信息安全技术应用专业
产业需求分析调研和可行性分析

一、专业及基本信息

1.专业名称

信息安全技术应用

2.调研目的

本调研旨在精确把握信息安全技术应用产业发展现状、人才需求规模与结构、岗位知识、能力需求等，为洛阳商业职业学院信息安全技术应用专业的设置、人才培养方案的修订提供数据支持与决策依据。

3.调研时间

2025 年 6 月-2025 年 7 月

4.调研对象

采用分类抽样选取产业内的企业 8 家，如洛阳众智软件科技股份有限公司、中移在线服务有限公司洛阳分公司等；政府主管部门如洛阳市工业和信息化局、河南省通信管理局洛阳市通信发展管理办公室等；及同类高校洛阳职业技术学院信息安全技术应用专业近 3 年毕业生等为调研对象。

5.调研方法

采用定量与定性相结合、线上与线下互补的多元化调研方法，确保数据收集的全面性和结果分析的可靠性。具体包括：

采用文献研究法：采用 AI 搜索收集相关政策、行业内部报告等资料，如《中华人民共和国网络安全法》、《数据安全法》、《个人信息保护法》等法律法规。熟悉信息安全技术应用产业发展现状及发展趋势；搜索同类院校专业资料，与洛阳商业职业学院同专业进行比较分析。

问卷调查法：分层制定不同问卷通过问卷星面向企业管理人员、从业人员及毕业生学生等群体调研信息安全技术应用产业人才能力素质要求、培养模式等。

访谈法：采用半结构化方式与企业负责人、行业专家、政府部门负责人深入交流，如对洛阳众智软件科技股份有限公司、中移在线服务有限公司洛阳分公司的相关主管部门进行访谈，询问了本专业人才需求规模、技能要求以及岗位核心知识等问题，了解信息安全技术应用产业人才需求规模、人才需求结构等。

实地考察法：走访企业生产一线、产业园区等，了解信息安全技术应用产业发展现状。

二、信息安全技术应用产业发展现状调研

（一）产业总体情况

1.产业定义与范围

信息安全技术应用产业是通过技术、产品、服务和管理体系来保护信息系统、数据及网络空间安全，确保其保密性、完整性、可用性，以防范网络攻击、数据泄露等安全威胁，保障个人隐私、企业资产和国家关键基础设施安全，支撑国家安全战略、数字经济发展以及企事业单位数字化转型的综合性产业。

其范围广泛，主要涉及网络与边界安全，如利用防火墙、入侵检测系统等产品保护网络通信和系统接入边界；终端和移动安全，借助终端检测响应、移动设备管理等保障终端设备和移动应用安全；数据安全与隐私保护，采用数据加密、脱敏、防泄漏等技术保护数据全生命周期安全；应用与系统安全，通过静态和动态应用安全测试、渗透测试等手段保护软件应用和系统安全；云计算与新兴技术安全，运用云工作负载保护、物联网设备认证等技术适配云计算、物联网等新技术场景的安全需求；安全服务与合规，提供渗透测试、安全运维、等保测评等专业服务和合规认证服务。此外，产业还关联物理安全等非核心领域，且随着技术发展，量子加密等新兴场景正逐步被纳入，产业链包括上游的安全芯片等供应商、中游的安全软件开发商和服务商以及下游的行业用户。

2.产业在区域及国家经济中的地位

信息安全技术产业是国家安全、数字经济和国际竞争的关键支柱，战略定位持续升级。首先，它是国家安全的“基石”，承担关键信息基础设施（如电力、金融、交通系统）的安全防护，相关投入占产业总产值的35%以上，是保障国家网络空间主权、落实《网络安全法》《数据安全法》的核心支撑，年处理百万级网络安全事件，维护社会稳定与经济安全。其次，作为数字经济发展的“底座”，该产业保障工业互联网（占安全需求30%）、金融科技（25%）、政务数据（20%）等数字经济三大支柱的安全运行，支撑“东数西算”等国家级工程（安全防护投入占数据中心建设成本的8%-12%），是数字技术与实体经济深度融合的前提条件。再次，它是国际竞争的“新赛道”，在中美科技博弈中成为焦点领

域，我国网络安全产品出口额年均增长25%（2023年突破120亿美元），华为、奇安信等企业进入全球安全解决方案提供商前十，同时积极参与国际标准制定（如ISO/IEC 27001标准数量十年增长300%），争夺全球数字治理话语权。最后，该产业是政策驱动的“新动能”，在数据要素市场化配置改革中，数据安全托管服务预计未来三年保持40%以上年增长率；地方政府每投入1元网络安全专项资金，可带动5-8元社会资本跟进（如广东“数字政府”安全建设带动千亿级投资），形成“政策牵引+市场扩围”的良性循环。

信息安全技术产业作为洛阳市数字经济与战略性新兴产业的重要组成部分，正逐步成为推动经济高质量发展、保障关键信息基础设施安全的核心支撑力量。当前，洛阳依托装备制造、工业互联网等传统产业基础，加速布局网络安全服务、数据安全、工业信息安全等细分领域，集聚了超过100家相关企业（含国家级/省级网络安全技术应用试点示范单位），年产值增速连续三年保持15%以上，对全市数字经济的贡献率逐年提升；同时，该产业不仅为智能制造、智慧城市等重点项目提供安全防护能力（如关键信息系统的漏洞检测、数据加密与应急响应），还通过培育本土信息安全技术人才、吸引产业链上下游配套企业，有效促进了产业结构升级与创新生态完善，在保障城市运行安全、服务“制造强市”战略中发挥着不可替代的基础性作用，已成为洛阳市抢占数字时代竞争制高点、构建现代化产业体系的关键新兴增长极。

综上，信息安全技术产业既是区域经济转型升级的“数字护城河”，也是国家参与全球数字竞争、保障经济与社会安全的核心能力载体，在

稳增长、保安全、促创新中具有不可替代的战略价值。

3.产业当前发展现状

信息安全产业是数字经济的“刚需赛道”，增速远超传统产业。全球市场年增速约10%-12%，中国市场更高达20%-25%（数据安全、云安全等细分领域增速超30%），远高于GDP增速（5%左右）及IT服务行业平均增速（10%-15%）。驱动因素包括：政策强制合规（如等保2.0、数据安全法推动政企安全投入占比IT预算提升至10%以上）、数字技术普及（云计算、工业互联网等场景安全需求爆发）、安全事件频发（勒索攻击、数据泄露倒逼企业主动防护）。其中，新兴领域（如AI对抗样本防御、量子加密）因技术迭代快、市场空白多，增速可达40%-50%。

同时该产业当前呈现明显的区域集聚与差异化发展特征。一线城市（如北京、上海、深圳、广州）凭借头部企业聚集（全国60%以上的网络安全龙头企业集中于此）、高端人才储备及国际化业务优势，成为产业研发中心、总部基地和高端安全服务主要承载地，贡献全国超70%的高端市场份额；新一线城市（如成都、武汉、杭州、西安）依托政策支持与高校资源，重点建设国家级网络安全产业园区（如武汉国家网络安全人才与创新基地、成都中国网安基地），聚焦应用技术研发、人才培养及区域级安全服务，形成“产业集聚+人才培育”双轮驱动模式；二三线城市则围绕特色场景发力，如无锡聚焦物联网安全、长沙深耕工业控制系统安全，通过差异化布局填补区域关键基础设施防护需求空白。整体上，产业空间格局呈现“头部引领、梯次分布、特色互补”的特点，区域协同推动产业生态不断完善。

