面向岗位需求的中职网络安全技术课程实践教学研究

刘德斌

青岛市供销职业中等专业学校，山东省青岛市，266000；

青岛市经济贸易技术学校，山东省青岛市，266000；

摘要：面向岗位需求的中职网络安全技术课程教学研究聚焦当前教学核心问题，系统分析课程体系与岗位需求脱节、实训条件与实战教学需求差距悬殊两大核心症结。研究以职业能力本位、认知学徒制等理论为支撑，提出重构岗位导向实践课程体系、校企协同共建实战化训练平台、开展情景模拟与攻防演练三大优化策略，通过任务拆解、平台共建、分层演练及反思优化等路径，构建适配岗位需求的技能培养链条，为提升中职网络安全专业学生岗位适配能力提供实践方案。

关键词：岗位需求；中职；网络安全技术课程；实践教学

DOI：10.64216/3104-9702.25.06.004

引言

网络安全行业快速发展催生大量技能型人才需求，中职院校作为技能人才培养主阵地，其网络安全技术课程教学质量直接影响人才输出适配度。当前中职网络安全教学普遍存在课程内容滞后岗位需求、实践教学与真实工作场景脱节等问题，难以满足企业对渗透测试、应急响应等核心技能的要求。基于此，本研究立足岗位需求导向，结合职业教育教学理论，探索实践教学优化路径，旨在破解教学与岗位需求错位难题，实现技能培养与企业需求的精准对接。

1 面向岗位需求的中职网络安全技术课程教学核心问题

1.1 网络安全课程体系与岗位需求存在显著脱节

多数中职院校的网络安全课程仍固守传统计算机课程框架，核心内容始终聚焦基础理论与通用技术的讲授；对于等保测评、数据安全、云安全、工控安全、渗透测试等企业高频需求的技术模块，课程内容涉猎匮乏。教材更新周期普遍偏长，难以精准匹配网络安全技术快速迭代的节奏，更无法同步跟进相关政策法规的更新动态。同时，课程设置呈现明显的“重理论、轻实践”倾向，理论课与实践课的课时比例严重失衡，部分院校的实践课时占比仅为总课时的 30%。实践内容多以验证性实验为主，严重缺乏攻防对抗、漏洞挖掘、应急响应等贴合岗位实际工作场景的综合训练项目。这样的课程体系既无法满足企业对技能型人才的核心需求，也难以助力学生构建适配岗位要求的能力体系，最终导致教学效果与岗位需求脱节严重。

1.2 实训条件与实战教学需求差距悬殊

网络安全实训的有效开展，必须依托专用攻防平台、虚拟化设备、专业安全设备、入侵检测系统等核心资源，但多数中职院校受经费投入限制，实训设备不仅数量严重不足，且型号普遍陈旧，根本无法搭建起贴近企业真实环境的攻防实训网络。现有实训平台多为模拟环境，既缺乏真实的网络流量、典型漏洞场景，也无法还原真实攻击行为，平台功能多局限于基础配置调试和简单攻防演示，难以支撑大规模渗透测试、应急响应演练、等保测试等核心实践操作项目的开展。同时，多数校企合作仅停留在企业参观、专家讲座等浅层次互动，尚未形成共建实训基地、共同开发实训项目、共担教学任务的深度协同模式，这进一步加剧了实训条件与实战教学需求之间的矛盾，制约了学生实践技能的提升。

2 面向岗位需求的中职网络安全技术课程实践教学优化策略

2.1 以岗位能力为锚点重构实践课程体系

2.1.1 任务设计

中职院校重构岗位导向的网络安全实践课程体系，需以职业能力本位理论为根基，围绕核心岗位任务链的拆解与重组展开系统性设计。为此，专业教师需主动深入企业开展调研，精准分析网络安全运维、渗透测试、应急响应等核心岗位的工作流程，将其拆解为可量化、可落地的任务模块，再结合模块细分法构建岗位任务矩阵，明确各模块对知识储备、技能掌握、职业态度的具体要求，从而搭建起以岗位能力为核心的课程目标架构。构建过程中要严格确保各模块间的有机关联，既让每个模块独立成章、重点突出，又能形成递进式的能力培养链条，比如将渗透测试任务细化为信息收集、漏洞扫描、

攻击实施、痕迹清除等子任务，每个子任务对应独立的教学单元，再通过项目整合、综合实训演练实现技能进阶。

例如，专业教师团队深入本地中小型制造企业开展网络安全岗位调研，调研团队通过参与企业日常网络运维工作、查阅岗位操作手册等方式，精准梳理出企业网络安全运维岗位中与防火墙配置相关的核心工作流程，该流程涵盖网络边界安全需求分析、防火墙规则规划、规则配置实施、配置效果验证及规则优化五个关键环节。基于调研结果，教师团队将防火墙配置核心工作流程拆解为三个可量化的任务模块，分别是企业网络边界安全需求分析模块、防火墙基础规则配置模块以及防火墙配置优化与验证模块，同时构建岗位任务矩阵明确各模块的具体要求。

