

高校计算机信息安全技术课程思政项目化教改实践研究

周小艳 王永周 *
重庆移通学院，重庆 401420

摘要：随着计算机信息安全技术的迅速发展，网络安全问题日益突出。高校作为信息安全人才培养的重要基地，其课程体系的改革对行业发展具有深远影响。传统的信息安全课程更多关注技术能力培养，往往忽视了学生责任意识、伦理素养和安全观念的培养。为实现知识传授与价值引领相结合，本研究提出将课程思政元素融入信息安全课程教学，通过项目化教学模式提升学生的专业能力和社会责任感。研究首先分析了信息安全技术课程的现状，论证了思政教育与专业课程融合必要性，进而基于项目化教学理念提出了教学体系优化的具体方法。研究结果表明，项目化教学改革不仅能够有效提升学生的技术应用能力和团队协作能力，还能促进思政素养的发展，为高校课程思政改革提供了有益借鉴。

关键词：信息安全；课程思政；项目化教学；实践改革；人才培养

Practical Research on Ideological and Political Project Teaching Reform of Computer Information Security Technology Course in Colleges

Zhou,Xiaoyan Wang,Yongzhou*
Chongqing College of Mobile Communication, Chongqing, 401420, China

Abstract: With the rapid development of computer information security technology, the problem of network security has become increasingly prominent. As an important base for training information security talents, the reform of the curriculum system in colleges has a far-reaching impact on the development of the industry. The traditional information security course pays more attention to the cultivation of technical ability, and often ignores the cultivation of students' sense of responsibility, ethical accomplishment and safety concept. In order to realize the combination of knowledge transfer and value guidance, this study proposes to integrate the ideological and political elements into the teaching of information security courses, and enhance students' professional ability and social responsibility through project-based teaching mode. Firstly, the research analyzes the current situation of information security technology course, demonstrates the necessity of the integration of ideological and political education and professional courses, and then puts forward specific methods to optimize the teaching system based on the project teaching concept. The results show that the project-based teaching reform can not only effectively improve students' technical application ability and teamwork ability, but also promote the development of ideological and political literacy, which provides a useful reference for the ideological and political reform in colleges.

Keywords: Information security; Ideological and political course; Project-based teaching; Practice reform; Personnel training

DOI: 10.62639/sspfed24.20250102

引言

信息安全是数字化时代的重要基础，其技术与应用涵盖网络安全、数据保护、系统防御等多个领域。高校信息安全课程承担着培养高素质专业人才的重要使命，但现有教学模式在实际运行中仍存在理论与实践脱节、技术教育与伦理教育分离等问题，难以适应社会对复合型信息安全人才的需求。

近年来，课程思政已成为高校教育改革的重点方向，强调专业教育与价值引领的有机融合。在信息安全课程中融入职业伦理、社会责任和法律法规等内容，能够有效增强学生的安全意识和责任感，提升综合素养。本研究基于项目化教学理念，探讨在信息安全课程中实施课程思政的具体路径，通过梳理现有教学模式的不足，提出教学优化方案，并对其实践效果进行评估，最终构建兼具技术性、实践性和育人价值的教学体

系，为信息安全课程的改革与创新提供理论依据和实践参考。

一、高校计算机信息安全课程思政教学概述

（一）信息安全技术课程的特点

信息安全技术作为计算机科学的重要分支，其核心任务是保障信息系统的安全性、完整性和可用性。高校信息安全课程内容广泛，涵盖密码学、网络攻防技术、系统安全管理和数据隐私保护等关键领域，注重理论与实践的结合，旨在培养学生的技术应用能力和实践操作水平。

然而，当前教学模式仍存在明显局限，过度强调技术知识的传授，忽视了安全伦理、社会责任以及技术应用边界等非技术性因素的引导。事实上，信息安全问题不仅关乎技术，更涉及社会信任、法律法规和道德规范等复杂层面。例如，学生在学习渗透测试技术时，若缺乏基本的法律

