

网络信息安全专业
信息安全技术应用专业
“3+2”中高职衔接人才培养方案

***学校

***学院

二〇二二年十一月

目 录

目 录.....	1
一、专业名称.....	3
二、招生对象.....	3
三、学制.....	3
四、职业面向.....	3
五、培养目标与培养规格.....	4
(二) 培养规格.....	4
1. 素质目标.....	4
2. 知识目标.....	4
3. 能力目标.....	5
六、典型职业活动核心技能分析.....	6
七、职业资格证书.....	10
八、毕业生规格职业能力要求.....	11
九、专业课程体系设置.....	12
(一) 课程结构.....	12
(二) 课程体系结构设计.....	12
十、课程说明及学时分配.....	13
十一、教学进程总体安排.....	21
十二、课时分配表.....	23
十三、实施保障.....	23
(一) 师资队伍.....	23
(二) 教学设施.....	24
1. 教室.....	24
2. 校外实训基地.....	24
3. 校内实训基地.....	25
(三) 教学资源.....	26
(四) 教学方法.....	27

(五) 考核评价	28
(六) 质量管理	28
1. 教学要求:	28
2. 教学管理	29
九、毕业要求	29
十四、其他说明	30
1. 军训	30
2. 入学教育	30
3. 社会实践	30
4. 解释	30

一、专业名称

高职专业名称：信息安全技术应用。

专业代码：510207

中职专业名称：网络信息安全。

专业代码：710207

二、招生对象

初中毕业生或同等学历者。

三、学制

全日制五年（中职阶段3年，高职阶段2年）。

四、职业面向

中职面向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岗位，如表1所示。

表1 中职职业面向

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（71）	计算机类（7102）	互联网及相关服务（64） 软件和信息技术服务业（65）	计算机硬件工程技术人员（2-02-10-02） 计算机软件工程技术人员（2-02-10-03） 计算机网络工程技术人员（2-02-10-04）	产品实施工程师 安全运维工程师 应急响应工程师 网络安全服务工程师	全国计算机等级考试一级（必考） 1+X 网络安全运维（初级）

高职职业面向网络安全运维、渗透测试、web 安全、等保测试等岗位，如表2所示。

表2 高职职业面向

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	计算机类 5102	互联网及相关服务 (64) 软件和信息服务 (65)	计算机硬件工程技术人员 (2-02-10-02) 计算机工程技术人员 (2-02-10-03) 计算机网络工程技术人员 (2-02-10-04)	渗透测试工程师 Web 安全工程师 逆向分析工程师 等保测评工程师	网络安全工程师 (CISO) (必考) 计算机网络管理员(三级) (选考) 1+X 网络安全运维(中级选考)
---------	-----------	-------------------------------	--	--	--

五、培养目标与培养规格

本专业培养拥护党的基本路线，德、智、体、美等方面全面发展的技术应用型人才，具有良好的政治素质、职业道德、敬业精神、守法意识，具备良好的文化素质。培养面向网络信息安全技术服务类岗位群，可以就职于各类互联网企业、事业单位、国家机关、电商与银行等与网络信息安全相关的技术岗位，承担企业网络信息安全服务工作。

根据企业用人需求，中职阶段培养能够从事网络管理与运维、售后技术支持等工作的初、中级技能型人才。高职阶段培养掌握网络信息安全、网络攻击与防御、渗透测试与安全加固技术，具备网络安全设计、网络硬件组网与调试、信息网络安全监察、黑客入侵与防御、网络安全运维能力的高端、优质、特色的技能人才。

(二) 培养规格

本专业毕业生应在素质、知识和能力等方面达到以下要求：

1. 素质目标

(1) 坚定拥护中国共产党领导和我国社会主义制度，在习近平新时代中国特色社会主义思想指引下，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。

(2) 具有崇尚宪法、遵法守纪、崇德向善、诚实守信、尊重生命、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。

(3) 具有质量意识、环保意识、安全意识、信息素养、工匠精神和创新思维。

(4) 具有勇于奋斗、乐观向上，具有自我管理能力、职业生涯规划意识，有较强的集体意识和团队合作精神。

(5) 具有健康的体魄、心理和健全的人格，掌握基本运动知识和运动技能，养成良好的健身与卫生习惯，以及良好的行为习惯。

(6) 具有一定的审美和人文素养，能够形成1-2项艺术特长或爱好。

(7) 具有树立正确的劳动观点和劳动态度，养成劳动习惯，热爱劳动和劳动人民。

2. 知识目标

- (1) 掌握中职生必备的思想政治理论、科学文化基础知识和中华优秀传统文化知识。
- (2) 掌握与本专业相关的法律法规以及网络信息安全的规章制度、规范和实施。
- (3) 掌握本专业所必需的网络基本知识。
- (4) 掌握虚拟化技术的基本知识。
- (5) 掌握网络常用工具软件的使用方法。
- (6) 掌握Windows和Linux网络操作系统的配置与管理相关知识
- (7) 掌握本专业所必需网络安全配置与测试相关知识。
- (8) 掌握网络安全配置与管理相关知识。
- (9) 掌握网络安全攻击与防御的相关知识。
- (10) 掌握Web安全的相关技术。
- (11) 掌握数据库的配置与管理相关知识。
- (12) 掌握网络安全脚本编程技术。
- (13) 掌握网页开发的相关知识。
- (14) 掌握APP开发及安全相关知识。
- (15) 掌握云存储的规划和部署，数据备份与恢复的方法。
- (16) 掌握高级路由器技术、无线网络安全。

3. 能力目标

- (1) 具备局域网组建的建设能力。
- (2) 具备网络操作系统的管理与配置及安全设置能力。
- (3) 具备网络安全配置与测试能力。
- (4) 具备广域网的配置及监管能力。
- (5) 具有Web技术安全技术的能力。
- (6) 具备系统渗透测试的能力。
- (7) 具备网络攻防的能力。
- (8) 具备熟练使用网络常用工具的能力。
- (9) 具备网页设计及配置能力。
- (10) 具备数据库管理与配置的能力。
- (11) 具备网络安全脚本编程的能力。
- (12) 具备虚拟化技术与云计算配置与管理能力。
- (13) 具备云数据中心维护和安全管理的的能力。
- (14) 具备信息安全测评与风险评估的能力。
- (15) 具备恶意代码分析的能力。
- (16) 具备病毒和木马分析、网络安全产品配置与管理能力。

六、典型职业活动核心技能分析

网络信息安全行业的典型职业岗位有：渗透测试、Web 安全加固、逆向分析、网络安全运维、等保测评以及售后技术支持，各岗位所需具备的核心技能描述如下表所示：

表 3：专业面向岗位与岗位职业能力

岗位名称	岗位描述	岗位能力要求	匹配层次
产品实施工程师	1. 终端安全产品交付 2. 网关类产品交付 3. 服务器安全产品交付	<p>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；</p> <p>熟悉路由交换技术，掌握 vlan、静态路由，动态路由、NAT、ACL 等配置；</p> <p>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；</p> <p>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；</p> <p>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；</p> <p>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；</p> <p>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；</p> <p>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；</p> <p>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；</p> <p>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；</p>	中职
安全运维工程师	安全运维工程师主要参与企事业单位网络环境的部署，软硬件设备的安装、配置、升级、运行维护与管理，服务器及安全系统等运行监控与管理，并撰写安全运维技术文档，统计整理运维数据，以满足网络系统安全稳定运行的需要。	<p>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；</p> <p>熟悉路由交换技术，掌握 vlan、静态路由，动态路由、NAT、ACL 等配置；</p> <p>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；</p> <p>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；</p> <p>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；</p>	中职

