深圳市龙岗区第二职业技术学校

网络信息安全专业人才培养方案

2024 年 6 月

目录

一、 专业名称及代码

网络信息安全专业（710207）

二、 招生对象与学制

（一）招生对象

初级中学毕业，或具有相同学历的其他人员。

（二）学制

基本学制 3 年。

三、 职业面向

本专业职业面向如下表所示：

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（71）	计算机类（7102）	信息安全渗透测试、网络安全运营维护服务业	工程技术人员	计算机网络工程技术人员 网络与信息安全管理员 网络系统运维技术人员 信息安全工程技术人员 信息系统运行维护工程技术人员	信息安全工程师（软考） 1+X 网络安全运维职业技能等级证书（初级） 颁证单位：中科软科技股份有限公司 1+X 企业网络安全防护职业技能等级证书（初级） 颁证单位：上海海盾安全技术培训中心 1+X 网络系统建设与运维职业技能等级证书（初级） 颁证单位：华为技术有限公司

四、 培养目标与规格

4.1 培养目标

本专业培养德智体美劳全面发展，掌握扎实的科学文化基础和信息技术、计算机网络、网络安全等知识，具备中小型网络搭建与防护、系统部署与安全管理、应用服务配置与安全运维、安全产品部署、初级网络信息系统安全测试等能力，具有工匠精神和信息素养，能够

从事网络系统安全运行维护、网络安全产品技术服务、网络系统渗透测试等工作，面向政府与企业等机构客户安全运维与服务岗位群，培养适应信息技术快速发展需要的，能够从事日常巡检、安全监测、安全分析、应急处置、安全评估、安全加固、安全运维、工程项目实施等工作的高素质技术技能人才。

4.2 培养规格

通过三年的学习，本专业的学生应该达到以下几方面的要求：

4.2.1 素质要求

(1) 具备正确的理念信念、家国情怀，以及积极践行社会主义核心价值观的良好思想品德

(2) 具有正确的网络安全观，坚定维护我国网络空间主权和国家安全，保障个人信息安全，维护公民在网络空间的合法权益

(3) 具有遵纪守法意识，自觉遵守与网络信息安全相关职业领域相适应的良好职业道德和法律法规

(4) 具有良好的人际交往、团队协作能力和主动服务意识，具备信息安全、知识产权保护、客户隐私保护、质量规范等专业意识

(5) 具备信息意识、计算思维、数字化学习与创新、网络强国社会责任等方面的信息安全核心素养，善于主动学习网络信息安全最新知识，并能综合运用于网络信息安全相关的业务领域中

