

**湖南信息职业技术学院**  
**2019 级信息安全与管理专业人才培养方案**  
**(610211)**

### 一、专业名称及专业群

专业名称：信息安全与管理

专业群：网络空间安全专业群

### 二、招生对象、学制

招生对象：高中毕业生或同等学历者

学 制：三年

### 三、培养目标

培养学生掌握信息安全基本理论、信息安全相关工具及渗透测试相关知识，具备网络安全规划设计、网络安全产品配置管理能力、网络安全风险评估与渗透测试能力、系统安全加固与修复能力、数据安全管理能力；具有良好的综合素质，能够用所学专业知识和解决专业相关实际问题，能够自主学习和触类旁通。能够胜任渗透测试工程师、安全运营工程师、安全产品运维工程师、信息安全风险评估师等岗位工作，适应社会发展需要，德、智、体、美、劳全面发展的高素质技术技能人才。

### 四、培养规格

#### (一) 知识结构

##### 1. 公共基础知识

(1) 掌握基本的政治法律知识、道德规范、数学知识、英语知识、计算机应用知识；

(2) 掌握必备的心理健康知识、就业、创新创业、人际交往礼仪知识；

(3) 掌握一定的传统文化、写作知识和技巧等；

(4) 掌握《中华人民共和国网络安全法》知识。

##### 2. 专业知识

(1) 掌握计算机网络体系架构及网络设备配置相关知识；

(2) 掌握计算机操作系统及其安全管理的相关知识；

- (3) 掌握服务器的安全配置管理的相关知识；
- (4) 掌握网络安全规划与管理的相关知识；
- (5) 掌握无线网络安全管理的相关知识；
- (6) 掌握安全行为管理的基础知识；
- (7) 掌握加密技术的基础知识。

## **(二) 能力结构**

### **1. 通用能力**

(1) 具备良好的政治识别和法律认知能力、数学运用能力、英语应用能力、信息技术应用与加工能力；

(2) 具备良好的创新创业能力、人际交往能力、心理调适能力、写作能力、表达能力、解决实际问题的能力、终身学习能力等；

(3) 具备独立查阅、翻译中英文专业资料及公文处理能力；

(4) 具备终身学习的意识和再学习的能力。

### **2. 专业技术技能**

(1) 具备计算机软硬件的维护、配置能力，熟练使用计算机常用工具软件的能力；

(2) 具备局域网系统的设计安装、调试、维护、运行与管理的能力；

(3) 具备服务器及网络配置、安全管理、维护的能力；

(4) 具备网络安全测试、分析的能力；

(5) 具备加密技术理论及其应用的能力；

(6) 具备无线网络安全配置的能力；

(7) 具备网络安全漏洞的发现、修补的能力；

(8) 具备渗透测试工具应用的能力；

(9) 具备信息安全规划与设计方案的撰写与阅读能力。

## **(三) 素质结构**

1. 具有正确的世界观、人生观、价值观。积极践行社会主义核心价值观，具有深厚的爱国情感、国家认同感、中华民族自豪感；崇尚宪法、遵守法律、遵规守纪；具有社会责任感和参与意识；

2. 具有良好的身心素质。具有健康的体魄和心理、健全的人格，能够掌握基本运动知识和一定的运动技能；

3. 具有良好的人文素养。具有感受美、表现美、鉴赏美、创造美的能力，具有一定的审美和人文素养，能够形成一两项传统文化爱好；掌握一定的学习方法，

具有良好的生活习惯、行为习惯和自我管理能力；

4. 具有良好的职业道德和职业素养。崇德向善、诚实守信、爱岗敬业，具有精益求精的工匠精神；具有质量意识、绿色环保意识、安全意识、信息素养、创新精神；具有较强的集体意识和团队合作精神，能够进行有效的人际沟通和协作；

