APP 源代码混淆与加固</p> <p>渗透测试：信息收集、存活主机扫描、端口扫描、服务识别、目标主机操作系统平台识别、漏洞利用工具使用、漏洞攻击、维护访问控制</p>	40
攻防实训室	<p>信息安全竞赛系统</p> <p>信息安全攻防演练系统</p> <p>信息安全展示系统</p>	40

（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。

(2)除自编校本教材外，还可选用反映计算机网络技术最新发展水平、特色鲜明，并能够满足高等职业教育培养目标要求的规划教材，并尽量选用近三年出版的高职高专教材。

2. 数字化（网络）教学资源

(1)专业信息库

专业信息库包括专业概况、对接的产业概况、专业建设、人才培养、质量评估、建设成果。

(2)课程资源

课程资源包括课程简介、课程标准、教学设计（整体设计、单元设计、项目设计）、说课录像、授课录像、素材资源（电子教材、电子课件、参考资料、习题题库、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

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）教学评价

通过对专业课程教学评价体系改革，突出能力考核，引入企业参与学生考核评价，建立多元化的课程考核评价体系，实现专业技能和岗位技能的综合素质评价。

建立“知识+技能+实践”的教学评价体系；以过程考核为主体，突出专业核心能力和学生综合素质的考核评价；注重课程评价与职业资格鉴定的衔接；建立多元评价机制，加强行业、企业和社会评价。评价体系包括理论考核、项目过程考核、职业资格认证、行业认证、技能竞赛等多种考核方式。课程考核可以选用以下一种或多种方式：

1. 建立“知识+技能+实践”的教学评价内容体系，突出项目成果评价。
2. 以过程考核为主体，突出专业核心能力和学生综合素质的考核评价。
3. 注重课程评价与职业资格鉴定的衔接。
4. 建立多元评价机制，加强行业、企业和社会评价。

（六）质量管理

为确保人才培养质量，学院建立质量监控体系。质量监控包括人才培养目标监控、人才培养方案和教学大纲监控、教学过程监控、学生信息反馈、教材质量监控。

1. 人才培养目标监控。通过行企业调研和评估，及时跟踪人才培养效果，不断完善人才培养模式，确保专业人才培养目标适应社会发展需要。

2. 人才培养方案和课程标准制订与执行监控。人才培养方案和课程标准是组织和实施人才培养工作的核心教学文件，也是开展教学工作和对教学工作监控与评估的主要依据。

3. 教学过程监控。主要通过听课、教学检查、教学督导、学生评教、教师评学、考试等实现监控目的。

4. 学生信息反馈。建立学生教学信息员制度，定期召开院系两级学生座谈会。

5. 教材质量监控。学院建立教材招标工作组，采用教材三级审核制：教研室申报、教学单位审核、教务处审定。

十、毕业要求

通过3年的学习,学生必须修满157学分，所有课程全部考核合格，并参加完成顶岗实习方可准许毕业。

附件1：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

以满足市场需求为根本宗旨，以培养社会最新型的信息安全技术应用专业人才为目标，以行业协会、典型企业、毕业生就业单位以及往届毕业生等为调研对象，采用专家访谈、网络调查、问卷等方式，充分调研该行业的人才需求和专业改革意见。

（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**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）专家访谈

选择行业协会和 8 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、企业一线技术人员面对面座谈，了解人才需求情况。

（3）网络调查

通过对权威招聘网站的数据进行汇总分析，如百度招聘汇集了各大招聘网站的招聘信息，了解信息安全技术应用专业人才需求情况及趋势。

（4）问卷调查

制作调查问卷 20 份，通过走访企业、邮寄至企业人力资源部门、委托往届毕业生带至企业等多种方式，了解企业的岗位及岗位能力需求细节。

3.调研范围

**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 10 家企业，企业情况如表 1-1 所示。

表 1-1 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	**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	**信息安全测评认证中心	**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	**豌豆信息技术有限公司	**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	**安酷网络安全技术有限公司	**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	**二零卫士信息技术有限公司	**市	民营	面向**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	**斗象科技有限公司	**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	**高嘉信息科技有限公司	**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	**视岳计算机科技有限公司	**市	民营	主营移动产品安全检测及 WEB 安全渗透测试服务

(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;
- 4) 企业一线的技术人员、工程施工人员;
- 5) 学校信息安全技术专业历届毕业生。

5. 调研过程

2018 年 11 月~2019 年 3 月, 进行走访企业现场调查, 问卷调查。

2019 年 4 月, 邀请企业一线专家召开工作任务分析会。

2019 年 5 月, 调研结果分析、完成调研总结报告。

二、调研内容

(一) 相关行业发展现状

1. 我国网络与信息安全发展的基本状况

（1）信息安全政策网络安全法实施，明确规范安全义务

法律的正式出台意味着我国网络安全建设迈向新高度。我国政府于 2016 年 11 月 7 日表决通过了《中华人民共和国网络安全法》，并自 2017 年 6 月 1 日起施行。此法明确指出：“要加强党政机关以及重点领域网站的安全防护，建立政府、行业与企业网络安全信息有序共享机制；建立实施网络安全审查制度，对关键信息基础设施中使用的重要信息技术产品和服务开展安全审查；健全信息安全等级保护制度。”《网络安全法》进一步从法律层面界定了公民和法人的行为边界和细节，为网络的健康和可持续发展奠定了基础。