4.2.2 知识要求

(1) 掌握本专业所必需的英语、数学、思想政治理论、科学文化基础知识和中华优秀传统文化知识。

(2) 熟悉《网络安全法》等与本专业相关的法律法规以及安全意识等知识。

(3) 掌握基础的计算机组装与维修知识。

(4) 掌握计算机应用的基本知识，掌握计算机网络、信息安全基础理论的基础知识。

(5) 掌握 Windows、Linux 网络操作系统的基本配置，熟悉操作系统安全加固知识。

(6) 掌握企业网综合布线，以及交换机路由器基本配置等知识。

(7) 掌握防火墙、终端安全管理常见等网络安全设备的相关知识。

(8) 掌握基础的网页设计开发的基本知识。

(9) 掌握常见的网络安全攻防的相关知识。

(10) 掌握企业网安全运维的相关知识。

4.2.3 能力要求

(1) 能使用网络设备组建中小型局域网并接入互联网，会根据设备运行状态与故障提示信息进行必要的网络维护

(2) 能对主流网络操作系统、常见服务应用进行配置、管理与维护

(3) 能进行动态网站开发环境的搭建及安全设置

(4) 会对数据库进行安全配置

(5) 能进行基本的操作系统、网络应用及信息内容的安全防护

(6) 能对主流网络安全产品进行安装、调试

(7) 能使用端口探测、漏洞扫描、Web 应用漏洞扫描等工具进行系统扫描与安全检测

(8) 能对常见桌面操作系统、服务器操作系统、数据库进行安全配置与管理

(9) 能利用渗透测试工具对信息系统进行信息收集，漏洞探测、分析、利用与验证

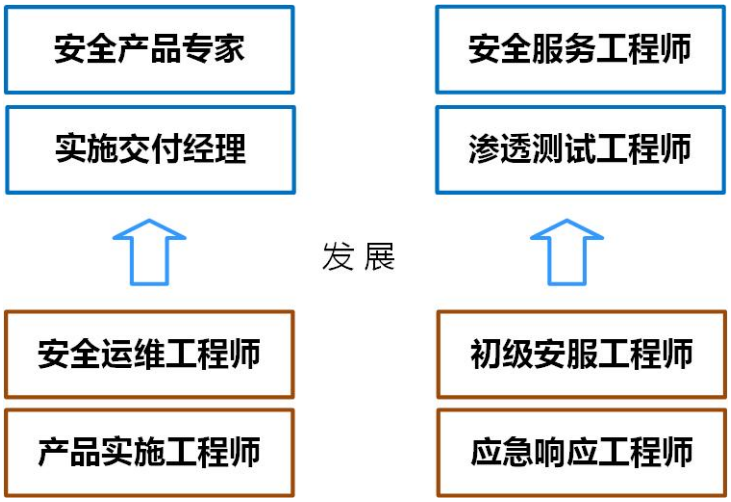
(10) 具有终身学习和可持续发展的能力

五、 专业课程体系

5.1 职业岗位核心能力分析

5.1.1 职业岗位

通过对网络信息安全专业的就业岗位进行分析，我们可以看到本专业的目标岗位、发展岗位之间的关系，如下图所示。



专业岗位发展路线图

5.1.2 典型岗位工作任务

通过对专业岗位的分析，这些岗位的工作任务如下：

序号	岗位名称	工作领域	工作任务
1	产品实施工程师	终端安全产品交付	1. 产品安装部署 2. 产品测试调优 3. 产品故障处理 4. 日志报表的生成及维护
		网关类产品交付	1. 产品安装部署 2. 产品测试调优 3. 产品故障处理
		服务器安全产品交付	1. 产品安装部署 2. 产品测试调优 3. 产品故障处理
2	安全运维工程师	产品运维	1. 日常巡检 2. 安全产品策略调优 3. 产品故障处理 4. 数据备份与还原

		安全监控	1.网络监控类设备监控 2.安全监控规则配置维护 3.网络安全事件应急响应
		安全运维管理	1.资产管理 2.安全态势监控 3.安全事件分析
3	**网络安全应急响应工程师**	应急演练	1. 应急演练方案制定 2. 应急演练实施 3. 应急演练总结
		应急事件分析	1. 第一时间响应客户请求 2. 系统信息收集分析 3. 日志分析 4. 流量分析 5. 威胁情报分析
		应急事件处置	1. 启动应急预案，信息上报 2. 启用备份系统，恢复客户业务系统运行 3. 应急事件排除 4. 撰写事件报告、应急响应总结
4	**初级安全服务工程师**	安全风险评估	1. 资产、制度、措施等安全现状调研 2. 资产价值、威胁因素、脆弱性分析 3. 编写安全风险评估报告
		漏洞扫描与验证	1. 方案制定 2. 漏洞扫描 3. 漏洞检测验证
		安全检查	1. 用户需求分析，形成 checklist 2. 基线检查 3. 检查报告提交
		威胁分析	1. 告警日志分析 2. 网络流量分析 3. 威胁情报读取 4. 编写威胁分析报告