5. 具有高度的责任感，有严谨、细致、认真的工作作风；

6. 具有团队合作意识、协调与组织管理能力；

7. 具有信息安全领域创新精神；

8. 具有遵守行业规程、保守国家秘密和商业秘密，不进行信息的窃取、盗卖活动的意识。

## 五、毕业标准

1. 所修课程的成绩全部合格，修满 157 学分

2. 至少获得以下 6 个职业资格证书中的一个

- 网络工程师（计算机技术与软件专业技术资格<水平>考试）
- 信息安全工程师（计算机技术与软件专业技术资格<水平>考试）
- RCSCA（锐捷认证安全工程师）
- ISEC 信息安全管理员（国家信息化安全教育认证）
- 360 企业安全认证工程师
- CISP-PTE 注册信息安全专业人员-渗透测试工程师（中国信息安全测评认证）

3. 参加全国高等学校英语应用能力考试（A 级）并达到学校规定成绩要求

4. 毕业设计答辩合格

## 六、职业面向

### （一）服务面向

在 IT 及互联网行业、政府、相关企事业单位，从事安全运营工程师、渗透测试工程师、信息安全风险评估师等岗位（群）工作。

表 1 信息安全管理专业主要服务面向与岗位类别表

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	计算机类	互联网及相关服务  软件和信息服务	计算机硬件工程技术人员  计算机软件工程技术人员  计算机网络工程技术人员	渗透测试工程师  安全运营工程师  信息安全风险评估师  安全产品运维工程师	信息安全工程师  360 企业安全认证工程师  CISP-PTE

## (二) 职业发展路径

通过对信息安全与管理专业的就业岗位进行分析, 获取了本专业的初入就业岗位、目标岗位、发展岗位及迁移岗位之间的关系, 如图 1 所示。

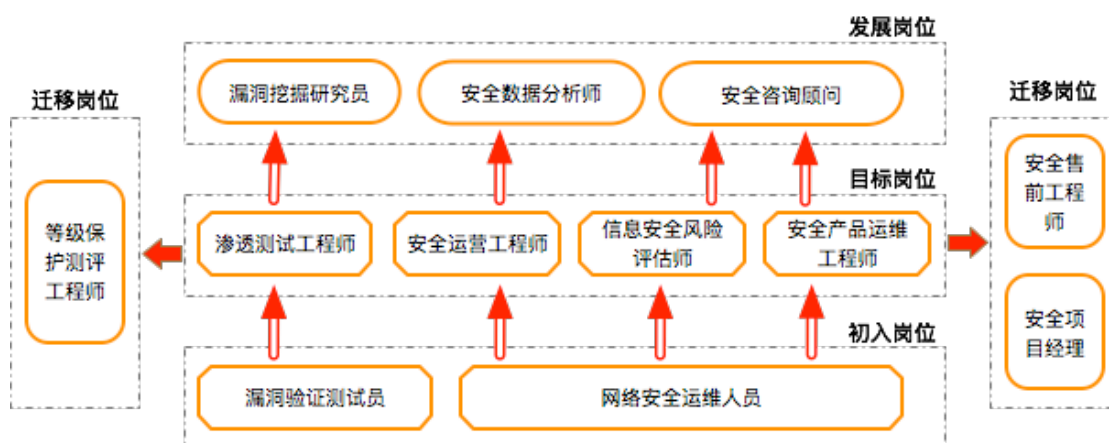


图 1 职业发展路径图

## (三) 职业岗位分析

通过对专业岗位的分析, 信息安全管理专业的初次就业岗位有: 漏洞验证测试员、网络安全运维人员; 目标岗位有: 渗透测试工程师、安全运营工程师、安全产品运维工程师、信息安全风险评估师; 发展岗位有: 漏洞挖掘研究员、安全数据分析师、安全咨询顾问; 迁移岗位有: 安全售前工程师、安全项目经理、等级保护测评工程师等。其目标岗位能力分析如表 2 所示。