（2）信息安全新技术驱动高增长

我国信息安全投入不足，经济损失位居全球第一，我国企业信息安全投入不足。根据数据，2014 年，我国信息安全投入占总 IT 投入比例距发达国家尚有至少 6、7 倍差距，我国信息安全投入占整体 IT 投入仅为 2% 左右，远低于欧美成熟市场 10% 左右的水平。随着国家战略的逐步落地，投入占比将逐渐向成熟市场看齐。我国信息安全保障投入不足造成经济损失位居全球第一。全球 20 个国家大约有 9.78 亿人在 2017 年遭受网络攻击，经济损失高达 1720 亿美元，过去 4 年复合增长 11%。而其中中国是遭受网络犯罪攻击最严重的国家，在 2017 年，大约 3.52 亿的中国消费者曾成为网络犯罪的受害者，经济损失达到 663 亿美元，过去 4 年复合增长 15.7%。相比之下，美国的损失却连续下降，由 2013 年的 380 亿美元下降到 2017 年的 194 亿美元。

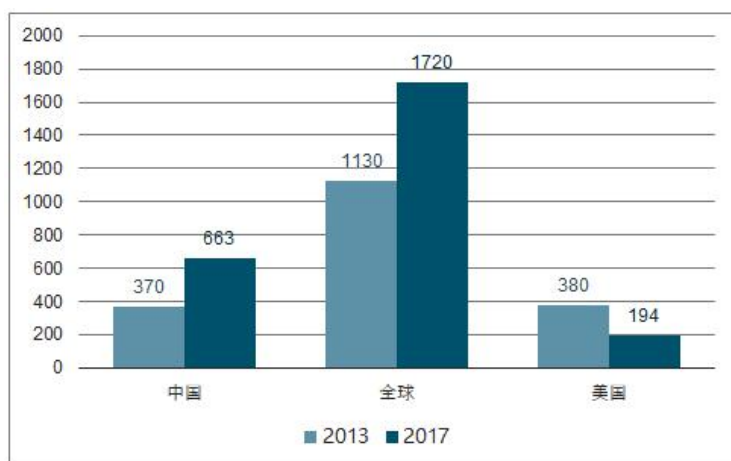


图 1-1 13 和 17 年全球及中美网络犯罪造成的经济损失

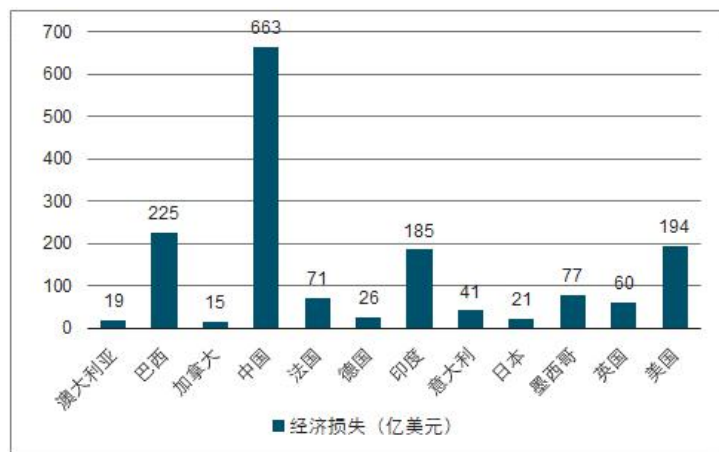


图 1-2 2017 年网络犯罪对各国造成的经济损失

我国信息安全行业市场规模增速有望保持 20%以上。近年来，网络安全威胁事件频发，网络罪犯造成的经济损失快速增多，损失量位居全球第一。持续增长的网路威胁促进我国信息安全产品的快速发展。根据数据，2016 年，中国的网络信息安全市场达到 336.2 亿元，同比增长 21.5%，高于全球增长率 12.05%。鉴于我国信息安全投入比例较低且相关政策的持续推动，国内网络信息安全市场前景可观，据预估，2017-2019 年国内网络信息安全市场呈持续高速增长，增长率都保持在 20%以上。