5.1.3 核心能力要求

序号	岗位名称	岗位能力要求
1	**产品实施工程师**	了解计算机网络原理，熟悉 TCP/IP 协议，掌握基础的网络信息配置能力； 熟悉路由交换技术，掌握 vlan、静态路由，动态路由、NAT、ACL 等配置； 掌握 Windows、Linux 操作系统的基础操作，能够使用基础命令进行日志查询和故障信息收集； 了解基础的网络攻防知识，了解常见的网络攻击行为应对和处置方法； 掌握各类网络安全产品的安装，能够根据要求和客户需求将产品部署在不同的网络场景中； 熟悉各类网络安全产品的功能模块，能够根据客户需求进行基本的策略配置、特征库更新； 了解常见的计算机病毒、木马特征，掌握常见病毒木马的处置和查杀方法； 具备日志报表使用能力，能够查询、筛选、导出、备份相关的日志报表； 能够熟练使用 wireshark 等工具进行流量抓取、数据包分析和网络问题定位； 能够对各种网络安全产品常见的网络故障、产品故障进行故障排查，能够抓取系统问题日志；
2	**安全运维工程师**	了解计算机网络原理，熟悉 TCP/IP 协议，掌握基础的网络信息配置能力； 熟悉路由交换技术，掌握 vlan、静态路由，动态路由、NAT、ACL 等配置； 掌握 Windows、Linux 操作系统的基础操作，能够使用基础命令进行日志查询和故障信息收集； 了解基础的网络攻防知识，了解常见的网络攻击行为应对和处置方法； 熟悉各种网络安全产品的功能原理，能够根据要求进行基本的策略配置、特征库更新； 了解常见的计算机病毒、木马特征，掌握常见病毒木马的处置和查杀方法； 具备日志报表使用能力，能够查询、筛选、导出、备份相关的日志报表； 能够熟练使用 wireshark 等工具进行流量抓取、数据包分析和网络问题定位； 具备常见网络安全产品故障的问题排查思路，能够抓取系统问题日志； 能够对产品的告警信息进行初步的分析； 能够对各种网络安全产品进行基础维护和日常巡检，并出具巡检报告；
3	**网络安全应急响应工程师**	了解计算机网络原理，熟悉 TCP/IP 协议，掌握基础的网络应用能力； 掌握常见操作系统的应急排查及安全加固工作； 熟悉各类操作系统及数据库常见的安全漏洞和隐患，熟悉 OWASP top10； 熟悉常见网络安全设备，如防火墙、终端安全系统等的基本操作； 了解网络安全应急响应的工作流程； 能够使用工具导出系统日志，并利用第三方工具进行日志分析可疑事件； 能够利用抓包工具，获取、保存网络流量并进行分析； 掌握常见威胁情报平台的使用方法； 能够对常见网络攻击进行初步分析，如网页篡改、勒索病毒挖矿木马、DDOS 拒绝服务、数据泄露、流量劫持等； 根据需求对业务系统进行定期备份，并能够在发生应急事件后快速恢复业务；

4	**初级安全服务工程师**	了解计算机网络原理，熟悉 TCP/IP 协议，掌握基础的网络应用能力； 掌握 Windows、Linux 操作系统的基础操作； 熟悉各类操作系统及数据库常见的安全漏洞和隐患，熟悉 OWASP top10； 掌握国内外主流安全工具的使用，如：Nessus、Nmap、AWVS、Burp、Appscan 等； 掌握常见威胁情报平台的使用方法,了解流行的 APT 攻击原理和特征； 熟悉病毒和木马的基本分类和特征，能根据分析常见的病毒和木马感染情况；

5.2 人才培养模式与课程体系设计思路

5.2.1 人才培养指导思路

教育是事关国家发展和民族未来的千秋基业。党的十九届五中全会明确了“十四五”时期建设高质量教育体系的战略任务。准确把握“十四五”时期教育改革发展宏观形势，深刻认识我国进入高质量发展阶段的新特征新要求，对谋划建设高质量人才培养体系至关重要。

本方案以十九大报告提出的“完善职业教育和培训体系，深化产教融合、校企合作”理念为指导思想，认真贯彻和落实《关于加强网络安全学科建设和人才培养的意见》、《网络安全法》、《一流网络安全学院建设示范项目管理办法》、《国家职业教育改革实施方案》（职教 20 条）、《2019 年教育信息化和网络安全工作要点》等文件精神，全面贯彻党的教育方针，坚持以服务为宗旨，以就业为导向，以能力为本位，走产学结合的发展道路，大力推进校企合作，创新人才培养模式，突出以学生为本的素质教育、职业技能教育和终身教育理念，以适应新形势发展对高等职业教育人才培养的要求，制定出具有针对性、灵活性和开放性，彰显职业教育特点及学院特色的人才培养方案，为社会主义现代化建设培养具有良好职业道德、较强专业技能和较强社会适应能力的高端技能型网络安全人才。

5.2.2 人才培养体系设计原则

人才培养方案在总体上要遵循职业教育规律和职业成长规律，坚持知识、能力、素质协调发展的原则，优化课程体系，改革教学内容、教学方法和教学手段，注重学生综合素质和职业能力的培养。