		<p>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；</p> <p>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；</p> <p>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；</p> <p>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；</p> <p>能够对产品的告警信息进行初步的分析；</p> <p>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；</p>	
应急响应工程师	<ol style="list-style-type: none"> 1. 应急演练 2. 应急事件分析 3. 应急事件处置 	<p>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；</p> <p>掌握常见操作系统的应急排查及安全加固工作；</p> <p>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；</p> <p>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；</p> <p>了解网络安全运维的工作流程；</p> <p>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；</p> <p>能够利用抓包工具，获取、保存网络流量并进行分析；</p> <p>掌握常见威胁情报平台的使用方法；</p> <p>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；</p> <p>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；</p>	中职
网络安全服务工程师	<ol style="list-style-type: none"> 1. 安全风险评估 2. 漏洞扫描与验证 3. 安全检查 4. 威胁分析 	<p>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；</p> <p>掌握 Windows、Linux 操作系统的基础操作；</p> <p>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；</p> <p>掌握国内外主流安全工具的使用，如：Nessus、Nmap、AWVS、Burp、Appscan 等；</p> <p>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；</p> <p>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；</p>	中职
售后	售后技术支持能深刻	1. 熟悉网络体系结构、TCP/IP 协议、路	中职

技术支持	<p>理解公司网络信息安全产品的业务功能，深入了解客户信安服务需求；能完成技术答疑、客户培训、测试环境搭建等工作内容。在完成产品的交付后，需要对客户进行测试、安装、维护、排故、使用等方面的培训，并能进行网络与信息安全方面的巡检，填写巡检报告。</p>	<p>由、交换技术，具有扎实的信息安全理论知识；</p> <ol style="list-style-type: none"> 对主流的网络攻防技术有一定的了解； 具有 Windows、Linux 系统知识，能够熟练操作 Linux、Windows 操作系统及系统指令； 熟悉数据库 mysql 的基础知识； 熟练掌握各类安全产品的工作原理，能够进行安装、配置与调试； 具有较强的 office 文档能力。 	
渗透测试工程师	<p>渗透测试工程师是从事网络与信息系统安全测试的一种职位，其工作目标是帮助网络与信息系统所有者发现其缺陷及潜在风险，进而能够有针对性地提高网络与信息系统安全防御能力。其主要工作内容及职责是利用各种手段对某个特定网络与信息系统进行测试，以期发现和挖掘系统中存在的漏洞，然后输出渗透测试报告，并提交给网络与信息系统所有者。</p>	<ol style="list-style-type: none"> 具有 Windows、Linux 等操作系统知识，熟悉操作系统的常用 DOS 及 shell 命令； 掌握网络基础知识，熟悉网络协议分析技术； 熟悉 IIS、Apache、Tomcat、nginx 等典型中间件； 熟悉数据库 mysql、sqlserver 的基础知识； 掌握 Python 脚本语言； 了解安全防护产品工作原理，如：防火墙、IDS、IPS 等； 掌握信息安全渗透测试的基本知识，工作流程以及渗透测试类方法及工具使用； 熟悉常见的 CMS 漏洞及利用方法； 熟悉信息安全法律法规。 	高职
Web 安全工程师	<p>Web 安全工程师是信息安全领域的一个职位，其工作目标是对公司网站、信息系统进行安全评估测试及安全加固；对公司网络与信息安全事件进行响应；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。</p>	<ol style="list-style-type: none"> 具有 Windows、Linux 等操作系统知识，熟悉操作系统的常用命令； 掌握网络基础知识，熟悉网络协议分析技术； 熟悉 Web 应用； 熟悉数据库的基础知识； 掌握 Python 脚本语言； 了解安全防护产品工作原理，如：防火墙、IDS、IPS 等； 熟悉常用渗透测试工具，掌握安全加固技术； 对安全事件能够及时响应并处理； 	高职

		<p>9. 掌握常见的安全漏洞，实现漏洞复现；</p> <p>10. 掌握发现及修复安全漏洞的技术和方法；</p> <p>11. 熟悉信息安全法律法规；</p> <p>12. 长期关注业界安全动态。对安全事件比较敏感。</p>	
逆向分析工程师	<p>逆向分析是一种对软件技术开发的再现过程，通过对目标软件（包括恶意代码、病毒、木马）进行逆向分析及研究，了解软件的技术实现原理，发现软件的安全问题，加强自身软件安全，保障软件运行环境安全。</p> <p>逆向分析工程师是信息安全领域的一个重要职位，需要熟悉逆向分析领域的专业知识和工作流程，熟练使用逆向分析工具和相关开发语言，通过对软件代码的反汇编、静态分析、动态调试等手段，协助企业完成技术技能学习，维护企业软件安全。</p>	<p>Windows 软件逆向方向</p> <p>1. 熟悉汇编语言、C++语言；</p> <p>2. 熟悉 PE 文件格式及其加载机制；</p> <p>3. 熟练使用常用加壳、查壳、脱壳工具，ASPACK、VMProtect、PEID、ImportREC 等；</p> <p>4. 熟悉病毒、木马、恶意软件的工作原理及行为分析，了解常用加解密算法；</p> <p>5. 熟练使用常用逆向分析工具，IDA、OD、WinDbg 等。</p> <p>APP 逆向方向</p> <p>1. 熟悉 Java 语言；</p> <p>2. 熟悉 Smali 汇编器语法，ARM 指令集，熟练使用 IDA pro、abb、ddms 等调试工具；</p> <p>3. 熟悉 APK 文件格式及其加载机制、Dalvik 虚拟机运行原理、Dex 字节码格式、结构与 Dex 加载流程，了解 Dex 逆向原理；</p> <p>4. 熟练使用 APK 反编译工具，Apktool, Apkiller 等。</p>	高职
等保测评工程师	<p>等保测评工程师应能协助公司销售人员完成信息安全等级保护、信息安全咨询、信息安全风险评估等项目的技术支持工作；能根据客户需求设计解决方案，按照文档规范整理编写技术支持文档，为相关人员提供等级保护、信息安全风险评估介绍和培训等；负责等保测评项目、信息安全风险评估项目的实施工作。</p>	<p>1. 熟悉主流网络设备、安全设备、操作系统、数据库的安装与调试；</p> <p>2. 熟悉市场上软硬件安全产品，如网关类、检测类、审计类、管理类等；</p> <p>3. 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；</p> <p>4. 熟悉国内外网络安全发展现状；</p> <p>5. 了解各类网络、安全产品、各主流厂家产品的技术优劣势；</p> <p>6. 熟悉信息安全等级保护、ISO 信息安全体系、ITIL 等相关标准、法律法规；</p> <p>7. 熟悉风险评估的内容、流程及方法；能够根据差距分析报告执行加固方法；</p>	高职

		8. 熟悉信息安全等级保护测评工作流程、工作内容及工作方法； 9. 具备编写等级保护中差距分析报告、建设方案、项目验收报告的能力。	
--	--	--	--

表 4：典型岗位工作任务及其工作过程

典型工作任务	工作过程
渗透测试	(一) 渗透测试需求分析 (二) 执行渗透测试 1. 信息收集 (踩点) 2. 漏洞扫描 3. 漏洞测试 4. 漏洞利用 5. 上传漏洞 6. 权限提升 7. 远程控制 8. 后门植入 9. 痕迹清理 (扫地) (三) 编写渗透测试报告 (四) 编写安全建议方案
Web 安全加固	(一) 分析渗透测试报告 (二) 编写 web 安全漏洞加固方案 (三) 执行 web 安全加固 (四) 漏洞复测
逆向分析	(一) 接收任务并进行任务分析 (二) 执行软件逆向分析 1. PE 分析 2. PE 加载 3. OEP 查找 4. Dump 抓取 5. 输入表重建 6. 源码分析 7. APK 反编译 8. APK 代码重构 9. APK 重新编译 10. APK 二次打包 11. APK 反破解 (三) 编写逆向分析报告
等级保护	(一) 定级 (二) 备案 (三) 整改 (四) 测评 (五) 整改
网络安全运维与管理	(一) 执行安全巡检 (二) 排查可疑事件 (三) 撰写安全巡检报告 (四) 处理安全事件 (五) 提交巡检报告