图 1-3 中国网络信息安全市场规模与增长率

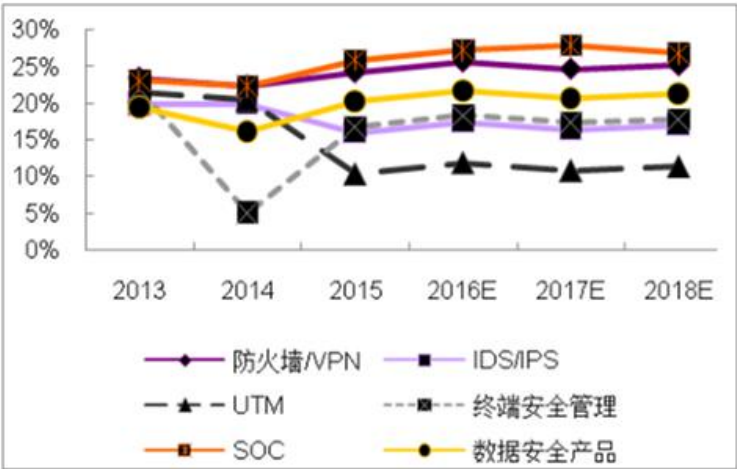


图 1-4 部分子领域规模增速及预测

信息安全以政府和大型国企投资为主。目前，我国信息安全产业链中，下游客户主要为政府部门、电信、金融、能源等信息化程度高且对信息较敏感的行业。而在投入来源中，政府领域的信息安全投入占比最大，接近三分之一，其次是电信（18.7%）和金融（17.9%）领域。信息安全以政府和大型国企投资为主，企业投入占比较低，这是因为信息安全的投入对于公司而言并不产生直接经济效益，主要起到防御作用，只有出现网络安全事件的时候才能凸显其价值。

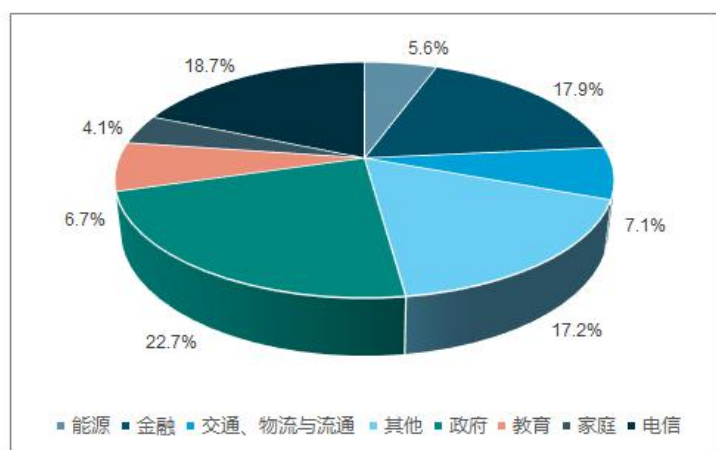


图 1-5 信息安全下游行业需求分布

目前中国网络信息安全市场仍是以硬件为主，占比 51.3%，其次是安全软件和安全服务分别占 37.5%和 11.2%，其中安全服务中安全集成和安全咨询占 90%的市场份额。值得一提的是，虽然信息安全硬件市场占比最大，但是市场规模占比持续下跌，由 2009 年的 54.3%下降到 2015 年的 51.3%。相比之下，全球信息安全市场却以安全服务市场为主，2016 年，安全服务占全球整体市场的 60%，而安全服务市场中各子市场基本各占 1/3。

网络安全服务市场加速。随着中国信息产业和网络技术的发展，传统的网络信息安全产品难以满足日益变化的复杂的网络空间，中国的信息安全产品行业必将向国际看齐，由硬件为主转换为以服务为主，安全服务是长期发展方向，安全人才短缺是这一转折的关键原因之一，并且在有限的时间内，尚看不到人才缺口得到较好弥补的可能。新形势下，产品和服务的联动更加紧密，安全服务逐渐从配合产品的辅助角色，转变成为安全产品发挥最佳效用的必要条件。

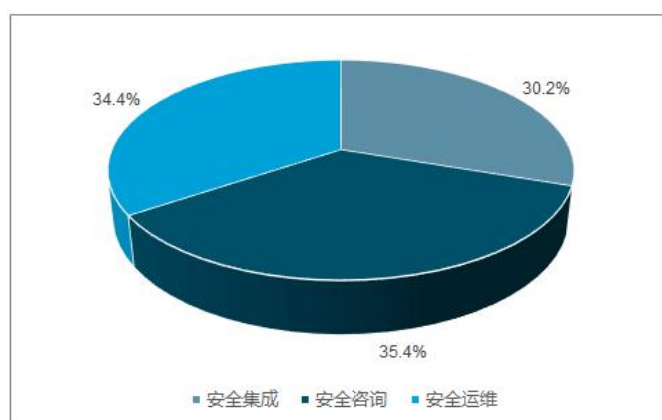


图 1-6 2016 年全球信息安全服务分类

新技术催生信息安全新需求主要表现在以下两个方面。一安全厂商是目前云安全市场的主体，行业正处爆发式增长趋势。二数据安全起步较早，大数据产业快速发展催生数据安全需求增加