2.1.2 课程体系结构优化

课程体系的结构化设计需严格遵循工作过程系统化原则，将岗位实际任务转化为学习性工作任务；可采用典型工作情景法，筛选出覆盖 80%以上岗位工作场景的典型任务，再按照完整的工作流程重构课程序列。例如在网络安全配置模块中，可设计企业网络边界安全防护的典型情景，要求学生依次完成防火墙规则配置、入侵检测系统部署、安全策略优化等任务，每个任务均包含任务分析、方法制定、工具选择、操作实施、效果验证等完整环节，形成闭环训练模式。同时要注重任务难度的螺旋式上升，通过设置基础型、提高型、创新型多级任务包，精准匹配不同学习水平学生的能力发展需求，确保全体学生都能在原有基础上实现技能提升。

例如，在模块细分过程中，教师团队将防火墙基础规则配置模块进一步拆解为地址池定义、访问控制列表编制、NAT 转换规则配置、安全区域划分四个子任务，每个子任务均对应独立的教学单元，各子任务之间形成递进式能力培养链条，前序子任务的完成质量直接支撑后续子任务的开展，例如地址池定义子任务的完成能够为访问控制列表编制提供准确的 IP 地址范围依据，而访问控制列表编制则是 NAT 转换规则配置的核心前提。为确保各模块的有机关联，教师团队通过设计企业网络边界防护综合项目将所有子任务整合，该项目要求学生以企业网络边界安全防护为核心目标，依次完成各子任务的操作后开展综合实训演练，最终实现从单一子任务技能掌握到综合项目实操能力进阶的培养目标。

2.2 校企协同共建实战化网络安全训练平台

2.2.1 协同平台建设

面向岗位需求的中职网络安全课程实践教学，须以高质量实战化平台为支撑，才能引领学生开展沉浸式操作性学习，将理论知识转化为实践能力，增强知识迁移应用水平。平台建设初期，需率先成立校企联合工作组，由企业技术骨干与学校专业教师共同制定平台建设规划，明确双方在技术资源输出、设备投入保障、人员配置分工等方面的责任，构建“企业提供真实场景与技术支持、学校提供场地与基础教学保障”的协同模式。合作过程中要注重校企文化深度融合，通过定期组织校企互访、技术交流研讨会、技能比武等活动，促进双方在管理理念、操作规范、职业素养要求上形成共识，为深度合作奠定文化基础，确保平台建设从规划阶段就植入校企协同基因。

例如，学校与本地网络安全服务企业联合成立平台建设工作组，工作组由企业 2 名资深网络安全运维工程师和学校 3 名专业教师组成，双方共同制定平台建设规划方案，方案明确企业负责提供真实的企业网络拓扑结构、华为 USG6000 系列防火墙等硬件设备的技术参数以及企业真实的防火墙配置案例资源，学校负责提供实训场地、基础教学设备以及实训教学组织保障工作，形成优势互补的协同建设模式。

在平台建设过程中，校企双方定期组织技术交流研讨会，企业技术工程师向教师团队讲解真实企业防火墙配置中的常见问题及解决技巧，教师团队则向企业技术工程师反馈中职学生的认知特点和技能基础，双方共同优化平台实训资源的适配性。

2.2.2 平台功能设计

平台功能设计需遵循情景认知理论的实践导向原则，通过模拟真实岗位环境打造实训场景：企业需全面开放实际网络拓扑结构、安全设备参数、典型攻击案例等核心资源；学校则负责将这些资源转化为可操作的实训任务，构建多层级、体系化的实训内容体系。平台架构需采用“虚实结合”的建设思路，既部署企业级防火墙、入侵检测系统等硬件设备，保障学生真实操作体验，又开发虚拟化攻击模拟平台，还原复杂攻击场景，最终形成“硬件支撑真实操作、虚拟环境模拟复杂攻击”的复合型实训场景。这种架构既能让学生在接近真实的工作环境中锤炼技能，又能有效降低实训成本与安全风险，保障实训教学安全有序开展。

例如，平台功能设计采用“虚实结合”的建设思路，硬件部分部署了 10 台华为 USG6000 系列防火墙、8 台交换机以及若干终端设备，搭建起与企业真实网络架构一致的硬件实训环境，保障学生能够进行真实设备的操作练习；虚拟部分开发了防火墙攻击模拟子系统，该子系统能够还原端口扫描、非法 IP 访问等常见攻击场景，学生可在虚拟环境中测试已配置的防火墙规则防御效果。平台还构建了多层级实训内容体系，企业技术工程

