附件 1

广东财贸职业学院

数字技术学院

信息安全技术应用专业

人才需求调研报告

人才需求调研报告

（一）调研目的和意义

随着互联网的普及，我国数字经济规模不断扩大，网络安全问题也引起了越来越多人的关注。保障网络安全不仅事关个人信息安全，也涉及国家安全、社会稳定等多个层面。2021年底，中央网络安全和信息化委员会印发《“十四五”国家信息化规划》（以下简称《规划》），对我国“十四五”时期信息化发展作出部署安排。《规划》围绕确定的发展目标，部署了10项重大任务，其中明确提出要“培育先进安全的数字产业体系”。加强网络安全和信息化工作、建设网络强国势在必行，而人才便是这其中的关键一环。

本次调研的目的是深入了解当前信息安全领域的行业趋势、技术发展动态以及市场需求，更好地把握市场动态，制定更符合市场需求的人才培养策略。同时明确信息安全领域所需的关键技能和知识点，通过调研，可以了解信息安全人才的需求和要求，更准确地评估学生的能力和潜力，提高人才与企业需求的匹配度。其次可以根据调研结果开发课程、教材和实验平台，实现资源共享和优势互补，推动信息安全领域的创新和发展。调研结果还可以帮助学校调整人才培养策略，提高学生的就业竞争力和适应能力。同时，企业也可以更精准地招聘到符合自身需求的人才，提高员工的整体素质和企业的竞争力。

（二）调研组织

广东财贸职业学院数字技术学院信息安全技术应用教研室

（三）行业现状和人才需求情况

一、我国网络安全领域政策规定不断完善

2023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。同年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。

二、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 年均有显著提升。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、我国网络安全人才培养加快

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。

（四）职业岗位（群）的情况

一、职业岗位（群）概述

信息安全技术应用专业的毕业生主要面向政府机构、企事业单位、金融机构等领域的信息安全岗位。随着信息技术的不断发展和网络安全问题的日益凸显，信息安全技术应用专业的毕业生需求量持续增长。

二、主要职业岗位（群）

网络安全工程师：负责网络系统的安全防护，包括防火墙配置、入侵检测、漏洞扫描等。

数据安全工程师：负责数据的保护、备份和恢复，确保数据的完整性和安全性。

应用软件安全工程师：负责应用软件的安全评估、漏洞修复和恶意代码检测，确保应用软件的安全性。

渗透测试工程师：通过模拟黑客攻击，评估系统的安全性，发现潜在的安全漏洞。

安全服务工程师：提供安全咨询、安全培训、安全应急响应等服务，帮助客户提升整体安全水平。

三、职业岗位（群）特点

技术性强：信息安全技术应用专业的毕业生需要具备扎实的计算机技术和信息安全技术基础，能够熟练掌握各种信息安全工具和技术。

实践经验丰富：企业对于信息安全人才的需求不仅要求掌握理论知识，还需要具备丰富的实践经验。因此，具备实习和项目经验的学生更受企业青睐。

综合素质要求高：信息安全岗位需要具备良好的沟通能力、团队协作能力和创新能力等综合素质。此外，还需要具备高度的责任心和保密意识。

四、职业岗位（群）发展趋势

人工智能与信息安全结合：随着人工智能技术的快速发展，信息安全领域也将逐步引入人工智能技术，提高安全防护的智能化水平。

云计算和大数据安全：随着云计算和大数据技术的广泛应用，云计算和大数据安全将成为信息安全领域的重要发展方向。

物联网安全：物联网技术的快速发展将带来更多的安全挑战，物联网安全将成为信息安全领域的重要研究方向。

五、相关数字和信息

据调查，信息安全产业迅速发展，中国信息安全产业规模已达千亿量级。用人单位对于信息安全岗位的需求量大，且对于毕业生的技术要求高。信息安全产业毕业生的起薪普遍在6k-8k之间，工作经验3年以上的薪资可达15k-30k。此外，企业对于信息安全人才的需求不仅限于技术能力，还注重毕业生的综合素质和社会能力。

（五）职业资格和行业规范要求情况

一、职业资格要求

专业认证：信息安全技术应用专业人才在就业市场上，通常需要具备一些专业的认证资格，以证明其专业能力和技术水平。常见的认证包括：

① CISSP（Certified Information Systems Security Professional）：这是国际信息系统安全认证联盟（ISC）组织下的旗舰认证，针对信息安全管理人员，覆盖信息安全管理的十个关键领域。

② CISM（Certified Information Security Manager）：该认证由 ISACA（信息系统审计与控制协会）颁发，专为信息安全管理经理设计。

③ CEH（Certified Ethical Hacker）：由 EC-Council（国际网络安全认证协会）颁发，针对网络安全专家，教授如何识别和评估系统脆弱性。

技术能力：除了专业认证，企业还期望信息安全技术应用专业人才具备一系列技术能力，包括但不限于：

① 网络安全：熟悉各种网络攻击和防御技术，如防火墙、入侵检测系统等。

② 数据隐私：了解数据保护法规，如 GDPR（通用数据保护条例），并能够设计和执行数据隐私策略。

③ 风险评估：具备对系统和网络进行风险评估和漏洞分析的能力。

④ 加密技术：熟悉常见的加密算法和协议，如 SSL/TLS、AES 等。

⑤ 沟通和团队合作能力：能够与团队成员、客户和其他利益相关者有效沟通。

⑥ 问题解决能力：能够独立分析和解决复杂的安全问题。

⑦ 持续学习能力：能够持续跟踪和学习最新的安全技术和威胁趋势。

二、行业规范要求

法律法规：随着数据保护法规的日益严格，如中国的《网络安全法》和欧洲的 GDPR，信息安全技术应用专业人才需要了解和遵守这些法规，确保组织的合规性。

职业道德：信息安全技术人员应遵守职业道德规范，保护客户的数据和隐私，不泄露机密信息，不进行非法的网络活动。

持续教育：信息安全领域的技术和威胁在不断变化，因此，信息安全技术应用专业人才需要持续学习和更新知识，以适应行业的发展。

（六）中高职学校课程设置情况

一、中职学校课程设置

中职学校的课程设置主要分为公共课和专业课两大类。

1. 公共课：

主要包括文化课，如语文、英语、数学、物理、化学、历史、地理等，这些课程与普通学校的课程相似，旨在培养学生的文化素养和基础理论知识。此外，还包括信息技术、科学等与现代科技相关的课程，以提升学生的科技素养。

2. 专业课：

专业课则更加注重实践技能的培养，涵盖了信息安全技术的基础理论知识，如信息安全技术基础、网络安全、数据安全等。同时，也包括与信息安全技术应用相关的实操课程，以提高学生的动手能力和实践操作。

二、高职学校课程设置

高职学校的课程设置在深度和广度上相对于中职学校有所提升，更加注重专业技能的培养和实际应用能力的提升。

1. 基础课程：

包括数学、英语、计算机基础等，为学生提供必要的基础理论知识和计算机操作能力。

2. 专业课程：

涵盖信息安全技术的各个方面，如网络安全技术、数据安全技术、应用密码学等，旨在培养学生全面的信息安全技术能力。课程设置中还包括实验和实训环节，通过实际操作来加深学生对理论知识的理解，并提升其解决实际问题的能力。

三、课程设置与行业需求对接

中高职学校的课程设置紧密围绕信息安全技术应用专业的培养目标进行，旨在使学生掌握信息安全技术的基本理论和方法，具备信息安全技术的实际应用能力，以及信息安全事件应急处理和安全评估能力。这样的课程设置有助于学生在未来的工作中灵活运用所学知识，提高信息系统的安全性。

（七）学生学习状况

一、学习基础与技能掌握情况

计算机技术基础知识：信息安全技术应用专业的学生普遍具备扎实的计算机技术基础知识，能够较好地掌握网络安全、密码学等相关技术。这是信息安全技术应用专业学习的基石，对于后续的专业技能培养至关重要。

信息安全技术应用能力：通过系统学习信息安全技术基础、网络安全、数据安全、应用密码学等课程，学生能够掌握信息安全技术的基本理论和方法，具备信息安全技术的实际应用能力。

二、实践技能与操作能力

实践教学重视度：信息安全技术应用专业注重实践教学的培养，通过开设实验课程、项目实训和实习等形式，提高学生的动手能力和实际操作能力。调研结果显示，这种教学方式能够使学生更好地掌握信息安全技术的实际应用。

实习与实训经验：学生通过参与实习和实训项目，能够在实际工作环境中锻炼自己的技能，并积累宝贵的经验。这些经验不仅有助于提升学生的就业竞争力，还能为其未来的职业发展奠定坚实的基础。

三、学习态度与职业发展意愿

学习态度：信息安全技术应用专业的学生普遍对学习充满热情，能够积极投入到学习中去。他们关注信息安全领域的最新发展动态，愿意不断学习和提升自己的技能。

职业发展意愿：学生对信息安全技术应用专业的就业前景持乐观态度，并希望能够在政府机构、企事业单位、金融机构等领域从事信息安全工作。同时，也有部分学生希望成为安全产品的研发人员，为信息安全领域的发展做出贡献。

（八）调研结论

一、市场需求持续增长

(1) 随着信息技术的迅速发展，信息安全问题日益突出，对信息安全技术的需求也日益增加。

(2) 信息安全技术应用专业的毕业生在数量上远远不能满足市场对人才的需求，特别是在政府机构、企事业单位、金融机构等领域，信息安全专业人才缺口巨大。

二、专业设置与课程设置符合行业需求

(1) 国内外多所大学和专业院校均设立了信息安全技术专业，涵盖了信息安全概论、网络安全、密码学、数据安全、信息安全管理等课程，从理论和实践两个方面全面培养学生的信息安全技术能力。

(2) 课程设置较为完善，涵盖了信息安全基础、网络安全技术、加密与解密技术、安全管理与评估等方面的内容，部分高校还结合实际案例开设了专业实践课程，为学生提供了丰富的实践机会。

三、实践教学与就业情况良好

(1) 信息安全技术应用专业注重实践教学的培养，通过开设实验课程、项目实训和实习等形式，提高学生的动手能力和实际操作能力。

(2) 信息安全技术专业的毕业生就业情况较好，大多数学生能够在信息安全公司、网络安全机构、金融机构、科研院所等单位找到理想的工作，且薪资水平普遍较高。

四、专业技能与综合素质并重

(1) 企业对于信息安全岗位的需求不仅限于技术能力，还注重毕业生的综合素质和社会能力，如沟通能力、团队协作能力和创新能力等。

(2) 信息安全技术应用专业的学生需要具备较强的社会能力，如与客户进行融洽的沟通，有较强的团队合作意识和人际交往能力等。

五、发展前景广阔

(1) 随着信息化进程的加快，信息安全问题将持续受到重视，信息安全技术应用专业的发展前景将更加广阔。

(2) 信息安全产业迅速发展，为信息安全技术应用专业的学生提供了更多的就业机会和发展空间。

（九）对策与建议

一、优化专业设置与课程体系

(1) 增强多学科交叉融合：鉴于信息安全技术应用专业的多学科交叉特点，建议在专业设置和课程设计上进一步整合计算机科学、数学、密码学、通信技术等多个学科的知识，

以提高学生的综合应用能力。

(2) 更新课程内容：考虑到信息安全技术更新迭代速度快，建议课程内容应及时更新，包括最新的信息安全技术、最新的行业规范和标准、以及最新的法律法规等。

(3) 强化实践教学：进一步增加实践课程的比例，通过开设实验课程、项目实训、企业实习等方式，让学生更多地参与实际项目的开发和运维，提高学生的动手能力和解决实际问题的能力。

二、加强师资队伍建设

(1) 引进高水平教师：积极引进具有丰富实践经验和理论水平的信息安全技术人才，以加强师资队伍的建设。

(2) 提高教师专业技能：定期对教师进行专业培训，使教师能够掌握最新的信息安全技术和教学方法，提高教学效果。

(3) 建立产学研合作机制：鼓励教师与企业、研究机构等建立紧密的合作关系，共同开展科研和教学工作，实现资源共享和优势互补。

三、深化产教融合，促进人才培养与行业需求对接

(1) 加强校企合作：与企业建立紧密的合作关系，共同制定人才培养方案、开发课程、建设实训基地等，实现人才培养与行业需求的无缝对接。

(2) 推动实习实训基地建设：加大实习实训基地建设的投入力度，建设一批具有示范性和引领性的实习实训基地，为学生提供更多的实践机会。

(3) 开展职业技能竞赛：定期举办信息安全职业技能竞赛，激发学生的学习兴趣和热情，提高学生的职业技能水平。

四、加强信息安全意识教育

(1) 普及信息安全知识：通过开设公共课程、举办讲座等方式，普及信息安全知识，提高全民的信息安全意识。

(2) 加强信息安全法律法规教育：加强信息安全法律法规的教育和宣传，使学生了解并遵守相关法律法规，增强法律意识和责任感。

五、关注行业发展趋势，提前布局未来人才培养

(1) 跟踪行业发展趋势：密切关注信息安全行业的最新发展动态和趋势，及时调整专业设置和课程内容，以适应行业发展的需求。

(2) 提前布局未来人才培养：针对人工智能与信息安全结合等未来发展趋势，提前布局相关课程和研究方向，培养具有前瞻性和创新性的信息安全技术人才。

附件2

信息安全技术应用专业人才培养方案

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

■所属专业群：信息安全技术应用专业群

二、入学要求

■要求：普通高级中学、中等职业学校毕业或具备同等学力

三、修业年限

■年限：学制3年，弹性学习不超过6年

四、职业面向

学段	所属专业大类（代码）	所属专业类（代码）	对应行业（代码）	主要职业类别（代码）	主要岗位群或技术领域举例	职业技能等级证书、社会认可度高的行业企业标准和证书举例
高职	电子与信息大类（51）	计算机类（5102）	互联网和相关服务（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)	渗透与测试工程师 网络安全运维工程师； web安全工程师； 网络安全系统集成	HCIA;华为认证ICT工程师 HCIP:华为认证ICT中级工程师 RHCSA;红帽认证系统管理员 RHCE;红帽认证系统工程师；网络信息安全工程师（中级）