安全厂商是目前云安全市场的主体，阿里云市场中 90%以上的云安全服务由安全厂商提供。安全厂商又分为平台型的安全服务集成商和专业型的安全服务

提供商。专业型厂商在云安全领域的入局早于平台型安全厂商。例如知道创宇在 2007 年就开始云安全技术的研究。因此从技术成熟度上来讲，专业安全服务商已能够提供较完整的安全服务，如创宇盾、安全狗、云锁、山石网科下一代虚拟防火墙、极验验证码等。国内平台型安全厂商的步伐相比较慢，仅有绿盟（2015 年）和安恒信息（2015 年）少量企业提供了完整解决方案。启明星辰、天融信、北信源等公司现有的云产品多在云安全管理平台布局，还未形成完整的云安全方案。相比于第三方云安全厂商，大部分云计算运营商（如阿里云、华为云和腾讯云等）以提供免费的基础云安全服务为主，如抗 DDos、WAF、漏洞扫描和加密服务等。

我国数据安全产业起步于 2000 年左右，近年来启明星辰、绿盟、天融信等国内企业纷纷进入这一领域。2004 年数据加密产品应运而生，数据安全产业开始起步，历经 10 年发展，2016 年数据安全市场规模达 18.1 亿元，同比增长 21%，随着大数据产业的快速发展将催生数据安全需求不断增加，预计数据安全未来还将保持 20%以上增速增长。竞争格局方面，启明星辰、绿盟科技、天融信、神州泰岳和时代亿信等企业市场份额排名靠前。

2. **网络与信息安全方向发展的基本状况

市政府较早确立了大力发展信息产业的经济发展战略，至今，的电子信息技术制造业产值已连续十余年居全国前列。计算机网络、通讯环境的建立为各行各业的计算机应用提供了良好的条件。为了配合信息化要求，**先后建立了多个国家级的软件园区，有力促进了计算机应用与软件产业的发展。目前，**以高新科技产业为主要经济发展方向的规划已经开始实施。这些高新技术企业大多以信息技术、软件技术和计算机应用技术为核心，研究和利用先进技术，从事如金融电子化、电子商务、多媒体信息处理、应用软件、电子出版物、电子电路系统等信息技术领域的应用开发和系统集成等工作。随着这些工作的开展，互联网上的业务流量得到了急剧增长，相对应的接入设备类型的多样性会致使流量类型迅猛增多，而新增业务对网络的稳定性、可靠性、安全性要求不断提高。与此同时，当前网络接入技术正向“IP+以太网”方向发展，已经走入了企业办公、工业生产、教育、金融、医疗等各个领域，电信级和工业级的以太网交换机应用范围变得更加广泛，不仅使得行业运作效率得到提高，还为用户带来直接或间接的经济效益，但同时也会带来各种各样的风险。下面为 2018 年各类单位信息安全事件单位发生率表 1-2。

表 1-2 2018 年各类单位信息安全事件单位发生率

事件类型 \ 发生次数	0	1	2	3
黑客攻击	93.75%	2.05%	0.68%	3.52%
计算机病毒	76.5%	1.37%	2.73%	19.4%
由于自身原因造成的系统瘫痪	97.95%	1.37%	0	0.68%
收到反动及黄色内容邮件	95.21%	1.37%	0.68%	2.74%

安全事件发的面广，涉及了各行各业。2018 年全易发信息安全事件的单位分类表 1-3 如下：

表 1-3 2018 年全易发信息安全事件的单位分类

事件种类	易发单位
黑客攻击	金融类、政府机关、通信网络类、工业企业类、高校
计算机病毒	政府机关、工业企业类、金融类、高校
由于自身原因造成的系统瘫痪	政府机关、金融类、工业企业类
收到反动及黄色内容邮件	政府机关、新闻媒体、金融类、工业企业类、高校

“十三五”期间，**加快推进“四个率先”和加快建设“四个中心”，实现经济发展转型的关键期；信息产业作为**基础性、先导性和战略性新兴产业，对**未来发展具有十分重要的意义。**将基本建成宽带、融合、安全、泛在的新一代信息通信基础设施，围绕智慧城市发展目标，推进城市光网和无线城市建设。加快“三网融合”国家战略的推进和实施。

未来**将“加强网络安全、数据安全、可信计算、安全测评等关键技术的研发与产业化，重点发展安全可靠的安全基础产品、电子认证公共服务平台、网络与边界安全产品、信息安全支撑工具等，发展云计算、物联网等新一代信息技术应用环境下的安全技术产品。加大相关标准的研制力度，推进国家信息安全产品制度建设。规范和促进风险评估、容灾备份和灾难恢复、安全集成、安全测评等信息安全服务。开展安全可靠产品应用试点示范和推广，提升重要信息系统和工业系统的安全可靠水平。”