表 2 职业岗位工作分析

岗位名称		主要工作内容概述	典型工作任务
初入就业岗位	网络安全运维人员	<ol style="list-style-type: none"> <li>负责网络、系统的安全运营。</li> <li>负责关注最新安全动态和安全漏洞，及时提供安全漏洞预警。</li> </ol>	<p>T1-1: 制定、设计全网的路由与安全策略。</p> <p>T1-2: 根据安全需求，定期对公司网络、业务系统进行安全评估、制定安全解决方案，并推进实施。</p>
目标就业岗位	渗透测试工程师	<ol style="list-style-type: none"> <li>负责公司的渗透测试工作与报告编写。</li> <li>负责对客户网络、系统、应用进行渗透测试和安全加固。</li> <li>针对客户网络架构，建议合理的网络安全解决方案。</li> </ol>	<p>T2-1: 在授权情况下，对用户系统、IT 基础架构实施渗透测试。</p> <p>T2-2: 推动企业网络安全漏洞整改。</p>
	信息安全风险评估师	<ol style="list-style-type: none"> <li>负责对网络与信息系统进行资产识别、威胁识别、脆弱性识别、已有安全措施有效性识别、风险分析。</li> <li>负责防范或者化解信息安全风险，制定针对性的抵御风威胁的防护对策及整改措施。</li> </ol>	<p>T3-1: 等保测评的项目实施及管理。</p> <p>T3-2: 完成信息安全等级保护测评、信息安全咨询、信息安全风险评估等项目的技术支持工作。</p>
	安全产品运维工程师	<ol style="list-style-type: none"> <li>负责面向用户的增值运营服务交付工作，包括平台的初始配置和优化维护、日常监测分析、安全预警、运营报告编写等工作。</li> <li>负责项目售后服务交付工作，包括平台巡检、产品培训、技术培训等工作。</li> </ol>	<p>T4-1: 针对产品应用运维及维护。</p> <p>T4-2: 安全配置巡检、服务器安全巡检。</p> <p>T4-3: 人际交流、表达能力。</p>
拓展岗位	安全项目经理	<ol style="list-style-type: none"> <li>负责咨询项目实施。</li> <li>负责信息安全的售前技术交流、技术方案撰写和项目投标等工作。</li> <li>负责信息安全项目的集成实施、项目管理等工作。</li> </ol>	<p>T5-1: 完成信息安全等级保护测方案设计、售前交流、服务实施。</p> <p>T5-2: 国内外主流厂商的相关安全产品、主流操作系统、数据库等安全使用。</p> <p>T5-3: 市场营销。</p>

## 七、工作任务与职业能力分析

表 3 工作任务与职业能力分析表

序号	工作岗位（群）	工作任务	职业能力
1	网络安全运维人员	T1-1：制定、设计全网的路由与安全策略。 T1-2：根据安全需求，定期对公司网络、业务系统进行安全评估、制定安全解决方案，并推进实施。	A1-1-1：网络安全设计及配置、维护能力。 A1-1-2：业务系统安全配置及维护能力。 A1-2-1：信息安全评估能力。
2	渗透测试工程师	T2-1：在授权情况下，对用户系统、IT 基础架构实施渗透测试。 T2-2：推动企业网络安全漏洞整改。	A2-1-1：使用渗透测试工具的对相应系统进行测试的能力。 A2-2-1：漏洞验证和漏洞利用的能力。 A2-2-2：能对应用系统进行安全加固的能力。
3	信息安全风险评估师	T3-1：等保测评的项目实施及管理。 T3-2：完成信息安全咨询、信息安全风险评估等项目的技术支持工作。	A3-1-1：熟悉常见的信息安全管理体 系。 A3-1-2：深刻理解信息安全管理制 度。 A3-1-3：物理安全测评、主机安全测 评、数据安全测评、应用安全测评等 实施及编制报告的能力。 A3-2-1：具备信息安全管理体 系核、培训的能力。
4	安全产品运维工程师	T4-1：针对产品应用运维及维护。 T4-2：安全配置巡检、服务器安全巡检。 T4-3：人际交往、表达能力。	A4-1-1：熟悉信息安全相关知识。 A4-1-2：熟悉主流安全厂商相关安全 产品运维。 A4-2-1：熟悉主机系统网络及数据库 相关操作。 A4-2-2：熟悉应用维护及系统安全相 关操作流程。
5	安全项目经理	T5-1：完成信息安全等级保护测方案 设计、售前交流、服务实施。 T5-2：国内外主流厂商的相关安全 产品、主流操作系统、数据库等安 全使用。 T5-3：市场营销。	A5-1-1：具备信息安全评估、测评的 能力。 A5-1-2：能够与客户进行业务洽谈， 具备营销理论知识。 A5-2-1：能够使用安全产品。