					工程师；数据恢复工程师	

五、培养目标与培养规格

（一）培养目标

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，良好的人文素养、科学素养、职业道德和创新意识，具备“家国情怀、职业素养、工匠精神”和诚信为本的立信职业精神，较强的就业创业能力和可持续发展的能力，掌握本专业知识和技术技能，面向互联网及相关服务、软件和信息服务业的计算机硬件工程技术人员、软件工程技术人员、计算机网络工程技术人员等职业群，能够从事渗透与测试、数据信息安全系统集成、网络安全运维、Web安全管理与评估、数据安全与恢复等工作的高素质技术技能人才。

（二）培养规格

本专业学生应在系统学习专业知识并完成有关实习实训基础上，全面提升素质、知识、能力，掌握并实际运用岗位（群）需要的专业核心技术技能，总体上须达到以下要求：

本专业学生应在系统学习专业知识并完成有关实习实训基础上，全面提升素质、知识、能力，掌握并实际运用岗位（群）需要的专业核心技术技能，总体上须达到以下要求：

1. 坚定拥护中国共产党领导和中国特色社会主义制度，以习近平新时代中国特色社会主义思想为指导，践行社会主义核心价值观，具有坚定的理想信念、深厚的爱国情感和中华民族自豪感；
2. 能够熟练掌握与本专业从事职业活动相关的国家法律、行业规定，掌握渗透测试、等保测评、安全防护、应急响应、软件安全测试及网络安全运维等相关知识与技能，遵守职业道德准则和行为规范，具备社责任感和担当精神，具备良好的立信传统文化认知和职业诚信素养；
3. 掌握支撑本专业学习和可持续发展必备的思想政治理论、中华优秀传统文化、应用文写作、应用数学、外语（英语等）等文化基础知识，具有良好的科学素养与人文素养，具备职业生涯规划能力；
4. 具有良好的语言表达能力、文字表达能力、沟通合作能力，具有较强的集体意识和团队合作意识，学习一门外语（英语等）并结合本专业加以运用；
5. 掌握现计算机科学和网络技术基础，具体包括：
   ① 掌握计算机的硬件组成，包括 CPU、内存、硬盘等关键部件的功能和性能指标。
   ② 理解计算机系统的软件架构，包括操作系统、应用软件等。

③ 熟悉计算机系统的性能指标评价体系。

④ 深入理解 TCP/IP 协议族，掌握各类网络协议的工作原理。

⑤ 熟悉网络通信原理，包括数据传输、路由选择等。

⑥ 能够设计和实施基本的网络拓扑结构，理解不同拓扑结构的优缺点。

6. 掌握本专业技术技能，具有信息安全防护技能与能力，具体包括：

① 精通各类防火墙的配置方法，包括包过滤防火墙、代理服务器等。

② 能够根据网络环境和安全需求，制定防火墙策略并进行优化。

③ 熟练掌握防火墙的日志分析和故障排除技能。

④ 理解 IDS 与 IPS 的工作原理和区别。

⑤ 能够部署和配置 IDS 与 IPS 系统，实时监控网络流量并发现异常行为。

⑥ 熟练掌握 IDS 与 IPS 系统的报警处理和响应机制。

7. 掌握本专业技术技能，具有安全审计和风险评估能力，具体包括：

① 掌握信息系统安全审计的方法和流程。

② 能够使用审计工具对系统进行全面的安全检查。

③ 精通安全审计报告的编写和解读，为组织提供改进建议。

④ 熟悉信息安全风险评估的方法和标准。

⑤ 能够进行定量和定性的风险评估，确定风险级别。

⑥ 制定有效的风险管理策略，包括风险降低、风险转移等。

8. 掌握本专业技术技能，具有渗透测试和网络攻防能力，具体包括：

⑦ Web 渗透测试与防护能力：包括使用特定技术和工具对 Web 应用程序进行安全测试，以发现潜在的安全漏洞，并提供相应的防护措施。

⑧ Web 安全评估能力：涉及 Web 应用程序的安全性进行全面评估，以确定是否存在安全威胁，并制定相应的解决方案。

⑨ 数据存储、备份、灾难恢复及备份方式的能力：包括如何安全地存储和备份数据，以及在数据丢失或损坏时如何迅速恢复数据的技能。

⑩ 网络规划、系统集成、安全管理的技能：涉及如何规划和设计安全的网络系统，包括系统集成和日常安全管理。

⑪ 防病毒系统部署、系统安全加固、数据加密解密、系统升级的综合能力：包括部署防病毒系统、加强系统安全性、加密和解密数据以及进行系统升级等操作的综合能力。

⑫ 信息安全相关软件开发、工具软件应用能力：涉及开发针对信息安全问题的软件解决方案，以及使用工具软件来检测和解决安全问题的能力。

⑬ 安全系统测试文档撰写能力：包括撰写安全系统测试报告和文档，以记录测试过程和结果，并为安全决策提供支持。

9. 具有探究学习、终身学习和可持续发展的能力，具有整合知识和综合运用知识分析问题和解决问题的

能力；

10. 掌握基本身体运动知识和至少 1 项体育运动技能，达到国家大学生体质测试合格标准，养成良好的运动习惯、卫生习惯和行为习惯；具备一定的心理调适能力；

11. 掌握必备的美育知识，具有一定的文化修养、审美能力，形成至少 1 项艺术特长或爱好；

弘扬劳动光荣、技能宝贵 、创造伟大的时代精神，热爱劳动人民、珍惜劳动成果、树立劳动观念、积极投身劳动，具备与本专业职业发展相适应的劳动素养、劳动技能。

六、课程设置及要求

（一）人才培养模式

以党建引领专业建设，坚持立德树人，与龙头企业共建产业学院，以信息安全和“上云数赋智”技术赋能专业建设，将人才培养与产业需求高度契合。开展现代学徒制培养，立足职业教育特征，构建职教本科等多层次纵向贯通的人才培养体系。校企深度合作，构建产业与专业群、技术与课程体系、业务与实践教学体系、企业专家与双师队伍建设、岗位与就业体系、国际业务与国际化人才培养等“六对接”的创新人才培养模式。

1. 校企共建产业学院，实现产业与专业群对接

联合行业领军企业共建产业学院，为学生提供真实业务和环境的实训；开展现代学徒制培养，重点研究大数据、云计算、人工智能等前沿技术在网络安全与信息安全行业的运用，在人才培养和技术技能服务等方面契合财经产业发展，助力财经产业变革和创新。

2. 深化引企入教，实现技术与课程体系的对接

聚焦大数据、云计算、人工智能等新技术，改造传统课程，开发新课程，注重培养学生的信息安全、计算机、互联网思维和能力。按照书证融通、课证融通的思路，对专业相关等课程进行改造和重构，实现学历教育证书与职业技能等证书相融通。利用虚拟仿真、大数据等技术，建成一批技术含量高、共享程度高、辐射带动力强的在线开放课程群、资源群。

3. 开展生产性实习实训，实现业务与实践教学体系的对接

与杭州安恒技术有限公司等行业领军企业，共建共享生产性实训基地，优化和完善网络攻防演练中心、渗透测试演练中心等行业真实场景的实训基地，对应国护及省护，让学生在真实情境中掌握知识，缩短理论知识与实际操作的距离，形成智能化的实践教学体系。

4. 利用企业培训资源，实现企业专家与双师队伍建设的对接

推动与大中型企业合作建设“双师型”教师培养培训基地，实施高层次人才“引聘培组”计划，引进企业领军人才，培育专业带头人和骨干教师，组建高水平的教产学研创新团队。产学研结合，定期安排专业教师下企业实践和挂职锻炼，培养教师“一专多能”，聘请行业企业大师名匠兼职任教，组建具有高超技术的高水平双师队伍。

5. 以产业需求为导向，实现岗位与就业体系的对接

精心设计符合信息安全产业发展趋势的课程体系。课程内容涵盖信息安全理论、技术与应用等多个方面，旨在为学生提供全面的知识结构和技能培养。同时采用多样化的教学方法，如案例分析、模拟演练、项目实战等，让学生在实践中掌握知识，提升能力。把市场供求比例、关联岗位就业质量作为信息安全技术应用专业群结构调整的重要依据，做好与企业人才供求对接。

6. 通过国际交流与合作，实现国际业务与国际人才需求的对接

提升教学科研人员国际素养，增强网络安全师资队伍国际化教学科研水平。对接国际化人才培养标准，建立国际化人才培养机制，满足中国企业境外网络安全人才需求，为企业提供国际化人才支持。

（二）课程体系设计

1. 课程设计及实现路径

基于人才培养模式，实现理论与实践双赋能，通过技术培育与职业素养培育的融合，完成职业发展能力的培养。开发与信息安全行业发展趋势相匹配的课程内容，包括新技术、新标准、新法规，以适应不断变化的行业需求。将信息安全意识、法律法规、伦理道德等元素融入专业课程，培养学生的职业责任感和法律意识。通过技术课程（如网络安全原理、密码学基础、系统安全、数据保护等）和实践课程（如实验室操作、模拟攻击与防御、安全审计等）的结合，提升学生的技术能力和实际操作技能。

2. 专业课程体系设计思路

信息安全技术应用专业面向就业岗位包括渗透测试工程师师、等保测评工程师、信息安全顾问、风险评估师等。课程设计以培养学生的基本职业素质为基础，通过网络安全原理等课程完成对网络安全基础的认知和技能的培养。通过密码学基础、系统安全等课程强化学生的专业知识和技能，通过实验室操作和模拟攻击与防御等课程提高学生的实践能力。通过信息安全管理、安全审计等课程培养学生的综合管理能力和审计评估能力。针对信息安全行业的新趋势，如云计算安全、物联网安全等，设计相应的课程，使学生掌握前沿的安全技术和解决方案。

3. 实践教学体系设计

实践教学体系基于信息安全岗位的核心工作能力设计，按照单项技能训练、综合能力培养和实际案例分析的顺序进行。每一门专业课程都以实际工作任务为导向，通过实验室模拟和案例分析完成单项技能训练。通过企业合作项目、信息安全竞赛等方式，提供综合能力培养的平台，使学生在实际操作中掌握信息安全的关键技能。安排学生参与企业实习，通过真实工作环境中的学习和实践，提高学生的职业技能和就业竞争力。

（三）课程描述

1.公共基础课程

序号	课程名称	学分	学时	课程目标	主要教学内容
1	思想道德与法治（一）-（二）	3	48	1.帮助学生理解马克思主义世界观、人生观、价值观、道德观和法治观的基本原理。 2.帮助学生筑牢理想信念之基，培育和践行社会主义核心价值观，引导学生尊重和维护宪法法律权威，帮助大学生提高思想道德素质和法治素养，成长为自觉担当民族复兴大任的时代新人。	针对新时代大学生成长过程中面临的思想道德和法律问题，主要包括马克思主义人生观、理想信念、中国精神、社会主义核心价值观、社会主义道德观特别是职业道德教育、中国特色社会主义法治观教育等内容。
2	习近平新时代中国特色社会主义思想概论	3	48	1.帮助学生理解习近平新时代中国特色社会主义思想的重大意义、科学体系、丰富内涵、精神实质、实践要求。 2.引导学生深刻理解习近平新时代中国特色社会主义思想贯穿的马克思主义立场观点方法。 3.帮助学生增强“四个意识”、坚定“四个自信”、做到“两个维护”。	主要讲授习近平新时代中国特色社会主义思想及其历史地位、新时代坚持和发展中国特色社会主义的总目标总任务、“五位一体”总体布局、“四个全面”战略布局、全面推进国防和军队现代化、中国特色大国外交、坚持和加强党的全面领导等内容。
3	毛泽东思想和中国特色社会主义理论体系概论	2	32	1.帮助学生准确把握马克思主义中国化的历史进程和理论成果，理解毛泽东思想、邓小平理论、“三个代表”重要思想、科学发展观、习近平新时代中国特色社会主义思想是一脉相承又与时俱进的科学体系。 2.引导学生深刻理解中国共产党为什么能、马克思主义为什么行、中国特色社会主义为什么好，坚定“四个自信”。	以马克思主义中国化为主线，主要讲授马克思主义中国化理论成果的主要内容、精神实质、历史地位、指导意义和实践要求，包括“毛泽东思想”、“邓小平理论、‘三个代表’重要思想、科学发展观”和“习近平新时代中国特色社会主义思想”三个部分。
4	形势与政策（一）-（六）	1	48	帮助学生准确理解党的理论创新最新成果、国内国际形势及党和国家决策部署，引导学生正确认识世界和中国发展大势，正确认识中国特色和国际比较，正确认识时代责任和历史使命，正确认识远大抱负和脚踏实地，坚定“四个自信”。	主要讲授党的理论创新最新成果，新时代坚持和发展中国特色社会主义的生动实践，马克思主义形势观、政策观、党的路线方针政策、基本国情、国内外形势及其热点问题。
5	劳动教育（一）-（二）	1	16	1.提高学生的劳动能力，丰富学生的劳动知识技能，增强学生劳动创新创造技能。 2.教育引导学生树立正确的劳动价值观、崇尚劳动、尊重劳动，培养学生爱岗敬业的工作态度，增强学生责任意识，提升学生综合职业素养。	通过有目的、有计划地组织学生参加日常生活劳动、生产劳动和服务性劳动，实现技术赋能。学生通过自我劳动、义务劳动、勤工俭学、社会实践、志愿服务、企业实践等，让学生动手实践，出力流汗，接受锻炼，磨炼意志。
6	体育与健康(一)-（四）	6	120	通过合理的体育教育和科学的体育锻炼过程，达到增强体质、增进健康和提高学生体育素养，养成良好的行为习惯，形成健康的	健身运动的基本方法和技能；常见运动创伤的处理方法，体能测试和评价体质健康状况；全面发展体能的知识与方

