

新工科视域下面向产业需求的网络安全人才培养模式研究*

段炼

江苏第二师范学院计算机工程学院、人工智能学院, 南京 211200

摘 要 针对新工科建设背景下网络安全人才培养与产业需求脱节、实战教学资源匮乏、数智技术应用不足、产教融合形式化等问题, 本文以岗位胜任力为核心, 构建产教融合、数智赋能的实战型网络安全人才培养模式, 从胜任力建模、课程重构、实践教学、评价体系、协同机制五维度推进改革。依托“双域八维”岗位胜任力模型明确培养标准, 通过四层递进模块化课程、三段阶梯式实践教学强化实战能力, 采用“三位一体”多元化评价衡量培养成效, 以“六共联动”机制保障校企协同, 引入 AI 助教等数智技术赋能教学全流程。教学改革后, 课程期末成绩优良率提升 60.9%, 不及格率下降 17.4%, 学生评教得分提升至 88.6, 3 个课程目标达成度显著提升, 验证了该模式对学生实战能力与岗位适配度的有效支撑, 为新工科背景下应用型高校网络安全专业的人才培养改革提供了参考。

关键词 新工科, 网络安全, 岗位胜任力, 产教融合, 数智赋能, 人才培养模式

Research on Cybersecurity Talent Cultivation Model Oriented Toward Industry Demand from the Perspective of Emerging Engineering Education *

Duan Lian

School of Computer Engineering, School of Artificial Intelligence
Jiangsu Second Normal University
Nanjing 211200, China
duanlian2313@jssnu.edu.cn

Abstract—In the context of emerging engineering education, cybersecurity talent cultivation faces several problems, including a disconnect between training outcomes and industry demand, a shortage of practice-oriented teaching resources, insufficient application of digital and intelligent technologies, and superficial industry-education integration. To address these problems, this paper proposes a practice-oriented talent cultivation model centered on job competency requirements, built upon industry-education integration and empowered by digital and intelligent technologies, and advances reforms across five dimensions: competency model, curriculum system, practical teaching, evaluation system, and collaboration mechanism. It defines cultivation standards via the "dual-domain, eight-dimension" post competency model, strengthens practical capabilities through a four-tier progressive modular curriculum system and three-stage tiered practical teaching, measures cultivation outcomes with a "three-in-one" diversified evaluation framework, secures school-enterprise collaboration by the "six-cooperation linkage" mechanism, and empowers the whole teaching process with digital-intelligent technologies such as AI teaching assistants. Following the reform, the proportion of students achieving good-or-above final course grades rose by 60.9%, the failure rate dropped by 17.4%, student evaluation scores rose to 88.6, and the attainment of three course objectives improved markedly, confirming the model's effectiveness in supporting students' practical competence and job readiness. The findings offer a reference for reforming cybersecurity talent cultivation at application-oriented universities under the emerging engineering education initiative.

Keywords—emerging engineering education, cybersecurity, job competency, industry-education integration, digital and intelligent empowerment, talent cultivation model

***基金资助**: 本文得到工业和信息化部人才交流中心人才大数据智能分析与评测工业和信息化部重点实验室 2026 年度一般课题(MIITECKT26020)、江苏第二师范学院人工智能赋能高等教育新生态专项课题(JSSNUZXKT2026XST05)、江苏第二师范学院“人工智能+教学”试点课程“网络信息安全”建设项目资助。

***通讯作者**: 段炼 duanlian2313@jssnu.edu.cn。

1 引 言

网络空间是国家主权延伸的第五空间, 网络空间安全面临的形势复杂多变, 对抗趋势越发凸显。网络空间的竞争, 归根结底是人才的竞争。“十四五”规划中强调, “国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训, 采取多

种方式培养网络安全人才,促进网络安全人才交流”,网络安全人才培养被纳入国家战略布局。2016年以来,中央网信办、教育部等部门先后出台多项政策文件,明确要求推动校企协同育人,创新网络安全人才培养机制。新工科建设的持续推进,也对工程型、实战型网络安全人才的培养标准与质量提出了更高要求。

当前,应用型高校人才培养供给与产业需求之间存在结构性矛盾。从需求侧来看,网络安全技术迭代周期短、速度快,产业端对人才的实战能力要求持续提升。从供给侧来看,网络安全作为一门综合性新兴学科,专业人才培养难度大、周期长^[1]。现有培养模式中,课程内容更新滞后于技术发展,实践教学场景与真实业务脱节,数智技术对教学的支撑作用未充分发挥,校企合作仍停留在表层等问题较为突出。在此背景下,培养适应产业需求的网络安全人才,已成为应用型本科高校网络安全相关专业建设的核心课题。

