新工科背景下信息安全课程教学创新实践*

包象琳 徐晓峰** 刘涛 章平

安徽工程大学计算机与信息学院，芜湖 241000

摘 要 在新工科背景下，为塑造学生信息安全能力素养和职业操守，本文针对安全理论技术难以内化调度等痛点问题，以学生为中心，采用层层递进的教学内容、攻防交替的案例情境、数字化课程资源、信息化评价手段，提出了 RAPETA 信息安全教学模型。学生通过螺旋递进式剖析实际案例安全需求(R)、参与多元多向学习活动(A)、切换信息安全攻防视角(P)、融入泛在互动学习环境(E)、落实灵活深度课程任务(T)、收获立体灵活全程评价(A)，进而实现安全理论的内化，形成技术应用和协作思辨能力，以适应未来信息安全技术和产业发展的新要求。课程开展“三合四融”思政育人，学生信息安全能力持续递进演化、素养逐步拓展提升。

关键字 新工科，信息安全，课程改革，教学模型，教学创新

Innovation Practice of Information Security Course Teaching Under the Background of New Engineering

Bao Xianglin Xu Xiaofeng Liu Tao Zhang Ping

School of computer and information of Anhui Polytechnic University, Wuhu 241000, China;
baoxianglin@ahpu.edu.cnxuxiaofeng@ahpu.edu.cn liutao@ahpu.edu.cn pingzhang@ahpu.edu.cn

Abstract—Under the background of new engineering science, the cultivation of students' information security literacy is of growing importance. Aiming to cultivate students' information security capabilities and professional ethics and build a security defense in the information field, the information security curriculum team, in response to the challenges of internalizing and applying security theory and technology, centers the curriculum around students. By adopting progressive teaching content, alternating attack - defense case scenarios, digital course resources, and information - based evaluation methods, the RAPETA teaching model is developed. Students analyze the security requirements of actual cases in a spiral - progressive manner (R), participate in diverse and multi - directional learning activities (A), switch between information security offense and defense perspectives (P), integrate into an ubiquitous interactive learning environment (E), carry out flexible and in - depth course tasks (T), and receive comprehensive and flexible evaluations throughout the process (A). This enables them to internalize security theory, develop technology application and collaborative thinking abilities, and meet the new requirements of future information security technology and industry development. The course implements the "Three Integrations and Four Integrations" of ideological and political education, promoting the continuous evolution and improvement of students' information security capabilities.

Keywords—Information Security, RAPETA Model, Attack-Defense Iteration, Ideological and Political Education

1 引 言

在数字化进程高速推进的当下，网络空间已成为与陆、海、空、天同等重要的第五维空间领域，深刻影响着国家安全格局，信息安全的重要性愈发凸显。与此同时，信息安全面临的挑战也日益复杂多样。新工科教育旨在顺应新一轮科技革命与产业变革趋势，强调学科交叉融合、创新实践能力培养以及对新兴产业需求的快速响应[1]。在此背景下，培育学生的信息安全素养成为高等教育的重要任务。信息安全课程建设不仅需要与操作系统、计算机网络等专业课程相互配合，还应与社会学、法学、管理学等学科深度交叉，助力学生构建全面的技术视角，增进对行业的理解[2]。

此外，信息安全课程应以实用性、创新性、挑战性问题为切入点，消除学生在安全实践方面的认知盲区，着重培养学生运用“攻击威胁分析-防御方案设计-安全风险评测”这一信息安全研究思路解决和预防实际威胁的能力，提升其实践与安全方案设计水平，强化创新意识与团队合作精神。同时，课程应激发学生

* **基金资助**：本文得到国家自然科学基金（62406004），安徽省教育厅重大教学研究项目（2023jyxm0451），安徽省高等学校科学研究重点项目（2024AH050122），安徽工程大学校级项目（2022jyxm38，2023hhkk14，2024hhkc07，2024jyxm03，2024gjxm004），中国科大 2024 年度创新创业教育研究课题（SCJY2024001）资助。