1．体现“校企合作”的办学理念

紧跟人才需求市场动态，以社会需求为依据，找准信息安全专业办学定位，明确人才培养规格，参照职业岗位技能要求，行业龙头企业与学校合作共同制定人才培养方案，探索建立“校中企”、“企中校”，引进产业专业人才参与专业课程和教学资源的开发。

2．突出“工学结合”的人才培养模式

贯彻 “工学结合”的人才培养模式，体现“教学与生产相结合，学习与工作相结合”，突出信息安全专业人才培养的特色。

3．构建“能力核心”的职业课程体系

充分调研、明确岗位群能力要求，结合《中等职业学校信息安全与管理专业教学标准》合理构建专业课程体系，重视学生职业能力、方法能力和社会能力的培养，重视学生综合素质的养成。

4．落实 1+X 证书制度

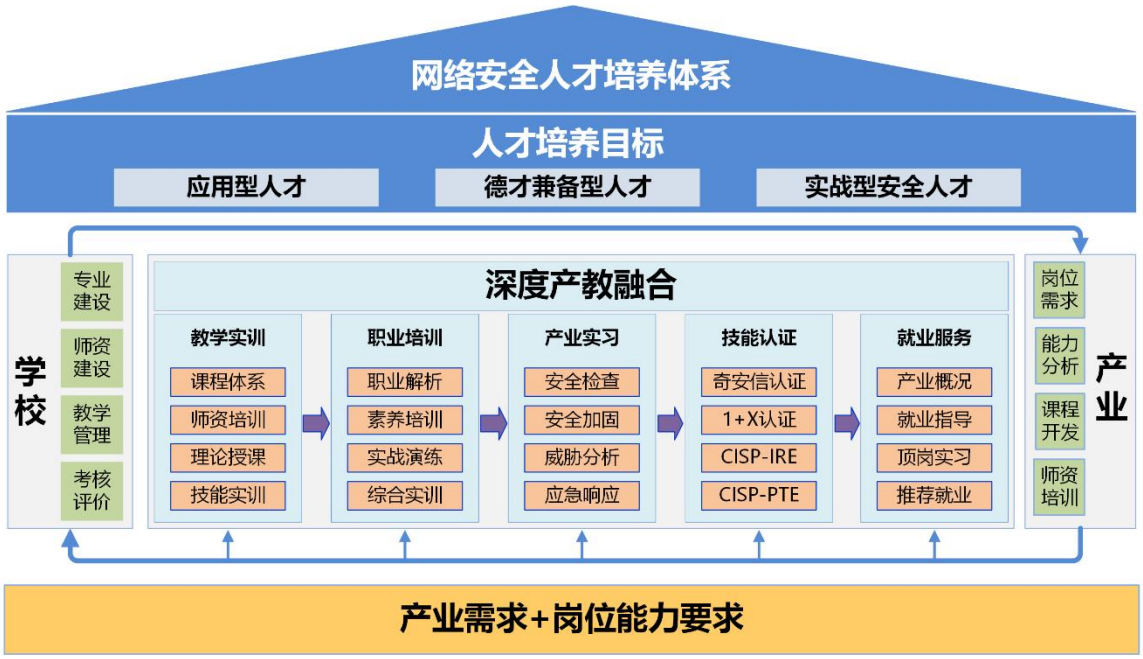
进一步推进职业院校 1+X 证书制度试点工作，促进教育教学改革，将产业用人需求贯彻在对学生的考核中，使得教学更具备针对性。

5．加强“教、学、做”一体的教学模式改革

继续推行任务驱动、项目导向、产教中心等教学做一体的教学模式改革，从教学内容、教学方法和教学手段等方面进行探索和实践，重点培养学生的职业能力、方法能力和社会能力，将素质教育贯穿于教育教学全过程。