2 网络安全产业人才培养现状与挑战

2.1 实战型人才成为产业刚需

随着数字化转型的深入推进,网络安全威胁的形态日趋复杂,勒索病毒、APT(高级持续性威胁)、供应链攻击等对抗频繁发生,产业对能够在真实场景中独立处置安全事件的人才需求持续增长。工业和信息化部教育与考试中心等单位联合发布的《AI时代网络安全产业人才发展报告(2025年)》显示,具备真实攻防对抗经验、熟练操作安全工具、能快速响应处置安全事件的实战型网络安全人才,正成为招聘市场上的稀缺资源^[2]。

2.2 实战能力的界定

网络安全实战能力是指从业者在真实业务场景中,运用专业知识、技术工具与工程方法,识别安全风险、实施攻防操作、处置安全事件的综合能力。从业务需求出发,网络安全人才实战能力可以归纳为“攻防实战能力”“漏洞挖掘能力”“工程开发能力”“战效评估能力”四种类型^[3]。尽管不同类型的岗位对实战能力的要求不同,但从岗位适配和培养路径角度看,实战能力应该至少覆盖四个层面:职业素养、理论基础、技术实操、工程实践。在国家标准与行业规范中对网络安全从业人员的能力维度作出分级界定,为人才培养的能力目标设定提供了参照依据。

2.3 网络安全课程教学中存在的问题

(1) 课程体系与产业需求脱节

现有网络安全课程体系一般以学科知识逻辑为主线组织,内容更新周期与技术迭代速度不匹配,新兴领域的技术内容与岗位技能要求难以及时纳入教学环节^[3]。课程设置对核心岗位胜任力要求的覆盖度不足,

学生完成课程学习后,仍难以直接承担企业核心岗位的工作任务。这种“学用分离”的现象,在很大程度上制约了人才培养质量的提升^[4]。

(2) 实战教学资源匮乏

网络安全实践教学对仿真环境要求较高,多数高校的实验室仅能开展验证性的实验,缺少覆盖完整业务流程的高仿真攻防场景^[5]。企业真实项目因涉密等限制,难以直接转化为教学资源,学生缺乏系统性工程实践经验积累。

(3) 数智技术教学应用不足

人工智能技术在教学环节的应用多以工具演示为主,缺少支撑个性化学习规划的智能分析机制。课堂学情数据的采集与应用缺乏系统设计,评价工具的智能化程度有限,教师在教学过程中难以实施精细化、动态化的课堂教学活动和资源配置^[6]。

(4) 产教融合流于形式

校企合作的深度与广度不足,企业参与多停留在提供实习岗位和开设讲座层面,未能实质性介入制定课程标准、设计教学方案与评价人才质量等环节,教学内容与岗位能力标准之间的偏差难以得到及时校正^[7]。

3 人才培养模式改革总体框架

针对网络安全课程教学中存在的问题,本文基于“学生中心、产出导向、持续改进”理念,按照“需求、标准、培养、评价、改进”的设计路线,提出以网络安全产业岗位胜任力为核心的产教融合、数智赋能的人才培养模式。以培养适应产业需求的网络安全实战型人才为改革目标,通过教学目标重构、教学过程再造、教学资源升级和评价方式创新等四个改革维度,形成“产业需求牵引、数智技术赋能、实战能力导向”人才培养和课程教学新范式。改革后的人才培养模式整体框架如图1所示。

在改革落地层面,基于产教协同育人共享资源,充分利用智慧教学平台和AI辅助工具等多种技术手段,在课程目标、教学内容、教学方式、实践过程和教学评价等方面,研究并实施课程教学改革方案。一是构建适配产业需求的岗位胜任力模型,明确人才培养的能力标准,重构模块化课程体系和教学质量评价体系,解决课程体系与产业需求错位的问题,实现课程标准与产业用人标准的精准对接。二是改变传统验证性实验为主的实践教学形态,通过虚实结合、层层递进的方式构设贴近产业的实践科目,升级实验资源,解决真实业务场景缺失、工程实践培养链条不完整的问题,构建从基础技能到综合实战的阶梯式能力培养路径。三是借助大语言模型、学情数据分析等数智技