师将真实企业的防火墙配置需求转化为不同难度的实训任务，学校教师则结合这些任务编写实训指导手册，明确任务分析要点、操作步骤规范及效果验证标准，形成适配中职学生能力水平的实训资源包。

2.3 中职院校以认知理论为指导开展情景模拟与攻防演练

中职网络安全技术课程教学需聚焦攻防实践核心，以认知学徒制理论为指导，通过整合代表性攻防场景，将企业实际网络拓扑结构、安全设备配置参数、典型攻击路径转化为适配中职学生能力水平的情景模拟模块。

2.3.1 任务导入

任务导入阶段，教师需采用引导式教学法，通过任务拆解、操作规范讲解、现场示范等方式，将复杂的攻防任务分解为信息收集、漏洞扫描、攻击实施、防御加固等子环节，同步详解各环节所需工具的使用逻辑、操作步骤与侧重边界，帮助学生建立任务执行的完整认知框架，为独立操作筑牢基础。

例如， 情景模拟环节以企业办公网络边界安全防护为典型情景，教师采用引导式教学法拆解该情景下的防火墙配置任务，先向学生展示企业办公网络拓扑图并分析网络边界的安全需求，再将整体任务分解为地址池定义、访问控制列表编制、NAT 转换规则配置、安全区域划分及效果验证五个子环节。

2.3.2 攻防演练组织

攻防演练组织需以最近发展区理论为参照，通过分层任务设计与动态指导相结合的方式，精准提升学生实践能力。教师可搭建基础型、提高型、挑战型三级任务包：基础型任务聚焦单一工具使用，如防火墙基础规则配置；提高型任务强调多工具协同应用，如漏洞扫描与入侵检测系统的联动调试；挑战型任务则要求学生自主设计攻防方案，模拟 APT 攻击链全流程。演练过程中，教师需实施动态指导策略：初期以观察记录为主，精准捕捉学生操作中的共性问题；中期针对典型错误及时干预，纠正操作偏差；后期逐步减少指导频次，鼓励学生通过小组探讨、查阅技术文档自主解决问题，培养独立分析与决策能力。

例如，基础型任务要求学生完成企业内部终端访问互联网的 NAT 转换规则配置，提高型任务要求学生完成禁止外部终端访问内网财务服务器 8080 端口的访问控制列表配置及防火墙安全区域划分，挑战型任务要求学生结合企业网络拓展需求自主设计防火墙规则配置方案，实现内部不同部门终端的网络访问权限隔离。演练过程中，教师实施动态指导策略，初期通过巡视观察记录学生在地址池定义和命令输入过程中出现的共性问题，中期针对部分学生在访问控制列表规则优先级设置上出现的偏差进行集中讲解纠正，后期减少直接指导，引导学生通过查阅平台提供的企业防火墙配置案例文档、小组探讨等方式解决规则配置后的连通性问题。

2.3.3 反思优化

演练后的反思优化阶段，需依托元认知理论，构建“操作复盘、经验总结、能力迁移”的三阶反思机制，深化学习效果。教师需引导学生从工具使用准确性、攻击路径合理性、防御措施有效性三个维度开展全面复盘，要求用流程图或思维导图呈现任务执行全过程，标注关键节点与操作失误环节。在此基础上，组织小组互评活动，对比不同方案的优势与不足，提炼可复用的攻防策略与技术要点。最后，教师需设计拓展任务，引导学生将演练中掌握的技能迁移至新情景，通过变式练习强化核心能力的理解与运用，实现技能从“会用”到“活用”的跨越。

3 结束语

综上，中职网络安全技术课程实践教学优化实践构建起岗位需求与教学实施的精准对接机制。其中，重构课程体系、校企协同共建平台及情景化攻防演练等策略的实施，不仅有效提升了学生的岗位适配技能，更形成了职业教育技术类课程“需求导向、实践赋能、能力迁移”的教学范式。这一范式为同类中职技术课程教学改革提供了可借鉴的思路，也为职业教育精准对接产业需求、提升人才培养质量拓展了实践路径。

参考文献

[1]王瑞霞.技能大赛助推中职网络信息安全专业教学改革的探索与实践[J].信息与电脑,2025,37(23):206-209.

[2]邓海恩.中职学校无线网络安全技术的探索与研究[J].信息与电脑,2025,37(19):90-92.

[3]韩亮.基于产业需求的中职计算机网络技术专业课程优化策略[J].数字通信世界,2025,(09):223-225.

作者简介：刘德斌(1981-09)，男，汉，山东省威海市，大学本科，青岛市供销职业中等专业学校（青岛市经济贸易技术学校），讲师，机电一体化，计算机，电子商务。