七、职业资格证书

根据专业所对应的职业岗位，学生完成规定课程考试合格后，本专业学生在毕业前可考取如下职业资格证书：

表 5：职业资格证书一览表

序号	职业资格证书名称	发证机构	取证要求	取证阶段
1	全国计算机等级考试一级	教育部考试中心	必考	中职
2	1+X 网络安全运维（初级）	教育部	选考	中职
3	计算机网络管理员（三级）	人力资源与社会保障部	选考	高职
4	网络设备调试员（三级）	人力资源与社会保障部	选考	高职
5	网络安全工程师（CISO）	国家信息化安全技术资格 认证管理中心	必选	高职
6	1+X 网络安全运维（中级）	教育部	选考	高职

八、毕业生规格职业能力要求

表 6：岗位能力与素养总要求

	能力素质项目	能力素质要素
基本 素质	抽象思维、逻辑推理能力	能利用所学知识分析问题和解决问题
	分析问题解决问题的能力	通过训练学会学习、学会做事的方法
	英语写作会话	能进行简单的英语听、说、读、写。（具备信息安全专业领域文章阅读的能力）
	体育素养	了解身体健康的重要性，并学会科学的体育锻炼，进行强身健体、缓解疲劳和压力
	热爱本职，尽职尽责	具有良好的职业道德，遵纪守法，文明礼貌，有事业心
	信息安全素养	了解基本的信息安全法律法规，培养信息安全的思维意识，掌握个人和企业员工的常见信息安全问题防护方法，熟悉网络安全运维工程师、渗透测试工程师、Web 安全工程师、逆向分析工程师的岗位职责、工作内容与工作过程
	职业沟通的能力	了解职业沟通的重要意义和基本方法，掌握有效沟通的技巧
	创新思维与创业意识	激发创新意识、增强创新欲望、训练创新思维、掌握创新方法、培养创新精神、提升创新能力
	信息处理能力	能熟练使用常用办公软件及工具解决相关信息处理问题
	健康人格	能进行自我认识、自我实现、自我成长、自我完善，树立健康的人格和积极向上的心态
信息 安全 基础	信息安全技术应用能力	了解信息安全技术的应用场景，体验技术方法、常用工具及岗位操作过程，学习和掌握从事信息安全工作所必备的基础知识
	数据库查询、管理、维护的能力	掌握常用 SQL 语句的使用、熟悉 SQL Server、MySQL 数据库及其应用，掌握数据库的安全配置与加固技能
	网络连接与传输协议	计算机网络通信的基本原理、网络体系结构、组建局域网技术、Internet 及其应用、计算机网络安全和常用网络操作系统。

能力	使用常用语言编程的能力	掌握 Android、C/C++、Python 编程基础
	网站建设能力	掌握 PHP 开发语言基础
信息安全核心技术能力	常用操作系统安装与配置的能力	熟悉 Windows 及 Linux 操作系统, 具备 Windows、Linux 系统的安全加固能力
	网络设备配置与管理的能力	掌握网络安全设备的配置与管理, 如防火墙、IDS、VPN、安全网关、UTM、安全管理系统、无线安全设备、安全隔离网闸等
	病毒与木马分析的能力	具备病毒、木马行为分析和源码分析能力
	信息安全技术的应用能力	熟悉物联网和工控应用安全, 具备物联网安全和工控安全防护技能
	信息安全等级保护实施的能力	熟悉信息安全等级保护的概念、工作内容及流程
	渗透测试全工作过程的执行能力	熟练掌握渗透测试工程师的岗位职责、工作内容和流程, 掌握渗透测试的工具和技巧
	WEB 安全加固全工作过程的执行能力	熟练掌握 WEB 安全工程师的岗位职责、工作内容和流程, 掌握 web 安全加固的方法和技巧
软件逆向分析全工作过程的执行能力	掌握软件逆向分析工程师所需的岗位职业能力, 熟悉逆向分析的工作内容和流程, 掌握逆向分析的方法和技巧以及源码分析等内容	

九、专业课程体系设置

(一) 课程结构

本专业课程设置分为公共基础课和专业技能课。

公共基础课包括思想政治、语文、数学、英语、信息技术、历史、体育与健康、艺术、等公共必修课, 以及其他自然科学和人文科学类公共选修课。

专业技能课包括专业基础课、专业核心课和专业拓展课。

(二) 课程体系结构设计

课程体系是育人活动的总体方案, 是培养目标的具体化与依托。本专业紧紧围绕培养目标开展校企合作, 针对就业岗位群, 分析岗位工作内容, 并将其转化成知识能力, 制定课程标准, 合理组建课程结构, 以工作过程和岗位职业能力要求为导向, 构建了“公共基础课+专业基础课+专业核心课程+专业拓展课程+顶岗实习课程”的课程体系, 如图 1 所示。

图 2 课程体系

“3+2”中高职衔接信息安全专业培养的是网络信息安全相关的技术岗位，承担企业网络信息安全服务工作。根据企业用人需求，采取分阶段培养人才的方式，制定分层次的人才培养方案，培养能够从事网络安全管理与运维、渗透测试、WEB 安全服务、逆向分析、等保测评及售后技术支持工作的初、中、高级技术技能型人才。

本专业的基础知识及专业能力涉及多个领域，专业课中高职衔接课程体系在保证各专业技能教学安排合理的基础上，根据学生目标工作岗位的典型职业活动，以工作过程为导向，以综合职业能力为核心，与职业资格标准相融合完成构建。通过专业基础课程和专业核心课程的有机融合实现学生专业知识和技能的合理贯通和提升。

整个课程体系大致将学生的学习活动划分为三个阶段：

1、专业基础知识体系构建阶段（1—4 学期）

本阶段学生主要学习公共基础课程及与网络与信息安全相关的专业基础知识课程，帮助学生构建对信息安全基础、计算机网络、服务器配置与管理、网站开发知识体系框架，奠定学生学习专业知识的理论基础与单项技能基础。

2、专业基础技术技能培养阶段（5—7 学期）

本阶段学生主要学习服务器安全管理能力、网络攻防基础能力、web 安全基础防护能力、网络等级保护能力、能力帮助学生完成从中职向高职的过渡。

3、专业技能及能力综合提升阶段（8—10 学期）

本阶段学生主要学习网络安全配置与测试、漏洞扫描、Android 开发、渗透测试、协议分析、逆向分析、病毒与木马分析、网络安全等级保护等方面的工作技能及相关理论知识，同时要求学生完成企业实际项目的综合实践工作和相关岗位顶岗实习，要求学生具备企业信息中心漏洞扫描、web 应用防护、等保测评、病毒分析等相关岗位的工作能力。通过生产性实训和顶岗实习，培养学生的综合职业能力，提高学生就业竞争力。

十、课程说明及学时分配

（一）公共基础课（1878 学时）

序号	课程名称	主要内容和要求	学时
1	思想政治	本课程讲授马克思主义基本原理、马克思主义中国化理论成果，用习近平新时代中国特色社会主义思想铸魂育人，对学生进行思想教育、政治教育、道德教育、法治教育、心理健康教育、职业生涯和职业精神教育，引导学生通过自主思考、合作探讨的学习过程，理解新时代中国特色社会主义经济建设、政治建设、文化建设、社会建设、生态文明建设的内容和要求，培育政治认同、职业精神、法治意识、健全人格、公共参与等核心素养，树立共产主义远大理想和中国特色社会主义共同理想，坚定中国特色社会主义道路自信、理论自信、制度自信、文化自信，自觉培育和践行社会主义核心价值观，为学生成为担当民族复兴大任的时代新人、成	216