序号	课程名称	学分	学时	课程目标	主要教学内容
				生活方式，培养良好的体育道德和合作精神。	法；人体需要的健康营养食品等。
7	大学生心理健康教育(一)-（二）	2	32	使学生明确心理健康的标准及意义，增强自我心理保健意识和心理危机预防意识，掌握并应用心理健康知识，培养自我认知能力、人际沟通能力、情绪调控能力，挫折应对能力、自我调节能力，切实提高心理素质，培育学生自尊自信、理性平和、积极向上的健康心态，促进学生心理健康素质与思想道德素质、科学文化素质协调发展。	心理学有关理论和基本概念；心理健康的标准及意义；大学阶段人的心理发展特征及异常表现，自我调适等基本知识；心理调适技能、自我探索技能、环境适应技能、生涯规划技能、学习发展技能等。
8	大学生职业生涯规划	1	16	使学生能正确认知自我，了解职业环境和社会需求，树立正确的择业观，掌握求职技巧，提高自身的就业竞争力和职业素养。	职业生涯规划步骤；自我认知的霍兰德人职匹配测试法、MBTI人格特征测试法、技能测试方法以及价值观测试方法和职业测评法；职业认知的生涯人物访谈法、招聘信息分析法；职业目标确立的SMART原则和目标的树型分解法；就业信息的搜集渠道和方法、求职材料的制作和投递方法、笔试及面试流程及技巧；求职过程中常见的侵权、违法行为；就业形势、了解就业政策法规。
9	就业指导	1	16	使学生认识自己，了解职业特性、专业要求和就业形势，帮助学生树立正确的职业理想和择业观念，合理规划自己的职业生涯；通过职业意识的训练与指导，掌握求职择业技巧，提高就业能力和职业素养，为择业、就业和自主创业做好充分的准备。	自我认知的途径和方法；了解职场的元素，认识职场的途径和方法；理解职业生涯规划及做好职业生涯规划对自己学业和人生事业的重大意义；现实的就业形势与政策法规；就业信息搜索方法，求职择业的方法与技巧；就业心理问题自我调适的方法和技巧；入职面试、笔试等的技巧和原则。
10	创新创业教育（一）-（二）	2	32	使学生掌握创新思维、创新技法和创业基础等知识和专业创新实践等技能，提升团队协作和管理、增强创新意识、提高综合素养等方面关键能力，培养学生主动适应国家社会经济发展和人的全面发展需求，正确理解创新与职业生涯发展的关系，树立正确的价值观和就业观。	创新意识的含义、作用及类型；创新与创业的关系；常见的创新技法；创业所需的基本知识；创业者的人格特质；创业精神的内涵和培养方式；创业构想及产生途径；创业团队的概念、成长特征，团队的冲突管理和制定方法；商机识别的主要影响因素和识别过程；商业风险的类型和防范方法；股权融资与债权融资，握融资的渠道，熟悉融资的过程等。

序号	课程名称	学分	学时	课程目标	主要教学内容
11	军事理论与技能训练	3	128	使学生掌握基本军事理论，增强国防观念，国家安全意识，初步掌握我国军事理论的主要内容等知识和军事训练等技能，培养学生学习和独立思考的能力，增强学生的参军报国想法、国防观念、国家安全意识，弘扬爱国主义精神，传承红色基因等方面关键能力，提高学生国防综合能力方面的职业素质。	国防、现代国防含义及类型，我国国防历史和现代化国防建设的现状；国家安全的内涵和原则、世界军事及我国周边安全环境；军事思想的形成和发展过程，我国古代军事思想、毛泽东军事思想、邓小平和江泽民新时期军队建设思想、胡锦涛国防和军队建设思想以及理解习近平强军思想的科学内涵和主要内容；战争的内涵、特点、发展历程，新军事革命的基本内涵、发展演变，机械化战争、信息化战争的形成、主要形态、特征、代表性战例和发展趋势；各国信息化作战平台的发展现状；信息化杀伤武器对现代战争的影响。
12	应用文写作	2	32	使学生掌握职场公务应用文和个人交际交往应用文的基本技能，包括通用类文书、党政公文、商务活动文书、契约文书等文种写作理论知识和写作技巧、文档处理技能，提升逻辑思维、品读、分析、书面交际等方面关键能力，形成具有较强政治素养、恪守法规意识、务实严谨、规范写作的职业素质。	了解应用文的性质、特点、写作基本要求；区别应用语体与文学语体的不同；职场公务处理和个人交往活动中“必需、够用”文种的写作基本理论、写作技巧；能写作规范的应用文；运用各类文种处理事务，解决实际问题。
13	大学英语（一）-（二）	4	64	促进学生英语学科核心素养的发展，培养具有中国情怀、国际视野，能够在日常生活和职场中用英语进行有效沟通的高素质技术技能人才。	英语语音、词汇、语法、语篇和语用知识；英语听、说、读、看、写、译技能；识别、运用恰当的体态语言和多媒体手段；根据语境运用合适的策略，理解和表达口头和书面话语的意义，有效完成日常生活和职场情境中的沟通任务等。
14	智慧财经素养	2	32	使学生掌握国民收入与分配、个人收入、金融投资、消费、社会保障、创新创业、财经法律、国际经济与发展趋势等知识和税务筹划、债务管理、保险规划、财务规划等技能，培养学生家庭财务分析、家庭资产配置、家庭风险管理等方面关键能力，帮助学生形成风险管理意识、懂财经法、懂财务管理的职业素质。	国民经济统计指标的内涵及其相互关系；财政收入、财政支出的含义、形式和分类，财政收入和支出的类别和范围；投资产品的收益和风险；收入的类别；个人或家庭可支配收入计算方法；投资产品的种类和特点；运用无差异曲线和预算约束线分析消费情况；信贷的概念和分类；社会保障的体系结构；社会保险和商业保险的联系与区别；了解保险合同的基本内容；劳动合同的内容，劳动合同解除的相关规定；劳动维权的

序号	课程名称	学分	学时	课程目标	主要教学内容
					途径；生活中遭遇消费侵权与维权；汇率的含义、标价方法、种类，区分直接标价法和间接标价法；影响汇率变动的主要因素以及汇率变动对经济的影响；区块链的定义及常见术语等；

2.专业（技能）课程

序号	课程名称	学分	学时	课程目标	主要教学内容
1	信息安全导论	2	32	1. 加强学生在网络信息安全方面的专业修养。 2. 了解网络信息安全的主要问题、分类和危害机制，并掌握解决这些安全问题的理论、技术和方案。 3. 能够利用所学知识实施和构建自己的安全防范体系和安全系统。 4. 培养学生对信息安全的基本认识和意识，为今后在信息安全领域的学习和工作奠定基础。	1. 信息安全基本概念与原则 2. 信息安全技术 3. 网络安全与防范 4. 系统与应用安全 5. 信息安全管理与风险评估
2	python 程序设计（信息安全）	2	32	1. 掌握Python编程语言的基础知识，包括语法、数据结构和基本算法。 2. 培养学生的逻辑思维能力、算法设计能力和问题解决能力。 3. 提升学生将理论知识应用于实践的能力，以及独立解决问题的能力。	1. Python基础语法 2. 数据结构 3. 函数与模块 4. 面向对象编程 5. 常用库与框架 6. 实战项目与应用
3	Linux 操作系统基础（信息安全）	2	32	1. 了解 Linux 操作系统的基本原理、内核结构和管理方法。 2. 掌握 Linux 操作系统的使用和管理技能，包括系统安装、配置、网络服务设置等。 3. 增强学生的系统安全意识，学会配置和维护系统的稳定性。	1. Linux 系统简介 2. 系统安装与基本配置 3. 文件系统与目录结构 4. 进程管理 5. 内存管理和虚拟存储 6. 网络配置与服务管理 7. 系统安全 8. 软件包管理 9. 系统维护与故障排查

序号	课程名称	学分	学时	课程目标	主要教学内容
4	数字素养	2	32	使学生掌握常用的工具软件和信息化办公技术，了解云计算、大数据、人工智能、物联网、区块链、虚拟现实与元宇宙等新兴信息技术，具备支撑专业学习的能力，能在日常生活、学习和工作中综合运用信息技术解决问题等技能；提升学生信息意识、计算思维、促进数字化创新与发展能力，树立正确的信息社会价值观和责任感，培养学生独立思考和主动探究能力等方面的职业素质。	信息技术对人类生产、生活的重要作用；现代社会信息技术发展趋势；常用的工具软件和信息化办公技术；云计算、大数据、人工智能、物联网、区块链、虚拟现实与元宇宙等新兴信息技术等。
5	应用数学	2	32	1. 掌握集合、不等式、基本初等函数等初等数学知识。 2. 结合“以应用为目的，以必需够用为度”的教学原则，加强对学生应用意识、兴趣、能力的培养。 3. 通过课程学习，培养学生的抽象思维能力、逻辑推理能力、运算能力、空间想象能力以及综合运用所学知识分析问题和解决问题的能力。	1. 微积分 2. 线性代数 3. 计算方法 4. 离散数学 5. 概率论与数理统计 6. 积分变换
6	PHP程序设计	5	92	1. 掌握动态网站开发技术的基本理论； 2. 掌握PHP 程序设计的基本知识； 3. 掌握动态网站 MySQL 数据库的操作； 4. 掌握动态网页的制作流程。	1. PHP开发环境 2. PHP基本语法 3. 目录与文件的操作 4. 组件的应用 5. 使用MYSQL数据库 6. 服务器行为和数据库 7. 编写简单的数据库应用程序
7	信息安全合规指引	2	32	1. 深刻理解信息安全合规的重要性，树立企业运营中的合规意识。 2. 熟悉国内外信息安全的相关法规、标准及合规要求。 3. 通过案例分析和实践操作，提升学生处理信息安全合规问题的能力。 4. 促进职业发展：为学生未来从事信息安全相关工作，特别是合规管理领域，奠定坚实基础。	1. 信息安全合规概述 2. 国内外信息安全法规与标准 3. 信息安全合规管理流程 4. 前沿动态与未来趋势 5. 道德与职业操守
8	密码学基础	2	32	1. 掌握密码学的基本原理、加解密算法和数字签名算法。 2. 理解密码学在现实生活中的应用，如银行、电子商务等领域的信息安全保护。	1. 密码学基本概念 2. 古典密码学 3. 现代密码学基础 4. 密码协议与分析

序号	课程名称	学分	学时	课程目标	主要教学内容
				3. 熟悉密码攻击和防护的基本方法。 4. 能够运用常见算法进行加解密和数字签名操作。 5. 能够评估密码系统的安全性，并了解密码破解的基本原理。	5. 密码攻击与防护 6. 密码学应用 7. 密码学前沿与伦理
9	网络安全协议分析	4	64	1. 能够明确网络安全协议在网络通信中的关键作用，以及它们如何保护数据的机密性、完整性和可用性。 2. 了解各种网络安全协议的工作原理、设计目标和实现方式。 3. 能够将理论知识应用于实际，通过配置和使用网络安全协议来保护网络环境的安全。	1. 网络安全协议基础 2. 主要的网络安全协议 3. 网络安全协议分析 4. 前沿技术和趋势
10	人工智能安全原理	2	32	1. 理解人工智能系统的潜在安全风险和挑战。 2. 学习如何设计和实现安全的人工智能系统。 3. 掌握评估和提高人工智能系统安全性的方法和工具。 4. 培养对人工智能伦理和法律问题的意识。 5. 准备学生应对未来人工智能安全领域的职业需求。	1. 人工智能基础：介绍人工智能的基本概念、原理和应用。 2. 安全理论：探讨人工智能系统中的安全理论，包括数据安全、模型安全、系统安全等。 3. 隐私保护：学习如何在人工智能系统中保护用户隐私和个人信息。 4. 伦理和法律问题：讨论人工智能在伦理和法律层面的问题，如算法偏见、责任归属等。 5. 安全评估方法：教授如何评估人工智能系统的安全性，包括风险评估、漏洞分析等。 6. 安全实践：通过案例研究和实践项目，让学生了解如何在实际中应用安全原理。 7. 政策与法规：了解与人工智能安全相关的政策、法规和标准。 8. 技术趋势与未来展望：分析当前人工智能安全领域的技术趋势，并对未来的发展方向进行展望。

序号	课程名称	学分	学时	课程目标	主要教学内容
11	信创适配	2	32	1. 理解信创适配概念、原理及其在信创产业中的重要作用； 2. 掌握信创适配的核心技术，包括迁移技术、适配测试、性能优化等； 3. 通过实际操作和实验，提升学员在信创适配方面的实践能力； 4. 信创适配过程中进行创新思维，提出新的适配方案和优化策略。	1. 信创适配概述 2. 信创适配技术 3. 适配案例分析 4. 实验操作与实训
12	Web攻防	5	92	1. 掌握web应用常见的攻击手段及防御手段，对网络应用安全技术有深入的了解，具备中小型企业网络安全解决方案实施和维护的能力； 2. 掌握排查和解决企业网中存在的安全隐患和故障； 3. 提高学生的职业素质，促进学生职业能力的培养和职业素养的养成。	1. web安全防护概述 2. web基础原理 3. web应用系统防护技术 4. 网络攻击介绍 5. 单包攻击防御原理 6. 流量型攻击防御原理及解决方案
13	网络安全设备	4	64	1. 掌握网络安全的基本概念、原理和核心技术； 2. 能够分析网络安全威胁、漏洞和风险，提出有效的防范策略； 3. 能够使用网络安全工具和软件，对网络进行安全检测和防护。	1. 通信协议的概念 2. 网络体系结构 3. TCP/IP网络中的数据传输过程 4. 交换机技术 5. 路由器 6. 典型网络拓扑结构
14	网络安全应急响应	4	64	1. 培养学生对网络安全威胁的识别和分析能力。 2. 教授学生如何制定和实施网络安全应急响应计划。 3. 训练学生在网络安全事件发生时，能够迅速采取有效的应对措施。 4. 提高学生的网络安全意识和风险管理能力。 5. 使学生掌握网络安全事件的调查、取证和报告技巧。 6. 培养学生的团队合作能力和沟通技巧，以应对跨部门的网络安全挑战。	1. 网络安全基础：介绍网络安全的基本概念、原理和常见威胁。 2. 风险评估：学习如何评估网络安全风险和确定潜在的漏洞。 3. 应急响应计划：制定网络安全事件的预防和响应策略。 4. 事件识别与分类：教授如何识别和分类不同类型的网络安全事件。 5. 事件响应流程：介绍网络安全事件的响应流程，包括检测、遏制、根除、恢复和后续改进。 6. 取证技术：学习网络安全事件的取证方法和工具，包括数据收集、分析和保存。 7. 法律和合规性：了解网络安全事件响应中的法律要求和合规性问题。