（稿件编号：FED-25-2-1022）

作者简介：周小艳（1991-），女，汉族，籍贯：湖北省荆州市，硕士研究生，讲师，研究方向：信息安全，计算机应用。

通讯作者：王永周（1982-），男，汉族，籍贯：河南省周口市，硕士研究生，正高级经济师，研究方向：高教研究。

基金项目：重庆移通学院：““金课”建设视角下基于成果导向的多元性考核评价体系实践与探索”（课题编号：23JG208）。

意识和职业伦理观念, 极易出现技术滥用现象, 甚至引发社会风险。因此, 在信息安全课程中融入课程思政, 通过价值引导帮助学生树立正确的安全观念, 是推动教学改革的重要课题。

(二) 课程思政在信息安全教学中的作用

课程思政在信息安全教学中的应用, 既能深化知识传授效果, 又在学生职业伦理塑造与社会责任培养方面发挥着重要作用。

首先, 课程思政有助于提高学生的网络安全意识。信息安全不仅是技术性问题, 还涉及社会稳定、国家安全及个人隐私保护等多重维度。教师可以通过结合典型的数据隐私保护案例, 引导学生认识数据合规管理的重要性, 从而加深其对信息安全社会意义的理解, 增强学生的综合认知能力。

其次, 课程思政在培养学生技术伦理观念方面具有显著作用。信息安全技术的应用必须严格遵循法律法规与职业道德标准。在教学过程中, 通过网络攻击案例的剖析与讨论, 引导学生深入理解技术滥用的潜在危害, 帮助其在掌握技术的同时, 树立正确的职业伦理观念, 规避技术滥用风险。

此外, 课程思政还能在培养团队协作能力方面发挥积极作用。信息安全问题通常涉及跨学科、跨部门的协作, 单靠个人难以高效解决。通过小组合作任务, 学生可以在团队中学习沟通技巧、协商方法及共同决策策略, 进而有效提升其综合素养和协作能力, 为未来职业发展奠定基础。

(三) 项目化教学模式的引入

项目化教学模式以任务驱动、团队协作和问题解决为核心理念, 在信息安全课程改革中展现出重要价值。与传统教学模式相比, 项目化教学更强调学生实践能力、自主学习能力及综合素质的培养。

首先, 通过构建仿真实验环境, 能够显著提升学生的实战能力。例如, 在“企业网络安全攻防演练”项目中, 学生在虚拟环境下分析系统漏洞、设计攻击策略并制定防御方案, 不仅加深了对网络攻防技术的理解, 还强化了安全责任意识。

其次, 项目化教学注重团队合作与角色分工。以“数据安全保护”项目为例, 学生在项目中分别扮演安全分析员、渗透测试员和合规审核员等角色, 共同完成安全策略的设计与优化任务。这种基于角色分工的协作模式, 不仅能提升学生的技术水平, 还有效增强了沟通、协作和应变能力, 帮助其更好地适应未来职业场景。

最后, 项目化教学在引导技术伦理思考与社会责任培养方面具有独特优势。例如, 通过组织“道德黑客挑战赛”, 学生在合法合规框架内进行安全评估与漏洞修复实践, 并针对具体问题提出改进方案, 进一步加深了对技术应用边界的理解, 强化了职业道德意识与社会责任感。

二、高校信息安全课程教学现状及问题

(一) 教学内容局限, 思政元素覆盖不足

目前, 信息安全课程主要集中在密码学、网络攻防、系统安全、数据隐私保护等技术领域, 强调核心技术知识, 而对数据伦理、信息安全法

规和行业规范等非技术性内容覆盖较少。学生更关注技术操作, 忽视社会责任与法律约束。

在技术教学中, 漏洞扫描、渗透测试等攻防技术受到较多关注, 但对这些技术的法律边界和伦理风险的讨论相对不足。例如, 未授权的渗透测试可能引发法律责任, 加密技术的使用需符合行业标准。然而, 课程在这些方面的内容较弱, 导致学生虽具备技术能力, 却缺少合规思维和风险意识。

此外, 数据隐私保护已成为全球信息安全的重要议题, 但现有课程对数据安全及个人信息保护法规的比重不足, 学生在职场中难以快速适应企业合规要求。因此, 在课程中有机融入思政元素, 培养学生的法律意识与社会责任感, 是优化课程的关键方向。