随着智慧城市建设的推进，“两化融合”、“三同融合”等重点工作的推进，信息化已深入经济社会的方方面面，信息安全也将深刻影响着经济发展、社会稳定和城市安全。为此，信息安全保障工作已与城市正常运转密不可分，成为保障经济又好又快发展、服务产业结构调整升级的重要领域。伴随着**信息化的发展，市场对于网络与信息安全人才的需求将呈现出要求不断提高、价值不断上升、领域不断扩展的趋势；信息产业作为**基础性、先导性和战略性新兴产业，对**未来发展具有十分重要的意义，知识型、发展型、技能型的信息安全技术应用人才将长期成为市场的宠儿。

（二）行业从业人员基本情况

了解企业网络与信息安全从业人员基本情况，我们通过进行访谈式调研及网络调研相结合方式。参与问卷调研的企业共 26 家，其中信息安全类企业 16 家，IT 信息相关类企业 7 家，其它 3 家。调查对象包括各公司从事网络信息安全相关工作相关技术人员和管理骨干，调查内容主要为部分技术人员的具体岗位需求、学历需求、薪资水平、职业技能和技能证书需求等。从企业岗位需求进行分析统计，目前网络与信息安全类的工作岗位有：网络管理员、信息安全评估员、信息安全工程师、网络安全评测工程师、安全渗透测试工程师、网络安全运维工程师、安全设备运维（调试）工程师等。而在这些岗位又按技能等级技能的熟练度及工作年限长短，可粗略进行一个高、中、低级能力的划分，如图 1-7：

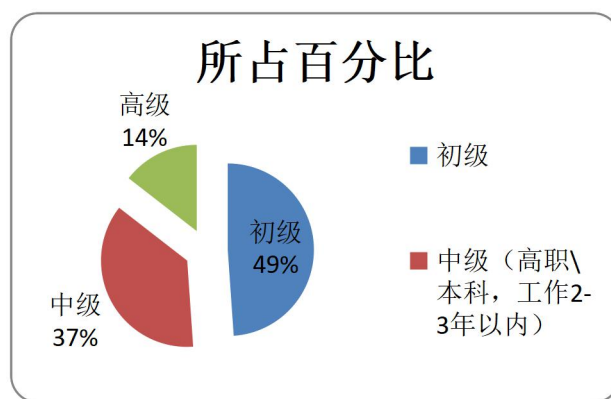


图 1-7 企业岗位能力需求比例

由上面的网络信息安全技术应用人员市场结构分析可知，市场需要 49%~86%左右的初中级网络安全技术人员，而这类人员完全可以从高职这个层次培养。在调研时当问及被访者对于信息系统安全的认识时，98.6%的被访者认为信息系统的安全事关单位运行，其余认为不很重要的被访单位均还未建立单位内部网络。由此看来，享受到信息共享的单位已充分意识到网络安全的重要性。同时我们通过调研发现，目前的企业、事业、政府、学校等单位，有 83%的单位迫切需要网络信息安全方面人才，不难看出网络安全市场还处于发展的初级阶段，具有很大的发展空间。由此可见，在信息安全产业本应大力发展的美好前景下，“一才难求”是当前信息安全产业发展遇到的尴尬问题，信息安全人才的匮乏，使得我国的信息安全产业面临着一段人才真空期。

另外，从技术研究层面分析，信息安全技术应用是一门比较特殊的学科，除了在校的信息安全技术应用专业学生及毕业生外，大量的安全人才都属于“自学成才”，都源自于对“黑客技术”的热爱和追捧。在中国黑客艰难的成长过程中，由于大量的技术人才属于自学成才，并且都具有低学历、甚至无学历的知识背景，只有少数技术人才因个人努力或成长机遇而进入信息安全行业，很大一部分技术人才在物质利益的吸引下加入了地下黑色产业链，这些技术人才并没有为国家和社会创造价值，从而使得现在的信息安全行业出现了人才奇缺的窘境！

**经济与社会的快速发展，带动了信息安全技术应用人才的需求。以下是从网络查询出的对信息安全类专业人才需求情况：

百度招聘，统计了**地区三天的岗位招聘数量（1035 条）：

信息安全岗位招聘数量（3 天）

统计时间段	招聘具体职位	招聘数量
2019 年 4 月 19 日至 21 日	信息安全专员、售前售后技术支持工程师、网络运维服务等信息安全类、安全测评工程师、渗透测试工程师、网络安全运维工程师、信息安全开发工程师、信息安全与技术反欺诈高级工程师等	1035 个