总之，信息安全技术产业当前处于高速增长期，规模快速扩张（中国年增速超20%）、集中度较高（头部企业占半数份额）、区域集聚特征显著（一线城市引领、新一线及特色集群互补），未来3-5年将随数字经济发展进一步向智能化、全域防护方向演进，同时中小企业的细分领域创新将成为产业活力重要来源。

（二）产业政策环境

1.国家层面政策

随着信息技术的快速发展和信息化应用的不断深入，信息技术、产品及网络已经融入社会经济生活的方方面面，但同时信息安全问题也越来越突出。面对严峻的信息安全形势，我国将信息安全上升至国家战略，积极推动信息安全发展，成立了中央网络安全与信息化领导小组，相继出台了《关于大力推进信息化发展和切实保障信息安全的若干意见》等政策法规。信息安全产业面临良好的政策环境，处于快速发展的历史机遇期。随着移动互联网、物联网、云计算等技术的快速发展，国家所面临的信息安全形势愈发严峻，信息安全愈发受到高度重视；新技术也为维护网络信息安全提供了新的手段，从而也为网络信息安全行业带来了新的市场发展空间，创新性的安全运维服务或云安全服务将成为国家网络信息安全领域的一个新兴增长点。2021年国务院发布了《关键信息基础设施安全保护条例》，随着我国信息安全等级保护工作的持续推进，一方面提升了政府、企业对信息安全的重视程度，带动社会信息安全建设投入的增长。另一方面政府及重点企业的等级保护工作经过前期的定级、评估等工作，已经进入实质实施与长期运维阶段，这将为信息安全

市场提供持续、稳定的市场空间。信息安全立法的完善和信息安全意识的强化，信息安全产品的需求程度也逐渐提升，这为我国的信息安全产业持续发展奠定了巨大的市场基础。

“十四五”规划明确将网络安全列为数字经济重点产业，提出强化网络安全保障体系建设，工信部等十二部门印发《网络安全产业高质量发展三年行动计划（2023 - 2025 年）》，要求到 2025 年网络安全产业规模超过 2500 亿元，年复合增长率超过 15%，并聚焦新兴领域安全技术研发与推广应用；提供财政补贴与税收优惠，如地方政府设立网络安全产业专项扶持资金，对符合条件的企业给予项目补贴，同时网络安全作为高新技术企业，可享受研发费用加计扣除、企业所得税减按 15%征收等税收优惠政策；制定严格的行业准入标准与质量监管政策，通过等保 2.0、数据安全法、个人信息保护法等法规，明确关键信息基础设施安全保护要求，规定企业安全投入比例与合规义务，规范网络安全产品和服务的质量标准，加强市场准入管理和安全审查，保障产业健康有序发展。

2.地方层面政策

地方层面信息安全技术应用政策以推动区域产业升级、强化关键领域安全防护为核心，典型政策包括：河南省 2022 年印发的《河南省“十四五”网络安全规划》（豫网办〔2022〕15 号），明确提出到 2025 年全省网络安全产业规模突破 300 亿元，重点支持郑州、洛阳等地建设网络安全产业园区，培育本土龙头企业和专精特新“小巨人”企业；2023 年河南省工信厅发布的《关于加快网络安全产业发展的实施意见》（豫工信联信〔2023〕87 号），聚焦工业互联网、政务服务、数据流通等重点领

域，要求关键信息基础设施运营者安全投入不低于IT预算的10%，并对网络安全企业给予研发费用补贴和税收优惠；洛阳市同期配套出台《洛阳市数字安全创新发展行动计划（2023—2025年）》（洛政办〔2023〕22号），提出建设中原网络安全产业园（洛阳基地）、引进培育10家以上网络安全规上企业，同时鼓励驻洛高校（如洛阳商业职业学院）开设信息安全相关专业，深化产教融合实训基地建设，通过地方财政资金支持学生实训与技能竞赛，形成“政策牵引+产业集聚+人才支撑”的区域特色发展模式。

3.政策对产业发展的影响

信息安全技术产业政策从多维度深刻影响产业发展：国家“十四五”规划等顶层设计将网络安全列为数字经济核心产业，通过《网络安全产业高质量发展三年行动计划》等政策明确技术攻关方向（如零信任架构、AI安全），引导企业加大研发投入（头部企业研发占比普遍超20%），推动产业从传统硬件防护向智能化、服务化（安全服务占比超40%）升级；在引导资源配置上，财政政策（如研发费用加计扣除、税收减免）与地方专项基金（如上海网络安全产业扶持资金）精准支持关键领域，促使资源向头部企业（如奇安信、深信服）和新兴技术（云计算安全、数据安全）集聚，形成“研发-应用-市场”良性循环；在规范市场秩序方面，等保2.0、数据安全法等法规强制要求关键行业（如金融、政务）安全投入占比不低于10%，统一技术标准（如ISO/IEC 27001）和测评体系（如等保测评机构资质），淘汰低质低价产品，倒逼企业提升服务质量与合规能力。政策变化对未来发展的潜在影响显著——随着数据要素市场化

配置改革推进，数据安全托管等新兴需求将爆发（预计年增速超40%），而国际竞争加剧（如中美科技博弈）可能推动国产化替代加速（如自主可控安全芯片、加密算法），同时政策对中小企业的安全合规要求（如等保延伸至小微企业）将拓宽下沉市场空间，整体加速产业向“全域防护、自主可控、生态协同”方向演进。

（三）产业发展趋势

1.现有主流技术

信息安全技术应用产业当前广泛应用的主流技术以“防护-检测-响应”为核心，形成覆盖多场景的技术体系。在核心技术方面，有防火墙（网络边界防护）通过包过滤、状态检测等技术原理，基于预设规则拦截非法网络流量，广泛应用于企业网络与数据中心入口，优势在于阻断外部攻击（如DDoS）的“第一道防线”；入侵检测/防御系统（IDS/IPS）通过实时监测网络流量与系统日志，利用特征匹配与异常行为分析技术（如机器学习模型），主动发现并阻断渗透攻击，适用于金融、政务等高安全需求场景；数据加密技术（如AES对称加密、RSA非对称加密）通过数学算法对数据（传输/存储状态）进行密文转换，保障医疗、金融等领域的敏感信息在传输和存储中的保密性，优势是即使数据被窃取也无法解密；零信任架构基于“默认不信任、持续验证”原则，通过多因素认证、微隔离与动态访问控制技术，解决云计算与远程办公场景下的身份仿冒与横向攻击问题，适用于企业分支互联与移动办公环境。