## 八、课程体系设计

### (一) 专业课程设计

本专业课程以工作岗位的职业能力为依据进行分析与设计,依据各岗位的特殊性分别设计其对应的核心课程,同时结合职业发展方向设计专业拓展课程。本专业课程设计关系如下表所示。

表 4 职业能力与专业课程对应关系

序号	课程名称	职业能力要素
1	交换技术 路由技术 实训—中小型网搭建项目 实训—企业网搭建项目	A1-1-1: 网络安全设计及配置、维护能力。
2	Windows 服务器安全配置 与管理 主机安全技术	A1-1-2: 业务系统安全配置及维护能力。 A2-2-2: 能对应用系统进行安全加固的能力。 A4-2-1: 熟悉主机系统网络及数据库相关操作。
3	信息安全技术	A2-2-1: 漏洞验证和漏洞利用的能力。 A4-1-1: 熟悉信息安全相关知识。
4	安全评估与安全管理	A1-2-1: 信息安全评估能力。 A3-1-1: 熟悉常见的信息安全管理体制。 A3-1-2: 深刻理解信息安全管理体制。 A3-1-3: 物理安全测评、主机安全测评、数据安全测评、应用安全测评等实施及编制报告的能力。 A5-1-1: 具备信息安全评估、测评的能力。
5	Python 安全工具开发 Web 前端技术 PHP 程序设计 渗透测试	A2-1-1: 使用渗透测试工具的对相应系统进行测试的能力。
6	Web 应用安全技术 数据库安全技术	A2-2-2: 能对应用系统进行安全加固的能力。 A4-2-1: 熟悉主机系统网络及数据库相关操作。 A4-2-2: 熟悉应用维护及系统安全相关操作流程。
7	防火墙技术与应用 VPN 技术与应用	A1-1-1: 网络安全设计及配置、维护能力。 A4-1-2: 熟悉主流安全厂商相关安全产品运维。 A5-2-1: 能够使用安全产品。

## （二）课程学习路径

遵从“从简单到复杂，从模仿到应用”的认知规律，遵从“从低级到高级、从单一到综合”的技能培养规律，对每个岗位核心课程进行重构，形成专业群内各专业底层共享、中层独立、顶层互选的专业课程体系，整体课程体系如图所示。