序号	课程名称	学分	学时	课程目标	主要教学内容
					8. 通信与协调：训练学生在网络安全事件中进行有效沟通和协调。 9. 恢复策略：教授如何制定和实施系统恢复计划，以最小化业务中断。 10. 案例研究：通过分析真实世界的网络安全事件，学习应急响应的实际应用。 11. 技术工具与资源：介绍和实践使用各种网络安全工具和资源。
15	数据安全	4	64	1. 使学生了解数据安全技术的基本概念和常见威胁； 2. 掌握数据安全技术的基本原理和方法； 3. 剧本数据安全风险评估和处理的能力； 4. 要求学生能够运用各种数据加密和认证技术，提升数据安全管理水平。	1. 数据安全基础知识 2. 数据加密和解密技术 3. 网络安全和防护措施 4. 数据备份和恢复 5. 社交工程和网络欺诈
16	渗透测试	5	92	1. 理解渗透测试的基本原理和方法； 2. 掌握常见的渗透测试技术和工具； 3. 学会评估和利用系统和应用程序中的漏洞； 4. 培养良好的法律和道德意识，确保渗透测试行为的合法和道德。	1. 网络基础知识 2. 操作系统安全 3. 渗透测试工具和技术 4. 编程和脚本技能
17	网络安全岗位综合实训	2	56	1. 掌握安全岗位所需的基本知识和技能，包括但不限于安全法规、安全操作规程、事故应急处理等方面。 2. 在实际工作环境中运用所学知识和技能的能力，提高其处理安全问题的能力。 3. 增强安全意识，能够主动发现和预防安全事故，提高工作环境的安全水平。	1. 安全法规与标准 2. 安全操作规程 3. 事故应急处理 4. 安全防护与设备使用 5. 安全巡查与记录 6. 安全培训与教育
18	毕业综合项目	3	84	1. 通过毕业综合项目，培养学生的综合应用能力，包括专业知识、实践技能、团队协作、问题解决和创新思维等多方面的能力。 2. 能够将所学的专业理论知识与实际项目相结合，进一步深化对专业知识的理解，提高专业应用水平。 3. 通过项目的实施，锻炼学生的实践能力，包括项目规划、方案设计、实验操作、数据分析、报告撰写等能力。	1. 项目选题与背景研究 2. 专业知识应用 3. 实践能力训练 4. 团队协作与沟通 5. 项目管理与进度控制 6. 成果展示与总结 7. 创新思维培养

序号	课程名称	学分	学时	课程目标	主要教学内容
19	岗位实习	24	576	1. 通过岗位实习，将所学的理论知识与实际工作相结合，加深对专业知识的理解和应用，提高实际操作能力； 2. 培养学生的职业素养，使其能够适应岗位要求，具备良好的职业习惯和职业责任感； 3. 通过实习，提高学生的团队协作和沟通能力，学会与他人合作、分享和协调，以更好地完成工作任务； 4. 培养学生的问题解决能力，使其在面对实际工作中的问题时，能够独立思考、分析问题、提出解决方案，并有效实施； 5. 帮助学生明确自己的职业目标和方向，了解行业发展趋势和岗位需求，为未来的职业规划和发展奠定基础。	1. 岗位基础知识与技能 2. 专业技能应用： 3. 职业素养培养 4. 团队协作与沟通训练 5. 问题解决能力锻炼 6. 职业规划与发展指导
	操作系统安全	2	32	1. 理解操作系统的基本原理：学习操作系统的基本概念，包括进程管理、内存管理、文件系统和设备驱动程序。 2. 掌握安全概念：了解计算机安全的基础概念，如认证、授权、加密、审计和安全策略。 3. 学习安全威胁和攻击类型：识别和理解操作系统可能面临的各种威胁和攻击，包括恶意软件、拒绝服务攻击、缓冲区溢出等。	1. 操作系统基础 2. 密码学 3. 认证和授权 4. 操作系统安全机制 5. 文件系统安全 6. 网络和通信安全 7. 系统漏洞和攻击 8. 安全测试和评估 9. 安全审计和监控
	c 语言程序设计	2	32	1. 掌握 C 语言基础：学习 C 语言的基本语法，包括变量定义、数据类型、运算符、控制结构（如循环和条件语句）以及函数的使用。 2. 理解程序设计原理：培养逻辑思维和算法设计能力，学习如何将复杂问题分解为可管理的编程任务，并使用 C 语言实现这些任务。 3. 实践编程项目：通过实际的编程项目，将理论知识应用于解决实际问题，提高编程技能，增强解决复杂问题的能力。	1. 理解 C 语言基础 2. 编程逻辑与算法 3. 控制结构 4. 函数编程 5. 模块化编程 6. 内存管理 7. 数组和字符串 8. 指针 9. 文件操作 10. 数据结构

序号	课程名称	学分	学时	课程目标	主要教学内容
	网络攻防技术	2	32	1. 理解网络攻击与防御的基础知识：学生应该掌握网络攻击的基本概念、步骤和常用的攻击手段，如信息收集、网络扫描技术、口令破解技术、网络嗅探技术、拒绝服务攻击和恶意程序等。 2. 掌握网络安全防护措施：课程旨在教授学生如何使用各种工具和技术来保护网络，包括防火墙技术、入侵检测系统、VPN 技术、加密技术等。 3. 培养实践应用能力：通过实验室实践和案例分析，学生应能够将理论知识应用于实际的网络攻防场景中，提高解决实际问题的能力。 4. 了解网络攻防的最新技术：课程应该涵盖网络安全领域的最新发展趋势，包括新兴的攻击手段和防御策略，以及网络安全相关的法规和标准。	1. 网络安全基础：介绍网络安全的基本概念、网络安全威胁、网络安全评估、安全事件响应、网络安全模型等。 2. 网络协议安全性：深入探讨网络协议的安全性，包括网际层协议、传输层协议、应用层协议等，以及它们在网络安全中的应用和潜在的安全问题。 3. 密码学理论与应用：学习密码体制的基本原理，包括古典密码、现代密码体制（如 DES、AES、SM4）、密码算法的设计和分析、以及密码协议的安全性分析。 4. 网络攻防技术与实践：包括信息收集技术、口令攻击技术、缓冲区溢出攻击、恶意代码分析、Web 攻击技术、网络嗅探技术、欺骗与会话劫持、拒绝服务攻击、网络渗透技术等。 5. 操作系统安全：涉及操作系统安全机制、账户和组的安全、权限管理、进程与服务的安全等方面。
	软件测试基础	2	32	1. 理解软件测试的基本原理 2. 掌握软件测试的类型和级别 3. 学习测试用例设计技术 4. 理解测试自动化的原理和工具 5. 掌握性能测试和压力测试 6. 学习软件缺陷跟踪和管理 7. 了解软件测试的标准和最佳实践 8. 培养测试计划和测试策略制定能力	1. 软件测试概念 2. 软件开发生命周期 3. 测试类型和级别 4. 测试用例设计 5. 测试自动化 6. 性能测试 7. 安全性测试
	安全工具和技术	2	32	1. 使学生了解计算机通信领域的信息安全技术，包括网络安全的基本原理、安全威胁的类型和来源、以及网络安全管理的基本内容。学生应该理解网络安全的重要性，并了解计算机安全所涉及的法律问题 2. 学生应了解网络攻击和网络入侵带来	1. 网络安全基础 2. 安全工具的使用 3. 应用安全 4. 安全管理 5. 安全法规和标准 6. 实践和案例研究

序号	课程名称	学分	学时	课程目标	主要教学内容
				的问题和危害，掌握常见的网络入侵技术和网络攻击技术，以及安全防范的基本原则和常见的安全检测技术 3. 通过实验室实践和案例分析，提高学生的实践技能，使学生能够将理论知识应用于实际的网络安全管理和维护中	
	Web 应用程序安全测试	2	32	1. 使学生认识到 Web 安全在保护数据和防御网络威胁中的关键作用。 2. 深入了解常见的 Web 应用安全威胁，如 SQL 注入、跨站脚本攻击（XSS）、跨站请求伪造（CSRF）等，以及它们的防御措施。 3. 通过实验和案例分析，培养学生使用各种工具进行 Web 安全测试的能力，如使用 Burp Suite、Nmap、Metasploit 框架等。 4. 通过实际的 Web 应用安全问题案例，训练学生分析和解决 Web 安全问题的能力。 5. 教育学生如何在 Web 应用开发和维护过程中实施安全最佳实践和防护措施。	1. Web 应用安全威胁 2. 安全测试方法 3. 安全测试工具 4. 安全配置和审计

3.专业（群）平台课程

序号	课程名称	学分	学时	课程目标	主要教学内容
1	计算机网络技术	2	32	1. 掌握计算机网络基本原理和关键技术。 2. 培养学生熟悉网络协议的设计和实现。 3. 理解网络安全和隐私保护的原理，使其能进行网络安全的评估与防护。 4. 增强学生的团队协作和沟通能力，以便其能有效解决实际网络问题。	1. 计算机网络基础 2. 局域网技术 3. 网络操作系统 4. 网络安全与隐私保护 5. 网络设计与管理
2	Web 前端开发	2	32	1. 能够熟练掌握 HTML5、CSS3、JavaScript 等前端开发技术。 2. 提高学生的动手能力和解决问题的能力。 3. 培养学生的团队协作能力、沟通能力以及创新精神，以适应不断变化的市场需求。	1. HTML5 与 CSS3 基础 2. JavaScript 编程 3. 前端框架与库 4. 响应式设计与移动端开发

序号	课程名称	学分	学时	课程目标	主要教学内容
3	数据库应用技术	2	32	1. 掌握数据库基础知识：使学生全面了解数据库的基本概念、原理和应用。 2. 够熟练使用 SQL 语言进行数据查询、更新和管理。 3. 理解数据库设计的基本原则，并能够对数据库系统进行基本的维护和优化。 4. 增强数据安全意识	1. 数据库基础 2. 数据库管理系统（DBMS）介绍 3. SQL 语言 4. 数据库设计 5. 数据库管理 6. 实践应用

4.专创赛证融通课程

序号	课程名称	学分	学时	课程目标	主要教学内容
1	HCIA-openEuler	2	32	1. 掌握 openEuler 操作系统的基本原理、设计方法和实际应用。 2. 提升学生的动手能力和问题解决能力，使其能够熟练运用操作系统知识解决实际软件工程问题。 3. 通过了解我国科技工作者在操作系统领域的努力和成果，激发学生的民族自豪感和开发基础软件的信心。 4. 岗课赛证融合，为学生多渠道高质量就业提供支持。	1. Linux 及 openEuler 基础 2. 文件系统与文本处理 3. 用户管理与权限设置 4. 网络管理与进程控制 5. 软件包管理与服务配置 6. 磁盘管理与 LVM 技术 7. Shell 编程基础 8. 系统启动与故障排除
2	NISP 二级	2	32	1. 掌握网络安全的基础知识和技能，包括密码技术、鉴别与访问控制、操作系统安全、数据库安全、网络安全、应用安全等。 2. 能够独立建立、完善和优化企业信息安全制度和流程。 3. 能够跟踪和验证安全措施的实施，建立起立体式、纵深的安全防护系统，并能进行安全监控，对未知的安全威胁进行预警和追踪。	1. 信息安全基础 2. 网络安全技术 3. 信息安全工程与管理 4. 信息安全法规与道德规范 5. 应急响应与灾难恢复 6. 实践操作与技能提升
3	1+x 企业网络安全防护（中级）	2	32	1. 掌握网络安全防护技能：学员能够掌握企业网络安全防护的核心技术和方法，提升网络安全防护能力。 2. 能够独立完成网络安全配置、管理和应急响应等任务。 3. 提高学员对网络安全重要性的认识，培养防范网络威胁的意识和能力。	1. 系统安全配置 2. 网络安全设备配置 3. 应用安全配置 4. 数据库安全 5. 网络安全管理与应急响应 6. 日志分析与审计 7. 应急响应计划 8. 网络安全法律法规与合规性

七、教学进程总体安排

（一）教学进程安排

2024级信息安全技术应用专业教学进程安排表

生源类别:(现代学徒制/全日制/订单班/特色班）　专业群：信息安全技术应用专业群　　学制:三年

课程属性	课程性质	课程模块	课程编码	课程名称	学分	总学时	课时分配表		考核方式	周学时/教学周数						开课学院	课程说明
							理论学时	实践学时		一	二	三	四	五	六		
公共基础课程	必修课	思想政治理论模块		思想道德与法治（一）-（二）	3	48	32	16	考查	1.5	1.5					马院	
				毛泽东思想和中国特色社会主义理论体系概论	2	32	24	8	考查		2					马院	
				习近平新时代中国特色社会主义思想概论	3	48	32	16	考查			3				马院	
				形势与政策（一）-（六）	1	48	32	16	考查	讲4	讲4	讲4	讲4	实践	实践	马院	根据教社科〔2018〕1号文件规定《形势与政策》专科每学期不低于8学时，共计1学分。其中1-4学期为课堂教学，5-6学期为实践教学。
		思想政治理论模块小计			**9**	**176**	**120**	**56**		**1.5**	**3.5**	**3**	**0**	**0**	**0**	**0**	
		通识课程模块		体育与健康（一）-（四）	6	120	8	112	考查	2	2	①	①			基础	
				大学生心理健康教育（一）-（二）	2	32	32		考查	1	1					学工	
				大学生职业生涯规划	1	16	8	8	考查	1						学工	
				就业指导	1	16	8	8	考查				1			学工	
				创新创业教育（一）-（二）	2	32	16	16	考查	1	1					创院	第一学期开设创新创业教育理论，第二学期开设创新创业教育实践