在关键工艺上，威胁情报分析依托全球攻击数据共享与AI关联分析，将漏洞利用趋势、恶意IP等情报实时融入防护策略，提升攻击预测能力；

安全服务化（SECaaS）通过云原生架构交付渗透测试、安全运维（MSS）等能力，降低中小企业安全投入门槛。核心设备包括下一代防火墙（NGFW）（集成应用识别与入侵防御）、统一威胁管理（UTM）平台（整合防火墙、防病毒等功能）、数据防泄漏（DLP）系统（通过内容识别技术防止敏感数据外传）。这些技术的共同优势在于：技术原理上结合规则匹配与智能分析（如 AI/机器学习），应用场景覆盖从网络边界到数据内核的全链路，优势突出表现为“主动防御+精准防护+灵活适配”，能够有效应对勒索软件、数据泄露、APT 攻击等复杂威胁，同时满足合规要求（如等保 2.0、GDPR），是产业支撑数字经济安全发展的技术基石。

2.新技术研发动态

信息安全技术应用产业的前沿技术研发聚焦人工智能、大数据、新能源等新兴技术的融合创新，推动安全防护向智能化、精准化升级。在人工智能领域，产业界积极探索 AI 驱动的威胁检测与响应，如利用机器学习算法实现网络攻击的自动化识别与溯源（如异常行为分析、恶意代码智能分类），河南企业郑州信大捷安信息技术股份有限公司研发了基于 AI 的“车联网安全通信模组”，通过机器学习模型实时检测车载终端的异常通信行为，有效防范针对智能网联汽车的远程攻击，该成果已应用于国内多个新能源汽车厂商，提升了车联网场景的安全防护能力。同时在大数据技术领域，隐私计算与数据安全成为研发热点，河南省大数据研究院联合本地企业开发了基于联邦学习的“医疗数据跨机构安全共享平台”，在不泄露原始数据的前提下实现多机构间健康数据的协同分析，解

决了医疗行业数据流通与隐私保护的矛盾，该技术已在河南省部分三甲医院试点应用。新能源与信息安全的交叉领域，河南科研机构针对智能电网的安全需求，开展了“电力物联网终端安全接入技术”研究，通过轻量级加密算法与动态身份认证机制，保障分布式能源（如光伏、风电）设备的数据传输安全，相关成果被纳入国家电网河南分公司的新能源并网安全标准体系。此外，河南高校（如郑州大学网络安全实验室）与本地企业合作，探索量子加密技术在政务数据传输中的应用，试验性部署了“量子密钥分发（QKD）+传统加密”的混合加密系统，为关键基础设施提供更高安全等级的通信保障。这些研发动态表明，河南在信息安全新技术应用中紧密结合本地产业特色（如新能源、医疗、智能网联汽车），通过“AI+大数据+行业场景”的融合创新，不仅推动了前沿技术的落地实践，也为全国信息安全产业的技术突破提供了区域实践样本，凸显了地方科研力量在产业升级中的关键作用。

3.技术发展趋势

信息安全技术应用产业当前新技术研发动态聚焦前沿领域突破与融合创新：在研发动态上，零信任架构（ZTA）、云原生安全（如 CSPM 容器安全）、数据安全（隐私计算/联邦学习）、人工智能安全（对抗样本防御）及工业互联网安全（IT/OT 融合防护）成为企业（如奇安信、华为云）与科研机构（如中国信通院）的重点攻关方向，其中隐私计算技术已在金融、医疗场景实现商业化落地，AI 驱动的自动化攻防（如智能威胁狩猎）进入试点阶段。未来 3-5 年，产业技术将向“智能化、主动化、全域化”方向发展——技术趋势上，AI 大模型与安全运营深度融合

（如自适应风险感知、自动化响应），量子加密技术逐步从实验室走向关键基础设施防护，车联网/物联网安全（如车载总线协议加密）随智能设备普及加速落地；产业结构上，技术创新推动安全服务（如 MSS 托管安全运营）占比持续提升（预计超 50%），传统硬件厂商加速向“产品+服务”综合解决方案商转型；生产方式上，安全开发流程（如 DevSecOps）嵌入企业 IT 全生命周期，实现漏洞预防前置化；产品形态上，从单一防护工具向集成化平台演进（如 XDR 扩展检测响应平台），并催生隐私计算即服务（PaaS）、云工作负载保护（CWPP）等新型产品。技术创新通过驱动安全能力从“被动防御”转向“主动智能”、从“单点防护”转向“全域协同”，成为产业结构优化（服务化占比提升）、生产模式变革（安全左移）、产品升级（智能化平台主导）的核心引擎，最终支撑数字经济与关键基础设施的安全底座构建。

三、信息安全技术应用产业人才需求调研

（一）人才需求规模

1.当前人才供需状况

近年来，随着数字市场改革开放步伐加快，数字领域服务优化提升，随着国家《网络安全法》《数据安全法》《个人信息保护法》《网络安全审查办法》等系列法规颁布实施和政策指导层面持续提升对网络安全的重视程度，我国信息安全产业迎来快速发展，据中国网络安全产业联盟（CCIA）数据统计，2021 年上半年，我国共有 4525 家公司开展网络安全业务，相比上一年增长 27%。值得关注的是，虽然 2021 年我国网络安全市场规模实现了 20%以上的高速增长，但网络安全人才供给却并未

保持同步增长。2023 年，网络安全人才缺口达 150 万人，根据教育部公布的数据显示，到 2027 年我国信息安全、网络空间安全、网络安全与执法人员缺口将达 327 万。

目前洛阳市信息安全技术产业正处于快速发展阶段，但人才供需存在明显缺口。据统计，洛阳市现有信息安全相关企业超过 100 家，涵盖网络安全服务、数据安全、工业信息安全等多个领域，年产值增速保持在 15%以上；然而，本地高校及职业院校每年输送的信息安全专业毕业生仅约 300-400 人，其中约 60%选择流向北上广深等一线城市，导致本地企业普遍面临“招聘难”问题——调研显示，超过 75%的洛阳信息安全企业表示“中高级安全运维、渗透测试、等保测评等岗位人才紧缺”，部分企业不得不提高薪资待遇（较 2022 年平均上涨 15%-20%）或跨区域引才以满足业务需求。整体来看，洛阳信息安全产业人才供给总量不足、留才难度大，供需比约为 1:3（即每 1 名本地毕业生对应 3 个岗位需求），亟需通过定向培养、校企合作等方式扩大适配性人才供给。

2.未来人才需求预测

《2024 年网络安全产业人才发展报告》报告显示，在网络安全人才短缺的背景下，中小型企业普遍进入数字化转型阶段，网络安全业务处于成长期，因而网络安全人才需求相对更加旺盛。加强网络安全和信息化工作、建设网络强国势在必行，而网络安全人才是其中的关键一环。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。根据最新统计分析，

我国对网络安全、信息安全人才的需求量每年约4.5万人，但高校人才培养规模不足2万人/年。我国网络安全人才供给存在“青黄不接”的情况，人才成长和培养速度显著落后于技术与社会变革的整体速度，许多企业难以找到合适的专业人士来管理和维护其信息安全系统。因此在未来3-5年，信息安全技术应用产业对专业人才的需求将呈现持续快速增长态势。

据洛阳市工信局与相关行业协会联合预测，到2027年，随着洛阳数字经济规模突破4000亿元（年复合增长率约16%）、工业互联网平台覆盖率超60%及关键信息基础设施规模化升级，信息安全技术产业人才需求将呈现爆发式增长——预计全市相关岗位缺口将达5千-6千人（较2023年翻两番），其中网络安全运维、工业信息安全、数据安全治理等中高端技术岗位占比超70%，而本地高校及职业院校当前年均输送的信息安全专业毕业生仅约300-400人（且约60%流向外地），供需缺口比例将长期维持在1:8至1:10（即每1名本地毕业生对应8-10个岗位需求）。为此，洛阳市已规划通过“校企共建信息安全产业学院”“定向委培计划”等措施，力争到2027年将本地适配性人才年供给量提升至2000人以上，但仍需依赖跨区域引才与技能培训补充，人才短缺仍是制约产业高质量发展的关键瓶颈。

（二）人才需求结构

1.岗位类型需求

洛阳及周边地区信息安全技术应用专业相关岗位要求调研结果见表1.