术手段，解决学情数据利用不充分、个性化教学支撑不足的问题，以数智技术支撑教学全流程的精准化与高效化。

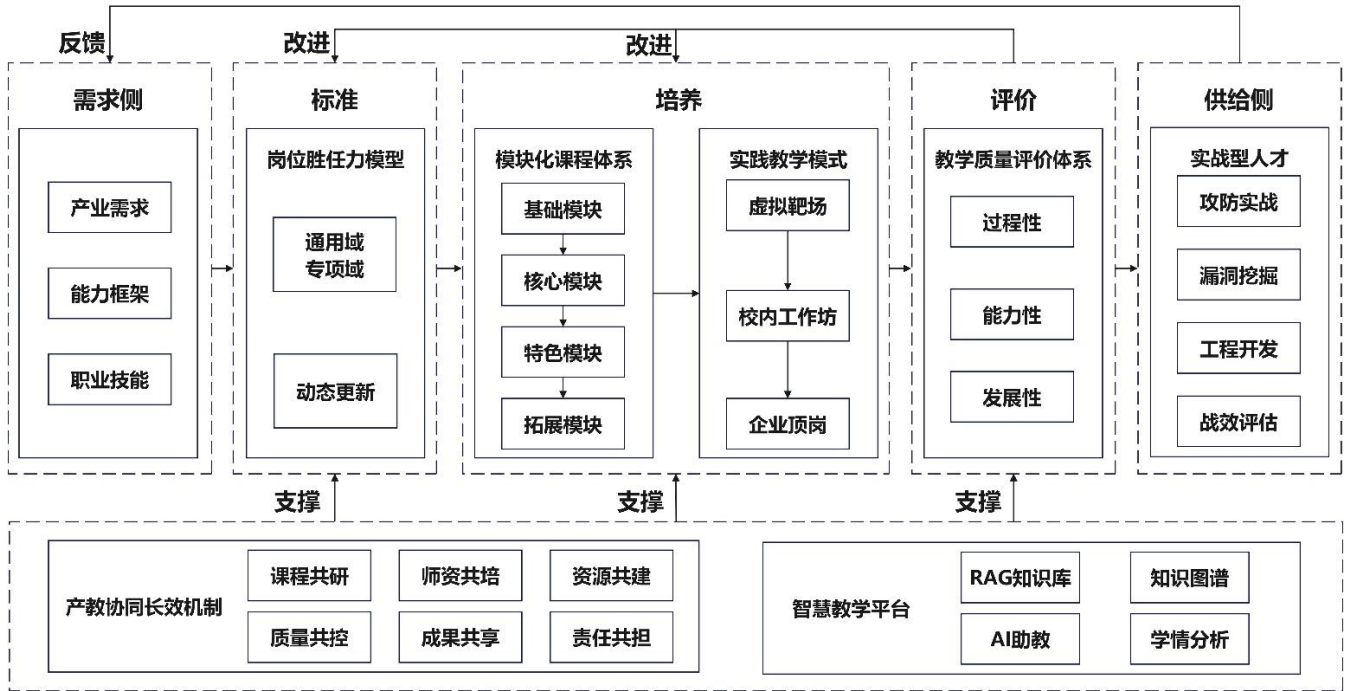


图 1 产教融合、数智赋能的网络安全人才培养模式总体框架

4 人才培养模式改革的实践路径

4.1 “双域八维” 岗位胜任力模型

岗位胜任力模型的构建采用理论研究和调研访谈相结合的方式。理论研究参考 GB/T 42446-2023《信息安全技术 网络安全从业人员能力基本要求》^[8]、T/MIITEC 007-2021《网络安全产业人才岗位能力要求》^[9]等通用能力框架，以及《信息安全测试员（渗透测试员）国家职业技能标准（2021 年版）》^[10]、《网络与信息安全管理员（数据安全管理员）国家职业标准（2024 年版）》^[11]等职业技能标准。通过梳理总结网络安全典型岗位能力要求，将模型分为通用胜任力和专项胜任力两个领域，各包含四个维度，见表 1。通用域包含职业素养、法律法规、网络安全基础理论、通用技术能力，是所有网络安全岗位须具备的基础能力要求；专项域包含专属综合能力、专业知识、专业技能、工程实践，对应不同细分岗位的差异化能力要求。

由校企联合开展调研访谈，调研对象涵盖安全规划与设计、安全建设与实施、安全运行与维护、安全运营与研究、安全分析与治理、安全合规与管理六类典型岗位。通过问卷调研、人员访谈等形式，采集各类岗位的工作任务清单、企业内部任职标准、近三年人才招聘与培训数据，以及护网行动中形成的真实岗位能力数据，经指标筛选、权重赋值与专家论证后形成最终指标体系。为防止胜任力标准滞后于技术迭代，

模型建立动态更新机制，企业按“半年微调、年度迭代”周期同步岗位需求变化，校企双方联合完成指标的优化调整，确保培养标准与产业前沿保持动态对接。

表 1 “双域八维” 岗位胜任力模型

领域	维度	领域要素
通用 胜任力	职业素养	职业道德、团队协作、持续学习意识
	法律法规	网络安全法律合规意识
	网络安全基础理论	密码学、网络协议、操作系统安全原理等
	通用技术能力	编程、系统运维、数据分析基础
专项 胜任力	专属综合能力	跨领域安全方案设计与实施能力
	专业知识	渗透测试、威胁情报、应急响应知识体系
	专业技能	靶场实操、工具使用、漏洞分析利用
	工程实践	真实项目交付、攻防演练、安全工程管理等