				军事理论与技能训练	3	128	16	112	考查	1						学工	
				劳动教育（一）-（二）	1	16	8	8	考查	0.5	0.5					总务	
				应用文写作	2	32	16	16	考试			2				基础	
				大学英语（一）-（二）	4	64	32	32	考试	2	2					基础	
				数字素养与技能	2	32	16	16	考查	2						数技	
				智慧财经素养												数金	
		通识课程模块小计			**24**	**488**	**160**	**328**		**10.5**	**6.5**	**2**	**1**	**0**	**0**	**0**	
		公共实践课模块		第二课堂	4	--		--	考查	①	①	①	①			学工	根据《共青团广东财贸职业学院委员会“第二课堂成绩单”制度实施办法（2024年修订）》（粤财院〔2024〕13号）执行。
	公共必修课合计				**37**	**664**	**280**	**384**		**12**	**10**	**5**	**1**	**0**	**0**	**0**	
	公共选修课	公共选修课模块		中共党史、新中国史、改革开放史、社会主义发展史、国家安全教育、节能减排、绿色环保、金融知识、社会责任、人口资源、海洋科学、管理、人文素养、科学素养、中华优秀传统文化、音乐鉴赏、摄影技巧、舞蹈表演、初级版画、毛笔书法、硬笔书法、艺术概论、合唱基础等	2	32	32		考查		2					马院学工基础数创等	公共选修课至少需修满6学分，美育类课程至少2学分。此外，学生必须从中共党史、新中国史、改革开放史、社会主义发展史、国家安全教育、中化优秀传统文化等课程中选修一门。
					2	32	32		考查			2					
					2	32	32		考查				2				
					2	32	32		考查					2			
	公共选修课模块小计				**6**	**96**	**96**	**0**		**0**	**2**	**2**	**2**	**2**	**0**		**额定6学分**
公共基础课合计					**43**	**760**	**376**	**384**		**12**	**12**	**7**	**3**	**2**	**0**		
专业（技能）课程	必修课	专业群平台课模块		计算机网络技术	2	32	16	16	考试	2						数技	
				Web前端开发	2	32	16	16	考试	2						数技	
				数据库应用技术	2	32	16	16	考试		2					数技	

		专业群平台课模块小计		**6**	**96**	**48**	**48**		**4**	**2**	**0**	**0**	**0**	**0**		
	专业基础课模块		信息安全导论	2	32	16	16	考查	2						数技	
			python 程序设计（信息安全）	2	32	16	16	考试	2						数技	
			Linux 操作系统基础（信息安全）	2	32	16	16	考试		2					数技	
			数字素养	2	32	16	16	考查	2						数技	
			应用数学	2	32	16	16	考试		2					基础	
			PHP 程序设计	5	92	32	60	考试		4					数技	4 课时+1 个实训周
			信息安全合规指引	2	32	16	16	考查		2					数技	
			密码学基础	2	32	16	16	考试			2				数技	
			网络安全协议分析	4	64	32	32	考试				4			数技	
			人工智能安全原理	2	32	16	16	考查			2					
		专业基础课模块小计		**22**	**364**	**168**	**196**		**6**	**10**	**4**	**3**	**0**	**0**		
	专业核心课模块		*信创适配	2	32	16	16	考查			2				数技	
			*Web 攻防	5	92	32	60	考试			4				数技	4 课时+1 个实训周
			*网络安全设备	4	64	32	32	考试			4				数技	
			*网络安全应急响应	4	64	32	32	考查				4			数技	
			*数据安全	4	64	32	32	考试				4			数技	
			*渗透测试	5	92	32	60	考试				4			数技	4 课时+1 个实训周
		专业核心课模块小计		**24**	**408**	**176**	**232**		**0**	**0**	**10**	**12**	**0**	**0**		
	专业实践模块		网络安全岗位综合实训	2	56		56	考查					②		数技	
			毕业综合项目	3	84		84	考查						③	数技	
			岗位实习	24	576		576	考查					④	⑳	数技	
		专业实践模块小计		**29**	**716**	**0**	**716**		**0**	**0**	**0**	**0**	**0**	**0**		
	专业必修课合计			**81**	**1584**	**392**	**1192**		**10**	**12**	**14**	**16**	**0**	**0**	**0**	**0**
专业选修课	渗透测试模		操作系统安全	**2**	32	16	16	考查		**2**					数技	专业限选课分为 2 个模块，每一个模块对应一个职业岗位，学生可以根据意向选择任一模块进行学习，选择其中一个模
			C 语言程序设计	**2**	32	16	16	考查			**2**				数技	
			网络攻防技术	**2**	32	16	16	考查				**2**			数技	

块															块后需要完成该模块全部三门课程学习，不可再选其他模块课程
软件安全测试模块		软件测试基础	2	32	16	16	考查		2					数技	
		安全工具和技术	2	32	16	16	考查			2				数技	
		Web 应用程序安全测试	2	32	16	16	考查				2			数技	
专业限选课模块小计			**6**	**96**	**48**	**48**		**0**	**2**	**2**	**2**	**0**	**0**	**0**	
专创赛证融通课模块		HCIA-openEuler	2	32	16	16	考查		2					数技	额定 6 学分，提供若干门专创赛证融通课程
		NISP 二级	2	32	16	16	考查			2				数技	
		1+x 企业网络安全防护（中级）	2	32	16	16	考查				2			数技	
				0											
专创赛证融通课模块小计			**6**	**96**	**48**	**48**		**0**	**2**	**2**	**2**	**0**	**0**		
专业选修课合计			**12**	**192**	**96**	**96**		**0**	**4**	**4**	**4**	**0**	**0**	**0**	**额定 12 学分**
专业（技能）课程合计			**93**	**1776**	**488**	**1288**		**10**	**14**	**16**	**18**	**0**	**0**		
总计（总学分/总学时）			139	2584	888	1696		22	26	23	21	2	0		

（二）教学学时分配

各类课程学分学时比例表

课程属性	课程性质	课程模块	小 计		小 计	
			学 分	比 例	学时	比 例
公共基础课程	必修课	思想政治理论模块	9	6.47%	176	6.81%
		通识课程模块	24	17.27%	488	18.89%
		公共实践课模块	4	2.88%	0	0.00%
	公共选修课	公共选修课模块	6	4.32%	96	3.72%
合计			43	30.94%	760	29.41%
专业（技能）课程	必修课	专业群平台课模块	6	4.32%	96	3.72%
		专业基础课模块	25	17.99%	412	15.94%
		专业核心课模块	24	17.27%	408	15.79%
		专业实践课模块	29	20.86%	716	27.71%
	专业选修课	专业限选课模块	6	4.32%	96	3.72%
		专创赛证融通课模块	6	4.32%	96	3.72%
合计			96	69.06%	1824	70.59%
总计			139	100%	2584	100%
实践教学学时			1696			
实践教学学时占总学时比（%）			65.63%			
公共基础类课程学时占总学时比（%）			25.70%			
选修课学时占总学时比（%）			11.15%			

（三）教学学历周安排

学年	学期	教学周		机动安排（含改卷、集中实训等）	入学教育（含军训）	合计
		课程教学(含实训)	考试			
一	一	14	1	1	2	18
	二	18	1	1	0	20
二	三	18	1	1	0	20
	四	18	1	1	0	20
三	五	20	0	0	0	20
	六	20	0	0	0	20
合计		**112**		**4**	**2**	**118**

八、实施保障

（一）校企合作

建立与杭州安恒信息技术有限公司等龙头企业深度融合的协同、协作机制。建立红蓝攻防实训基地、信创适配实训中心等，联合开发专业课程，共同制定人才培养方案，共同举办师资培训，实现校企协同育人和协作创新。校企深度合作，实现企业实战课堂。在深化网络安全课程建设的过程中，进一步延伸引企入校的理念，与企业合作，转换教学场景，构建职业化氛围，探索校企双师授课的模式。

（二）师资队伍

1.队伍结构

学生数与本专业专任教师数比例为120:1，双师素质教师占专业师比为100%，专任教师队伍职称、年龄结构合理，形成合理的队伍结构。专业部分师资列表如下：

序号	姓名	年龄	职称	学位	双师状况
1	项尚清	50	讲师	硕士	是
2	孟威	40	助教	工学硕士	是
3	毛颖	42	讲师	管理学硕士	是
4	吴建立	28	软件设计师	工学学士	是
5	黄纯	43	大学讲师	工学硕士	是
6	唐剑雄	34	通信工程师	工学学士	是
7	张英	25	网络工程师	工学学士	是
8	高燚	41	工程师	工学硕士	是
9	张素金	27	无	工学学士	是

2.专任教师

具有高校教师资格和本专业领域有关证书；有理想信念、有道德操、有扎实学识、有仁爱之心；具有网络安全相关专业本科及以上学历；有扎实的本专业相关理论功底和实践能力；

具有较强的信息化教学能力，能够开展课程教学改革和科学研究；每5年累计不少于6个月的企业实践经历。

3.专业带头人

专业带头人能够较好地把握国内外行业、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需求实际，课程体系设计、专业研究能力强，组织开展教科研工作能力强，在本区域或领域具有一定的专业影响力。

4.兼职教师

主要从相关行业企业聘任，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，具有行业中级及以上职称，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。

（三）教学设施

1.校内实训基地

按照“职业化、智能化、共享化”的标准和要求建设实训环境，学院为课程提供环境支撑，建设了多个实训基地，包含红蓝攻防实训基地、“麒麟工坊”实训基地、商业信息安全赋能中心等实训场所。满足网络安全基本技能训练、渗透测试职业能力训练、网络安全技能比赛、信创适配等课程的教学需要。

序号	实践基地名称	主要项目名称
1	红蓝攻防实训基地	网络安全攻防演练
2	“麒麟工坊”实训基地	信创适配
3	商业信息安全赋能中心	网络安全虚拟仿真设备

部分实训室功能如下：

红蓝攻防实训基地：营造仿真网络安全攻防环境，基于红队角色攻击演练场景，基于蓝队网络安全防护及应急响应演练场景，以行业岗位为依据，为学生提供真实的网络安全攻防演练实训。

麒麟工坊”实训基地：为国家培养急需紧缺的国产操作系统专业技术人才。通过实训基地，可以系统地对学生进行国产操作系统的培训和实践，以满足国家对这方面人才的需求。通过实训基地，学生可以参与到各种实践项目中，如实验室实训、训练营、项目实战等，从而积累更多的实践经验，为未来的职业发展打下坚实的基础。

商业信息安全赋能中心：配置教学及竞赛靶场，互联网接入环境。支持网络安全及信息安全类专业课程实训。

2.校外实训基地

具有稳定的校外实训基地。能够提供开展网络安全及信息安全专业相关实训活动，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。能提供渗透测试、应急响应等相关实习岗位；能涵盖当前信息安全技术应用专业的主流实务，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。专业实习实训的校外实训基地包括：杭**州安恒信息技术股份有限公司、云仓库(广东)信息科技有限公司、广州云图腾科技有限公司等**。

3.学生实习基地基本要求

具有稳定的校外实习基地。能提供渗透测试、应急响应等相关实习岗位；能涵盖当前信息安全技术应用专业的主流实务，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。

4.支持信息化教学基本要求

具有利用数字化教学资源库、文献资料、常见问题解答等的信息化条件。引导鼓励教师开发并利用信息化教学资源、教学平台，创新教学方法、提升教学效果。

（四）教学资源

主要包括能够满足学生学习、教师教学和科研等需要的教材、图书资料以及数字资源等。

1.教材选用

按照国家规定选用优质教材，禁止不合格的教材进入课堂。学校建立了由专业教师、行业专家
和教研人员等参与的教材选用机构，完善教材选用制度，经过规范程序择优选用教材。鼓励校企共同编制教材，教材编写与产业需求、岗位职业标准和1+X证书标准对接，契合模块化课程，打造立体化活页式教材。专业使用的部分教材包括：

课程名称	教材名称	出版社	备注
计算机网络技术	计算机网络技术（第八版）	大连理工大学出版社	教育部规划
Linux 操作系统基础（信息安全）	Linux 操作系统及应用（第五版）	大连理工大学出版社	教育部规划
PHP 程序设计	PHP 基础案例教程（第 2 版）	人民邮电出版社	行业统编
web 攻防	web 应用安全与防护	电子工业出版社	行业统编
网络安全设备	网络设备配置与管理（第 2 版）	电子工业出版社	行业统编

课程名称	教材名称	出版社	备注
数据安全	数据安全与流通——技术、架构与实践	机械工业出版社	行业统编
渗透测试	渗透测试基础教程	人民邮电出版社	行业统编
信创适配	信息技术应用创新导论	高等教育出版社	行业统编

2.图书文献配备

图书文献配备能满足人才培养、专业建设、教科研等工作的需要，方便师生查询、借阅。专业
类图书文献包括：有关信息安全技术应用专业理论、技术、方法、思维以及实务操作类图书。

3.数字教学资源

建设、配备与本专业有关的音视频素材、教学课件、数字化教学案例库、虚拟仿真软件、数字教材等专业教学资源库，种类丰富、形式多样、使用便捷、动态更新、满足教学。部分在线课程如
下表。

课程	上线平台
Web 攻防	商业信息安全赋能中心教学平台
渗透测试	商业信息安全赋能中心教学平台
网络安全设备	商业信息安全赋能中心教学平台

（五）教学方法

1.推行基于业务场景的行动导向教学。借鉴新加坡教学工厂的教学模式，倡导“在业务场景中学理论，在理论应用中强实践”的教学理念，开发以职业为导向的专业课程，以网络安全攻防业务场景驱动信息安全课程学习。通过仿真实训式课程将工作任务与知识性学习有机串联，变革学生角色，让学生以“职业人”的身份在企业工作环境中自主工作、独立学习、共同研究。

2.利用信息技术，实现智慧课堂和移动课堂。借助校内财贸在线平台和校外学习通、雨课堂、语雀等移动教学平台，利用校内智慧教室、商业信息安全赋能中心等智慧学习空间，实施线上线下混合式教学，达到“简、通、活”的课堂教学效果：师生通过简单的操作，转换手机、投屏、终端等多种学习工具，就能实现课堂互动，达到课前、课中、课后、课外的环环相通，通过随机抢答、弹幕等工具激活课堂氛围，将“低头族”学生变为课堂学习的主体。

（六）学习评价

建立“主体多元，成效导向、过程评价”的全过程闭环学习评价模式。

1.主体多元

探索与实践校企“双主体”评价及“能力+素养”双分测评，即“能力学分、素养积分”并行的综合能力评价机制。同时，在课程内部建立多元评价机制。在会计岗位综合实训等课程中，按分岗的要求组织教学，过程性评价，按照组员自评、小组互评、教师评价三种方式进行加权综合评价。

2.成效导向

在课程中实施以职业能力考核为主线的评价方法，使工作成果与学业评价有机结合。在Web攻防等课程中，通过商业信息安全赋能中心教学平台和组织专业能力考试，实现教考分离，提高了学业评价的科学性与客观性。

3.过程评价

在主要实训课程中，注重过程性考核和结果性考核相结合，强化过程性考核。

（七）质量管理

1.学校专门成立了教学督导与评价中心，组建了专业建设与教学指导委员会，建立了专业建设和教学质量诊断与改进机制，健全了专业教学质量监控管理制度，完善了课堂教学、教学评价、实习实训、毕业设计以及专业调研、人才培养方案更新、资源建设等方面质量标准建设，通过教学实施、过程监控、质量评价和持续改进，达成人才培养规格。