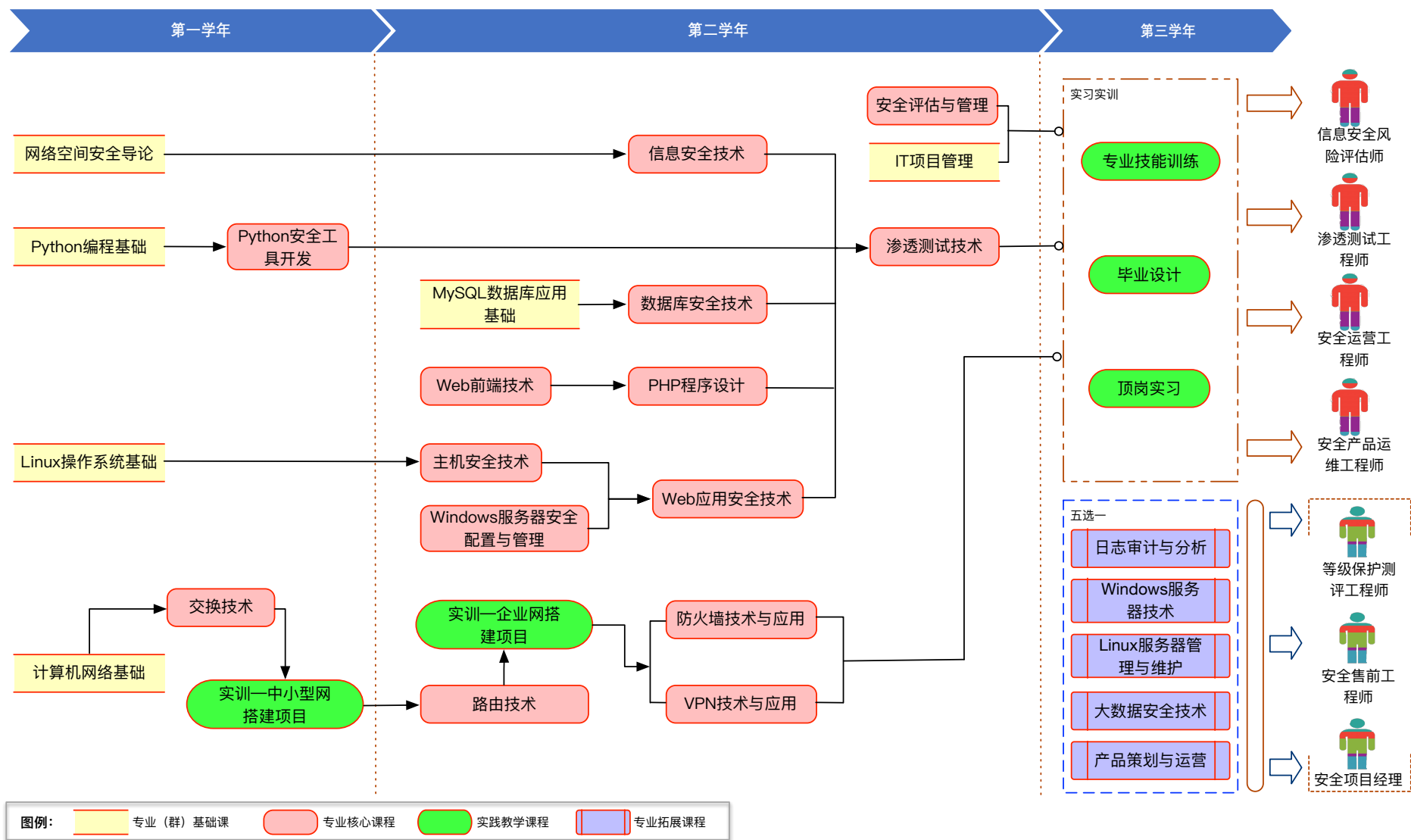


图 2 专业课程学习路径图



### (三) 认证考试与专业课程

序号	课程名称	职业资格证书或技能等级证书
1	主机安全技术	CIPS-PTE 注册信息安全专业人员-渗透测试工程师
2	Windows 服务器安全配置与管理	
3	数据库安全技术	
4	Web 应用安全技术	
5	渗透测试技术	

序号	课程名称	职业资格证书或技能等级证书
1	交换技术	360 企业安全认证工程师
2	路由技术	
3	信息安全技术	
4	主机安全技术	
5	VPN 技术与应用	
6	Web 应用安全技术	
7	渗透测试技术	
8	安全评估与管理	
9	Python 安全工具开发	
10	防火墙技术与应用	

### (四) 专业实训教学

序号	实训项目	总课时	第一学年		第二学年		第三学年		备注
			1	2	3	4	5	6	
1	实训—中小型网搭建项目	24		24					
2	实训—企业网搭建项目	32			32				
3	专业技能训练	80					80		