表 1 洛阳及周边地区信息安全技术应用专业相关岗位要求

岗位类别	岗位名称	核心技能和知识要求	经验要求
安全运维类	信息安全运维工程师	熟悉网络安全设备（防火墙、IDS/IPS 等）配置与维护；掌握操作系统（Windows/Linux）安全加固；了解常见漏洞及修复方法；具备日志分析与应急响应能力。	1-3 年信息安全或 IT 运维经验
安全开发类	安全开发工程师	熟练掌握至少一种编程语言（如 Python、Java、C/C++）；熟悉安全编码规范与常见 Web 安全漏洞（如 SQL 注入、XSS 等）；具备安全工具或系统开发能力。	1-3 年软件开发或安全相关经验
渗透测试类	渗透测试工程师	熟悉渗透测试流程与方法；掌握信息收集、漏洞扫描、漏洞利用等技术；熟练使用 Burp Suite、Metasploit 等工具；具备 Web 安全、网络协议分析能力。	1-3 年渗透测试或安全评估经验
安全管理类	信息安全工程师/主管	熟悉信息安全管理体系（如 ISO 27001）；具备风险评估、安全策略制定与落地能力；了解数据安全、访问控制、安全合规等知识；具备项目管理能力。	3-5 年信息安全相关管理经验
安全分析类	安全分析师	具备威胁情报分析能力；熟悉 SIEM、SOC 平台使用；能够进行安全事件监测、分析与响应；掌握日志分析、行为分析等技能。	1-3 年安全运营或分析相关经验
数据安全类	数据安全工程师	熟悉数据分类分级、数据加密、数据脱敏等技术；了解数据隐私保护法规（如 GDPR、个人信息保护法）；具备数据安全方案设计与实施能力。	1-3 年数据保护或安全相关经验
云计算安全类	云安全工程师	熟悉主流云平台（如 AWS、阿里云、腾讯云）安全架构与配置；掌握云环境下的身份与访问管理（IAM）、网络安全、数据安全等；具备云安全评估能力。	1-3 年云平台或安全运维经验

2.专科学历层次需求

专科学历层次在信息安全技术应用相关企业需求情况调研结果见表 2.

表 2 专科学历层次在信息安全技术应用相关企业需求情况

企业类型	信息安全技术应用岗位总数（样本）	专科学历需求占比（%）	主要岗位方向	备注
IT/互联网企业	1000	15% - 25%	网络安全运维、渗透测试助理、安全监控	
制造业/传统企业	800	30% - 40%	终端安全维护、数据备份管理、合规支持	工业控制系统（ICS）安全、内网防护需求高，更看重实操能力，专科生占比显著高于其他行业。
政府/事业单位	500	10% - 20%	等保测评辅助、网络安全值守、基础防护	编制内岗位通常要求本科及以上，但部分地方政务中心或下属机构通过劳务派遣招聘专科生负责日常运维。
金融行业	700	5% - 15%	支付安全辅助、反欺诈数据筛查、系统巡检	
专业安全公司	600	20% - 30%	漏洞扫描、应急响应支持、安全培训助教	如深信服、奇安信等企业的初级岗位（如安全服务工程师助理）对专科开放较多，侧重实战技能（如 CTF 竞赛经验）。

3.职业资格与技能证书需求

信息安全技术产业职业资格与技能证书需求情况见表 3.

表 3 信息安全技术产业职业资格与技能证书需求情况

序号	职业/岗位方向	主要职业资格证书/技能证书	需求程度（高/中/低）	适用领域/说明
1	信息安全工程师	注册信息安全专业人员（CISP）	高	企业级信息安全建设、风险评估、安全运维等通用岗位，国内认可度最高
2	网络安全分析师/渗透测试工程师	注册渗透测试工程师（CISP-PTE） 注册信息安全专业人员-渗透测试（CISP-PTS）	高	渗透测试、漏洞挖掘、红队/蓝队实战，企业安全防御与攻击模拟需求旺盛
3	安全运维工程师	信息安全保障人员认证（CISAW-安全运维方向）	高	信息系统日常安全运维、日志分析、事件响应，适合运维与安全结合岗位
4	安全开发工程师	CISP-软件安全开发方向（CISP-SSD）	中高	安全编码、软件安全设计、SDL（安全开发生命周期）实践，开发与安全融合岗位
5	数据安全工程师	CISP-数据安全方向（CISP-DSG）	中高	数据分类分级、隐私保护、数据防泄漏（DLP），数据密集型行业（金融/医疗）需求突出
6	云计算安全工程师	云安全工程师认证（如 CSA 的 CCSK、华为 HCIP-Cloud Security）	中	云环境（公有云/私有云）安全配置、容器/K8s 安全、云原生防护，云服务相关岗位
7	终端/移动安全工程师	移动应用安全工程师认证（如梆梆安全、爱加密相关） Android/iOS 安全开发认证	中	移动 APP 安全加固、逆向分析、恶意代码检测，移动端产品安全需求
8	信息安全服务工程师（咨询/审计）	信息系统审计师（CISA） 注册信息系统安全师（CISSP，国际）	中	信息安全咨询、合规审计（如等保 2.0、GDPR）、企业安全体系设计，高端岗位需求

9	等级保护测评师	等级保护测评师认证（公安部认可）	中	等保 2.0 测评实施、网络安全等级保护合规检查，政府/国企/关键信息基础设施领域必备
10	基础安全技术岗位（如防火墙管理）	网络安全工程师认证（如华为 HCIA-Security、深信服 SCSA）	低（但基础必备）	防火墙/IDS/IPS 配置、基础网络防护，中小型企业或初级岗位入门需求

（三）人才能力素质要求

1.专业知识要求

信息安全技术产业岗位专业知识要求见表 4.