通过企业访谈统计出企业需用工人数对学历的要求如图 1-8：

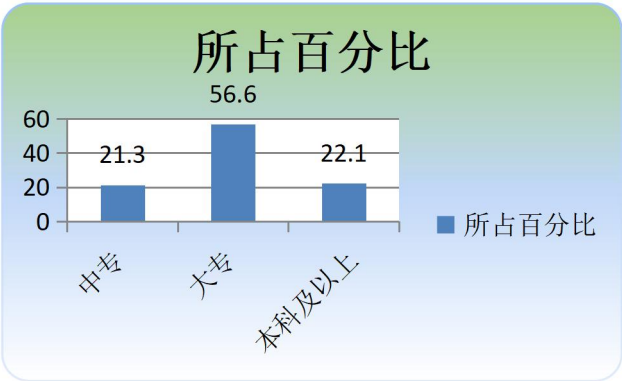


图 1-8 企业对信息安全技术应用岗位学历要求

依据企业对高职层次需求，我们仅统计高职层次企业对工作经历要求，统计数据见图 1-9。

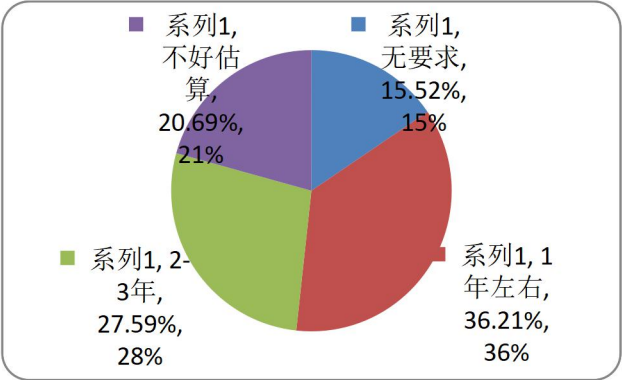


图 1-9 企业对高职层次工作经历要求

三、专业现状调研

（一）专业点分布情况（113所高职专科学校）

表 1-4 专业分布点情况

地区	学校	是否重点专业
**	**信息职业技术学院（网络安全方向）	否
	**政法职业学院侦查类（涉外安全信息分析与管理）	否
	**网络职业学院	否
**	**电子信息职业技术学院	否
	**科学技术职业学院	否
**	**科技职业技术学院	是
	**现代信息工程职业技术学院	否
	**职业技术学院	否
	**华夏职业学院	否
**	**信息职业技术学院	是

	**职业技术学院	否
	**海事职业技术学院	否
	**科技职业学院	是
	**信息职业技术学院	否
	**百年职业学院	否
	**信息职业技术学院	否
**	**金融职业学院	是
	**职业技术学院	否
	**科技职业学院	否
**	**职业技术学院	否
	**冶金科技职业学院	否
	**国防科技职业学院	是
	**邮电职业技术学院	否
	**绿海商务职业学院	否
	**职业学院	否
	**粮食工程职业学院	否
	**经济管理干部学院	否
**	**职业技术学院	否
	**信息职业技术学院	否
	**英华职业学院	否
	**软件职业技术学院	否
	**安防科技职业学院	否
**	**机电职业技术学院	否
	**工业职业学院	是
	**城市职业学院	是
**	**职业技术学院	否
	**职业技术学院	否
	**能源职业技术学院（中标华安就业订单班）	否
	**财经职业学院	否
	**科技职业技术学院	否
	**司法警官职业学院	否
**	**铁路职业技术学院	否
	**工程技术学院	否
	**职业技术学院（云安全技术与应用方向）	否
	**工业和信息化职业学院	否
	**司法警官职业学院	否
	**职业技术学院	否
	**经贸职业学院（移动安全方向）	否
	**城市职业学院	否

**	**职业学院与济南博赛网络技术有限公司校企合作	否
	**信息职业技术学院	否
	**师范高等专科学校	否
	**电子职业技术学院	否
	**城市建设职业学院	否
	**理工职业学院	否
**	**省财政税务专科学校	否
	**职业技术学院（原计算机网络与安全管理）	否
	**职业技术学院	否
	**信息职业技术学院	否
	**警官职业学院	否
	**电力职业技术学院	否
**	**交通职业技术学院	是
	**工商职业学院	否
**	**邮电职业技术学院	是
	**机电职业技术学院	否
	**托普信息技术职业学院	否
	**商务职业学院	否
	**信息职业技术学院	是
	**科技职业学院	是
	**城市职业学院	否
	**工业职业技术学院	是
	**工贸职业技术学院	否
**	**电子工程职业学院	是
	**传媒职业学院	是
	**工程职业技术学院	是
	**青年职业技术学院	是
	**科创职业学院	是
	**电讯职业学院	是
	**安全技术职业学院	是
**	**电子信息职业技术学院	是
	**轻工职业技术学院	是
**	**航海职业技术学院	否
	**软件工程职业学院	否
	**生物科技职业学院	否
	**科技职业学院	是
	**青年职业学院	否
**	**信息职业技术学院	否
	**铁道职业技术学院	否
	**石油化工职业技术学院	否
	**安全技术职业学院	否
	**汽车工程职业学院	否
	**汽车工程职业学院	否

**	**铁道职业技术学院	否
	**职业学院	是
	**安全工程职业技术学院	否
**	**职业技术学院（网络入侵与防范方向）	是
	**职业技术学院	否
	**工程学院	否
	**司法警官职业学院	否
	**应用技术职业学院	否
	**机电职业技术学院	否
	**工业贸易职业技术学院	否
	**科技职业学院	否
**	**职业学院	否
	****工职业学院	否
**	**司法警官职业学院	否
	**电子信息职业技术学院	是
	**职业技术学院	否