## 九、教学计划

### 1. 教学进程安排表

课程模块	分类及序号	课程代码	课程名称	考核类型	学分	学时分配			周学时安排 (周平均课时*周数或总课时)						备注	
						合计	理论	实践	第一学年		第二学年		第三学年			
									第一学期 18周	第二学期 16周	第三学期 18周	第四学期 16周	第五学期 18周	第六学期 15周		
公共必修课程	1	001001	军事理论与军事训练		9	148	36	112	8*14 4*9							
	2	001002	思想道德修养与法律基础		3	48	32	16	4*12							
	3	001003	毛泽东思想和中国特色社会主义理论体系概论		4	64	40	24		4*16						
	4	001004	形势与政策		2	32	16	16	8*1	8*1	8*1	8*1				
	5	001005	劳动技能		2	40	0	40		20*1	20*1					
	6	001006	大学体育		9	150	2	148	2*15	2*15	(30)	(30)	(30)			
	7	001007	大学生就业指导		2	40	8	32	2*4	2*4	2*4	2*4	(8)			
	8	001008	大学生心理健康与素养提升		2	40	24	16	2*10	2*10						
	9	001009	数学建模		3	60	30	30	2*15	2*15						
	10	001010	大学英语		7	120	96	24	4*15	4*15						
	11	001011	计算机应用基础		3	48	10	38	4*12							
	12	001012	创新创业基础与实践		2	40	16	24	2*1	2*16	2*1	2*1	2*1	2*1		
	13	001013	诵读与写作		1	30	14	16			2*15					
	14	001014	安全教育		1	20	0	20	4*1	4*1	4*1	4*1	4*1	4*1		
小 计					50	880	324	556	23/406	17/276	6/102	3/52	2/44			
专 业 课 程	专业基础课程	1	042002	计算机网络基础	考试	3	60	52	8	6*10						
		2	042003	Python 编程基础	考试	3	60	20	40	6*10 后						
		3	042001	网络空间安全导论	考查	1	20	20	0	2*10 前						
		4	042006	Linux 操作系统基础	考试	3	48	16	32		6*8 前					
		5	042005	MySQL 数据库应用基础	考试	3	48	16	32			6*8 前				
		6	042004	IT 项目管理	考查	1	20	20	0				2*10			
	专业核心课程	7	042032	交换技术	考试	4	66	22	44		6*11 前					
		8	042067	Python 安全工具开发	考试	3	60	20	40		6*10 后					
		9	042033	实训—中小型网搭建项目	考查	1	24	0	24		8*3 后					
		10	042034	路由技术	考试	4	66	22	44			6*11 前				
		11	042068	Windows 服务器安全配置与管理	考试	4	66	22	44			6*11 前				
		12	042035	实训—企业网搭建项目	考查	2	32	0	32			8*4 后				
		13	042028	信息安全技术	考试	3	60	20	40			6*10 后				
		14	042023	Web 前端技术	考试	3	60	20	40			6*10 后				
		15	042036	主机安全技术	考试	3	60	20	40			6*10 前				

课程模块	分类及序号	课程代码	课程名称	考核类型	学分	学时分配			周学时安排 (周平均课时*周数或总课时)						备注
						合计	理论	实践	第一学年		第二学年		第三学年		
									第一学期 18周	第二学期 16周	第三学期 18周	第四学期 16周	第五学期 18周	第六学期 15周	
	16	042045	VPN 技术与应用	考试	3	48	16	32				6*8 前			
	17	042062	数据库安全技术	考试	3	60	20	40				6*10 后			
	18	042047	PHP 程序设计	考试	3	48	16	32				6*8 前			
	19	042054	Web 应用安全技术	考试	3	60	20	40				6*10 前			
	20	042069	渗透测试技术	考试	3	60	30	30				4*15			
	21	042041	防火墙技术与应用	考试	3	48	16	32				6*8 后			
	22	042070	安全评估与管理	考试	3	48	16	32				6*8 后			
	23	042024	专业技能训练	考查	5	80	0	80					12*6 8*1		
	24	042025	毕业设计(毕业项目综合训练)	考查	5	80	0	80					4*10	(40)	
	25	042026	顶岗实习	考查	25	400	0	400					20*5	20*15	
专业拓展课程	26	042020	日志审计与分析	考试	3	60	20	40					6*10		选择一门
	27	042013	Linux 服务器管理与维护	考试	3	60	20	40					6*10		
	28	042037	Windows 服务器技术	考试	4	66	22	44					6*11		
	29	042018	大数据安全技术	考试	3	48	16	32					6*8		
	30	042031	产品策划与运营	考查	3	48	16	32					6*8		
小 计					100	1742	444	1298	8/140	12/198	22/392	25/392	16/280	23/340	
公共选修课程	1	003001	艺术素养必修课		2	32	32			32					
	2	003002	人文素养必修课		1	20	20			20					
	3	003003	人文素养任选课		2	40	40			20	20				
	4	003004	兴趣体育选修课		1	30		30			30				
	5	003005	信息素养选修课		1	20		20			20				
小 计					7	142	92	50		72	70				
合 计					157	2764	860	1904	30/546	34/546	31/564	16/444	18/324	23/340	