4.2 四层递进模块化课程体系

依据“双域八维”岗位胜任力模型，将传统课程体系重构为“基础模块—核心模块—特色模块—拓展模块”四层递进模块化结构，如图2所示。每个课程模块、教学单元与考核标准均对应具体的胜任力指标，实现能力要求、课程目标、教学内容、考核评价的精准匹配。

在课程体系中，基础模块对应通用域胜任力要求，覆盖密码学原理、网络协议安全、操作系统安全、职业规范等专业入门课程，侧重培养学生的基础理论、通用技术和职业素养。核心模块对应专项域核心能力要求，以网络安全核心技术课程为主，提升攻防实战、应急处置类实操课程的占比，强化学生核心技术技能。特色模块针对网络安全细分领域设置，新增工业互联网安全、车联网安全、数据安全治理、云原生安全等新兴方向的专项课程，适配产业发展需求。拓展模块包含前沿技术微课程、产学研项目实践、创新创业类课程，由校企联合开发，拓宽学生的技术视野，培养创新能力。

采用“课证岗研”融合的方式，将企业真实工作任务拆解为项目化教学单元，嵌入到课程模块中。将CISP（注册信息安全专业人员）、CISSP（注册信息系统安全专家）等职业资格认证考点纳入课程内容，实现课程学习与证书备考相结合。联合企业开发项目化教材与讲义，使得课程内容与行业技术标准同步更新。将产学研横向科研项目的典型案例提炼为教学素材，推广项目式、案例式教学方法，拓展学生对前沿技术的认知。

依托超星泛雅平台集成大语言模型能力，建设智慧课程平台。平台将课件、教案等教学资源清洗后形成RAG（检索增强生成）知识库，转化为理论知识图谱、技术工具图谱与实战场景图谱^[3]。生成式人工智能承担助教职能，提供全天候答疑服务，辅助学生自主学习。课前预习、课堂练习、课后作业、实验任务等教学环节均与知识图谱关联，可自动识别学生的知识薄弱点。教师可通过AI学情分析功能实时掌握班级整体学习状态，及时调整教学内容和节奏。

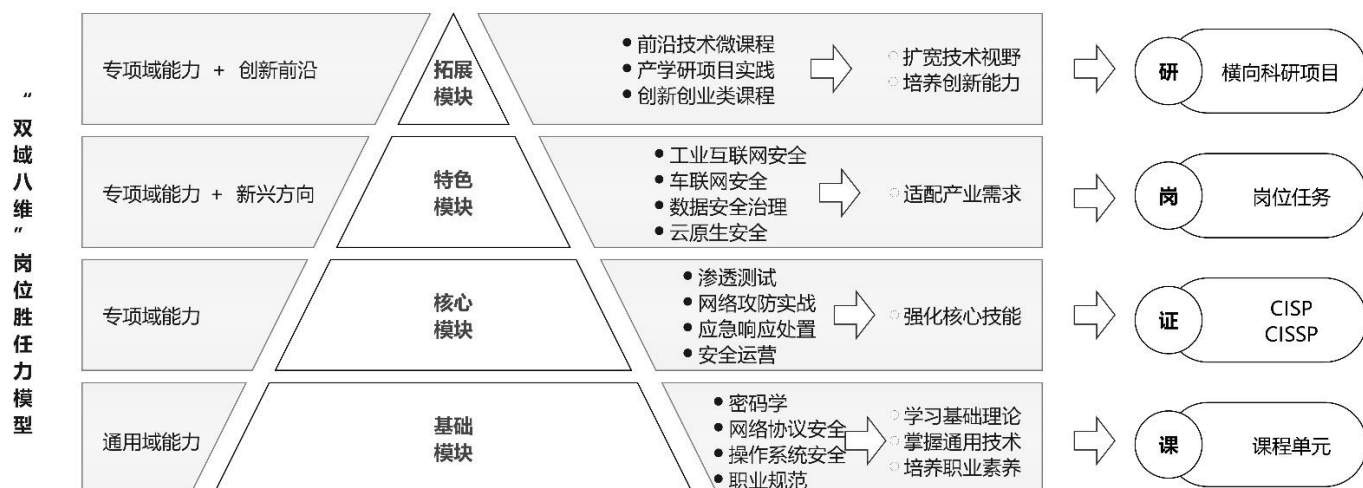


图2 四层递进模块化课程体系

4.3 三段阶梯式实践教学模式

针对实战教学资源匮乏的问题，构建“虚拟靶场、校内工作坊、企业顶岗”三段阶梯式实践教学模式，覆盖从基础技能训练到综合实战能力检验的完整链条，如图3所示。基础阶段为虚拟仿真实训，依托虚拟靶场实训平台开展攻防场景实训。学生在隔离的仿真环境中完成单一技术点的验证与微型攻防场景练习，掌握基础攻防工具的使用方法与常见漏洞的利用、加固方法。