5.2.3 人才培养体系框架

人才培养建设以推动安全人才培养与产业合作的发展为目标，我们对于网络安全人才的培养建设思路其整体架构设计如下图所示。



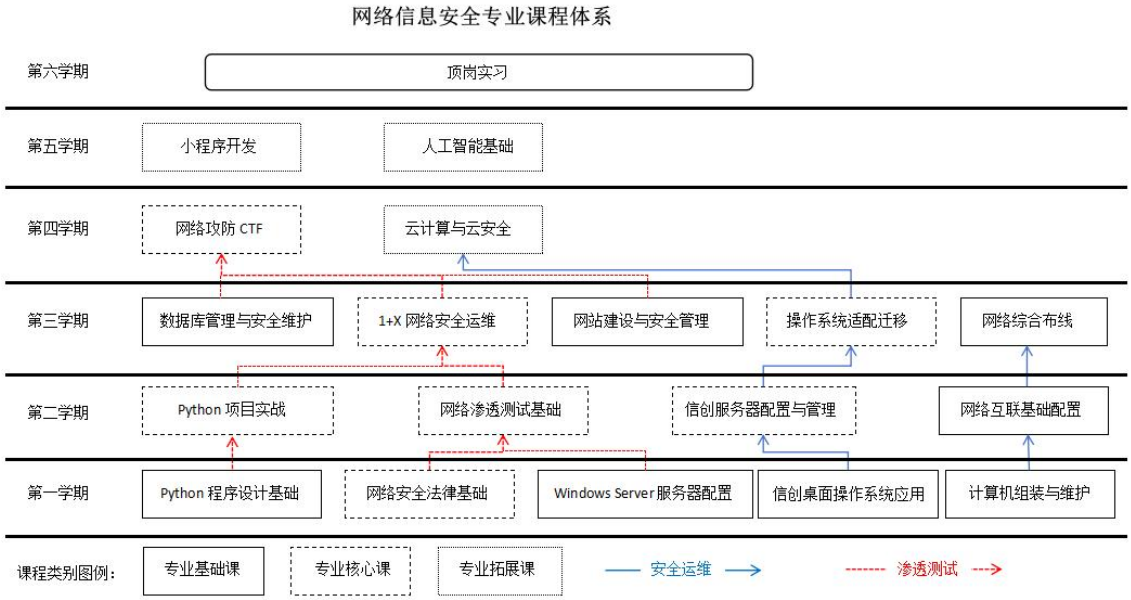
网络安全人才培养闭合体系

信息安全人才培养体系的建立应即具有开放性和兼容性的特点，为信息安全相关专业提供基础课程学习和相关实验实践环境，实施专业学历教育与职业能力培养，建设高级网络安全人才培养课程体系及配套实训环境，完成学历性课程共建，满足学校培养学历教育需求，同时从高校整体利益出发学历教育与产业培训相结合的网络安全人才培养新模式，开展认证培训、师资培训等多种校企服务。

5.2.4 专业课程体系设计

网络信息安全专业的课程体系设计以先进的职业教育理论与实践为指导，调研了行业龙头企业的用人需求和岗位职业能力，制定了采用职业岗位分析法进行课程体系设计，从岗位的工作领域入手，分析职业岗位工作任务，明确职业岗位的核心能力要求；根据核心岗位能力要求构建专业技术课程，并按照“够用、实用”的原则整合与设置专业基础课程，形成链路课程；同时充分考虑学生的可持续发展能力与综合素质培养设置文化课与专业选修课；将分析结果进行系统化设计，构建出岗位针对性强、能力主线清晰、理论与实践融合的课程体系。

在六个学期的人才培养过程中，理论教学与实践教学比例总体上达 1:1。课程体系设计图如下：



5.3 课程体系

5.3.1 课程设置

（一）基础课

根据学校要求开设，具体课程略。

（二）专业基础课

类型	课程名称	学分	学时	授课学期	备注
必修	Python 程序设计基础	4	80	1	
必修	Python 项目实战	4	80	2	
必修	信创桌面操作系统应用	4	80	1	
必修	Windows Server 服务器配置	4	80	1	
必修	信创服务器配置与管理	3	60	2	
必修	网络互联基础配置	4	80	2	
必修	数据库管理与安全维护	4	80	3	
必修	网站建设与安全管理	4	80	3	
必修	网络综合布线	4	80	3	
必修	计算机组装与维护	3	60	1	
必修	操作系统适配迁移	2	40	3	
	小计	39	780		

（三）专业核心课

类型	课程名称	学分	学时	授课学期	备注
必修	网络渗透测试基础	4	80	2	
必修	1+X 网络安全运维	4	80	3	
必修	网络攻防 CTF	4	80	4	
必修	网络安全法律	2	40	1	
	小计	14	280		