序号	课程名称	主要内容和要求	学时
		为德智体美劳全面发展的社会主义建设者和接班人奠定正确的世界观、人生观和价值观基础。	
2	语文	本课程学生通过阅读与欣赏、表达与交流及语文综合实践等活动,在语言理解与运用、思维发展与提升、审美发现与鉴赏、文化传承与参与几个方面都获得持续发展,自觉弘扬社会主义核心价值观,坚定文化自信,树立正确的人生理想,涵养职业精神,为适应个人终身发展和社会发展需要提供支撑。	288
3	数学	本课程在数学知识学习和数学能力培养的过程中,使学生逐步提高数学运算、直观想象、逻辑推理、数学抽象、数据分析和数学建模等数学学科核心素养,初步学会用数学眼光观察世界、用数学思维分析世界、用数学语言表达世界。	252
4	英语	本课程帮助学生进一步学习语言基础知识,提高听、说、读、写等语言技能,发展中等职业学校英语学科核心.素养;引导学生在真实情境中开展语言实践活动,认识文化的多样性,形成开放包容的态度,发展健康的审美情趣;理解思维差异,增强国际理解,坚定文化自信;帮助学生树立正确的世界观、人生观和价值观,自觉践行社会主义核心价值观,成为德智体美劳全面发展的高素质劳动者和技术技能人才。	252
5	信息技术	本课程帮助学生认识信息技术对当今人类生产、生活的重要作用,理解信息技术、信息社会等概念和信息社会特征与规范,掌握信息技术设备与系统操作、网络应用、图文编辑、数据处理、程序设计、数字媒体技术应用、信息安全和人工智能等相关知识与技能,综合应用信息技术解决生产、生活和学习情境中各种问题;在数字化学习与创新过程中培养独立思考和主动探究能力,不断强化认知、合作、创新能力,为职业能力的提升奠定基础。	144
6	历史	本课程以唯物史观为指导,促进中等职业学校学生进一步了解人类社会形态从低级到高级发展的基本脉络、基本规律和优秀文化成果;从历史的角度了解和思考人与人、人与社会、人与自然的关系,增强历史使命感和社会责任感;进一步弘扬以爱国主义为核心的民族精神和以改革创新为核心的时代精神,培育和践行社会主义核心价值观;树立正确的历史观、民族观、国家观和文化观;塑造健全的人格,养成职业精神,培养德智体美劳全面发展的社会主义建设者和接班人。	72
7	艺术	本课程积极引导学生主动参与艺术学习和实践,进一步积累和掌握艺术基础知识、基本技能和方法,培养学生感受美、鉴赏美、表现美、创造美的能力,帮助学生塑造美好心灵,健全健康人格,厚植民族情感,增进文化认同,坚定文化自信,成为德智体美劳全面发展的高素质劳动者和技术技能人才。	72
8	体育与健康	本课程是以身体练习为主要手段,以体育与健康的知识、技能和方法的传授为主要内容,以培养中等职业学校学生的体育与健康学科核心素养和促进学生身心健康发展为目标的	324

序号	课程名称	主要内容和要求	学时
		综合性课程。对于建设健康中国和人力资源强国, 实现中华民族伟大复兴的中国梦具有重要意义。	
9	读本	本课程教学内容包括了经典故事、爱国故事、抗战故事和中国发展故事, 使学生认识中国历史中经典的事迹, 引导学生珍惜现在的来之不易的生活, 系好人生第一粒扣, 传承红色基因。	18
10	国防教育	本课程是以马列主义、毛泽东思想、邓小平理论和“三个代表”重要思想、习近平关于国防建设思想为指导, 贯彻和落实新发展理念, 按照教育要面向现代化、面向世界、面向未来的要求, 适应我国人才培养战略目标和加强国防后备力量建设的需要, 为培养高素质的社会主义事业的建设者和保卫者服务。	18
11	劳动教育	本课程教学内容: 包括劳动岗位的劳动内容和安全, 劳动工具、劳保护品, 团队精神的实质内容, 劳动态度、工作责任心等内容。基本要求: 提高学生的综合素质, 树立学生的劳动观念, 培养学生的劳动技能和文明行为的养成, 增强学生的团结协作、自我管理和自我服务意识, 保持艰苦奋斗、吃苦耐劳的优良传统, 引导和帮助学生树立正确的人生观、价值观和世界观。	36
12	思想道德修养与法律基础	《思想道德修养与法律基础》课程是高职大学生的必修课程, 是高等职业院校进行素质教育的核心课程。是对大学生系统地进行思想政治教育的主渠道和主阵地。思想政治理论课教学承担着培养学生做人的基本素质(如理想信念、创新精神、敬业精神、人格品质和心理素质等)的任务, 在课程体系结构中起主导作用, 而本课程又是思想政治理论课的核心课程。《思想道德修养与法律基础》课程是学院各专业的公共基础课, 为此, 本课程从培养面向生产、经营、管理一线高素质技能型人才的具体要求出发, 配合专业教育, 着重解决培养高职学生良好的职业素质问题, 通过本课程的教学改革与建设, 使学生具有明确的职业理想、良好的职业道德、科学的职业价值观和较完善的职业纪律素质, 为高职各专业人才培养目标的实现以及 高职学生成长成才和终生发展打下坚实的基础。	60
13	毛泽东思想和中国特色社会主义特色概论	课程以中国化的马克思主义为主题, 以马克思主义中国化为主线, 以中国特色社会主义建设为重点, 从理论与实践、历史与逻辑的统一上揭示马克思主义中国化的理论轨迹, 准确阐述中国共产党在把马克思主义基本原理与中国实际相结合的历史进程中, 创造了中国化的马克思主义, 形成了毛泽东思想和中国特色社会主义理论体系两次飞跃成果, 党的十八大以来又在它们的基础上不断的创新和探索新的理论。课程充分展示了毛泽东思想、邓小平理论、“三个代表”重要思想和科学发展观在中国革命、建设、改革和实现中华民族伟大复兴中的重要历史地位和作用。在教学中采用“以社会发	60

序号	课程名称	主要内容和要求	学时
		展实践和学生实践为载体,进行理论学习、理论应用、理论创新”的全新教学模式。采用“学生参与,师生联动”的方式,遵循分析形势讲理论,结合理论说形势的原则,针对学生及知识模块的特点,选用相应的教学方法,进行教学过程的安排。遵循“以工作过程为导向”的现代职业教育理念,依据职业院校人才培养目标和学生特点,总体把握教材内容,确立教学模块,创设教学情境,制定工作任务。	
14	职业礼仪	本课程旨在丰富学生的知识结构,提高学生的礼仪素质。具体来说:通过课程学习,培养学员的礼的意识,加强自身的礼仪修养,提高实际的与人交际及办事能力。如:了解和理解礼仪的基本问题;礼仪学习的意义;礼仪的规范等。在方法能力方面:了解和掌握人与人沟通的过程、手段、方法和技巧,从而打造自身良好的个人形象。在社会能力方面:使学生通过学习,通过实践,提高自身的认识,树立良好的形象。通过教师的系统讲授、示范操作与训练,使学生掌握礼仪的基本概念、常识、基本原理及方法技巧,为今后塑造良好形象,奠定坚实的基础。	36
15	职业沟通	了解职场沟通的基本技能,能够熟练掌握各种沟通方式在上行沟通、平行沟通和下行沟通的中具体运用,培养学生良好的职业心态、明确自身的为学生为将来事业的良好发展,掌握更多的企业管理技能奠定基础。	30

(二) 专业基础课 (900 学时)

序号	课程名称	主要内容和要求	学时
1	网络技术基础	本课程的主要任务是使学生学会网络基础知识,掌握网络基本操作技能。为更好地学习网络工程、网络管理与应用、网站建设与维护三个专业化方向的核心课程 打好基础。主要包括:计算机网络基础知识;计算机网络体系结构与协议基础知识;OSI 和 TCP/IP 参考模型;局域网基础;网络互联设备基础;IP 地址基础;文件夹和 打印机共享设置;家庭网络的搭建;家庭无线网络的路由配置;IE 的使用与安全设置;常见 NOS 的安装与简单使用;网络安全、数据加密、防火墙、入侵检测、计算机病毒防范基础。	72
2	常用工具软件	本课程的任务是使学生具备选择、安装、使用网络技术常用工具软件的能力,具备借助软件说明或帮助文档安装、使用软件的能力,具有软件知识产权保护意识、安全意识和服务意识。	72
3	信息安全技术基础	了解信息安全基本概念与原理,包括信息安全的基本概念、基本目标;熟悉信息安全威胁和信息安全体系结构;了解与体验加密与解密、操作系统安全、Web 安全、软件安全与恶意代码、信息内容安全、数据安全等内容。	72
4	数据库安全技术	了解数据库的基本概念;熟悉 Mysql、SQL Server 数据库安装与基本配置;掌握常用 SQL 语句的使用;熟悉 Mysql、SQL Server 数据库设计的方法和步骤;掌握数据库的安全配	72