提升阶段为校内工作坊实战，由高校教师与企业安全工程师组成双导师团队，共同设计项目、共同授课、共同指导实践、共同开展评价。引入脱敏后的企业真实项目，例如护网行动、重大活动网络安保及应急响应演练等行业场景。学生以团队形式完成项目任

务和结果交付，锻炼综合技术应用能力与团队协作能力。

综合阶段为企业顶岗实习，学生进入企业安全运营中心等业务岗位，在企业导师指导下参与安全监控、事件研判与处置、数据分析等真实业务工作，实现从校园实训到工程岗位的能力提升。

每一轮实践教学结束后，由校企双导师与学生分别从教学内容设计、实训组织安排和学习效果三个方面进行评价。校企导师重点反馈实训项目难度设置是否合理、教学方法是否便于学生掌握技术要点，学生则就实训过程中的具体困难和需求提出意见。评价结果汇总后，用于调整下一轮实训项目的内容设置和教学方法，例如增减实训案例的难度、调整讲解与实操的时间分配等，以此提升实践教学的质量。

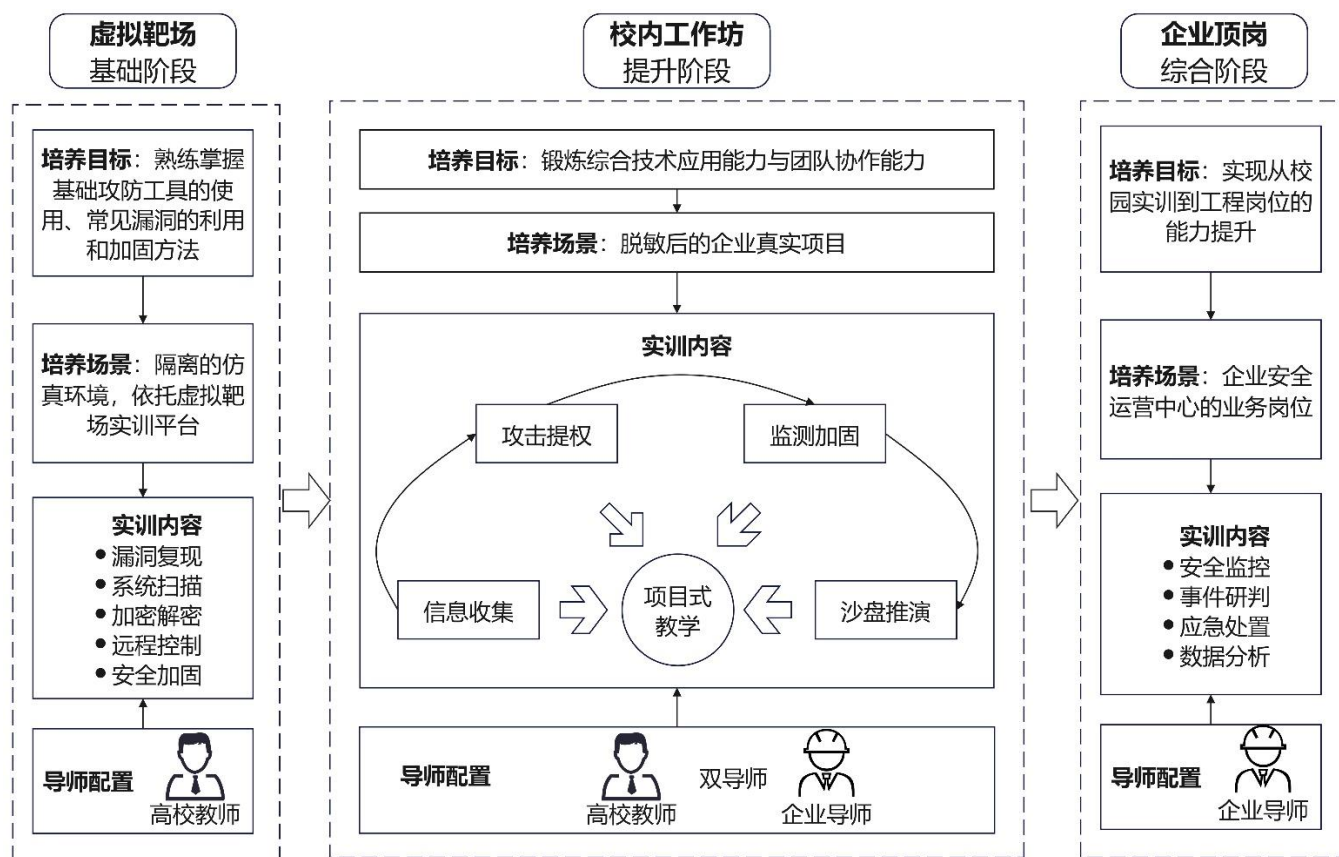


图 3 三段阶梯式实践教学模式

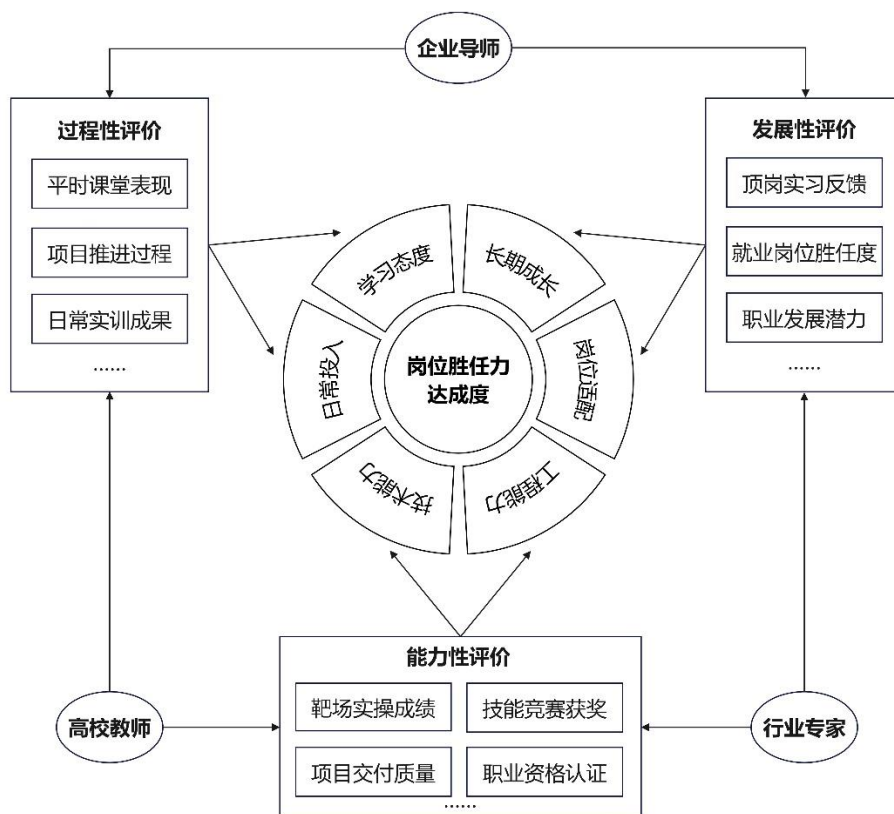


图 4 “三位一体”教学质量评价体系

4.4 “三位一体”多元化教学质量评价体系