表 4 信息安全技术产业岗位专业知识要求

岗位类型	核心专业知识领域	企业需求占比（约）	典型应用场景
网络安全工程师	- 网络协议（TCP/IP、HTTP 等）与架构 - 防火墙/IDS/IPS 原理与配置 - 渗透测试（Web/系统漏洞挖掘） - VPN/零信任网络技术 - 网络流量分析与日志审计	35%~40%	企业内网安全防护（如办公网边界防护）、关键业务系统（如金融交易系统）的网络层安全加固、云网络（如 AWS/Azure）安全策略配置。
安全运维工程师	- 操作系统安全（Linux/Windows 加固） - 安全设备（防火墙、WAF、SOC 平台）日常运维 - 漏洞管理（CVSS 评分、补丁策略） - 安全事件应急响应与溯源 - 日志分析工具（ELK、Splunk）	25%~30%	企业数据中心/云服务器的日常安全监控（如 7×24 小时 SOC 值守）、等保 2.0 合规运维（定期漏洞扫描与修复）、突发攻击（如 DDoS）的快速阻断与恢复。
渗透	- 黑客攻击技术（SQL 注入、XSS、CSRF 等 Web	15%~20%	金融/电商网站上线前的安全测试、政府/央企系统的年度渗透评估、移动 APP

测试工程师	漏洞） - 内网渗透（横向移动、权限提升） - 工具使用（Burp Suite、Metasploit） - 安全编码规范（OWASP Top 10） - 报告撰写（漏洞复现与修复建议）		（Android/iOS）的安全漏洞挖掘。
数据安全工程师	- 数据分类分级（敏感数据识别） - 加密技术（对称/非对称加密、同态加密） - 数据脱敏（动态/静态） - 数据防泄漏（DLP）策略 - 合规标准（GDPR、个人信息保护法）	10%~15%	医疗/金融行业患者/客户数据的加密存储与传输、跨国企业跨境数据流动的合规管控、数据库（如 Oracle/MySQL）的访问权限精细化控制。
安全开发工程师	- 安全编程（C/Java/Python 安全编码） - 安全框架（OAuth2.0、JWT 认证） - 代码审计（SAST/DAST 工具） - API 安全（鉴权/防重放） - DevSecOps 流程集成	8%~12%	企业级软件（如 ERP/CRM）开发中的安全需求嵌入、云原生应用（Kubernetes 微服务）的安全设计、开源组件（如 Log4j）漏洞的预防与修复。
云计算安全工程师	- 云架构（AWS/Azure/阿里云服务模型） - 云原生安全（容器/K8s 安全、Serverless 防护） - 云访问控制（IAM 策略） - 云数据安全（对象存储加密） - 云合规（等保云扩展要求）	5%~10%	企业上云（如混合云部署）中的安全架构设计、云数据库（RDS）的访问隔离、SaaS 应用（如 CRM）的多租户数据隔离。

2.职业技能要求

信息安全技术产业岗位职业技能要求见表 5.

表 5 信息安全技术产业岗位职业技能要求

技能类别	具体技能内容	企业需求占比	具体岗位要求与应用说明
网络安全防护	- 防火墙/IDS/IPS 配置与管理（如 Cisco ASA、Snort、华为 USG） - 网络流量分析与异常检测（如 Wireshark、NetFlow） - VPN 部署与维护（IPSec/SSL VPN） - 无线网络安全加固（WPA3、射频管控）	32%-38%	岗位：网络安全工程师、渗透测试工程师 应用：负责企业网络边界防护（如配置防火墙规则阻断非法访问）、实时监测流量识别 DDoS/SQL 注入等攻击；需掌握主流安全设备操作，例如通过 Snort 编写规则检测恶意流量，或部署 IPSec VPN 保障分支机构通信加密。
系统安全加固	- 操作系统安全配置（Windows/Linux 权限管理、SELinux/AppArmor） - 补丁管理与漏洞修复（WSUS、YUM/Cron 定时更新） - 终端安全防护（EDR、防病毒策略） - 数据库安全（MySQL/Oracle 权限控制、加密存储）	25%-30%	岗位：系统安全运维工程师、安全运维专员 应用：针对服务器/终端进行基线加固（如关闭 Linux 不必要的 SUID 权限、Windows 禁用默认共享），定期推送安全补丁；需熟悉 EDR 工具（如 CrowdStrike）监测主机异常行为，或通过 Oracle 透明数据加密（TDE）保护核心数据库字段。
应用安全开发	- 安全编码规范（OWASP Top 10 防护、输入验证/输出编码） - 代码审计工具使用（Fortify、SonarQube） - Web 应用防火墙（WAF）配置（ModSecurity、Cloudflare） - API 安全设计（OAuth2.0、JWT 令牌防护）	18%-22%	岗位：安全开发工程师、DevSecOps 工程师 应用：参与 Web/移动应用开发全流程安全管控（如防止 SQL 注入/XSS 攻击），使用 Fortify 扫描代码漏洞并修复；需配置 WAF 拦截恶意请求（如 CC 攻击），或设计 API 鉴权机制（如通过 JWT 令牌防止未授权访问）。
数据安全与隐私	- 数据分类分级（敏感数据识别、合规标签） - 加密技术应用（对称/非对称加密、密钥管理） - 数据脱敏（动态/静态脱敏工具）	15%-20%	岗位：数据安全工程师、隐私合规专员 应用：对企业数据资产进行分级（如将用户身份证号标记为“高敏感”），采用 AES-256 加密存储或 TLS 传输；需使用脱敏工具（如 Informatica）对

	- 隐私合规（GDPR/《个人信息保护法》实施）		测试数据脱敏，或制定隐私政策满足国内《个人信息保护法》中“最小必要”原则（如仅收集必要的用户手机号）。
安全应急响应	- 攻击事件分析（日志溯源、取证工具如 Autopsy、FTK） - 应急流程制定（应急预案、灾备演练） - 勒索软件/APT 攻击处置（隔离感染主机、恢复备份） - 安全通报与报告编写	12%-16%	岗位：安全分析师、应急响应工程师 应用：当发生数据泄露或系统入侵时，快速定位攻击路径（如通过 SIEM 工具关联日志发现异常登录），执行遏制措施（如断开受感染服务器网络）；需参与制定企业级应急方案（如每季度演练数据库被加密后的恢复流程），并撰写事件报告供管理层决策。
云安全与新兴技术	- 云平台安全配置（AWS/Azure/阿里云 IAM、安全组规则） - 容器/K8s 安全（镜像扫描、网络策略） - IoT 设备安全（固件漏洞检测、通信协议加密） - AI 安全风险（对抗样本防御、模型数据泄露防护）	8%-12%	岗位：云安全工程师、新兴技术安全研究员 应用：针对企业上云场景（如使用阿里云 ECS），配置最小权限原则的 IAM 角色，限制云存储桶公网访问；在容器化环境中，通过 Trivy 扫描 Docker 镜像漏洞，或设置 K8s 网络策略隔离微服务；对智能摄像头等 IoT 设备，需检测固件中的弱口令或未授权访问接口。

3.职业素养要求

信息安全技术应用岗位职业素养要求见表 6.