序号	课程名称	主要内容和要求	学时
		置与加固技能, 包括控制角色和授权、数据库账号和密码安全、数据库安全审计、数据库安全补丁等。	
5	网页制作	能够使用网页制作的主流软件, 建立正确、规范的站点; 能够使用框架和层、表单和表格、模板和库的知识, 整体规划网页; 熟悉 HTML 语言, 能够编写简单脚本语言, 增强网页的功能; 初步具备编写简单网页代码的能力; 具备对网站进行调试的能力。	72
6	动态网站程序开发基础	掌握 PHP 系统开发的环境的配置, PHP 语言的规范, HTML 表单的检验方法和 PHP 与客户机之间的交互方法, 并能开发与用户交互的动态网站。能对网站进行安全策略管理, 熟悉安全参数配置及数据安全保护。	108
7	脚本语言基础 (Python)	本课程主要学习变量、表达式与语句; 条件执行; 函数调用使用方法; for 循环结构的用法; 文件的使用方法; 字典; 正则表达式。	72
8	Python 高级编程	了解 Python 语言基本概念, 熟悉 Python 开发环境; 熟悉 Python 的关键要素, 包括数据类型、对象引用、组合数据类型、控制流语句、逻辑操作符、算数操作符、输入/输出、函数的创建与调用、模块; 熟练使用 Python 语言对数据安全、网络安全、Web 安全、系统安全编程; 熟练掌握 Python 程序的调试、测试与 Profiling 的技能。	60
9	虚拟化技术	主要学习虚拟机、CPU 虚拟化、内存虚拟化、存储虚拟化、虚拟化架构。	60
10	云存储的规划与部署	本课程介绍 NAS、DAS、IP-SAN、FC-SAN 等网络存储技术特点, 结合互联网应用部署相应网盘存储方案。	60
11	无线网络与安全	本课程主要内容为无线地勘软件的使用; 无线拓扑结构; 无线协议原理; AC 热备及集群技术; 无线网络安全管理。能够根据项目要求, 进行无线地勘, 合理部署 AP 点位; 能够进行产品选型; 能够进行无线网络部署及调优; 能够进行无线网络排障; 能够进行无线安全网络加固。	60
12	高级路由技术	本课程内容主要包括路由协议的高级应用配置与管理, 包括: RIP、EIGRP、OSPF、BGP、ISIS 等; 配置多种路由选择协议管理多用户的大型企业网络; 路由策略和策略路由的应用; 使用访问控制列表实现网络访问安全控制; IPv6 的概念和 IPv6 路由协议的配置。	60
13	信息安全法律与法规	通过本课程的学习, 要求学生掌握信息安全法律、法规的概念; 熟悉关于信息安全犯罪的刑法规定; 熟悉关于信息安全的刑事责任; 熟悉知识产权的种类和概念; 了解我国关于信息安全的一些法规和规章; 掌握隐私权的基本概念和保护措施。	60

(三) 专业核心课 (1038 学时)

序号	课程名称	主要内容和要求	学时
----	------	---------	----

序号	课程名称	主要内容和要求	学时
1	局域网组建及监管	掌握网络基础概念和网络协议基础知识；掌握交换机和路由器的基本配置与管理；具备局域网与无线局域网的搭建、调试、故障排查的能力；熟练进行网络的日常管理及维护。	108
2	Windows 服务器配置与管理	了解计算机操作系统基本概念；掌握 Windows 和 Linux 系统的安装与基本配置；熟练使用常用的 Dos 命令和 Linux Shell 命令；掌握 Windows、Linux 的安全加固方法与技能，包括系统备份、账号权限、网络服务、数据访问控制、网络访问控制、口令策略、用户鉴别、审计策略、漏洞等的安全加固；熟悉 windows、Linux 下 web 服务的搭建、检查及故障处理。	72
3	Linux 服务器配置与管理	本课程主要任务是使学生掌握 Linux 服务器的安装、配置、调试、测试与验收的相关技术，具备 Linux 服务器配置的能力，具备 Windows 服务器知识迁移到 Linux 上的能力。	72
4	广域网接入与监管	本课程的主要任务是使学生掌握广域网接入、远程安全接入、网络互连方面的基本技能，提高从事广域网接入、维护、监管等工作的方法能力，培养学生独立思考、自主学习和与人团结协作的能力，具备良好的职业道德与科学的工作态度。	72
5	网络安全配置与测试	本课程的主要任务是使学生具备网络安全设备配置、网络安全策略设置、远程接入安全设置、相关安全报告撰写的能力，提高学生在网络运行环境中的监控、管理网络和保障网络安全运行的实际应用能力，加强对网络管理与安全技术的理解，并具有沟通能力、团队合作精神和自我学习能力。	72
6	操作系统安全配置与管理	具备检测服务器的硬件组成部件和硬件参数的能力；具备安装主流 Windows 操作系统和虚拟机的能力；熟练使用常用的 Dos 命令；具备安装防病毒软件，升级病毒库、安装系统补丁、保证服务器基本安全运行的能力；具备 Windows Server 的安装与配置能力，包括活动目录、DNS 服务器、Web 服务器、FTP 服务器、DHCP 服务器、DFS 服务器；具备调试 Windows 系统下的常用服务的能力。	72
7	系统渗透测试	能够使用常用网络命令确定目标主机 IP 地址及开放端口；能够使用监控工具进行局域网监控；能够使用扫描工具进行端口及服务扫描；能够使用嗅探工具进行网页内容嗅探；能够使用工具进行渗透测试，并编制渗透测试报告。	72
8	web 安全技术	WEB 安全技术课程主要介绍 WEB 安全防范相关知识，包括安全评估、等级保护测评、安全监控、漏洞扫描、安全加固、安全事件应急响应等具体工作的理论基础、工作流程、实际操作方法。旨在提高学生网络信息安全维护人员技能水平，提升学生网络安全风险意识，加强维护人员网络安全实践能力，并具有人际沟通能力、团队合作精神和客户服务意识和自我学习能力。	72
9	网络安全攻击与防	熟悉常见 Web 安全架构，熟悉网络协议及 Web 安全原理；	72

序号	课程名称	主要内容和要求	学时
	御	<p>了解安全加固、渗透测试的全工作过程，内容包含分析渗透测试报告、编写 Web 安全漏洞加固方案、执行 Web 安全加固及漏洞复测。</p> <p>了解安全检测工具，如天镜脆弱性扫描软件；熟悉渗透测试技术和方法，熟练掌握渗透测试相关工具，包括 AWVS、sqlmap、Burp、chopper、nmap 等，能自行进行 Web 渗透测试；熟悉 Web 漏洞分析防范，包括 SQL 注入、XSS、CSRF 等 OWASP Top10 安全风险及对应解决方案；掌握恶意代码监测和分析能力，能有效防御挂马和恶意流量攻击熟悉 Web 系统安全风险及防护方案；了解 DDoS 攻击的类型和原理，掌握遭受 DDoS 攻击的解决办法；能够使用 Python 编写漏洞 poc，熟悉代码审计，挖掘 Web 安全漏洞；熟悉 Web 系统安全风险及防护方案；能对用户的安全管理体系提出安全建议；熟悉 App 逆向分析方法及相关工具的使用，了解 App 安全检测包括资源访问安全、认证鉴权安全、敏感信息安全、通信安全、终端输入安全、反逆向安全。</p> <p>了解其他网络攻击与防御技术的基本术语、概念与原理；了解常见网络攻击类型、手段、方法、原理；熟悉网络攻防专项技术技能，包括 Web 攻击、密码破解与防御、ARP 攻击、中间人劫持、端口爆破、远程控制与反控制、后门创建与检测、网络代理与追踪、入侵检测、痕迹清理及日志检查；掌握 wifi 无线网络攻防专项技能；正确使用常用的攻防工具。</p>	
10	网络协议分析	<p>通过该门课的学习，使学生深入学习 TCP/IP 协议体系结构和基本概念，分析各个协议的设计思想、流程及其所解决的问题。通过该门课程的学习，进一步提高学生作为网络管理员的技能水平。学生能够胜任中小型企业网络维护的日常工作。</p>	54
11	网络安全产品配置与管理	<p>培养学生信息安全系统的集成能力。学生需要掌握各类安全产品的应用背景、工作原理、基本配置、设备维护及故障排除等基本知识，并熟悉信息安全工程项目施工流程、工程施工和验收标准。安全设备包括：防火墙、IDS、VPN、安全网关、UTM、安全管理设备、无线安全设备、安全网闸等。课程采用项目教学法，学生将在实际的工程背景完成学习项目，项目步骤包括：明确任务，制定工作计划；与用户沟通（或根据任务书描述），撰写用户需求报告；根据用户需求报告，进行信息安全系统规划，制定系统安全系统方案；按照规划方案，组织项目施工；对照用户需求，测试工程性能；工程验收，提出改进建议。</p>	60
12	病毒与木马分析技术	<p>了解病毒和木马的基本知识；能够创建与配置虚拟机；掌握病毒木马样本的行为分析、源码分析、特征提取等方法与技能；熟练使用 IDA、OD、WinDBG、Process Monitor 等常用病毒木马分析工具。</p>	60
13	恶意代码分析	<p>本课程是信息安全专业的核心课程，主要学习 PC 端软件</p>	60