传统的评价方式主要依据考试成绩，难以全面反映学生实战能力。为此，评价指标体系应以岗位胜任力达成度为核心，从过程、能力与发展三个维度对学生的能力成长情况进行考查，如图4所示。

过程性评价主要依据课堂表现、项目推进过程中的记录以及日常实训成果，考查的重点是学生的学习态度和日常投入程度。能力性评价以攻防靶场实操成绩、真实项目交付质量、职业资格证书获取情况以及技能竞赛获奖情况作为主要指标，用以反映学生的技术能力和工程能力。发展性评价综合企业顶岗实习期间的反馈意见、毕业后就业岗位的胜任情况以及职业发展潜力，考查学生在较长时间跨度内的成长能力和岗位适应能力，这一维度更关注人才培养的中长期效果。

在评价主体方面，引入企业导师和行业专家参与评价过程。其中，在项目实战和顶岗实习两个环节，企业导师的评价权重不低于40%，目的是使评价标准更贴近行业用人需求。评价结果应当用于调整能力培养目标、优化课程内容以及修订学生的个性化培养方案，使评价、教学与培养方案之间形成相互反馈、持续改进的关系。

4.5 产教协同长效机制

校企合作中存在的短期化、形式化问题，主要源于双方权责边界不清、师资培养缺乏稳定渠道以及合作效果缺少持续跟踪。针对上述问题，可以从权责划分、师资培养与持续改进三个方面构建产教协同长效机制，如图5所示。