** 通讯作者：徐晓峰 xuxiaofeng@ahpu.edu.cn

信息安全自主学习的内驱力，提供丰富的学习资源与交流平台，鼓励学生不断更新知识，以适应快速变化的技术环境与行业需求[3]。

信息安全作为国家战略安全的关键组成部分，直接关系到国家各领域的稳定与发展。因此，信息安全课程建设与教学改革不仅是顺应时代发展的必然选择，更是计算机领域人才职业素养培育的重要基石。在信息安全威胁日益严峻的今天，计算机专业人才除需掌握扎实的编程技能与算法知识外，还应具备强烈的信息安全意识、敏锐的风险识别能力以及高效的防护与应对策略[4]。然而，随着技术的迅猛发展，新型安全威胁不断涌现，传统的教学内容与方法已难以满足培养高素质信息安全人才的需求[5]。此外，信息安全具有很强的实践性，但学生在校期间往往缺乏充足的实践机会与平台，导致理论与实践脱节，影响了学生信息安全素养的全面提升[6]。

本课程致力于培养学生在信息安全领域的理论知识与实践能力，涵盖信息安全基本概念、目标、研究内容，包括密码学基础、对称密码体制与公钥密码体制、访问控制技术、网络攻击技术、网络防御系统、信息安全协议以及国内外信息系统安全评估标准等，帮助学生全面认识信息安全领域，掌握基本技能。

2 新工科背景下课程痛点检视

信息安全课程的开设对提升大学生信息安全素养和能力发挥了重要作用，但仍存在一些亟待解决的问题。当前，信息安全理论与技术难以被学生内化、学生信息安全高阶能力难以构建、学习诱导力和原动力不足等问题较为突出。

课程旨在帮助学生构建坚实的信息安全概念理论体系，提升技术应用能力。然而，信息安全理论抽象且技术覆盖面广，课程学习既需要学生具备理论推导证明能力，又要掌握技术聚合应用能力。但学生学习态度普遍较为功利，多数学生存在理论与实践能力不均衡、关联融合意识不足的问题，缺乏针对信息安全的演绎归纳系统性思维，导致难以有效内化安全理论、灵活运用攻防技术。

在实际工程场景中，解决信息安全问题的基本思路是根据软硬件环境条件分析攻击威胁、针对攻击威胁设计防御方法、面向安全保护对象评测安全风险。然而，非信息安全专业学生缺乏攻防思维训练。实际工程场景下的信息安全攻防关系复杂，技术更新换代频繁。作为培养学生信息安全能力素养的关键专业课，学生在授课前未经过视角转换与攻防对抗训练，缺乏针对信息安全的辨析创新持续性思维，难以构建深入分析、解决实际安全问题的高阶能力。

非信息安全专业学生通常未接受过系统的信息安全培训，对信息安全的了解多停留在生活层面，对学习信息安全在未来职业发展、科研深造中的重要作用认识不够准确，对信息安全作为社会生产、科学研究、国计民生必要条件的理解不够直观，导致缺乏学习信息安全的诱导力和原动力。因此，亟需帮助学生树立保障信息安全的责任感与使命感，激发其学习潜能，使其能够勇敢面对信息安全领域的挑战。

3 课程改革创新方法及途径

3.1 以实际案例为主线，螺旋递进教学内容

教学团队将信息安全知识和技能划分为多个层次，这些层次从基础到深入，逐步引导学生掌握信息安全的核心知识，形成了“安全需求-概念原理-规律应用-综合工程”这一循序渐进的学习阶梯。

在“安全需求”层次，引导学生认识到信息安全在现实生活中的重要性和紧迫性，激发学生学习信息安全知识的兴趣和动力。通过引入真实的安全事件和案例，让学生直观感受到信息安全问题的严重性和普遍性，从而明确学习的目标和方向。

进入“概念原理”层次，系统地讲解信息安全的基本概念、原理和理论框架，为学生打下坚实的理论基础。在这一阶段，教学团队注重培养学生的逻辑思维能力和抽象思维能力，帮助学生理解信息安全技术的内在逻辑和运行机制。

在“规律应用”层次，着重培养学生的实践能力和应用能力。通过设计一系列实践操作任务，如防火墙配置、入侵检测实验、数据加密实验等，让学生在实践中掌握信息安全技术的具体应用方法。同时，教学团队鼓励学生将所学知识应用到实际安全场景中去，通过模拟攻击和防御过程，加深对信息安全技术的理解和掌握程度。

最后，在“综合工程”层次，组织学生参与信息安全项目实训，如 Web 应用安全测试等，培养学生的团队协作能力和解决实际问题的能力。通过参与项目实训，学生不仅能够将所学知识综合运用起来，还能在实践中发现新的问题和挑战，从而进一步提升自己的信息安全素养。