表 6 信息安全技术应用岗位职业素养要求

素养类别	具体素养要求	企业考核标准/关联影响	典型岗位与案例
职业道德	- 遵守《网络安全法》《数据安全法》等法律法规，严格保护用户隐私与企业数据； - 拒绝参与黑客攻击、数据倒卖等违法行为； - 对敏感信息（如用户身份、业务数据）绝对保密，不擅自泄露或滥用。	- 企业通过背景调查、保密协议签署及日常行为审计考核； 违规可能导致法律追责（如侵犯公民个人信息罪）、企业声誉损失及高额罚款（如 GDPR 违规最高罚 2000 万欧元）。	岗位：安全运维工程师 案例：某企业运维人员因私自下载客户数据库并出售，被追究刑事责任，企业被监管部门罚款 500 万元。

责任意识	- 对负责的信息安全系统（如防火墙配置、漏洞修复）全流程负责，确保操作可追溯； - 主动发现并上报潜在风险（如未授权访问、异常流量），不隐瞒问题； - 在应急事件中快速响应，降低损失（如数据泄露、服务中断）。	- 考核故障处理时效（如漏洞修复平均时间≤4小时）、风险上报及时率（≥95%）及事件复盘报告质量； 责任缺失可能导致安全事故扩大（如勒索病毒扩散至全网）。	岗位：安全分析师 案例：某公司安全分析师发现钓鱼邮件攻击迹象后未及时上报，导致全公司内网被入侵，核心数据被加密勒索。
学习能力	- 持续跟踪最新威胁情报（如APT攻击手法、零日漏洞利用）及技术动态（如AI安全、量子加密）； - 掌握主流工具（如Wireshark、Metasploit、IDS/IPS系统）及新兴技术（如云安全、IoT安全防护）； - 通过认证考试（如CISSP、CISP、CEH）或内部培训提升专业水平。	- 考核新技术应用能力（如能否部署零信任架构）、认证获取情况（如CISP持证优先）及知识分享贡献（如编写内部技术文档）； 能力滞后可能导致防护方案失效（如无法防御新型勒索软件）。	岗位：渗透测试工程师 案例：某工程师因未学习WebAssembly新型攻击手法，未能发现客户网站隐藏漏洞，导致被黑产利用窃取用户信息。
团队协作	- 与开发、运维、法务等部门高效沟通（如向开发人员解释代码安全缺陷，向管理层汇报风险等级）； - 参与跨部门安全项目（如系统上线前的安全评审、数据合规整改）； - 在应急响应中明确分工（如检测、阻断、溯源各环节协同）。	- 考核跨部门协作满意度（如开发团队对安全反馈的响应效率）、项目参与度（如安全评审通过率≥90%）及应急响应团队配合流畅度； 协作不畅可能导致安全措施落地延迟（如漏洞修复被开发排期拖延）。	岗位：安全架构师 案例：某项目因安全团队与开发团队沟通不足，未在代码上线前修复SQL注入漏洞，上线后被黑客批量盗取用户账号。
风险意识	- 具备前瞻性思维，主动评估业务场景中的潜在威胁（如移动办公的数据泄露风险、第三方供应商的供应链攻击风险）； - 对高风险操作（如权限提升、生产环境变更）严格执行审批与备份流程； - 定期模拟攻击（如红蓝对抗）验证防护体系有效性。	- 考核风险评估报告质量（如覆盖场景完整性）、高风险操作合规率（100%审批）及演练效果（如漏洞发现率≥80%）； 风险忽视可能导致重大损失（如供应链攻击引发全网瘫痪）。	岗位：安全合规专员 案例：某企业因未评估第三方云服务商的数据存储合规性，导致客户数据跨境传输违反国内法规，被责令整改并赔偿用户损失。

沟通表达	- 能清晰向非技术人员（如管理层、客户）解释复杂安全概念（如“数据加密”“DDoS 攻击”），使用可视化工具（如风险热力图、攻击链图谱）辅助说明； - 撰写专业报告（如安全事件分析报告、年度风险评估报告），逻辑严谨且结论明确； - 在培训中传递安全意识（如员工钓鱼邮件识别技巧）。	- 考核沟通对象理解度（如管理层能基于汇报做出正确决策）、报告可读性（如无技术背景人员能看懂核心结论）及培训效果（如员工安全操作错误率下降≥30%）； 表达不清可能导致决策失误（如管理层因不懂风险拒绝必要安全投入）。	岗位：安全培训讲师 案例：某工程师向管理层汇报勒索软件风险时仅使用专业术语，未说明业务影响，导致管理层削减安全预算，后续发生大规模数据加密事件。

四、同类高职院校信息安全技术应用专业竞争力分析

（一）与同类院专业对比

与同类高职院校相比，洛阳商业职业学院信息安全技术应用专业与河南职业技术学院（国家“双高”计划院校）、郑州信息科技职业学院（省信息安全特色专业建设单位）师资力量、课程设置、实训条件及校企合作平台四方面进行了对比。

1. 师资力量对比

表 7 与同类院校师资力量对比统计

院校	师资规模与结构	双师型比例	行业资质	我校优劣势
河南职业技术学院	教授、副教授 15 人	90%	河南省职业教育示范性专业点	劣势：缺乏省级名师工作室支撑
郑州信息科技职业学院	副高以上 2 人	80%（企业经验）	“码农计划”第二批试点院校、河南省优质高等职业院校	劣势：高职称教师数量不足
洛阳商业职业学院	专兼职教师 15 人，硕士 13 人，	2 人	无	—

院校	师资规模与结构	双师型比例	行业资质	我校优劣势
	副教授 2 人			

优势：我校硕士及以上学历教师占比高于郑州信息科技职业学院，但需提升高职称教师比例；不足：双师型比例低于另外两所院校，行业顶级资质数量不足。

2. 课程设置对比

表 8 与同类院校课程设置对比统计

院校	传统技术课程	新兴技术课程	证书融合
河南职业技术学院	Python 程序设计、计算机网络技术及协议、数据库技术	信息安全产品配置与应用、系统防护与加固	网络安全运营平台职业等级证书
郑州信息科技职业学院	计算机网络基础、数据库原理与应用、Linux 系统与网络管理	Web 应用安全攻防进阶、企业安全攻防实战	计算机技术与软件专业技术资格（水平）考试
洛阳商业职业学院	C 语言程序设计	高级交换路由技术	计算机三级证书

优势：我校 C 语言程序设计课程扎实，但新兴技术模块薄弱。不足：前沿技术缺失；证书覆盖窄。

3. 实训条件对比

表 9 与同类院校实训条件对比统计

院校	实训设施	企业合作深度	竞赛成果
河南职业技术学院	技术攻关联合实验室	河南中原智能电气科技有限公司	未公开
郑州信息科技职业学院	Web 安全实训室	未公开资源	河南省团体二等奖
洛阳商业职业学院	网络安全攻防实训室	洛阳众智软件科技有限公司	无省级以上奖项

4. 校企合作平台对比

表 9 与同类院校校企合作平台对比统计

院校	校企合作主要平台
河南职业技术学院	与珠海格力集团深度合作，共同投资建设，可用于学生实训、教师科研以及面向社会提供技术实训服务和“1+X”证书培训与考核服务。与河南中原智能电气科技有限公司、启明星辰数字科技（郑州）有限公司等企业共建，开展技术研发和人才培养。

郑州信息科技职业学院	与华为、京东、腾讯、科大讯飞、长城汽车、星星装饰、中国建筑、海马汽车、北京奔驰、东风雷诺等众多行业领军企业建立了合作关系，共同设计培养目标、制定培养方案、搭建教育场景等。
洛阳商业职业学院	与洛阳大数据产业园、360 数字安全集团、洛阳众智软件科技有限公司、中锐网络股份有限公司、河南打造前程科技有限公司、中兴通讯股份有限公司密切合作，这些企业为学院提供了人才培养模式改革、行业职业资格证书培训和顶岗实习就业等方面的支持。