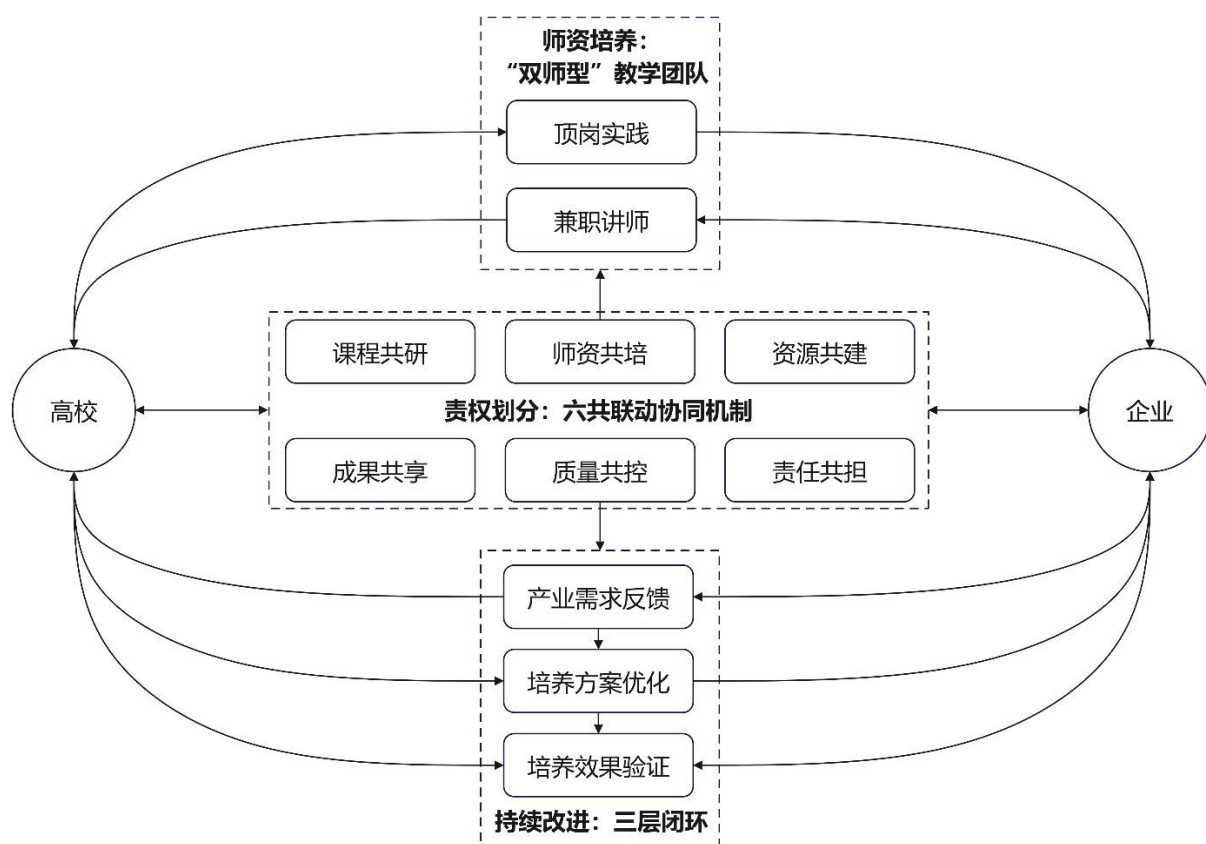


图5 “六共联动”产教协同长效机制

在权责划分方面，建立“课程共研、师资共培、资源共建、成果共享、质量共控、责任共担”的六共联动协同机制。在课程开发环节，学校负责教学内容的整体设计，企业负责提供真实案例并对技术内容的适用性进行审核；在师资培训环节，企业派出技术骨干承担部分实训课程的教学任务，学校则提供教学方法方面的指导；在实训资源建设环节，企业提供设备、平台和实战环境支持，学校负责场地和基础设施配套；

在成果转化环节，项目成果经企业内部评审后用于实际业务参考；在质量监控环节，双方共同制定考核标准并对培养质量进行联合评估；在出现合作问题时，由双方协商确定责任归属和改进措施。以上各环节的具体实施流程、考核标准与激励措施在校企合作协议中予以明确。

在师资培养方面，实施“双师型”教师双向培养，企业为高校教师提供每年不少于2个月的顶岗实践岗

位,使教师全程参与真实工程项目;高校向企业安全工程师颁发兼职讲师聘书,将其纳入课程教学团队;双方共建“双师型”教师培养基地,形成校企师资的常态化互动与能力互补。

在持续改进方面,建立“产业需求反馈、培养方案优化、培养效果验证”三层闭环。企业定期向院校反馈岗位需求变化与毕业生岗位胜任度评估结果,院校依据反馈同步完成培养方案调整。调整效果由下一周期的培养结果数据加以验证,实现人才培养体系的动态迭代。

5 应用价值与实践成效

5.1 理论与应用价值

以岗位胜任力为核心的产教融合、数智赋能的人才培养模式,回应了应用型高校网络安全人才培养的四个制约因素。“双域八维”胜任力模型与配套动态更新机制,将课程设计与岗位能力标准对应起来,缩减了课程内容与产业需求之间的差距,也可为同类专业的能力标准制定提供理论参照。四层递进模块化课程与三段阶梯式实践教学模式将企业真实项目纳入实训环节,弥补了现有实训平台仿真度不足的缺陷。智慧课程平台的AI学情分析功能,可支持教师实时掌握班级知识薄弱环节分布,而非仅依赖期末考试结果。“六共联动”长效协同机制通过明确权责的制度设计,为校企深度合作提供了可操作的实施路径。