注:①公共必修课程总课时控制在 718—834;专业课程总课时控制在 1666—1836;公共选修课程总课时 142;专业总课时: 2546—2812。

②《数学建模》可根据专业特点和需求调整课程名称,动漫制作技术、环境艺术设计、商务英语、商务日语等专业不开设,理工类、经管类专业开设 60 课时(每学期 30 课时)。

③各专业开设《创新创业基础与实践》,40 课时,《诵读与写作》,不超过 30 课时,由创新创业教育学院、基础课部负责课程建设和组织实施;开设《安全教育》课程(20 课时),由学生工作处组织实施。

④以专业群为单位开设专业拓展课程,群内各专业学生必修选修专业拓展课程模块中的 1-3 门课程,每个专业群的拓展课程在第 3-5 学期开设;群外专业可根据实际情况确定专业拓展课程的开设。

⑤第五学期的课程安排中:《专业技能训练》、《毕业设计(毕业项目综合训练)》总课时不超过 200 课时,教学周数和周课时可根据专业实际情况进行分配,其中《毕业设计(毕业项目综合训练)》不少于 80 课时,《专业技能训练》须排在前九周;顶岗实习的时间由各二级学院根据各专业特点确定,学院不做统一要求。

⑥各专业开设《艺术素养必修课》,以学生至少选修 1 门艺术类尔雅通识课的形式实施,由基础课教研

部统一管理和具体组织实施。

⑦各专业开设《人文素养必修课》，学生在《茶艺与茶文化》、《剪纸》、《书法》、《摄影》等课程中至少选修1门，由基础课教研部统一管理和具体组织实施。（机电工程学院和软件学院、网络空间安全学院执行“[]”内的课时）。

⑧各专业开设《人文素养任选课》（2\*20 课时），可采用尔雅通识课的形式实施或由学校教师主讲，由基础课教研部统一管理和组织实施。

⑨《兴趣体育选修课》（30 课时），由基础课教研部统一管理和组织实施（机电工程学院和软件学院、网络空间安全学院执行“[]”内的课时）。

⑩《信息素养选修课（网络伦理）》（2\*10 课时，由基础课教研部统一管理和组织实施）。软件学院和网络空间安全学院学生必选，软件学院第二学期开设，网络空间安全学院第三学期开设；电子工程学院、机电工程学院和经济管理学院学生任选，电子工程学院和经济管理学院第二学期开设，机电工程学院第三学期开设。

⑪奇、偶学期周数分别为 20 周和 18 周（包括考试及机动周），上表周数为实际上课周数。

⑫考核类型由各课程管理部门明确是考试或考查课程，专业课程模块中每学期考试课程要求至少有 1-3 门。

## 2. 学时分配统计表

统计项目 课程类型	总学分	总学时	理论学时	实践学时	理论学时 比例 (%)	实践学时 比例 (%)
公共必修课程	50	880	324	556	36.8	63.2
专业课程	100	1742	444	1298	25.5	74.5
公共选修课程	7	142	92	50	64.8	35.2
合计	157	2764	860	1904	31.1	68.9