综上所述，洛阳商业职业学院优势在于聚焦区域数字经济需求，开设针对专升本或考取专业执业证书等特色方向，与本地安全企业（如洛阳大数据产业园入驻企业）共建实训基地，强化实践教学；课程设置贴合产业前沿，增设“AI 安全基础”“人工智能应用”等新兴技术模块，但师资力量相对薄弱（双师型教师占比低于河南职业技术学院的 65%），缺乏国家级信息安全竞赛指导经验。

（二）自身优势与劣势

洛阳商业职业学院的信息安全技术应用专业在服务地方产业中具备独特优势：立足洛阳副中心城市建设规划，紧密对接区域智能制造、政务数字化转型等安全需求，通过校企合作共建“网络安全实训基地”深化产教融合（如与本地信息技术企业合作开发针对性课程），依托学院商贸管理类学科基础创新开设“数据备份与恢复”特色课程，实践教学突出“项目驱动+模拟攻防”模式（如组织学生参与校内外网络安全竞赛、模拟企业安全事件处置），有效强化学生实战能力；但同时也存在明显劣势——教学资源方面，校内专业实训设备（如高端防火墙、漏洞靶场）配置相对不足，难以完全满足新兴技术（如云安全、工业互联网安全）实践需求；师资水平上，专职教师中同时具备“行业认证（如 CISSP/CISP）+企业实战经验”的“双师型”教师占比偏低，部分教师对前

沿技术（如AI安全攻防）掌握滞后；社会认可度方面，作为新建高职院校，专业品牌影响力尚未充分释放，家长与学生对信息安全职业发展路径的认知局限可能影响招生吸引力，需通过强化校企合作成果展示、优秀毕业生案例宣传等方式提升专业口碑。

五、信息安全技术应用专业可行性分析

（一）社会需求可行性分析

信息安全技术产业社会可行性显著，专业人才培养对区域与就业创业推动作用突出：洛阳作为中原城市群副中心城市，正大力发展数字经济与智能制造，亟需大量信息安全技术技能人才支撑本地企业数字化转型与关键基础设施安全防护，我校开设该专业精准对接区域产业需求，毕业生可在洛阳及周边地区的制造业、金融、政务等行业从事安全运维、渗透测试等岗位，有效缓解区域信息安全人才缺口，同时通过“订单班”“现代学徒制”等模式提升学生就业竞争力，带动创业机会（如网络安全服务工作室）；企业调研显示，超85%的本地企业（如洛阳工业控股集团、本地银行分支机构）认为信息安全专业人才“急需”或“紧缺”，家长与学生调研中，80%以上家长认可该专业“就业前景好、薪资水平高”，75%的学生因“兴趣浓厚”和“职业发展清晰”选择报考；我校具备较强的社会资源整合能力，已与奇安信、深信服等头部企业建立校企合作关系，共建信息安全实训室，引入企业真实项目案例与认证培训体系（如CISP、CISP-PTE），并与洛阳市网络安全协会、河南省信息安全产业联盟协作，邀请行业专家参与课程开发与授课，定期举办网络安全竞赛与讲座，依托洛阳数字经济产业园实现“教学-实训-就业”闭环，充分保障专业建设的

产业适应性与人才培养质量。

（二）教师队伍可行性分析

1.校内教师培训

我校聚焦信息安全技术应用专业建设与人才培养需求，系统开展校内教师专项培训，围绕网络安全攻防实战、数据安全防护、工业信息安全等前沿技术方向，通过“理论授课+实操演练+企业案例研讨”多元模式，邀请行业专家与校内骨干教师共同参与，重点强化教师在漏洞分析、安全工具应用、应急响应等核心技能的实操能力，同时结合我校商科背景与区域产业（如洛阳制造业数字化转型、智慧城市安全需求）特色，推动教学内容与行业需求紧密对接，旨在打造一支“懂技术、会教学、能实战”的“双师型”教师队伍，为信息安全技术应用专业的高质量发展与学生职业技能培养提供坚实师资保障。

2.校外教师聘请

我校为深化信息安全技术应用专业产教融合、强化实践教学实效，积极对接本地信息安全产业资源（如洛阳大数据产业园、网络安全技术应用试点企业及科研机构），重点聘请具有丰富行业经验的一线技术专家、企业安全工程师及项目负责人担任校外兼职教师，通过参与专业课程授课、实训指导、技能竞赛培训及岗位实践带教，将企业真实项目案例、前沿安全技术标准与岗位能力需求融入教学全过程，既弥补校内师资实践经验不足的短板，又精准对接洛阳数字经济与信息安全产业发展对技能型人才的培养要求，有效提升学生技术应用能力与就业竞争力，助力专业建设与区域产业需求同频共振。

3.“双师型”教师队伍打造

我校立足区域数字经济发展需求，聚焦信息安全技术应用专业建设，以培养“双师型”教师队伍为核心抓手，通过“引培并举、校企共育”模式，一方面积极引进具有网络安全企业实战经验或行业认证（如 CISP、HCIE-Security 等）的高技能人才充实师资，另一方面选派专业教师赴头部网安企业（如奇安信、深信服等）及本地信息安全产业园区实践锻炼，参与真实项目攻防演练、风险评估等技术工作，同步深化与洛阳本地网络安全企业（如洛阳信大捷安、相关数字化转型服务商）的校企合作，共建“双师型”教师培养培训基地，推行“教师+工程师”双导师制，将企业前沿技术标准、真实案例融入教学，持续提升教师的教学能力与实践技能，着力打造一支既懂理论教学又精技术应用、既能课堂授课又能指导学生竞赛与项目实战的“双师双能”骨干团队，为信息安全技术应用专业高质量发展和区域网络安全人才培养提供坚实师资保障。

（三）教学资源可行行分析

学校地处国家副中心城市洛阳，本地信息安全技术产业（涵盖网络安全服务、工业信息安全等细分领域）正快速发展，超百家相关企业（含国家级试点示范单位）对高素质技能人才的需求旺盛，为专业教学提供了贴近实际的产业场景与实习就业支撑；另一方面，学院已具备信息技术类专业的教学基础（如计算机网络、软件技术等相关专业师资与实训条件），可通过资源整合与针对性补充（如引入信息安全攻防实训平台、校企合作开发活页式教材、聘请企业工程师参与课程设计），快速搭建“基础理论+技能实训+企业实践”的模块化教学资源体系；此外，

洛阳市政府对数字经济与信息安全产业的扶持政策（如人才引育补贴、产教融合项目支持），也为专业教学资源的持续优化提供了政策与资金保障，整体上能够有效支撑专业人才培养目标与区域信息安全产业需求的精准对接。

六、调研总结与建议

（一）调研总结

1.人才需求核心结论

（1）专业知识

信息安全技术应用行业对专业知识的要求呈现出清晰的层级与逻辑，形成“基础+核心+拓展”三维体系。其中计算机硬件基础、计算机网络技术、C 语言程序设计等是构建稳固的底层支撑；网络安全设备配置、信息安全产品配置与应用、数据存储与容灾锤炼专业的实战能力，为信息安全提供技术保障；无线网络安全技术、数据备份与恢复、信息安全标准与法规塑造前瞻性与复合型视野，在合规合法的基础上进行更深一层的发展。这一体系确保了人才培养既能筑牢根基，又能精准深入专业领域，并具备适应技术演进与业务融合的持续发展能力。