该人才培养模式从能力标准、课程体系、实践教学、质量评价到协同机制形成了完整的解决方案,可直接应用于应用型本科院校网络安全专业的教学改革。每个环节均具备较强的通用性,对计算机类相关专业的人才培养改革亦具有参考价值。

5.2 教学改革实践成效

基于该人才培养模式的教学改革已在2022级学生中完成第一轮实施。相比采用传统教学模式的2021级,2022级网络安全理论教学期末成绩优良率提升了60.9%,不及格率下降了17.4%。网络安全实践教学的教学模式变化较大,因此成绩不具备可比性。学生评教得分由85.8提升至88.6,96%的学生在结课调研中表示深化了对“没有网络安全就没有国家安全”的总体国家安全观与工程师职业责任的理解。课程目标达成度方面,理论教学的3个课程目标达成度由0.7、0.78、0.72变为0.77、0.78、0.8,目标1(工程与社会)和目标3(职业规范)分别提升10%和11.1%。实践教学的3个课程目标达成度由0.85、0.85、0.87变为0.86、0.86、0.84,目标1(工程与社会)和目标2(项目管理)均提升了1.1%,表明学生在发现工程实践中的信息安全问题、树立安全责任意识、测算项目成本等方面的能力显著增强。目标3(自主学习能力)有所下

降,主要因为2022级的实践教学中增加了工作坊和企业顶岗等环节,学生首次接触产业内容存在学习门槛,在推进项目时存在一定困难,后续将在课程实施前增加产业相关背景知识的导入培训环节加以改善。

6 结束语

本文针对网络安全产业实战型人才需求与应用型高校培养供给的结构性矛盾,提出以岗位胜任力为核心的产教融合、数智赋能的人才培养模式,从胜任力建模、课程重构、实践教学、评价机制与产教协同五个维度进行系统设计,形成覆盖培养全流程的闭环改革范式。下一步,将在本模式的指导下,基于实施数据继续优化胜任力模型和达成度评价指标,探索AI技术在实践教学评价与个性化培养路径规划中的深度应用。

参考文献

- [1] 教育部高等学校网络空间安全专业教学指导委员会,北京航空航天大学,中国科学技术大学,等.网络安全人才实战能力白皮书:攻防实战能力篇[R],2022:6.
- [2] 工业和信息化部教育与考试中心,安恒信息,中国联合网络通信有限公司软件研究院,等. AI时代网络安全产业人才发展报告(2025年)[R/OL].https://www.dbappsecurity.com.cn/content/details2166_55657.html.
- [3] 施莹娟,沈才有,郑秀峰,等.实战型网络空间安全人才“三强六阶”递进式人才培养模式探索[J].计算机教育,2025,(12):47-53.
- [4] 王慧,邢红梅,德世洋,等.产教融合视角下软件工程实践课程改革研究[J].计算机技术与教育学报,2026,14(5):58-64.
- [5] 曾文丽,陈继鑫,石睿,等.产教融合背景下的网络安全综合实验课程教学改革[J].计算机教育,2024,(3):144-147+153.
- [6] 张昱.人工智能赋能课堂教学:价值意蕴、现实挑战与实践路径[J].教育理论与实践,2025,45(18):51-55.
- [7] 陈治宏,曹越,林海.网络安全校企对接实践教学平台建设[J].计算机教育,2025,(7):203-207.
- [8] GB/T 42446-2023 信息安全技术 网络安全从业人员能力基本要求[S/OL].<https://openstd.samr.gov.cn/bzgk/std/newGbInfo?hcno=AD7E0F02219B63653BF850759A1030C4>.
- [8] 工业和信息化部人才交流中心,工业和信息化部网络安全产业发展中心.T/MIITEC 007-2021 网络安全产业人才岗位能力要求[EB/OL].(2022-01-12)[2026-06-12].https://www.miitec.cn/fwpt/xw/rcbz/art/2022/art_10d0fc2070fc24defda28ce96d875f3f.html.
- [10] 人力资源和社会保障部,中央网信办,工业和信息化部,等.信息安全测试员(渗透测试员)国家职业技能标准(2021年版)[EB/OL].(2021-10-19)[2026-06-12].<https://osta.gpy.org.cn/uploads/20230616/5df2e83da9916ad6eee968ffef15db8e5.pdf>.
- [11] 人力资源和社会保障部,公安部,工业和信息化部.网络与信息安全管理员(数据安全管理员)国家职业技能标准(2024年版)[EB/OL].(2024-02-20)[2026-06-12].https://www.mohrss.gov.cn/xgk2020/fdzdgknr/rcrs_4225/jnrc/202402/W020240227604801668472.pdf.