3.2 以攻防迭代为手段，构筑高阶能力思维

在信息安全课程改革与创新过程中，教学团队不仅重视理论知识的传授，更注重实践能力的培养和思维方式的拓展。为此，教学团队构建了针对不同学习阶段、涵盖各领域的信息安全“自主学习、泛在实践、沟通协同”线上线下课程资源，为学生打造一个全方位、多层次的学习平台。团队注重实践活动的组织与

开展，通过构设安全攻防视角交替场景，让学生在模拟的攻防环境中亲身体验信息安全技术的实际应用。这些场景涵盖渗透测试、威胁分析、漏洞利用等多个方面，并融入攻防转换的课前、课中、课后任务，引导学生在攻防两个视角之间切换思考，培养学生的逆向思维和综合解决问题的能力。在攻防场景的构设中，教学团队合理设置攻防对抗切入点，让学生根据不同的安全问题和场景，扮演不同的攻防角色。通过定期交换角色，学生在攻防过程中不断学习和掌握安全攻防技能，实现知识的迭代演进。同时，教学团队鼓励学生进行思辨探究和攻防实践，为学生提供充足的机会去发现问题、解决问题，并总结经验教训。

为激发学生的自我提升动力，教学团队创设了多元多向的学习活动，包括师生沟通合作、分析探讨、对话互动、归纳总结等，旨在培养学生的沟通协同能力和批判性思维能力。通过这些活动，学生能够深入了解和运用攻防工具和技术，在团队协作中发挥自身优势，共同解决信息安全问题。在每次迭代过程中，教学团队都强调总结和反思的重要性。学生通过总结经验教训，及时调整解决问题的方法，优化解决问题的思路和方案。这种由浅入深、由粗到细的反复优化过程，全面深化了学生对安全问题的认识和解决能力，强化了学生的安全建模力、决策思辨力、系统优化力和严谨全面的安全思维。

3．3　以泛在互动环境为支撑，锤炼职业素养

为进一步深化信息安全教育，教学团队搭建了信息安全课程泛在学习云平台、智能助教、在线互动社区和信息安全创新开放活动室。这些平台为学生提供了丰富的在线学习资源和实践机会，促进了师生、科研领域专家、安全企业专家、从业人员及爱好者之间的广泛交流与合作。通过线上讨论、视频会议、线下沙龙等多种形式，学生可以积极参与学习研讨，共同探讨安全问题和解决方案，交流分享学习体会和心得。

为提升学生的学习效果和质量，教学团队积极邀请企业和科研导师参与信息安全课程教学和实践指导。通过与科技企业、研究机构、高校和安全社区的合作，共同构建灵活多样的课程任务和学习路线，帮助学生建立系统的学习框架。课程教师与导师的合作指导，不仅为学生提供专业的反馈和建议，还鼓励学生尝试多种解决方法，推动创新，提升学习成果。

3．4　以及时多维反馈为激励，提升培养成效

为改变“考前突击”和“唯分数论”等传统教育评价模式的弊端，教学团队积极探索并实施了基于多元化评价主体的立体灵活全程评价体系。该体系不再单纯依赖传统的试卷测试来评价学生的学习成果，而是引入同学、教师和先进的信息技术工具作为评价主体，全方位、多角度地收集和分析学生的学习数据和行为习惯。

首先，教学团队鼓励同学之间开展互评，通过小组合作、项目协作等方式，让学生相互了解彼此的学习态度、团队协作能力和问题解决能力。这种互评机制不仅促进了学生之间的交流与互助，还帮助学生从同伴的视角审视自己的学习表现，从而更加全面地认识自己。其次，教师作为评价的重要一环，会结合课程测试、探究记录、总结报告、现场汇报等多种形式的学习成果，对学生的信息安全学习进行全面而深入的评价。教师不仅关注学生的知识掌握程度，还重视学生的实践能力、创新思维和问题解决能力，从而为学生提供更加全面、客观的评价反馈。

此外，教学团队还充分利用现代信息技术手段，如学习管理系统、大数据分析等，收集学生的学习数据和行为习惯。这些数据包括学生的在线学习时间、互动频率、作业完成情况等，为教学团队提供了更加细致、准确的学生学习画像。通过分析这些数据，教学团队可以更加精准地了解学生的学习状态和需求，为个性化教学提供有力支持。为了帮助学生掌握适合自己的学习策略，教学团队还为学生提供了个性化的学习建议和资源推荐。通过分析学生的学习数据和评价反馈，教学团队可以为学生量身定制学习计划和学习路径，帮助学生更高效地掌握信息安全知识和技能。