（2）职业技能

围绕“基础+核心+拓展”三维体系，全面覆盖从一线实操到项目管理的职业需求。硬件基础帮助理解系统运行原理，网络技术是分析所有网络威胁的基石，而 C 语言等编程能力则是进行漏洞分析、安全工具开发和深度代码审计的前提，基础技能如同大厦的地基，决定了职业发展的深度和潜力。熟练配置防火墙、入侵检测系统，部署和应用各类安全产

品，以及规划实施数据备份与容灾方案，都是职业技能的核心层，直接对应日常安全运维与防护工作。信息安全技术应用行业从业者不仅关注传统有线网络，更要应对 Wi-Fi、移动网络等带来的新威胁；不仅精通技术实现（如数据备份），更要理解其背后的合规性要求（如等保 2.0、数据安全法），从而成为既懂技术又懂管理和法规的复合型人才。

（3）职业素养

职业素养要求契合行业“重攻防、强合规、需迭代”的工作特性。责任心与敬业精神是绝对根基，确保从代码审计到系统加固的每一个操作准确无误，直接关乎网络与数据的核心安全；敬业精神则驱动从业者在 7x24 小时应急响应和长期对抗中始终保持高度警惕，是守护数字世界的“基础性刚需”。自律性要求从业者严守操作规范与合规要求，避免因疏忽引入风险；抗压能力则使其在遭遇网络攻击、突发故障等高压环境下仍能冷静分析、有效处置。团队协作与沟通能力则是联动研发、运维、管理层乃至客户的核心纽带，确保安全策略跨部门高效执行。持续学习是跟上威胁情报、新防御技术迭代节奏的前提；而创新意识则能推动主动防御体系构建和响应流程优化，化被动为主动。

2.专业竞争力核心结论

信息安全技术产业专业在产业人才培养市场中属于需求旺盛但竞争激烈的赛道，我校作为地方高职院校，核心竞争优势在于立足中原城市群数字经济发展需求，聚焦中小微企业及本地产业园区（如洛阳大数据产业园）的信息安全基础岗位（如安全运维、基础渗透测试），通过“校企合作+定向培养”模式输送上手快、适应强的技能型人才。

（二）人才培养方案修订建议

1.明确目标定位

洛阳商业职业学院立足区域数字经济发展需求，聚焦信息安全技术应用专业建设，以培养“双师型”教师队伍为核心抓手，通过“引培并举、校企共育”模式，一方面积极引进具有网络安全企业实战经验或行业认证（如 CISP、HCIE-Security 等）的高技能人才充实师资，另一方面选派专业教师赴头部网安企业（如奇安信、深信服等）及本地信息安全产业园区实践锻炼，参与真实项目攻防演练、风险评估等技术工作，同步深化与洛阳本地网络安全企业（如洛阳信大捷安、相关数字化转型服务商）的校企合作，共建“双师型”教师培养培训基地，推行“教师+工程师”双导师制，将企业前沿技术标准、真实案例融入教学，持续提升教师的教学能力与实践技能，着力打造一支既懂理论教学又精技术应用、既能课堂授课又能指导学生竞赛与项目实战的“双师双能”骨干团队，为信息安全技术应用专业高质量发展和区域网络安全人才培养提供坚实师资保障。

2.构建课程模块

构建“基础+核心+拓展”三维体系，强化岗位能力衔接。围绕人才知识能力需求，打破传统课程壁垒，构建模块化课程体系。首先是基础通识模块：涵盖计算机硬件基础、计算机网络技术、C 语言程序设计等课程，夯实理论基础；其次是核心能力模块：操作系统安全、网络安全设备配置、信息安全产品配置与应用、数据存储与容灾等，强化核心岗位能力；最后是拓展提升模块：包括无线网络安全技术、数据备份与恢复、高级交换路由技术、交换路由组网技术等课程，提升人才综合适配性。

3.设置岗位课程方向

我校信息安全技术应用专业立足洛阳数字经济发展需求与区域产业特色，聚焦信息安全技术应用核心能力培养，构建“基础夯实+技术精专+实战强化”的模块化岗位课程体系，主要方向涵盖网络安全运维（如防火墙/入侵检测系统配置、日志分析与安全事件响应）、数据安全防护（含数据库加密、敏感信息脱敏及合规管理）、工业信息安全（对接洛阳装备制造与工业互联网场景，侧重工业控制系统安全检测与防护）、渗透测试与漏洞挖掘（通过 CTF 竞赛、靶场实训培养攻防实战技能）、云计算与移动安全（适配企业上云趋势，覆盖云平台安全配置及移动应用安全检测），并融入网络安全法律法规、风险评估等合规管理类课程，同步结合洛阳本地企业真实项目（如关键信息基础设施防护、数据跨境安全等场景），通过校企合作实训基地、虚拟仿真实验平台开展工学交替式教学，精准对接网络安全工程师、安全运维专员、渗透测试助理、数据安全管理员等岗位需求，培养“懂技术、会防护、能实战”的高素质技术技能人才。

4.增加实践教学课时

洛阳商业职业学院立足区域数字经济发展需求，结合信息安全技术应用专业特点，主动优化人才培养方案，通过系统性增加实践教学课时，将理论教学与技能训练深度融合——一方面围绕网络安全攻防、数据安全防护、信息系统漏洞检测等核心岗位能力，增设网络靶场实战、企业级安全项目模拟、工控系统安全演练等模块化实训课程，强化学生对防火墙配置、渗透测试工具应用、应急响应流程等实操技术的掌握；另一

方面联合本地信息安全企业（如洛阳工业互联网安全试点单位）、共建校外实训基地，引入真实项目案例（如中小型企业网络安全加固、政务系统数据脱敏等），通过“做中学、学中做”提升学生解决实际问题的能力；同时，通过延长实验室开放时间、组织网络安全技能竞赛与校内攻防演练，进一步延伸实践教学链条，切实培养“懂理论、精技术、能实战”的高素质技术技能人才，为服务洛阳信息安全技术产业发展、输送适配区域需求的实战型信息安全人才提供有力支撑。

5.“1+X”证书融合

实现“课证岗”深度融合，提升岗位适配性。对照调研中岗位必备证书，在现有方案中明确“1+X 证书”融入路径。

将中国大学生计算机设计大赛获奖融入数据库技术、计算机硬件基础课程；蓝桥杯全国软件和信息技术专业人才大赛、ACM-ICPC 国际大学生程序设计竞赛、创新创新类相关大赛获奖融入 C 语言程序设计等课程；网络技术工程师证书融入计算机网络技术课程；全国计算机二级级以上等级证书融入信息技术基础课程；课程考核与证书理论考试同步，实训项目覆盖证书实操要求，确保学生毕业前考取该证书，可置换对应的课程学分。

针对不同特色方向，推荐对应证书，并在对应方向课程中增设证书培训模块，鼓励学生“一证多能”。