序号	课程名称	主要内容和要求	学时
		加壳、PC 端软件脱壳、注册破解、PC 端源码分析、PC 端木马分析、PC 端病毒分析、移动端恶意代码分析、移动端反破解技术	
14	云数据中心的架构与安全管理	本课程培养学生认识云计算技术特点,了解 PaaS、IaaS、SaaS 等架构,能用利用基于 Openstack 开源技术搭建云计算应用平台,并在云平台上安全部署相关应用服务。	
15	信息安全测评与风险评估	本课程要求学生掌握的内容包括:事前的安全配置检查及安全漏洞扫描报告分析,事中的违规审计分析,事后取证调查。了解安全合规检查的概念、流程和方法,了解安全日志审计工作要求、工作内容、工作流程,熟悉操作系统日志、Apache 等典型应用日志的格式,掌握事前、事中、事后合规检查的基本技能,掌握日志收集方法及分析工具使用,进行运维实战工作中的安全日志审计工作。	60
16	渗透测试与 web 安全	本课程是信息安全专业的核心课程,主要学习 SQL 注入漏洞、文件上传漏洞、数据库漏洞、XSS 跨站漏洞、网站程序漏洞;ftp/mysql 提权,远程桌面认证漏洞,本地溢出漏洞	60

四、专业拓展课程 (198 学时)

序号	课程名称	主要内容和要求	学时
1	PHOTOSHOP 平面图像处理	本课程主要任务是学习 Photoshop 的图片处理功能美化修饰图像;使用操作命令进行色彩编辑、制作文字特效等,提高学生的平面设计能力、创作能力、信息管理能力;最终掌握图形、图像的处理方法,从而培养学生正确的审美观和创造性思维能力。	36
2	Premier 视频剪辑	本课程主要任务是能够熟练进行素材采集,并对素材进行处理;能为影片添加转场、特技、字幕和音乐;根据作品的使用要求输出适当的视频格式。	54
3	FLASH 动画制作	主要内容包括:初识矢量图及二维动画基础知识、绘制图形、文本的输入和编辑、图层与场景、元件与实例、滤镜与混合模式、骨骼动画、声音与视频、使用 Action Script 编程、组件等基础知识。	72
4	常用绘图软件	该课程其主要任务是使学生学会使用 Auto CAD,具备使用该软件绘制机械、建筑、电子线路板、网络工程等不同行业图纸的能力,提高学生的综合专业素质,使学生能够较熟练地看懂多个行业的图纸,同时初步了解计算辅助设计的一些相关知识。	36

五、实训实习课程 (420 学时)

序号	课程名称	主要内容和要求	学时
1	网络管理员取证实训	通过实训学习使学生掌握参加网络管理员认证所需的全部技能和知识	30
2	信息安全员取证实训	根据国家信息安全员大纲的要求,复习以前所学的知识,包括:操作系统安全、数据库安全、病毒分析与防御、防火墙技术和网络隔离器、扫描和入侵检测技术、密码技术应用、网络应用服务安全技能、安全审计技术、安全策略管理技能、应急事件处理技能等知识,并组织学生进行取证。	30
3	毕业设计与顶岗实习	毕业设计是高职教学过程的最后一个环节,着重培养学生运用所学知识,独立完成应用设计的能力,为今后从事计算机网络技术的相关工作打下良好的基础。毕业设计的任务包括选题、查阅文献资料、方案设计、网络设计、网络应用开发等。毕业设计鼓励学生到企业参加实际设计任务。毕业设计完成后,要提交毕业设计论文,并进行毕业答辩。	360

十一、教学进程总体安排

表 7: 网络信息安全专业“3+2”贯通培养教学计划表

课程类别	课程序号	课程名称	学时	学年学期安排课程时数(周课时)									
				第一学年		第二学年		第三学年		第四学年		第五学年	
				1	2	3	4	5	6	7	8	9	10
公共基础课程	1	思想政治	216	2	2	2	2	2	2				
	2	语文	288	3	3	3	3	2	2				
	3	数学	252	3	3	2	2	2	2				
	4	英语	252	3	3	2	2	2	2				
	5	信息技术	144	2	2	2	2						
	6	历史	72	2	2								
	7	体育与健康	324	3	3	3	3	3	3				
	8	艺术	72	1	1	1	1						
	9	读本	18	1									
	10	国防教育	18		1								
	11	劳动教育	18	1									
			职业沟通	30							2		
		思想道德修养与法律基础	60							2	2		
		毛泽东思想和中国特色社会主义理论体系概论	60							2	2		
公共基础课小计			1878	21	20	15	15	11	11	6	4	0	0
专业基础	13	网络技术基础	72	4									
	14	常用工具软件	72	4									
	15	信息安全技术基础	72	2	2								
	16	数据库配置与应用基础	36			4							

课程	17	网页制作	72				4					
	18	动态网站程序开发基础	108					4				
	19	脚本语言基础 (python)	72				4					
	20	python 高级编程	60						4			
	21	虚拟化技术	60							4		
	22	云存储的规划与部署	60							4		
	23	无线网络与安全	60							4		
	24	高级路由技术	60						4			
	25	信息安全法律与法规	60							2		
专业基础课程小计			900	10	2	6	8	6	0	10	12	8
专业核心课程	26	局域网组建及监管	108		4							
	27	windows 服务器配置与管理	72		4							
	28	linux 服务器配置与管理	72			4						
	29	广域网接入及监管	72			4						
	30	网络安全配置与测试	72			4						
	31	操作系统安全配置与管理	72				4					
	32	系统渗透测试	72						4			
	33	web 安全技术	72						4			
	34	网络安全攻击与防御	72				4					
	35	网络协议分析	54						4			
	36	网络安全产品配置与管理	60								4	
	37	病毒与木马分析技术	60							4		
	38	恶意代码分析	60									4
	39	云数据中心的架构与安全管理	60									4
40	信息安全测评与风险评估	60									4	
41	渗透测试与 web 安全	60									4	
专业核心课程小计			1098	0	10	12	8	0	11	4	4	16
专业拓展课程	42	PHOTOSHOP 平面图像处理	36	2								
	43	Premier 视频剪辑	54					3				
	44	FLASH 动画制作	72					4				
	45	常用绘图软件	36						2			
	46	专业拓展类公共任选课建议	60				2			2	2	
	47	人文素质类公共任选课选课建议	60							2	2	
专业拓展课程小计			318	2	0	0	2	7	2	4	4	
实习实训	48	网络管理员取证实训	30							30		
	49	信息安全员取证实训	30								30	
	50	毕业设计+顶岗实习	360									360