3．5　立足“三合四融”育人育才

教学团队将知识教育与思想教育紧密结合，构建了“三合四融”思政育人模式。此模式旨在深度挖掘课程育人元素，将思政教育有机融入教学全程，同步推进价值塑造、知识传授与能力培养[7]。

“三合”即结合职业要求、中华精神文化及民族成就、国际国内时事挖掘课程育人元素。具体而言，教学团队剖析信息安全领域职业要求，明确学生应具备的专业素养与职业道德；深入挖掘中华精神文化和民族成就中的信息安全元素，如古代保密技术、现代网络安全成就等，激发学生的民族自豪感与责任感；关注国际国内时事中的信息安全事件，引导学生分析其原因、影响与应对策略，培养学生的全球视野与危机意识。“四融”是把思政元素融入课程教案、课堂教学、实践教学和学生自主学习。在课程教案设计阶段，教学团队将思政教育目标融入其中，确保每堂课都传递正确价值导向；课堂教学中，通过案例分析、小组讨论等方式，引导学生思考信息安全问题背后的社会价值与道德责任；实践教学环节，组织学生进行攻防演练、项目实践等活动，让学生在实践中体悟思政教育内涵；学生自主学习过程中，鼓励学生通过在线学习、阅读文献等途径，自主探索和挖掘信息安全领域的思政元素。

4 创新成效

4．1 满意度显著提升

随着课程教学创新实践的深入推进，学生对信息安全课程的满意度得到了显著提升。从课程满意度调查结果（见图 1）所示，在 2020 年传统教学模式下，课程满意度处于较低水平，这主要是因为传统教学方式侧重于理论灌输，实践环节薄弱，学生难以将抽象的安全理论与实际应用相结合，导致学习积极性不高。

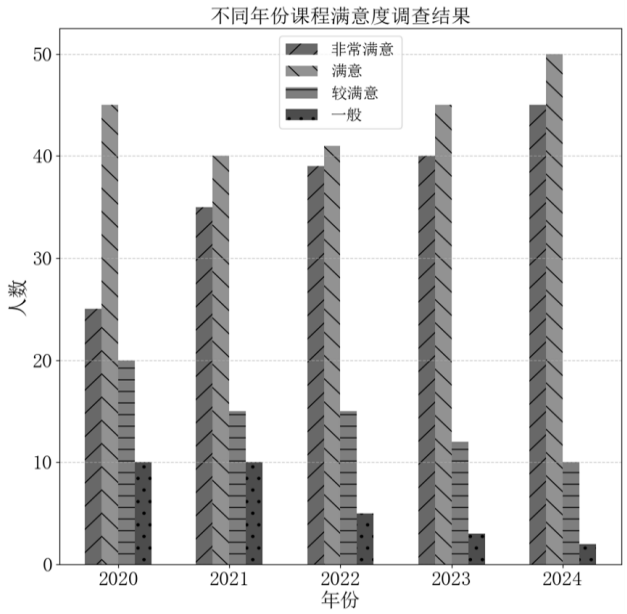

图 1 2020-2024 年课程满意度对比

从课程满意度调查结果（见图 1）所示，自 2021 年开展教学创新实践后，情况有了明显改善。这一年，课程增加了实际案例分析环节，让学生通过分析真实的信息安全事件，初步感受到理论知识在实际中的应用，提高了学生的学习兴趣和参与度。到 2022 年，“非常满意”和“满意”的学生占比之和进一步上升，这得益于教学团队搭建的线上线下课程资源平台，学生可以通过线上视频教程自主学习，利用虚拟实验室进行实践操作，学习的灵活性和自主性大大增强。2023 年，随着攻防迭代教学方法的深入实施，学生在模拟攻防环境中锻炼了实践能力，对课程的满意度持续提升，学生在这种教学模式下，不仅掌握了专业知识和技能，还培养了团队协作和解决问题的能力。到 2024 年，课程满意度达到了新的高度，这主要归功于“三合四融”思政育人模式的融入，以及大模型赋能的精准化个性化教学。