（四）专业拓展课

类型	课程名称	学分	学时	授课学期	备注
选修	小程序开发	3	60	5	
选修	云计算与云安全	3	60	4	
选修	人工智能导论	2	40	5	
	小计	8	160		

六、 专业教学规划

6.1 教学进度计划表

课程类别	课程类型	序号	课程名称	课时总数			每学期周课时数						学分
				合计	理论	实操	第一学年		第二学年		第三学年		
							一	二	三	四	五	六	
必修课	公共基础课	1	语文	324	324		2	2	2	6	6		18
		2	数学	360	360		2	2	2	6	8		20
		3	英语	360	360		2	2	2	6	8		20
		4	信息技术	144	72	72	4	4					8
		5	体育与健康	270		270	3	3	3	3	3		15
		6	历史	72	72				2	2			4
		7	思想政治	144	144		2	2	2	2			8
		8	艺术	36	36			2					2
		9											0
		10											0
		11											0
		12											0
			小 计	**1710**	**1368**	**342**	**15**	**17**	**13**	**25**	**25**	**0**	**95**
	专业通用课	13	Python 程序设计基础	80	40	40	4						4
		14	python 项目实战	80	40	40		4					4
		15	信创桌面操作系统应用	80	40	40	4						4
		16	Windows Server 服务器配置	80	40	40	4						4
		17	信创服务器配置与管理	60	30	30		3					3
		18	网络互联基础配置	80	40	40		4					4
		19	数据库管理与安全维护	80	40	40			4				4
		20	网络综合布线	80	40	40			4				4
		21	计算机组装与维护	60	30	30	3						3
		22	网站建设与安全管理	60	30	30			3				3
		23	操作系统适配迁移	40	20	20			2				2
			小 计	**780**	**390**	**390**	**15**	**11**	**13**	**0**	**0**	**0**	**39**
	专业核	24	网络渗透测试基础	80	40	40		4					4
		25	1+X 网络安全运维	80	40	40			4				4
		26	网络攻防 CTF	80	40	40				4			4

	心课	27	网络安全法律基础	40	40		2						2
		28											0
		29											0
		30											0
		31											0
		32											0
			小　　计	**280**	**160**	**120**	**2**	**4**	**4**	**4**	**0**	**0**	**14**
	实践课	33	军训与入学教育				1周						1
		34	岗位认知实习					1周					1
		35	岗位见习							4周			4
		36	顶岗实习									六个月	24
			小　　计	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**30**
限选课	专业方向课	37	小程序开发	60	30	30					3		3
		38	云计算与云安全	60	30	30				3			3
		39	人工智能基础	40	20	20					2		2
		40											0
		41											0
		42											0
		43											0
		44											0
			小　　计	**160**	**80**	**80**	**0**	**0**	**0**	**3**	**5**	**0**	**8**
任选课	拓展课	人文课	职业素养	36	36						2		2
			中国优秀传统文化	36	36				2				2
			自主跑操	90		90	1	1	1	1	1		5
			岗位体验	30		30	1周						0
		专业课											0
													0
			小　　计	**192**	**72**	**120**	**0**	**0**	**2**	**0**	**2**	**0**	**9**
必修课程合计				2770	1918	852	32	32	30	29	25	0	178
限修课程合计				160	80	80	0	0	0	3	5	0	8
任选课程合计				192	72	120	0	0	2	0	2	0	9
技能证书		1	英语等级证										5
		2	计算机等级证										5
		3	专业技能证										5
		4	其他证书（2-5分）										
合　　计				3122	2070	1052	32	32	32	32	32	0	195

七、 毕业要求

在校学习期间，无违纪处分，或有纪律处分，于毕业前按照学校规定撤销处分的；在修业年限内，完成教学计划规定的全部课程及教学实践、实习环节，且成绩合格；在校期间获得与所学专业相关的职业资格证书和计算机等级证书；符合学校学生学籍管理规定中的相关要求。

八、 后续对接专业

中职网络信息安全专业的学生如果后续升学，主要对接专业为：

- 高职专科：信息安全技术应用、密码技术应用、计算机网络技术、区块链技术应用、计算机应用技术
- 高职本科：信息安全与管理、计算机应用工程、网络工程技术
- 普通本科：信息安全、网络空间安全、网络工程、计算机科学与技术