2.学校和二级学院完善教学管理机制，加强日常教学组织运行与管理，定期开展课程建设水平和教学质量诊断与改进，建立健全巡课、听课、评教、评学等制度，建立与企业联动的实践教学环节督导制度，严明教学纪律，强化教学组织功能，定期开展公开课、示范课等教研活动。

3.学校建立了毕业生跟踪反馈机制及社会评价机制，并对生源情况、在校生学业水平、毕业生就业情况等进行分析，定期评价人才培养质量和培养目标达成情况。

4.专业教研组织充分利用评价分析结果有效改进专业教学，持续提高人才培养质量。

（八）继续学习深造建议

本专业学生可以继续完成本科深造，亦可通过考试取得注册信息安全专业人员、信息安全管理师等专业证书提升专业能力。

九、毕业要求

学生在规定年限内，满足以下条件，可以获得毕业证书：

（1）学分

学生须在规定年限内获得专业人才培养方案所规定课程的学分，且总学分达139学分（含）以上。

（2）体质测试

根据教育部关于印发《国家学生体质健康标准（2014年）修订》的通知（教体艺〔2014〕5号）文件要求，体质测试成绩达不到50分者按结业处理，如因病或残疾学生，可凭医院证明向学校提出申请并经审核通过后可准予毕业。

（3）德智体美劳全面发展

学生素质、知识、能力达到本专业人才培养目标和培养规格的要求。

（4）职业资格（技能等级）证书

鼓励学生获取与职业能力要求相匹配的职业资格（技能等级）证书（含1+X证书）、职业素质证书。

十、方案编制人员

编制参与人：项尚清、孟威、吴建立、唐剑雄、张英、王幸涛

校内：项尚清、孟威、吴建立、唐剑雄、张英

校外：王幸涛

编制执笔人：孟威

编制负责人：孟威

审核人：

学院论证：数字技术学院专业建设与教学指导委员会

学校论证：广东财贸职业学院专业建设与教学指导委员会

审定：广东财贸职业学院党委会

审定日期：2024年9月9日

十一、附录

（一）典型工作任务职业能力分析表

工作项目		工作任务		职业能力		学习水平
项目编号	项目名称	任务编号	任务名称	能力编号	能力名称	高职Li
01	目标信息收集	01-01	确定目标范围	01-01-01	能够准确定义渗透测试的目标，包括要测试的系统、网络、应用程序等	L1
				01-01-02	能够避免越权测试和对不相关资源的干扰	L2
		01-02	网络信息收集	01-02-01	能够使用工具（如Sublist3r、Amass等）查找目标组织的域名和子域名	L1
				01-02-02	能够通过工具（如Nmap、Masscan等）扫描目标组织的IP地址范围，确认存活的主机和开放端口	L1
		01-03	域名和IP信息	01-03-01	能够利用Whois查询获取域名注册信息，如域名所有人、注册日期等。	L1
				01-03-02	能够通过DNS查询了解域名解析信息	L1
		01-04	分析网络拓扑	01-04-01	能够借助网络扫描和Traceroute等工具，探明目标网络的结构、服务器位置等	L2
		01-05	社会工程学信息收集	01-05-01	能够通过搜索引擎、社交媒体等渠道收集关于目标的信息，如员工详情、组织架构等。	L2
		01-06	查询漏洞信息	01-06-01	能够使用漏洞数据库（如CVE、NVD等）查询目标系统、应用程序的已知漏洞	L1
		01-07	服务指纹识别	01-07-01	能够利用工具识别目标主机上运行的服务和应用程序版本信息	L1
		01-08	开源情报(OSINT)收集	01-08-01	能够利用开源情报工具和技术，查找关于目标的公开信息，如泄露的凭据等	L1
02	漏洞扫描与发现	02-01	扫描工具	02-01-01	能够根据测试需求和目标系统的特点，选择合适的漏洞扫描工具。这些工具可以自动化地检测系统中的安全漏洞。	L1
		02-02	配置扫描参数	02-02-01	能够根据目标系统的具体情况，配置扫描参数，如扫描范围、扫描深度、漏洞类型等。	L1
		02-03	执行漏洞扫描	02-03-01	能够利用选定的扫描工具对目标系统进行全面的漏洞扫描。这包括对网络服务、操作系统、应用程序等的扫描。	L1
		02-04	分析扫描结果	02-04-01	能够仔细分析扫描结果，识别出系统中的潜在漏洞。这需要对漏洞扫描报告进行详细的解读和评估	L1
		02-05	验证漏洞	02-05-01	能够对于扫描出的潜在漏洞，需要进行进一步的验证，以确保其真实性。这通常涉及手动测试或利用专门的验证工具。	L3
		02-06	评估漏洞	02-06-01	能够对验证后的漏洞进行分类和评估，确定其严重性和可能对系统安全造成的影响。这有助于后续的漏洞修复工作	L1
03	漏洞验证与利用	03-01	漏洞验证准备	03-01-01	能够分析漏洞扫描阶段得到的结果，确定需要验证的漏洞列表	L3
				03-01-02	能够根据漏洞的性质和类型，制定验证计划和方案	L1
		03-02	环境搭建与模拟	03-02-01	能够避免对实际生产环境造成影响，在沙盒或测试环境中模拟漏洞存在的条件	L2
				03-02-02	能够配置与目标系统相似的测试环境，以确保验证的准确性	L2
		03-03	漏洞验证	03-03-01	掌握手动测试、自动化脚本或专用工具对漏洞进行实际验证的能力	L3

工作项目		工作任务		职业能力		学习水平
项目编号	项目名称	任务编号	任务名称	能力编号	能力名称	高职Li
				03-03-02	能够复现漏洞，确认其存在并评估其可利用性	L3
		03-04	漏洞利用	03-04-01	能够确认存在的漏洞，进行实际的利用尝试，以评估其对系统安全性的真实威胁	L2
				03-04-02	能够根据漏洞类型，采用不同的利用技术，如SQL注入、跨站脚本攻击（XSS）、远程命令执行等	L2
		03-05	绕过安全机制	03-05-01	能够在漏洞利用过程中，绕过目标系统的某些安全防护措施，如防火墙、入侵检测系统（IDS）或安全软件	L1
				03-05-02	能够测试并识别这些安全机制的弱点，以便成功利用漏洞	L2
		03-06	数据收集与回传	03-06-01	能够在验证和利用漏洞的过程中，收集有关目标系统的敏感信息，如用户数据、配置文件、数据库凭据等	L1
				03-06-02	能够将收集到的数据安全地回传到测试人员的控制服务器，以便进一步分析	L1
		03-07	清理测试痕迹	03-07-01	能够在测试结束后，确清理所有测试过程中留下的痕迹，包括上传的文件、创建的账户、修改的配置等。	L2
				03-07-02	能够恢复目标系统到测试前的状态，以避免对后续操作造成干扰。	L2
04	权限提升与横向移动	04-01	权限提升	04-01-01	能够根据目标系统的具体情况，选择合适的提权技术，如利用操作系统漏洞、配置错误、弱密码等	L1
				04-01-02	能够利用已识别的漏洞或配置弱点，尝试提升攻击者的权限级别，从普通用户提升至管理员或更高权限	L1
				04-01-03	能够验证权限是否成功提升，例如尝试访问之前无法访问的资源或执行更高权限的操作	L1
		04-02	横向移动	04-02-01	能够在获得初始访问权限后，探测目标网络的拓扑结构，了解其他可能的目标系统。	L3
				04-02-02	能够在Windows环境中利用IPC$等共享资源进行横向移动，访问其他主机上的文件和服务	L3
				04-02-03	能够通过远程命令执行工具（如PsExec、WMI等）在远程主机上执行命令，实现横向移动。	L3
				04-02-04	能够使用专门的内网渗透工具（如Meterpreter、Empire等）来自动化横向移动的过程	L2
				04-02-05	能够在成功横向移动到其他系统后，留下后门以确保未来能够持久化访问	L2
05	数据窃取与篡改尝试	05-01	数据窃取	05-01-01	能够明确测试的目标，确定需要窃取的数据类型，如用户个人信息、财务数据、敏感业务数据等	L1
				05-01-02	能够通过信息收集和侦查，定位存储目标数据的数据库、文件服务器或云存储位置	L1
				05-01-03	能够利用已获得的权限或提升后的权限，尝试访问存储目标数据的系统或数据库。	L1
				05-01-04	能够根据数据的存储方式和系统的安全机制，选择合适的数据窃取技术，如SQL注入、文件包含漏洞利用等	L2
				05-01-05	能够在不触发警报或不影响系统正常运行的前提下，秘密地将目标数据复制或传输到测试人员控制的服务器上。	L2
		05-02	数据篡改	05-02-01	能够明确测试的目标，确定需要篡改的数据类型，如用户信息、交易记录、系统配置等	L1
				05-02-02	能够定位目标数据的位置，并获取修改这些数据的必要权限	L1
				05-02-03	能够根据测试目的和系统的特性，制定数据篡改的策略，如修改用户余额、更改交易状态等。	L2
				05-02-04	能够在确保不会造成系统崩溃或数据丢失的前提下，对目标数据进行篡改	L2
				05-02-05	能够验证数据篡改是否成功，并观察系统对篡改数据的反	L3

工作项目		工作任务		职业能力		学习水平
项目编号	项目名称	任务编号	任务名称	能力编号	能力名称	高职Li
					应，如是否触发警报、是否影响系统正常运行等。	
				05-02-06	能够在测试结束后，将数据恢复到原始状态，确保不会对系统的正常运行造成影响	L2
06	编写渗透测试报告	06-01	整理和分析测试数据	06-01-01	能够在渗透测试完成后，对测试过程中收集的数据进行整理和分析。包括整理测试过程中的截图、漏洞报告、渗透测试结果等信息。	L1
		06-02	确认漏洞修复情况	06-02-01	能够在编写报告之前，确认哪些漏洞已经被修复，并在报告中更新这些信息。如果漏洞已经修复，需要提供相应的证据	L1
		06-03	确定报告格式和排版	06-03-01	能够选择清晰简洁的设计来确保报告的易读性，并避免使用过多的技术术语和缩写，使得报告更易于被非技术背景的管理人员理解。	L1
		06-04	撰写报告	06-04-01	报告通常包括简介、测试方法、测试结果、安全建议和总结等部分。其中，简介部分介绍测试背景、目的和范围等；测试方法部分描述测试的具体方法和工具；测试结果部分列出发现的漏洞和安全隐患；安全建议部分提供针对测试结果的改进建议；总结部分对整个测试过程进行评估。	L1
		06-05	审核报告的准确性和可靠性	06-05-01	能够在提交报告之前，对报告的准确性和可靠性进行仔细审核。这包括对测试数据和分析结果的确认，以及对漏洞修复情况的核实。	L1
07	安全策略制定	07-01	全面评估安全风险	07-01-01	能够对组织的信息系统和数据进行全面的安全风险评估。包括对网络、服务器、应用程序以及员工行为等方面的评估，以了解并量化这些风险，为制定有效的安全策略提供依据。	L1
		07-02	制定安全策略	07-02-01	能够评估安全风险之后，针对各种威胁制定恰当的安全策略。如设置网络防火墙、入侵检测系统和数据加密等	L1
		07-03	法务合作	07-03-01	能够在制定安全策略的过程中与法务团队紧密合作，确保制定的安全策略符合适用的法律法规和行业合规要求。这有助于避免因违反法律规定而给组织带来不必要的法律风险。	L1
08	数据分类与分级保护	08-01	数据分类	08-01-01	能够深入了解业务、业务流程和数据资产，以便准确地对数据进行分类。	L1
				08-01-02	能够确定分类标准根据数据的性质、用途和敏感性，制定合理的数据分类标准。例如，可以将数据分为公开、机密、绝密等类别。	L2
				08-01-03	能够实施分类操作依据分类标准，对组织内的数据进行分类，并确保分类的准确性和一致性。	L1
		08-02	数据分级保护	08-02-01	评估数据价值对分类后的数据进行价值评估，确定数据的重要性级别，如核心数据、重要数据和一般数据。	L2
				08-02-02	能够制定分级保护措施，根据数据的不同级别，制定相应的保护措施。例如，对于核心数据，可能需要采取最严格的访问控制和加密措施。	L2
				08-02-03	能够监控和调整保护策略，定期检查和评估分级保护策略的有效性，根据需要进行调整和优化。	L2
		08-03	合规性和政策遵循	08-03-01	能够确保数据分类和分级保护工作符合相关法律法规的要求，如《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等。	L1
				08-03-02	能够跟踪数据安全领域的最新动态和政策变化，及时调整数据分类和分级保护策略，以确保合规性。	L1
09	数据安全风险评估	09-01	制定数据安全评估	09-01-01	能够确定评估的目标、范围和具体方法，明确评估的重点和步骤。	L1