（二）专业招生与就业岗位分布情况

1. 信息安全技术应用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 1-5。

表 1-5 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	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

序号	任务领域	典型工作任务	职业需求技能
		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。	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; 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;

序号	任务领域	典型工作任务	职业需求技能
			18. 能够利用工具对信息系统进行初步的安全评估。
3	安全渗透测试工程师	1. 参与安全测评项目、安全服务项目的具体实施； 2. 实施主机、网络和 Web 安全渗透测试； 3. 信息安全渗透测试、风险评估与加固工作的组织实施； 4. 构建 WEB 内容安全体系，评估上线业务安全问题，指导安全测试，跟踪解决内容安全问题； 5. 了解信息安全技术应用趋势，及时掌握新的安全技术、安全攻击及防御技术； 6. 在出现网络攻击或安全事件时，配合提供应急响应的技术支持，帮助用户恢复系统及调查取证。	1. 掌握 WINDOWS、LINUX 操作系统安全防护设置； 2. 掌握路由与交换技术； 3. 掌握各类网络安全和防攻击技术，具有一定的系统与网络的攻防对抗能力； 4. 能进行内外网分段安全测试； 5. 熟悉数据安全与行为安全；熟悉数据备份与远程容灾； 6. 能够制定简单的被评估对象的核查列表； 7. 能够对被评估对象进行脆弱性分析； 8. 可以结合重要性和发现的脆弱性进行系统综合风险分析； 9. 能够利用相关安全评估扫描工具对测评对象进行扫描； 10. 能够利用应用渗透评估扫描工具对测评对象； 11. 能够利用网络截包工具对网络数据进行分析； 12. 能够发现渗透对象可能存在的漏洞； 13. 能够利用渗透工具对漏洞进行验证； 14. 能够充分利用网络资源查找了解相关渗透性攻击方法和工具； 15. 能够对网络安全方案进行实施与检测。
4	信息安全评估员	1. 负责对信息安全(网络、系统、数据安全等)策略规划及协调部署； 2. 信息安全审计（包括操作系统、数据库、应用系统和网络，及信息安全体系）； 3. 负责信息安全政策、流程及管理制度建设和完善； 4. 负责定期完成信息安全自查工作，撰写自查报告并提出整改措施； 5. 信息安全监控和预警； 6. 安全系统的维护。	1. 信系统安全分析评估工作计划能够根据系统特征对被评估对象重要性进行赋值； 2. 制定简单的被评估对象的核查列表； 3. 对被评估对象进行脆弱性分析； 4. 结合重要性和发现的脆弱性进行系统综合风险分析； 5. 撰写风险评估报告； 6. 能够利用相关安全评估扫描工具对测评对象进行扫描； 7. 能够利用应用渗透评估扫描工具对测评对象； 8. 能够利用网络截包工具对网络数据进行分析； 9. 能够发现渗透对象可能存在的漏洞； 10. 能够利用渗透工具对漏洞进行验证； 11. 能够充分利用网络资源查找了解相关渗透性攻击方法和工具。
5	网络运维安全管理员	1. 能熟练配置 Windows、Linux 下的各类服务器及相关软件； 2. 能对服务器的安全进行评估； 3. 对系统安全 BUG 进行评估和测试； 4. 了解服务器性能，能架设高	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；

序号	任务领域	典型工作任务	职业需求技能
		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份和灾难性恢复; 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。	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; 5. 建立安全设备运维文档、完成安全运维报告。	1. 掌握路由与交换技术; 2. 能进行内外网分段安全测试; 3. 熟悉市场上的各类型主流安全产品特性及功能应用情况; 4. 会调试防火墙、UTM、VPN、IDS、审计认证等安全设备; 5. 了解安全产品中 IPV6 技术; 6. 熟悉安全产品的高级配置与部署, 如分布式出口部署、高可用性 HA 部署等; 7. 熟悉安防系统功能和构成, 如监控、门禁、防盗等系统的配置使用; 8. 学会基本的的功能测试与分析; 9. 具备选择适当技术的规划设计能力; 10. 能够按应用需求, 进行安全角色与权限的划分与管理。

2. 人才规格与培养目标分析

从信息安全技术应用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**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、心理健康。

●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**市一级等通识教育模块知识。

依据以上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**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，掌握网络安全安全管理技能，有很强的实际操作能力、有较强的英语功底，“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）专业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 and 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能力 。

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,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、新方法无法通过实验验证,不利于学生掌握。

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

根据调研中对安全服务的深入了解,将本专业定位于 Web 安全工程师岗位,这是信息安全领域的一个职位,它负责对公司网站、业务系统进行安全评估测试;对公司各类系统进行安全加固;对公司安全事件进行响应,清理后门,根据日志分析攻击途径;安全技术研究,包括安全防范技术,黑客技术等;跟踪最新漏洞信息,进行业务产品的安全检查。通过用人单位反馈,高职学生在这个安全服务岗位的胜任度最高。