(二) 教学方法以理论讲授为主, 实践环节不足

现阶段, 信息安全课程仍以传统讲授式教学为主, 课堂互动较少, 案例教学比重偏低, 导致理论与实践脱节。部分高校已引入实验教学, 但多为标准化流程, 学生按照固定步骤完成操作, 缺少真实安全环境中的探索与实践, 难以提升自主分析与解决问题的能力。

实验内容多为静态漏洞分析、加密解密等基础任务, 真实场景覆盖不足, 缺少企业级安全架构部署、动态攻防训练及应急响应等训练, 学生在行业中需较长时间适应。此外, 实验任务多为个人操作, 未能充分训练团队协作能力。因此, 提升实验教学的真实场景模拟能力, 强化团队合作任务设计, 是课程改革的重点方向。

(三) 考核体系以知识测试为主, 综合能力评估不足

当前信息安全课程考核方式以笔试和基础实验为主, 主要评估理论知识和基础操作能力, 但对创新能力、团队协作能力及安全责任意识考核较少。笔试难以全面衡量学生应对实际安全挑战的综合能力, 实验考核则偏重固定流程操作, 缺乏综合分析自主探索。此外, 现有考核方式较少涉及团队协作评价, 学生更关注个人技术实现, 忽视网络安全事件处置中的团队协同要求。

三、项目化教学在信息安全课程中的实践路径

(一) 构建基于项目化教学的课程体系

项目化教学模式强调任务驱动与问题解决, 课程设计需紧密结合信息安全领域的实际需求, 帮助学生在完成具体任务的过程中掌握核心技能, 同时培养其安全防护意识和综合素养。

在教学内容安排上, 课程应涵盖密码学应用、网络攻防策略、系统安全管理等技术模块, 同时有机融入团队协作、职业伦理和安全合规等关键内容, 确保学生在实践过程中形成全局安全观念与合规意识。

课程可采用任务递进模式进行设计, 分为初级、中级和高级三个阶段。初级阶段注重基础安全技术的掌握, 例如基本加密技术与漏洞扫描; 中级阶段聚焦企业级安全架构分析及常见攻击防

御策略;高级阶段则引入综合性攻防演练,要求学生在复杂安全场景中完成攻防任务,提升其应对真实安全威胁的能力。这种递进式学习路径能够有效促进学生的实践能力,帮助其在任务解决过程中不断深化对安全防护体系的理解。

(二) 优化教学方法, 提高学生实践能力

传统信息安全课程以理论讲授为主,课堂互动较少,案例分析和实验训练比重不足,导致学生在实践能力和问题解决能力方面存在短板。项目化教学强调多元化的教学方法,鼓励学生在任务执行中自主探索与协作,进而培养系统化的安全思维能力。

案例教学是理论与实际应用相结合的重要途径,能够通过分析典型案例帮助学生深入理解信息安全技术。翻转课堂模式则鼓励学生课前自主学习基础知识,课堂上通过小组讨论和方案设计进一步巩固并深化对知识的理解。情境式实验教学通过构建仿真的网络攻防环境,让学生在模拟情境中完成安全评估、防护策略制定及应急响应等实践任务,增强其实战经验。这些多样化教学方法的结合,不仅能够有效提升学生的学习主动性,还能培养其综合分析并解决复杂安全问题的能力。

(三) 完善考核体系, 促进学生全面发展

现有信息安全课程的考核方式主要依赖笔试与实验操作测试,评价重点集中于知识掌握情况,较难全面衡量学生的实践能力、团队协作能力及安全责任意识。项目化教学需构建多维度评价体系,综合考核学生的技术能力、决策分析能力及合规意识,促进其全面发展。

考核方式应涵盖理论测试、项目实践、案例分析及团队协作表现等多个维度,确保评价体系的科学性与全面性。过程性考核可通过课堂互动、任务反馈及项目过程跟踪等方式,持续关注学生的学习进展,并评估其在安全管理和问题解决中的综合能力。考核不仅要关注学生对核心技术的掌握程度,还应注重思考能力与综合分析能力的评估,引导学生在实践中不断优化自身的安全策略思维。