工作项目		工作任务		职业能力		学习水平
项目编号	项目名称	任务编号	任务名称	能力编号	能力名称	高职Li
			计划	09-01-02	能够规划所需资源和时间，确保评估过程的顺利进行。	L1
		09-02	进行系统漏洞扫描与分析	09-02-01	能够使用专业的安全工具和技术，对组织的信息系统、应用程序和网络进行全面扫描。	L2
				09-02-02	能够分析扫描结果，识别系统中存在的安全漏洞和潜在威胁。	L2
		09-03	数据分类与标记方案制定	09-03-01	能够根据数据的敏感性和重要性，制定合理的数据分类和标记方案。	L1
				09-03-02	能够确保不同类型的数据得到适当的保护，降低数据泄露的风险。	L1
		09-04	安全审计与合规性检查	09-04-01	能够审查系统配置、权限设置和访问控制，确保其符合行业最佳实践和内部安全策略。	L1
				09-04-02	能够验证组织是否遵守相关的法规、标准和政策，如GDPR、HIPAA、PCI DSS等。	L1
		09-05	编写评估报告与改进建议	09-05-01	能够撰写详细的评估报告，列出发现的安全问题和潜在风险。	L1
				09-05-02	能够针对评估结果，提出具体的改进措施和建议，帮助组织提升数据安全水平。	L1
10	数据安全事件监控与响应	10-01	建立监控机制	10-01-01	能够部署和配置安全监控工具，以实时监测网络流量、系统日志、异常行为等关键指标。	L1
				10-01-02	能够设定合理的阈值和警报机制，以便在出现异常情况时能够及时触发警报。	L1
		10-02	事件检测与识别	10-02-01	能够通过监控工具和系统日志分析，检测异常活动或潜在的数据安全事件。	L2
				10-02-02	能够利用安全信息和事件管理（SIEM）系统或其他相关技术，对安全事件进行快速识别和分类。	L2
		10-03	初步分析与响应	10-03-01	能够对触发警报的事件进行初步分析，判断其严重性和可能的影响范围。	L2
				10-03-02	能够根据分析结果，采取紧急响应措施，如隔离受影响的系统、阻止恶意活动、保护现场数据等。	L2
		10-04	深入调查与取证	10-04-01	能够对安全事件进行深入调查，收集相关证据，如网络流量记录、系统日志、用户行为数据等。	L3
				10-04-02	能够分析攻击者的手段、目的和来源，以及事件中可能存在的漏洞或弱点。	L3
		10-05	恢复与加固	10-05-01	能够在确保数据完整性和安全性的前提下，恢复受影响的系统或服务	L2
				10-05-02	能够针对事件中暴露出的安全问题，加固系统防御措施，如更新安全策略、修补漏洞、提升权限管理等	L2
11	数据备份与恢复	11-01	制定备份策略	11-01-01	能够根据业务需求和数据重要性，制定定期或实时的数据备份策略。	L2
				11-01-02	能够确定备份的频率、存储位置以及备份数据的保留期限。	L2
		11-02	管理和维护备份系统	11-02-01	能够选择并配置适当的备份硬件和软件，确保备份过程的可靠性和效率。	L1
				11-02-02	能够定期检查备份系统的运行状态，确保其正常工作并及时解决可能出现的问题。	L1
		11-03	执行数据备份操作	11-03-01	能够按照备份策略定期或实时执行数据备份操作。	L1
				11-03-02	验证备份数据的完整性和可用性，确保在需要时能够成功恢复数据。	L1
		11-04	制定数据恢复计划	11-04-01	能够根据可能的数据丢失或损坏场景，制定详细的数据恢复计划	L1
				11-04-02	能够确定数据恢复的步骤、方法和工具，以及必要的恢复	L1

工作项目		工作任务		职业能力		学习水平
项目编号	项目名称	任务编号	任务名称	能力编号	能力名称	高职Li
					时间目标（RTO）和数据恢复点目标（RPO）	
		11-05	数据恢复操作	11-05-01	能够在发生数据丢失或损坏时，迅速启动数据恢复计划。	L2
				11-05-02	能够使用备份数据进行恢复操作，确保业务的连续性和数据的完整性。	L2
12	数据访问控制与权限管理	12-01	设计和实施访问控制策略	12-01-01	能够根据业务需求和安全原则，设计合理的数据访问控制策略，确保只有经过授权的用户或系统才能访问特定数据	L1
				12-01-02	能够制定访问控制列表（ACL）或角色基础访问控制（RBAC）模型，明确不同用户或用户组的访问权限。	L1
		12-02	管理用户账户和权限	12-02-01	能够创建、修改和删除用户账户，确保每个用户都有适当的访问权限。	L2
				12-02-02	能够根据用户的职责和需要，分配或撤销对特定数据资源的访问权限。	L2
		12-03	实施多因素身份验证	12-03-01	能够实施多因素身份验证机制，如指纹、动态令牌或短信验证码等。	L2
				12-03-02	能够配置和管理身份验证系统，确保其有效性和可靠性。	L2
		12-04	监控和审计数据访问行为	12-04-01	能够利用日志管理和监控工具，追踪和记录用户对数据的访问行为。	L1
				12-04-02	能够定期进行审计，检查是否存在未授权的访问尝试或滥用权限的情况。	L1
		12-05	处理权限请求和变更	12-05-01	能够响应来自用户或业务部门的权限变更请求，如增加、修改或删除某些权限。	L2
				12-05-02	能够确保权限变更符合组织的安全政策和程序。	L2
		12-06	更新和维护权限管理系统	12-06-01	定期更新权限管理系统，以适应组织结构和业务需求的变化。	L1
				12-06-02	修复权限管理系统中的漏洞和缺陷，确保其稳定运行。	L1
13	合规性检查与报告	13-01	了解并跟踪相关法规标准	13-01-01	能够不断学习和更新对数据安全相关的法律法规、行业标准以及最佳实践的了解	L1
				13-01-02	能够跟踪新的法规动态，确保企业的数据处理活动始终符合最新的法律要求。	L1
		13-02	制定和执行合规性检查计划	13-02-01	能够根据法律法规和行业标准，制定定期的合规性检查计划。	L1
				13-02-02	能够执行计划中的合规性检查，这包括对数据处理流程、数据存储和访问控制等方面的审核。	L1
14	网络监控与日志分析	14-01	网络监控	14-01-01	能够实时监控网络流量利用安全设备（如防火墙、入侵检测系统等）对网络流量进行实时监控，以识别和阻止恶意流量。	L2
				14-01-02	能够监控网络设备状态，监测监控网络设备（如路由器、交换机、防火墙等）的运行状态和性能，确保它们正常运行且性能良好。	L2
				14-01-03	能够监控各种网络服务（如邮件服务、Web服务、数据库服务等）的可用性和响应时间，以确保服务质量和用户体验。	L2
		14-02	日志收集与管理	14-02-01	能够收集各种设备和系统的日志数据包括网络设备日志、防火墙日志、操作系统日志、数据库日志等。	L1
				14-02-02	能够将日志文件发送到中央日志服务器或日志管理平台，以便进行统一管理和分析。	L1
		14-03	日志分析	14-03-01	能够解析原始的日志数据转化为结构化的数据，便于后续的分析和查询。	L2
				14-03-02	能够通过分析日志数据，检测网络中的异常行为和安全事件，如异常的连接请求、数据泄露、恶意软件传播等。	L2

工作项目		工作任务		职业能力		学习水平
项目编号	项目名称	任务编号	任务名称	能力编号	能力名称	高职Li
				14-03-03	能够利用日志数据追踪安全事件的来源和影响范围，为安全事件的调查和处理提供线索和证据。	L2
		14-04	报警与响应	14-04-01	能够设定报警阈值根据网络监控和日志分析的结果，设定合理的报警阈值，以便在发生异常情况时及时触发报警	L1
				14-04-02	能够迅速响应并处理异常情况，如隔离受影响的系统、阻止恶意活动等。	L2
15	系统补丁与漏洞管理	15-01	补丁信息收集与筛选	15-01-01	能够定期收集操作系统、应用程序和其他软件的最新补丁信息。	L1
				15-01-02	能够根据漏洞扫描结果和系统需求，筛选出适用于当前系统的补丁	L1
		15-02	补丁测试与部署	15-02-01	能够在应用补丁之前，进行充分的测试，以确保补丁与现有系统的兼容性，并防止引入新的问题	L1
				15-02-02	能够通过自动化工具或手动方式，将经过测试的补丁部署到生产环境中。	L1
16	防火墙与入侵检测系统（IDS/IPS）管理	16-01	防火墙配置与管理	16-01-01	能够配置和管理防火墙设备，确保内外网络的隔离和安全访问控制	L2
				16-01-02	能够根据安全策略，设置防火墙规则，允许或阻止特定的网络流量。	L2
				16-01-03	能够定期审查和更新防火墙规则，以适应网络架构和安全需求的变化。	L2
		16-02	入侵检测系统（IDS）与入侵防御系统（IPS）部署与监控	16-02-01	能够在网络关键部位部署IDS/IPS系统，以实时监测和识别潜在的入侵行为。	L2
				16-02-02	能够配置IDS/IPS的规则和策略，以确保能够准确检测到异常流量和攻击行为。	L2
				16-02-03	能够监控IDS/IPS系统的警报，及时响应和处理安全事件。	L2
		16-03	日志分析与审计	16-03-01	能够收集和分析防火墙及IDS/IPS系统产生的日志数据，以发现潜在的安全威胁	L1
				16-03-02	能够定期对日志进行审计，确保网络系统的安全性和合规性。	L1
17	安全事件响应与处置	17-01	安全事件监测	17-01-01	能够实时监控网络和系统，以及安全设备和日志，以便及时发现异常行为和安全事件。	L1
				17-01-02	能够利用入侵检测系统（IDS）、安全信息和事件管理（SIEM）系统等工具进行事件监测。	L1
		17-02	应急响应计划执行	17-02-01	能够确认安全事件，立即按照预定的应急响应计划行动。	L1
				17-02-02	能够协调团队成员，分配任务，确保响应工作有序进行。	L1
18	安全培训与意识提升	18-01	制定安全培训计划	18-01-01	能够根据组织的需求和员工的安全知识水平，制定全面的安全培训计划。这个计划应该涵盖网络安全的各个方面，包括但不限于密码安全、社交工程防范、防病毒和恶意软件等。	L1
		18-02	提升员工安全意识	18-02-01	能够通过各种渠道（如内部网站、电子邮件、公告板等）定期发布安全提示和警示，以增强员工对网络安全的警觉性。	L1
19	安全测试	19-01	设计和执行安全测试用例	19-01-01	能够根据软件的功能需求和安全标准，设计针对软件系统的安全测试用例。	L1
				19-01-02	能够执行测试用例，通过模拟各种攻击场景来检测软件中的安全漏洞。	L1
		19-02	漏洞扫描与验证	19-02-01	能够利用自动化工具和手动测试技术，对软件系统进行全面的漏洞扫描。	L2
				19-02-02	能够验证扫描出的漏洞，确认其真实性和可利用性，并对漏洞进行风险评级。	L2
		19-03	安全风险	19-03-01	能够分析软件系统的安全架构，评估潜在的安全风险。	L1

工作项目		工作任务		职业能力		学习水平
项目编号	项目名称	任务编号	任务名称	能力编号	能力名称	高职Li
			评估	19-03-02	能够提供风险缓解策略和建议，协助开发团队修复已知的安全问题。	L1
		19-04	编写安全测试报告	19-04-01	能够整理安全测试的结果，编写详细的安全测试报告。	L1
				19-04-02	报告中需包含测试过程、发现的漏洞、漏洞的严重性等级以及改进建议。	L1
20	源代码安全审计	20-01	源代码审查	20-01-01	能够逐行审查源代码，检查是否存在安全漏洞、逻辑错误或潜在的风险点。	L3
				20-01-02	能够特别关注用户输入的处理、数据验证、权限控制等关键部分。	L3
		20-02	安全漏洞检测	20-02-01	能够利用源代码安全审计工具或手动分析，检测代码中可能存在的常见安全漏洞，如SQL注入、跨站脚本攻击（XSS）、跨站请求伪造（CSRF）等。	L3
				20-02-02	能够验证漏洞的真实性，并评估其对系统安全性的影响。	L3
		20-03	编码规范检查	20-03-01	能够检查源代码是否符合安全编码规范，如是否存在不安全的函数调用、是否使用了不安全的加密算法等。	L2
				20-03-02	能够提出改进建议，推动开发团队采用更安全的编码实践。	L2
		20-04	安全加固建议	20-04-01	能够根据审计结果，提供针对性的安全加固建议，包括修复已知漏洞、增强身份验证机制、优化错误处理等。	L1
				20-04-02	能够协助开发团队实施这些建议，提高软件系统的安全性。	L1

（二）典型工作任务与能力对接表

序号	典型工作任务	对应职业能力（技能、工具、方法、要求、知识） 对应典型工作任务职业能力分析表中项目编号、任务编号和能力编号
1	目标信息收集	01-01-01、01-01-02、01-02-01、01-02-02、01-03-01、01-03-02、01-04-01、01-05-01、01-06-01、01-07-01、01-08-01
2	漏洞扫描与发现	02-01-01、02-02-01、02-03-01、02-04-01、02-05-01、02-06-01
3	漏洞验证与利用	03-01-01、03-01-02、03-02-01、03-02-02、03-03-01、03-03-02、03-04-01、03-04-02、03-05-01、03-05-02、03-06-01、03-06-02、03-07-01、03-07-02
4	权限提升与横向移动	04-01-01、04-01-02、04-01-03、04-02-01、04-02-02、04-02-03、04-02-04、04-02-05
5	数据窃取与篡改尝试	05-01-01、05-01-02、05-01-03、05-01-04、05-01-05、05-02-01、05-02-02、05-02-03、05-02-04、05-02-05、05-02-06
6	编写渗透测试报告	06-01-01、06-02-01、06-03-01、06-04-01、06-05-01
7	安全策略制定	07-01-01、07-02-01、07-03-01
8	数据分类与分级保护	08-01-01、08-01-02、08-01-03、08-02-01、08-02-02、08-02-03、08-03-01、08-03-02
9	数据安全风险评估	09-01-01、09-01-02、09-02-01、09-02-02、09-03-01、09-03-02、09-04-01、09-04-02、09-05-01、09-05-02
10	数据安全事件监控与响应	10-01-01、10-01-02、10-02-01、10-02-02、10-03-01、10-03-02、10-04-01、10-04-02、10-05-01、10-05-02
11	数据备份与恢复	11-01-01、11-01-02、11-02-01、11-02-02、11-03-01、11-03-02、11-04-01、11-04-02、11-05-01、11-05-02
12	数据访问控制与权限管理	12-01-01、12-01-02、12-02-01、12-02-02、12-03-01、12-03-02、12-04-01

序号	典型工作任务	对应职业能力（技能、工具、方法、要求、知识） 对应典型工作任务职业能力分析表中项目编号、任务编号和能力编号
		、12-04-02、12-05-01、12-05-02、12-06-01、12-06-02
13	合规性检查与报告	13-01-01、13-01-02、13-02-01、13-02-02
14	网络监控与日志分析	14-01-01、14-01-02、14-01-03、14-02-01、14-02-02、14-03-01、14-03-02、14-03-03、14-04-01、14-04-02
15	系统补丁与漏洞管理	15-01-01、15-01-02、15-02-01、15-02-02
16	防火墙与入侵检测系统（IDS/IPS）管理	16-01-01、16-01-02、16-01-03、16-02-01、16-02-02、16-02-03、16-03-01、16-03-02
17	安全事件响应与处置	17-01-01、17-01-02、17-02-01、17-02-02
18	安全培训与意识提升	18-01-01、18-02-01
19	安全测试	19-01-01、19-01-02、19-02-01、19-02-02、19-03-01、19-03-02、19-04-01、19-04-02
20	源代码安全审计	20-01-01、20-01-02、20-02-01、20-02-02、20-03-01、20-03-02、20-04-01、20-04-02