(二) 专业课程内容优化建议

根据高职高专应用型人才的培养目标,实施以基础理论知识的应用和实践能力培养的原则,以应用为目的,以“必需、够用”为度,加强针对性和实用性。另外,高职高专学生毕业后主要从事网管员等应用型岗位,针对此类岗位必须具备的职业技能,从日常的网络安全维护及管理为出发点,作者认为高职高专信息安全技术应用专业课程教学目标应当定位在了解网络安全技术的基本原理基础上,掌握网络系统的安全性维护和系统的安全构建等实用技能。同时根据课程实际与培养应用型人才的需要,加大课程中实训的内容,使理论课与实训课达到比例 1:1。

(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**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,重构课程体系,重点打造《网络安全设备配置与管理》、《Linux 服务与安全管理》、《WEB 应用安全》、《安全检测与评估》、《渗透测试》5 门信息安全技术专业核心课程,制定课程标准,并着力打造精品课程资源。

依托本专业的学生网络信息安全工作室，专业课程建设与工作室项目实施应形成良好的互动关系。课程的项目内容取材于工作室的真实项目，实现了课程内容的开放性和实践性。在项目实施过程中，教师、学生的参与，提高实践水平，由此形成了相互依存，互相促进的关系。

（四）专业师资与实训条件配置建议

进一步开展“双师型”教师团队建设国家教委在 1995 年的《关于开展建设示范性职业大学工作的原则意见》中首次提出了“双师型”教师的概念后，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。“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。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。在“4 + 1 + 1”的人才培养模式中涉及的企业认证课程，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。





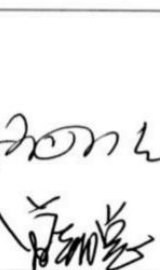

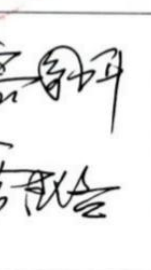
附件2：专业建设指导委员会审定意见

3.2 专业建设指导委员会审定意见

专业名称	信息安全与管理专业（高职）		
适用年级	2019 级		
评审时间	20190513		
<p>专家评审意见：</p> <p>专家组听取、审阅了信息职业技术学院关于高职信息安全与管理专业（2019 级）人才培养方案的汇报，审阅了人才需求调研报告、人才培养方案、部分核心课程课程标准，经讨论，形成意见如下。</p> <p>该专业人才培养方案符合人才培养目标，课程体系结构框架较清晰合理，课程主要教学内容符合人才能力培养要求。</p> <p>(1) 建议相关的理论课与实训课可以进行整合，提升教学效果。比如《windows 系统管理与应用》和《windows 系统安全实训》课程，《linux 服务于安全管理》和《linux 服务安全管理实训》。并且，《计算机系统配置》《windows 系统安全实训》课程可以调整到第一、第二学期。</p> <p>(2) 《渗透测试实训》《网络攻防实训》调整到第五学期。</p> <p>(3) 按照 操作系统+网络+编程基础+安全基础+安全实践等技术路线安排课程。可考虑按照人才培养技术主线将课程合理安排在各个学期，便于学生技术技能逐级提升。</p>			
评审专家	姓名	单位	签名
	吴杰舜	德网络科技股份有限公司	吴杰舜
	尚金龙	科技信息有限公司	尚金龙
	杨寅春	第二工业大学	杨寅春

附件3：学术委员会审定意见

附件 3 学术委员会审批意见表

时间	2019 年 6 月 26 日	地点	A205
评审专业	信息安全与管理		
<p>委员会审批意见：</p> <p>2019 年 6 月 26 日，信息职业技术学院学术委员会听取了信息安全与管理专业负责人对该专业 2019 级人才培养方案修订工作所作的专题汇报，与会委员对 2019 级信息安全与管理专业人才培养方案进行了集体讨论，形成如下意见：</p> <p>信息安全与管理专业在广泛调研的基础上修订了该专业的人才培养方案，基础数据和资料真实可靠，符合人才培养方案修订的程序和要求。</p> <p>在专业调研的基础上，专业培养目标体现安全评估与检测服务能力的培养，根据信息安全技术发展要求，调整了培养规格中的知识目标和能力目标，理由充分。方案中优化了课程安排，将与专业课程相关的实训课程的开出顺序做了调整，保证课程的相关性连贯性更好。方案中优化了相关专业课程，在专业课程中融入了思政和创新创业的内容，公共课占比 33%，选修课占比 11%，实践课时占比大于 50%，实习时间达 6 个月，符合社会人才需求。</p> <p>与会委员一致认为，优化后的信息安全与管理专业人才培养方案能够满足人才培养要求，同意按其开展教学活动。</p> <div style="text-align: right;">  信息职业技术学院学术委员会 2019 年 6 月 26 日 </div>			
<p>专家签名：</p> <div style="display: flex; justify-content: space-around; align-items: flex-end;">       </div>			