课 程													
总 计		3510	27	28	30	30	30	30	24	24	24		

十二、课时分配表

各类课程教学学时分配如下表所示：

表 8：课时分配表

序号	课程类别	学时	占学时总比例
1	公共基础课	1194	34%
2	专业基础课	900	25.6%
3	专业核心课	1098	31.2%
4	专业拓展课	318	9%
合计	总学时	3510	100%

十三、实施保障

（一）师资队伍

践行校企深度融合打造的创新型人才培养方针，在学院师资配备上，校企双方充分发挥各自的资源和技术优势，针对不同阶段的人才培养目标，匹配不同类型的师资，形成兼具理论水平与实践能力的高素质师资队伍。组建公共课和专业基础课由学校教师负责，专业核心课及职业特色课由企业教师负责的校企混合型师资队伍。

表 12：信息安全专业贯通培养师资配备状况

阶段	类型	师资团队介绍
中职阶段	院校师资	朝阳区骨干教师：3 名、北京市骨干教师 1 名。
	企业师资	企业安全高级顾问 1 名；企业培训负责人 1 名；网络运维专家 1 名；渗透测试专家 1 名；Web 安全专家 1 名；就业指导咨询顾问 1 名；助教 2 名；企业联盟客座讲师 3 名。
高职阶段	院校师资	学科带头人：2 名，院级骨干教师：7 名，北京市教学名师：1 名； 学历：博士学位 1 人，硕士学位 18 人，学士学位 10 人； 职称：高级（副教授、高级工程师）8 人；中级（讲师）18 人； 初级（助教）3 人。
	企业师资	企业安全高级顾问 1 名；企业培训负责人 1 名；渗透测试专家 2 名；Web 安全专家 2 名；软件逆向专家 1 名；就业指导咨询顾问 1 名；助教 3 名；企业联盟客座讲师 6 名。

(二) 教学设施

1. 教室

本专业配备现代化的多媒体多功能教室，包括电子白板，信息化环境主要是通过基于WIFI的无线局域网、移动通信、电信网作为接入方式，实现从内容呈现、环境管理、资源获取、及时互动、情感认知五个维度为教学提供支撑服务。

2. 校外实训基地

校外实训活动是人才培养中的重要一环，可以充分让学生理论联系实际，应用和巩固自己的专业知识，为了满足学生的实训需求，神州泰岳集团以及实习就业企业联盟充分利用自身的资源优势 and 人力优势，为信息安专业“3+2”贯通培养的学生提供校外实训场所，并为学生提供技术支持和相关指导。

表 9：中职校外实训基地

序号	校外实训基地	实训项目	实习内容	实训进程安排
1	北京神州泰岳信息安全技术有限公司	岗前培训	1. 企业文化 2. 项目文档制作 3. 项目现场值守	4 周
2	中电集团长城网际系统应用有限公司	岗前培训	1. 企业文化 2. 项目文档制作 3. 项目现场值守	4 周
3	北京永信至诚科技股份有限公司	网络安全运维	1. 企业文化 2. 网络运行监控 3. 网络应急响应 4. 网络值守	4 周

表 8：高职校外实训基地

序号	校外实训基地	实训项目	实习内容	实训进程安排
1	神州数码网络技术公司	岗前培训	1. 企业文化 2. 项目文档制作 3. 项目现场设备调试 4. 项目现场值守	4 周
2	网御星云网络技术公司	岗前培训	1. 企业文化 2. 项目文档制作 3. 项目现场设备调试 4. 项目现场值守	4 周
3	兆维集团	网络安全运维	1. 企业文化 2. 网络运行监控 3. 网络应急响应 4. 主机、网络安全维护	4 周

			与加固 5. 网络值守	
4	中国电信	网络安全运维	1. 企业文化 2. 网络运行监控 3. 网络应急响应 4. 主机、网络安全维护 与加固 5. 网络值守	4 周以上

3. 校内实训基地

学校按照“以工作过程为导向”的课程理念及信息安全技术专业岗位工作流程,建立了真实或仿真的实训环境,其中:

***学校网络信息安全专业教师团队拥有专任教师 20 名,兼职教师 10 名。在专任教师队伍中,具备高级职称 8 名,中级职称 8 名;硕士研究生 8 名;团队平均年龄 36.3 岁;具备“双师”素质的专任教师人数占全体专任教师队伍的 100%;其中北京市优秀教师 1 人,2 名教师获北京市优秀青年骨干教师称号;10 名兼职教师均源于企业一线,有丰富的生产实践经验。

表 10: 中职校内实训基地

序号	技术中心名称	实训室名称	主要设备要求
1	云计算实训中心	渗透测试与 WEB 安全实训室	网络空间安全实战教学平台、网络空间安全实战对抗平台、互联网 Web 攻防教学实训平台
		信息安全基础实训室	交互模拟沙盘
		网络安全实训室	安全网关、防火墙、 攻防堡垒、PC 机
2	网络技术实训中心	路由交换实训室	二层、三层交换机、路由器、PC 机
		综合布线实训室	综合布线设备、光纤溶解设备
		计算机故障检测与排除实训室	计算机维修设备、故障就机、PC 机

北京信息职业技术学院计算机工程与通信工程学院已建成三个占地面积共计 4000 平方米的校内实训基地提供校内实践教学保障,技术中心的设备先进,工位数量充足,可同时承担 500 人以上的实践教学。学院北信软件园可提供学生毕业年的生产性实训项目教学,因此,校内实训基地为专业的实践教学提供了有利的保障。

表 11: 高职校内实训基地

序号	技术中心名称	实训室名称	主要设备要求
----	--------	-------	--------

1	信息安全技术中心	信息安全攻防实训室	IPS、安全网关、防火墙、 攻防堡垒 PC 机
2		网络互联实训室	二层、三层交换机、路由器、PC 机，支持无线组网
3		逆向分析实训室	支持 PC 端软件加壳、PC 端软件脱壳、注册破解、 PC 端源码分析、PC 端木马分析、PC 端病毒分析、 移动端恶意代码分析、移动端反破解技术
4		渗透测试与 WEB 安全实训室	支持渗透测试工程师岗位技术、技能的专项训练与综合训练；支持 web 安全岗位全工作过程链的专项训练与综合训练
5		网络存储实训室	NAS,IP-SAN,FC-SAN，支持云存储
6		信息安全意识培养与对抗竞赛实训室	支持常规教学、信息安全意识教育、信息安全竞赛训练、对抗比赛，以及网络空间安全展示与体验平台中的体验与实训
7		移动安全、物联网安全与工控安全实训室	Modbus 协议解析；基于 Modbus 协议功能码漏洞的工控设备攻击； 基于 Modbus 协议网络端口开放的工控设备攻击； Siemens S7 协议解析；网络端口与服务安全防护； PLC 网络隔离防护；提供移动终端安全、移动通信安全、安全审计与加固以及移动安全服务方向的攻防教学和实训；支持物联网感知层、网络层、应用层的安全攻防教学和实训
8		网络数据库实训室	PC 机、常用的软件开发环境

（三）教学资源

1. 教材选用

根据《关于加强和改进新形势下大中小学教材建设的意见》，在教材选用过程中，严格执行国家规定，对涉及国家主权、国家安全、海洋权益、社会安定、民族宗教、重大革命题材和重大历史题材等方面的内容进行严格审查把关。优先选用中等职业教育改革创新示范教材、全国中等职业教育教材审定委员会审定教材。

为了进一步加强信息安全专业的建设,满足人才培养发展的需要,专业将建立本专业的教学资源库。教学资源库包括以工作过程为导向的核心课程的教学文件资源、校本教材等。通过建立资源库,有利于实现课程资源整合,实现优质资源共享,同时使课程体系的管理更加规范化。

2. 精品课程资源

以打造精品课程为突破口,与企业合作,共同建设2门精品课程网站,包括教学计划、课时教案、教学课件、校本教材、工作任务书、考核评价表、典型课例、学生反思和教师总结等教学资源。精品课程教学网站按照课程分类,将与之相关的所有内容收入专业教学资料库中。精品课程无论在教学设计、教学资源开发、课程教学实施等方面都具有创新和示范作用,以此为龙头,带动其他课程建设,全面提高教学质量。