（三）就业岗位与人才培养规格对应关系表

序号	岗位（群）	岗位（群）业务描述	岗位（群）核心能力	培养目标的相关表述	对应的培养规格 对照前文的培养规格
1	渗透测试工程师岗位	1. 渗透测试与漏洞挖掘 2. 安全评估与加固建议 3. 日志分析与应急响应 4. 编写测试报告与安全方案 5. 跟踪安全技术动态与漏洞研究 6. 团队协作与沟通 7. 持续学习与技能提升	1. 熟练掌握渗透测试技术和工具，能够高效地发现和利用安全漏洞。 2. 具备良好的问题分析和解决能力，能够迅速定位并验证安全漏洞。 3. 具备良好的文档编写能力，能够撰写易于理解且专业的安全方案。 4. 能够与团队等有效沟通，协同工作以解决安全问题。 5. 持续学习新的安全技术和工具，以适应不断变化的网络环境。 6. 熟悉并遵守相关的网络安全法律法规和标准，确保渗透测试活动的合法性。	能够对目标系统的安全性进行全面评估，遇到复杂的安全问题时，能够综合运用各种技术和资源进行深入研究，提出有效的解决方案。并提供针对性的加固建议。	1-4、8①、②、⑦、9-11
2	数据安全工程师岗位	1. 数据安全项目管理 2. 日常安全维护与管理 3. 风险整改与应急响应 4. 制定与管理安全标准规范 5. 全生命周期数据安全工作 6. 技术研发与安全工具运用	1. 熟练掌握数据加密、数据脱敏、数据防泄露等数据安全保护技术，能够有效应用这些技术来保护数据的机密性、完整性和可用性。 2. 能够根据企业或组织的实际情况，制定合理的数据安全策略和规范，并监督其执行情况。 3. 对数据分级分类保护有深入理解，能够根据数据的敏感性和重要性制定不同的保护措施。 4. 具备全面的数据安全风	培养熟练掌握数据加密、数据脱敏、数据防泄露等关键技术，以及相关的数据安全管理工具和平台的使用方法，深入理解数据安全的基本原理和概念，包括数据保密性、完整性、可用性等，以及常见的数据安全威胁和防御策略。据组织的需求和相关法律法规，制定合适的数据安全政策和流程，并监督其执行，确保数据的安全性和合规性。	1-4、7、8③、④、9-11

序号	岗位（群）	岗位（群）业务描述	岗位（群）核心能力	培养目标的相关表述	对应的培养规格 对照前文的培养规格
			险评估能力，能够识别潜在的数据安全风险并提出有效的整改措施。 5. 具备数据恢复能力，能够在数据丢失或损坏后尽快恢复数据的完整性和可用性。		
3	网络安全运维岗位	1. 网络安全监测与分析 2. 安全防护与策略制定 3. 应急响应与事件处理 4. 安全设备与系统管理 5. 持续学习与技能提升	1. 能够利用各类监控工具实时检测和分析网络的安全状况，及时发现并报告异常行为。 2. 通过对日志、流量等数据的深入分析，准确识别安全威胁和攻击模式。 3. 熟悉各类网络安全设备和系统的配置与管理，如防火墙、入侵检测系统、安全信息和事件管理（SIEM）系统等。 4. 在网络安全事件发生时，能够迅速启动应急响应计划，控制事态发展，减少损失。 5. 负责网络设备和安全系统的日常管理和维护，保证其稳定运行。	培养学生全面掌握网络安全的基本概念、原理和方法，深入理解网络安全的重要性及其对企业和组织的影响，通过学习和实践，使学员能够熟练掌握各类网络安全设备和系统的配置与管理，提高网络环境的安全防护能力。解并遵守网络安全相关法律法规和标准，提高网络安全风险评估和管理能力，为企业的安全决策提供有力支持。	1-4、5④、⑤、6①、②、9-11
4	软件安全测试岗位	1. 安全测试执行 2. 安全策略与流程制定 3. 漏洞分析与报告 4. 安全工具与技术应用	1. 能够设计和执行有效的安全测试用例，以确保软件系统的安全性。 2. 对测试中发现的安全漏洞进行深入分析，准确评估其严重性和影响范围。 3. 熟练掌握各种安全测试工具，如自动化测试框架、漏洞扫描器、网络抓包工具等。 4. 面对复杂的安全问题时，能够迅速定位问题根源，提出有效的解决方案。	培养学生全面了解软件安全的基本概念、原理和方法，包括常见的安全漏洞类型、攻击手段和防御策略，为后续的安全测试工作打下坚实基础。通过系统的学习和实践，使学员熟练掌握安全测试的技术和方法，包括渗透测试、漏洞扫描、恶意代码分析等，能够独立执行软件系统的全面安全测试。	1-4、7④、⑤、⑥、8⑥、⑦、9-11

（四）课程对培养规格的支撑关系分析表

序号	课程	课程目标	培养规格 对照前文的培养规格
1	信息安全导论	1. 加强学生在网络信息安全方面的专业修养。 2. 了解网络信息安全的主要问题、分类和危害机制，并掌握解决这些安全问题的理论、技术和方案。 3. 能够利用所学知识实施和构建自己的安全防范体系和安全系统。	1-4、9-11

序号	课程	课程目标	培养规格 对照前文的培养规格
		4. 培养学生对信息安全的基本认识和意识，为今后在信息安全领域的学习和工作奠定基础。	
2	python程序设计（信息安全）	1. 掌握Python编程语言的基础知识，包括语法、数据结构和基本算法。 2. 培养学生的逻辑思维能力、算法设计能力和问题解决能力。 3. 提升学生将理论知识应用于实践的能力，以及独立解决问题的能力。	1-4、8①②、9-11
3	数字素养	使学生掌握常用的工具软件和信息化办公技术，了解云计算、大数据、人工智能、物联网、区块链、虚拟现实与元宇宙等新兴信息技术，具备支撑专业学习的能力，能在日常生活、学习和工作中综合运用信息技术解决问题等技能；提升学生信息意识、计算思维、促进数字化创新与发展能力，树立正确的信息社会价值观和责任感，培养学生独立思考和主动探究能力等方面的职业素质。	1-4、9-11
4	应用数学	1. 掌握集合、不等式、基本初等函数等初等数学知识。 2. 结合“以应用为目的，以必需够用为度”的教学原则，加强对学生应用意识、兴趣、能力的培养。 3. 通过课程学习，培养学生的抽象思维能力、逻辑推理能力、运算能力、空间想象能力以及综合运用所学知识分析问题和解决问题的能力。	1-4、9-11
5	PHP程序设计	1. 掌握动态网站开发技术的基本理论； 2. 掌握PHP 程序设计的基本知识； 3. 掌握动态网站 MySQL 数据库的操作； 4. 掌握动态网页的制作流程。	1-4、8①、②、9-11
6	信息安全合规指引	4. 深刻理解信息安全合规的重要性，树立企业运营中的合规意识。 5. 熟悉国内外信息安全的相关法规、标准及合规要求。 6. 通过案例分析和实践操作，提升学生处理信息安全合规问题的能力。 7. 促进职业发展：为学生未来从事信息安全相关工作，特别是合规管理领域，奠定坚实基础。	1-4、9-11
7	密码学基础	1. 掌握密码学的基本原理、加解密算法和数字签名算法。 2. 理解密码学在现实生活中的应用，如银行、电子商务等领域的信息安全保护。 3. 熟悉密码攻击和防护的基本方法。 4. 能够运用常见算法进行加解密和数字签名操作。 5. 能够评估密码系统的安全性，并了解密码破解的基本原理。	1-4、8⑤、9-11

序号	课程	课程目标	培养规格 对照前文的培养规格
8	网络安全协议分析	1. 能够明确网络安全协议在网络通信中的关键作用，以及它们如何保护数据的机密性、完整性和可用性。 2. 了解各种网络安全协议的工作原理、设计目标和实现方式。 3. 能够将理论知识应用于实际，通过配置和使用网络安全协议来保护网络环境的安全。	1-4、5④⑤、9-11
9	信创适配	1. 理解信创适配概念、原理及其在信创产业中的重要作用； 2. 掌握信创适配的核心技术，包括迁移技术、适配测试、性能优化等； 3. 通过实际操作和实验，提升学员在信创适配方面的实践能力； 4. 信创适配过程中进行创新思维，提出新的适配方案和优化策略。	1-4、9-11
10	Web攻防	1. 掌握web应用常见的攻击手段及防御手段，对网络应用安全技术有深入的了解，具备中小型企业网络安全解决方案实施和维护的能力； 2. 掌握排查和解决企业网中存在的安全隐患和故障； 3. 提高学生的职业素质，促进学生职业能力的培养和职业素养的养成。	1-4、8①②⑥、9-11
11	网络安全设备	1. 掌握网络安全的基本概念、原理和核心技术； 2. 能够分析网络安全威胁、漏洞和风险，提出有效的防范策略； 3. 能够使用网络安全工具和软件，对网络进行安全检测和防护。	1-4、6、9-11
12	物联网安全攻防	1. 理解物联网安全的重要性和挑战，增强物联网安全防护意识。 2. 掌握物联网安全攻防的基本原理和技术，包括网络攻击手段与防御策略。 3. 培养学生分析物联网安全漏洞并提出针对性解决方案的能力。 4. 提升学生的实践操作能力，能够在实际环境中应用所学知识进行物联网安全防护。	1-4、8①②⑥、9-11
13	数据安全	1. 使学生了解数据安全技术的基本概念和常见威胁； 2. 掌握数据安全技术的基本原理和方法； 3. 剧本数据安全风险评估和处理的能力； 4. 要求学生能够运用各种数据加密和认证技术，提升数据安全管理水平。	1-4、7、8⑤、9-11
14	渗透测试	1. 理解渗透测试的基本原理和方法； 2. 掌握常见的渗透测试技术和工具； 3. 学会评估和利用系统和应用程序中的漏洞； 4. 培养良好的法律和道德意识，确保渗透测试行为的合法和道德。	1-4、7-11

序号	课程	课程目标	培养规格 对照前文的培养规格
15	网络安全岗位综合实训	1. 掌握安全岗位所需的基本知识和技能，包括但不限于安全法规、安全操作规程、事故应急处理等方面。 2. 在实际工作环境中运用所学知识和技能的能力，提高其处理安全问题的能力。 3. 增强安全意识，能够主动发现和预防安全事故，提高工作环境的安全水平。	1-11
16	毕业综合项目	1. 通过毕业综合项目，培养学生的综合应用能力，包括专业知识、实践技能、团队协作、问题解决和创新思维等多方面的能力。 2. 能够将所学的专业理论知识与实际项目相结合，进一步深化对专业知识的理解，提高专业应用水平。 3. 通过项目的实施，锻炼学生的实践能力，包括项目规划、方案设计、实验操作、数据分析、报告撰写等能力。	1-11
17	岗位实习	1. 通过岗位实习，将所学的理论知识与实际工作相结合，加深对专业知识的理解和应用，提高实际操作能力； 2. 培养学生的职业素养，使其能够适应岗位要求，具备良好的职业习惯和职业责任感； 3. 通过实习，提高学生的团队协作和沟通能力，学会与他人合作、分享和协调，以更好地完成工作任务； 4. 培养学生的问题解决能力，使其在面对实际工作中的问题时，能够独立思考、分析问题、提出解决方案，并有效实施； 5. 帮助学生明确自己的职业目标和方向，了解行业发展趋势和岗位需求，为未来的职业规划和发展奠定基础。	1-11
18	计算机网络技术	1. 掌握计算机网络基本原理和关键技术。 2. 培养学生熟悉网络协议的设计和实现。 3. 理解网络安全和隐私保护的原理，使其能进行网络安全的评估与防护。 4. 增强学生的团队协作和沟通能力，以便其能有效解决实际网络问题。	1-4、5、9-11
19	Web前端开发	1. 能够熟练掌握HTML5、CSS3、JavaScript等前端开发技术。 2. 提高学生的动手能力和解决问题的能力。 3. 培养学生的团队协作能力、沟通能力以及创新精神，以适应不断变化的市场需求。	1-4、8①②、9-11
20	Linux操作系统基础	1. 了解Linux操作系统的基本原理、内核结构和管理方法。 2. 掌握Linux操作系统的使用和管理技能，包括系统安装、配置、网络服务设置等。 3. 增强学生的系统安全意识，学会配置和维护系统的稳定性。	1-4、5①②③、9-11
21	数据库应用技术	1. 掌握数据库基础知识：使学生全面了解数据库的基本概念、原理和	1-4、9-11

序号	课程	课程目标	培养规格 对照前文的培养规格
		应用。 2. 够熟练使用SQL语言进行数据查询、更新和管理。 3. 理解数据库设计的基本原则，并能够对数据库系统进行基本的维护和优化。 4. 增强数据安全意识	
22	HCIA-openEuler	1. 掌握openEuler操作系统的基本原理、设计方法和实际应用。 2. 提升学生的动手能力和问题解决能力，使其能够熟练运用操作系统知识解决实际软件工程问题。 3. 通过了解我国科技工作者在操作系统领域的努力和成果，激发学生的民族自豪感和开发基础软件的信心。 4. 岗课赛证融合，为学生多渠道高质量就业提供支持。	1-4、5①②③、9-11
23	NISP二级	1. 掌握网络安全的基础知识和技能，包括密码技术、鉴别与访问控制、操作系统安全、数据库安全、网络安全、应用安全等。 2. 能够独立建立、完善和优化企业信息安全制度和流程。 3. 能够跟踪和验证安全措施的实施，建立起立体式、纵深的安全防护系统，并能进行安全监控，对未知的安全威胁进行预警和追踪。	1-11
24	1+x企业网络安全防护（中级）	1. 掌握网络安全防护技能：学员能够掌握企业网络安全防护的核心技术和方法，提升网络安全防护能力。 2. 能够独立完成网络安全配置、管理和应急响应等任务。 3. 提高学员对网络安全重要性的认识，培养防范网络威胁的意识和能力。	1-11