四、信息安全课程的未来发展趋势

(一) 智能化教学的应用

人工智能和大数据技术的引入为信息安全课程的智能化教学提供了重要支持。智能学习系统能够根据学生的学习数据和掌握情况进行动态分析,及时调整教学内容,优化个性化学习路径,显著提高学习效率与教学效果。

云端实验室和自动化评测系统的应用进一步提升了实验教学的灵活性和实践效果,使学生能够随时随地进行实验操作,并通过系统的实时反馈不断完善实践能力。借助人工智能技术,教师可以更高效地跟踪学生学习进展,精准定位薄弱环节,提供有针对性的辅导,全面提高教学的精准性和互动性。

(二) 跨学科融合提升综合素养

信息安全作为一个高度交叉的学科领域,涉及法律、心理学、伦理学等多学科内容。未来,

课程将进一步强化跨学科融合,提升学生的综合素养与多维度思维能力。

引入法律模块可以帮助学生深入理解数据合规管理、网络安全法规及国际标准,增强其合规意识;安全心理学课程则能够提高学生对社会工程攻击的认知与防范能力;伦理学内容将引导学生树立正确的技术应用观,增强社会责任感与职业道德意识,从而在面对复杂的网络安全问题时具备更强的全局判断力和道德决策能力。

(三) 实战化教学强化实践能力

实战化教学是提升学生实践能力和应变能力的方向。未来,信息安全课程将通过真实安全事件分析、漏洞挖掘、红蓝对抗演练等多样化实践活动,增强学生在真实网络安全环境中的实战经验。

课程将引入动态安全环境与自动化安全运维平台,使学生在模拟现实场景中进行防御策略设计和应急响应训练,培养其快速反应和解决实际安全问题的能力。同时,通过加强与行业的合作,邀请企业安全专家参与教学,基于行业前沿案例开展专项讲座与联合项目,帮助学生更好地了解行业需求,缩短学校教育与企业实践的差距。

五、结束语

信息安全课程的改革不仅要强化技术教育,更应注重培养学生的安全意识、职业伦理与社会责任。项目化教学模式的引入为课程思政的实施提供了切实可行的路径,能够在提升教学质量的同时,实现技术教育与价值引领的协同育人目标。

面向未来,信息安全课程需进一步融合智能技术、跨学科资源与实践教学,不断优化教学体系,创新教学方法,全面提升学生的技术能力与综合素养,培养既具备高水平专业技能、又具备强烈社会责任感和职业道德意识的复合型信息安全人才,助力行业长远发展。

参考文献:

- [1] 陈金木, 陈峰, 郑少朋.《高校计算机网络信息安全问题及其防范措施研究》[J]. 网络空间安全, 2023.
- [2] 尚涛, 毛剑, 关振宇等.《“信息系统安全”课程思政的实践》[J]. 工业和信息化教育, 2022.
- [3] 陕西国际商贸学院信息工程学院.《课程思政建设改革的探索与实践——以信息安全课程为例》[J]. 陕西教育(高教), 2022.
- [4] 杨国正, 刘京菊, 钟晓峰.《研究生课程思政教学改革方法探索实践》[J]. 计算机教育, 2021.
- [5] 山西省财政税务专科学校.《信息安全课程思政教学改革探索》[J]. 山西经济管理干部学院学报, 2021.
- [6] 杨淑棉, 马宾, 赵大伟.《课程思政在信息系统安全教学设计中的探索与实践》[J]. 高教学刊, 2023.
- [7] 张小林, 鲁雷, 罗汉云.《融入课程思政的“信息安全导论”课程教学探索》[J]. 网络安全技术与应用, 2024.
- [8] 西华大学计算机与软件工程学院.《课程思政视角下研究生案例教学探索与实践——以西华大学“密码学与网络安全”课程为例》[J]. 软件导刊, 2024.
- [9] 田永民.《基于课程思政的《计算机网络安全技术》课程教学模式分析》[J]. 电脑知识与技术, 2021.
- [10] 曹腾飞, 牛国清, 刘薇等.《融合思政元素的网络攻防实验教学研究与探索》[J]. 软件导刊, 2022.