教学文件资源:教学文件资源主要包括课程标准、教学计划、电子教案、多媒体课件、学习指导、任务单、评价表、案例、文献等。按课程分类,将与本课程相关的所有教学资料,收集、整理、归类存放于资源库中。

校本教材资源:依据“校企联盟、工学赛相结合”人才培养模式及校企共建的课程体系,结合我校实际,开发突出职业能力培养、以工作过程为导向的理实一体化专业特色教材;建立与“校企合作、学岗对接”人才培养模式相适应的质量评价体系,激发学生兴趣,全面提高课程教学质量。校本教材资源分为两部分,一为校本教材的电子文稿,二为校本教材所涉及的项目实训的各种资料。收集、整理本专业的所有校本教材电子资料,并按课程分类,存放于教学资源库。当完成一轮教学工作后,要求教师对于教材的课程设计、课程实施及课程评价等环节的内容及时地补充、完善,不断地更新教学资源库中的相关内容。

相关资料资源:搜集、查找本专业相关社会和行业需求文件与文献,如国家标准、行业标准和行业动态等。

(四) 教学方法

采用任务驱动法、情景教学法、项目教学法等,进行教学方法的改革;选择企业典型的真实工作项目,发挥校企联盟的作用,聘请企业专家参与课程设计与实施。

学生在教师的指导和企业专家的辅导下,完成专业核心课程的学习。教师利用企业提供的实际项目案例设计课程结构。企业专家全程参与教学设计、课程实施及考核评价。学生以小组形式在实训基地完成模拟项目实训,在岗位分工、岗位轮换活动中锻炼职业能力和社会能力。依托企业联盟,以企业真实项目为依托开展技能教学,借助工作室承接实际工程项目,亲身体验实际工作流程,明确企业标准及行业规范。

借助教学资源库、BB平台、现代化信息化手段,将课堂学习与网络学习有机结合,拓宽教学渠道,提高学生的动手能力和实际操作能力,引入企业专家评价,对学生进行过程性和终结性评价,激发学生的学习动机,有效达到职业人的标准。

公共基础课:根据学生认知水平、年龄、学科特点、社会经济发展及专业实际,从学生的思想、生活实际出发,深入浅出,寓教于乐,循序渐进,多用鲜活通俗的语言,多用生动典型的事例,多用喜闻乐见的形式,多用疏导的方法、参与的方法、讨论的方法,增强吸引力和感染力。着力于自我控制能力和团队精神的培养,调动学生主动学习的积极性。在规划

设计过程中，为学生加强交流、互相启发创造条件；在规划落实过程中，为学生互相帮助、互相促进创造条件。

专业技能课：利用行动导向教学方法，根据实际课程特点，灵活使用任务驱动教学法或项目式教学法，学法主要采用自主探究与小组合作的学习，学生通过对教学载体进行“产品”的设计、制作和测试，学习掌握专业必备的知识与技能。教学中要充分利用信息化教学手段，辅助提升教学效果。利用各种教学资源 and 教学媒体，创设情境，增加学生动手实践操作的机会，提高学习兴趣，激发学习动力，强化实践技能的培养。以学生发展为本，重视培养学生的综合素质和职业能力，以适应技术快速发展带来的职业岗位变化，为学生的可持续发展奠定基础。为适应不同专业及学生需求的多样性，可通过对选学模块教学内容的灵活选择，体现课程内容的选择性和教学要求的差异性。教学过程中，应融入对学生职业道德和职业意识的培养。

（五）考核评价

公共基础课程教学，教师要执行教育部和北京市教委有关教学基本要求，重在改革教学方法，调动学生学习的积极性，为学生综合素质的提高、职业能力的形成和可持续发展奠定基础。

专业课教学，教师要根据专业核心课程标准，进行行动导向的教学设计，以任务、案例、项目等为载体，实现理论与实践一体化教学。要尊重学生的主体地位和创新精神，充分发挥实训基地在创设教学情境中的作用，保证动手操作时间，强化职业技能训练，通过教学过程有效培养学生的职业能力。

考核评价应体现评价主体、评价方式、评价过程的多元化。各校要将学生应具备的职业素质和职业能力作为评价教育教学质量的依据，并根据企业要求和学生实际，在已有的核心课程考核标准的基础上，确定更有针对性、分层次的考核内容和评价标准。

（六）质量管理

1. 教学要求：

中高职衔接方案规划完成所有课程的学习时间为5年，其中中职阶段课程3年，高职阶段课程2年，完成所有规定课程的学习并成绩合格(包括德育考核)。

公共基础课：教学要符合教育部有关教育教学基本要求，按照培养学生基本科学文化素养、服务学生专业学习和终身发展的功能来定位，重在从素质养成的角度来把握职业教育的德育与文化知识教学本质，以“做中学、做中教”为基本形态，在教学方法、教学手段、教学

模式及教学组织形式上进行改革创新为学生综合素质的提高、职业能力的形成和可持续发展奠定基础。

专业技能课：教学遵循“以工作过程为导向”的指导思想，依据网络安全防御与监控工作岗位对知识与能力的要求确定学习领域与课程教学内容，做到“理实一体化”。以网络安全管理工作过程为主线，兼顾学生认知的先后顺序，由基础到专业、由单到综合安排课程，使各门课程教学内容的衔接更加顺畅与合理。根据行业的发展不断调整教学内容，教学所讲的应是当今行业需要的内容。

2. 教学管理

注重教学全程控制，确保记录完整，根据发生的质量问题，及时发现和解决课堂教学中的问题，总结推广先进经验，改进教学质量的方法，不断促进课堂教学质量的提高。实训教学前指导教师必须认真制定实训计划，并做好实训前的准备（包括设备检查、材料准备等）。实训指导教师须先到班级向全体学生讲清实训目标、实训任务、要求、纪律及注意事项，然后有组织地带领学生进入实训场地。实训过程中指导教师要悉心指导，严格要求。对违规操作、不守实训纪律的学生指导教师要及时批评教育。指导教师要精心指导学生完成实训报告，并在该项目实训结束前认真进行实训总结、评价学生优劣，并认真进行实训成绩考核。以校企合作、工学结合为载体，以岗位工作流程为主线，强化实践性训练，提高学生的实践技能。专业建设指导委员会进行专业论证，修订人才培养方案，参与人才培养全过程。

九、毕业要求

本专业的学生除了修满必须的学分之外，还必须取得相关的职业资格证书才能达到毕业的标准。本专业的学生在校期间，可选考的职业资格证书有：

表 13：职业资格证书一览表

序号	职业资格证书名称	发证机构	取证要求	取证阶段
1	全国计算机等级考试一级	教育部考试中心	必考	中职
2	云计算运维与开发（初级）	教育部	选考	中职
3	计算机网络管理员（三级）	人力资源与社会保障部	选考	高职
4	网络设备调试员（三级）	人力资源与社会保障部	选考	高职
5	网络安全工程师（CISO）	国家信息化安全技术资格 认证管理中心	必选	高职

中高职转段工作要求：在第六学期期末进行转段测试，由中高职衔接学校共同制定考核方案和考核大纲，主要包括对语文、数学等公共基础课程知识和专业综合技能为内容的考核，对学生进行筛选，考试合格且学分达到毕业要求的学生直通高职对接专业就读。

十四、其他说明

1. 军训

新生军训安排在第一学期完成, 为期 1 周。

2. 入学教育

入学教育安排在新生入学后的第一周。入学教育的主要内容包括: 帮助学生了解学校、了解专业, 进行树立职业理想、遵守校规校纪、养成良好的学习习惯 和行为习惯等的教育。

3. 社会实践

社会实践可在三、四、五、六学期, 共计安排一周时间。社会实践的主要内容包括: 校内实践劳动、企业参观、社会调查、社会公益活动等。

4. 解释

与本方案相关的其它事宜, 由学校教务处会同专业系部共同解释。