4．2 毕业设计中课程知识运用广泛

从毕业设计中课程知识运用的情况来看（见图 2），学生对各类课程知识的运用较为广泛。信息安全理论知识作为基础，在较多毕业设计中被运用，为学生分析和解决信息安全问题提供了理论支撑。例如，在“基于区块链的供应链信息安全系统设计”毕业设计中，学生运用密码学原理确保数据的加密传输和不可篡改，利用访问控制理论设计用户权限管理模块。学生通过实际操作和模拟，展现出对课程中所学攻防技能的掌握和应用能力。例如，在“Web 安全漏洞检测与修复”相关毕业设计中，学生运用渗透测试技术检测网站漏洞，并根据所学防御技术进行修复，有效提升了系统的安全性。这表明课程教学内容能够有效引导学生在毕业设计中进行实践，学生也能够较好地将课程知识转化为实际项目中的应用能力，进一步验证了课程教学的有效性和实用性。

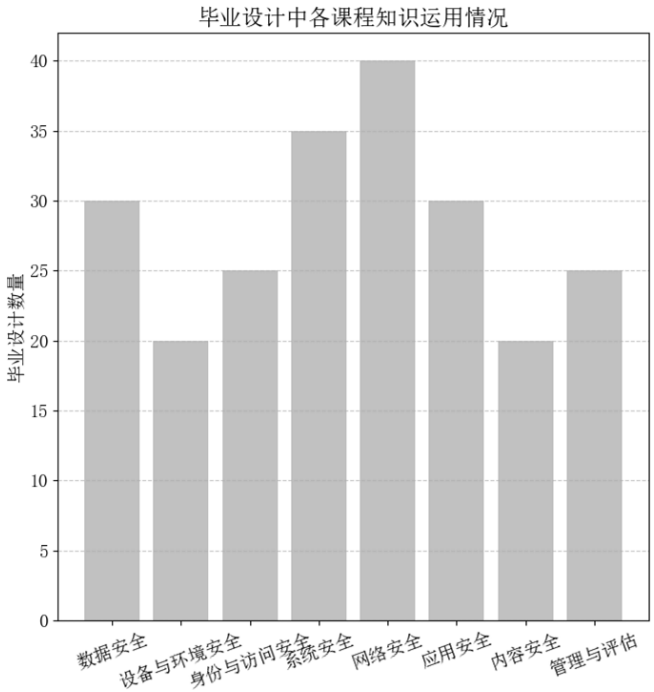

图 2 毕业设计涉及课程知识运用情况统计

4．3 课程目标达成度显著提升

自 2021 年开展教学创新实践后，课程知识与能力目标达成度呈现出良好的提升态势（见图 3 上），这得益于教学过程中对实际案例的深入剖析，如引入金融领域数据泄露案例，让学生从数据加密、访问权限设置等方面分析安全威胁，学生对相关知识的理解和应用能力显著增强。在课程实践中，通过组织学生参与网络攻防模拟项目，学生不仅熟练掌握了系统安全、网络安全和应用安全技术，还能根据攻击场景推理威胁传播路径，设计出有效的防御方案，极大地提升了学生的实践和创新能力。教学团队借助信息安全管理与评估的实际项目，引导学生运用所学知识评测安全风险、制定管理策略，学生在跨领域知识融合和实际问题解决方面的能力得到明显提升。