## 十、教师要求

### 1. 专业教学团队要求

校内专任教师由网络与信息安全教研室为主，熟悉信息安全行业发展趋势，能把握专业发展方向、具有一定的团队建设能力。教学理念与方法先进，能有效把握课堂教学过程。同时聘请信息安全企业能工巧匠和技术工程人员担任兼职教师。具体要求如下：

（1）具备本专业本科或研究生以上学历，并接受过职业教育教学方法论的培训，具有独立开发职业课程的能力；

（2）从事实践教学的主讲教师应具备信息安全技术专业相关证书，如信息安全工程师，网络工程师等中级水平及以上资格证书（含高级工程师）或“双师型”教师；从事辅助教学的实训指导教师要具有 1 年以上企业工作经历，熟悉设备操作。

（3）本专业“双师型”教师（讲师以上教师系列职称，并具备中级以上专

业技术职称或职业资格或两年以上企业经历)的比例要达到 90%以上;

## 2. 本专业目前教学团队的基本情况

专任教师: 总共 11 人。其中, 副高职称以上 2 人, 中级职称 8 人; 硕士以上 8 人; 其中: 项目管理师或网络规划设计师 5 人, 信息安全工程师 3 人, 专业带头人 2 人。

兼职教师: 总共 13 人。其中企业专业带头人 2 人, 企业能工巧匠 6 人, IT 培训师 5 名。

## 十一、实践教学条件要求

序号	实验实训室(基地)名称	功能	面积、设备、台套基本配置要求	地点	备注
1	网络系统集成实训室	LINUX 操作系统基础、Windows 服务器安全配置与管理、主机安全技术	60m <sup>2</sup> 、PC 机、50 台、2G 内存	校内	已有
2	网络基础实验实训室	交换技术、路由技术、中小型网搭建项目、企业网搭建项目	60m <sup>2</sup> 、PC 机、50 台、2G 内存	校内	已有
3	Web 安全实验室	PYTHON 编程基础、PYTHON 高级编程、代码审计	60m <sup>2</sup> 、PC 机、50 台、4G 内存	校内	未建
4	信息安全程序实验室	WEB 前端技术、数据库应用基础、PHP 程序设计、企业网站项目	60m <sup>2</sup> 、PC 机、50 台、2G 内存	校内	未建
5	信息安全实验实训室	信息安全技术、渗透测试技术、安全评估与管理、WEB 安全	60m <sup>2</sup> 、信息安全平台、路由器、交换机、PC 机、50 台、4G 内存	校内	未建
6	网络安全实验实训室	交换技术、路由技术、中小型网搭建项目、企业网搭建项目、防火墙技术及应用、VPN 技术及应用、入侵检测技术及就用	60m <sup>2</sup> 、交换机、路由器、防火墙、PC 机、50 台、2G 内存	校内	未建
7	校外实训基地	顶岗实习	按企业运作要求建设	校外	

## 十二、培养方案特色

1. 对接就业岗位需求, 遵循认知规律和技能培养规律构建专业课程体系由“工作岗位->职业能力->课程设计”的思路进行分析, 确定专业岗位群基

基础课程、专业核心课程和专业拓展课程。

2. 课程教学安排由浅入深，与考证相结合

专业课程设计由浅入深、逐层递进，遵循学生的认知规律。结合资格认证考试进行课程体系设计。

3. 安排信息安全项目实战课程，提高学生的学习兴趣和信息安全理念

综合训练课程通过搭建虚拟信息安全实战平台，采取“夺旗赛”方式开展实验教学，提高学生的专业学习兴趣，加强信息安全保护的理念。

4. 任选一门专业拓展课程，提高学生兴趣范围

本专业学生可选取一门本专业领域外的拓展课程，开阔学生在 IT 领域的视野，拓宽职业范围。

**方案执笔人：**肖瑶星、莫裕清

**方案审核人：**孙洪淋 曹文

**管理院部：**网络空间安全学院

**定稿日期：**2019年5月20日