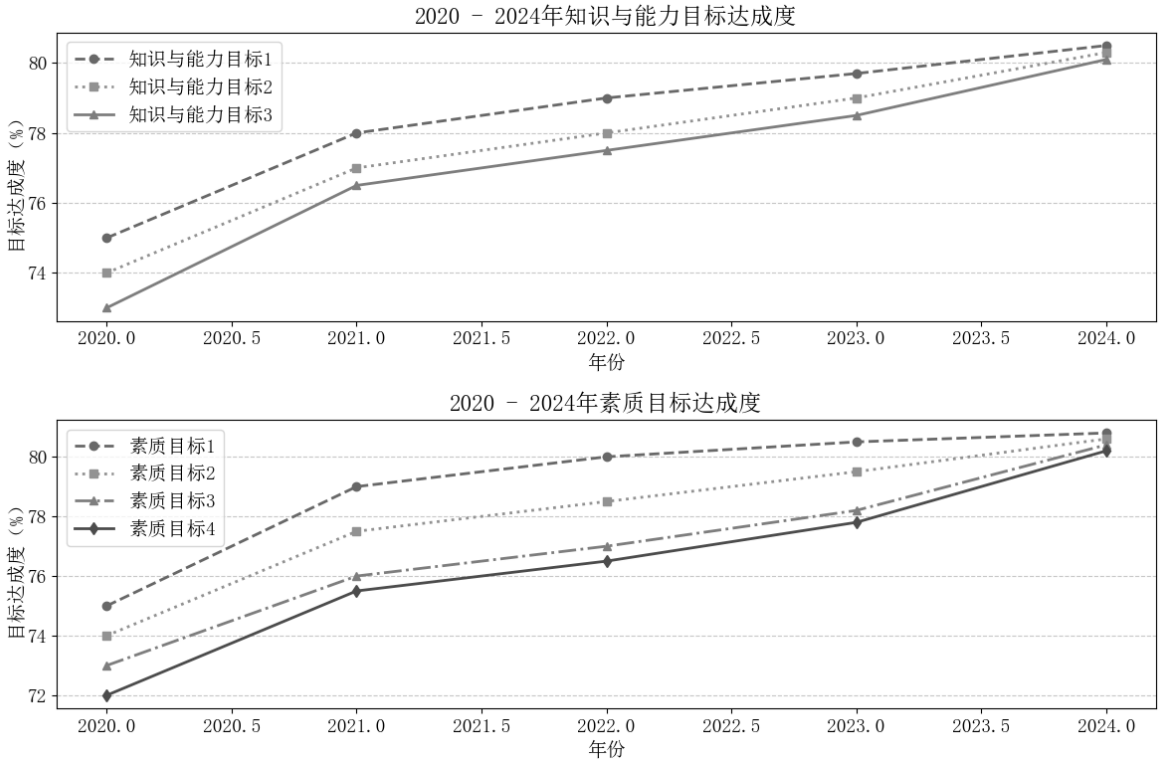

图 3 2020-2024年课程目标达成度对比

素质目标同样进步显著（见图 3 下），学生对信息安全政策法规等的关注度大幅提高，课程通过引入国际信息安全事件，如某知名社交平台数据泄露引发的监管风波，引导学生关注信息安全政策法规的重要性，学生逐渐将信息安全意识融入日常学习和生活中。学生的辩证思考与批判性思维能力逐步增强，在课堂讨论和项目实践中，学生学会从多个角度分析问题，对现有技术和解决方案提出合理质疑，并尝试改进，展现出较强的批判性思维能力。学生在遵循行业规范、践行安全责任方面表现更为出色，在实习和实践活动中，学生严格遵守企业的安全规范，积极参与安全防护工作，得到了实习单位的高度认可。学生对技术创新和自主可控的使命感显著增强，部分学生主动参与信息安全技术创新项目，致力于解决关键技术难题，展现出强烈的使命感和责任感。

5 结束语

信息安全课程以学生为中心，通过构建 RAPETA 教学模型，有效解决了安全理论技术难以内化调度等痛点问题。学生通过螺旋递进式剖析实际案例安全需求、参与多元多向学习活动、切换信息安全攻防视角、融入泛在互动学习环境、落实灵活深度课程任务、收获立体灵活全程评价，实现了安全理论的内化，形成了技术应用和协作思辨能力，适应了未来信息安全技术和产业发展的新要求。课程开展的思政育人工作成效显著，学生信息安全能力持续提升、素养不断拓展，得到了学生的高度评价。

参 考 文 献

[1] 张锦,史长琼,向凌云,黄园媛.结合工程教育认证的地方高校计算机类专业创新人才培养模式研究,计算机技术与教育学报，2023.11(4):71-76.

[2] 罗芳，郭小兵，石兵,工程教育认证背景下面向创新能力培养的程序设计课程群改革[J].计算机教育，2024(2):31-36.

[3] 田俊峰,何欣枫,刘凡鸣,等.两大课堂互动互融的信息安全新工科人才培养模式[J].高等工程教育研究,2022,(02):23-29.

[4] 张敏,郝素冰,龚子捷,等.大学生信息安全认知的测量及其与人格特征的关系[J].高等工程教育研究,2016,(06): 144-148+174.

[5] 张炜,陈洁.学术共同体建构视域下美国工程教育研究的演进历程及其经验启示[J].清华大学教育研究,2023,44(03):94-103.

[6] 余玲,彭必友.地方工科院校教学引导式项目设计与评价方法创新实践[J].高等工程教育研究,2024,(02): 91-96.

[7] 杨涛.网络安全实践类教学课程思政的探索与实践,计算机技术与教育学报，2024.12(1):95-99.