

人工智能时代安全类专业思政课教学改革与创新研究

邱楚珈

山东科技大学, 山东 青岛 266590

DOI: 10.61369/ETR.2025360019

摘 要 : 随着人工智能技术的发展, 网络安全面临新的机遇、挑战, 其中网络安全类专业的人才培养效果, 影响到国家网络安全战略的实施效果。专业思政课的开展, 有助于实现立德树人根本目标, 发挥了重要作用。本文从人工智能时代背景出发, 分析了网络安全类专业思政课教学改革意义, 并提出具体的教学创新策略, 旨在提升网络安全人才培养质量, 促进思政课程教学质量的提高, 为后续的思政课教学改革积累经验。

关 键 词 : 人工智能; 网络安全专业; 思政课

Research on the Reform and Innovation of Ideological and Political Courses Teaching for Cybersecurity Majors in the Era of Artificial Intelligence

Qiu Chuja

Shandong University of Science and Technology, Qingdao, Shandong 266590

Abstract : With the development of artificial intelligence technology, cybersecurity is facing new opportunities and challenges. The talent training effect of cybersecurity-related majors affects the implementation effect of the national cybersecurity strategy. The development of professional ideological and political courses is conducive to achieving the fundamental goal of establishing morality and cultivating people, and has played an important role. Starting from the background of the artificial intelligence era, this paper analyzes the significance of the teaching reform of ideological and political courses for cybersecurity majors, and puts forward specific teaching innovation strategies. It aims to improve the quality of cybersecurity talent training, promote the improvement of the teaching quality of ideological and political courses, and accumulate experience for subsequent ideological and political course teaching reforms.

Keywords : artificial intelligence; cybersecurity major; ideological and political courses

引言

基于数字时代背景, 人工智能技术逐渐应用于教学活动, 加快了教学方式的革新。高校是人才培养的重要场所, 为了应对网络安全威胁, 需要重视网络安全类专业调整, 并加强与思政课程的融合。其中人工智能技术具有数据驱动、智能交互特点, 有助于打破传统技能轻价值问题。对此, 高校需要重视教学创新, 加强网络安全类思政课教学创新, 切实提升育人效果。

一、人工智能时代网络安全类专业思政课教学改革意义

随着人工智能技术逐渐应用于各行业, 网络空间成为基础设施、社会发展以及群众生活的重要组成, 网络安全也上升为核心

议题。网络安全类专业承担着培养网络防护、应急响应等人才的重任, 具体的人才培养活动, 要求学生掌握专业知识, 并需要其具有社会责任与家国情怀, 其中思政课的开展, 有助于该目标的达成。^[1] 基于人工智能时代背景, 网络安全类专业思政改革发挥了重要作用, 可以提升育人效果。根据国家的战略需求, 可以明

确当前全球的网络空间存在激烈竞争,出现了许多网络攻击、数据泄露问题,影响到整体的网络安全。高校开展网络安全类专业思政课教学,可以提升相关人才素质,做到勇于担当,有效维护国家的网络安全,保障实际的发展利益。在思政教学活动中,思政课发挥了载体作用,可以帮助网络安全专业学生清晰认识国家网络安全形势,并养成良好的网络安全观念,有效结合个人发展与国家网络安全事业,切实提升学生的使命感与责任感。若思政课无法适应人工智能时代需求,则难以传递出国家安全思想,很难培养出满足战略需求的网络人才,阻碍国家网络安全战略的落实。^[2]在网络安全类专业的人才培养环节,人工智能技术为网络安全提供了新技术与场景,如智能漏洞扫描工具等,但对网络安全人才素质提出了严格要求。网络安全人才不仅要掌握良好技术素养,还需要提升自身的职业与伦理素质,可以适应复杂网络环境,真正做到坚持底线,避免网络违法行为的出现。^[3]思政课程借助职业道德、法治等教学方式,帮助网络安全专业学生养成正确价值观念,并形成良好的法律和伦理观念,有效规范职业行为。

二、人工智能时代网络安全类专业思政课教学面临的挑战

(一) 技术应用层面:安全风险与适配难题并存

在人工智能技术与思政课教学的融合环节,其存在一些安全漏洞和技术适配问题,不利于开展教学创新。第一,智能教学平台和工具安全防护面临较高难度。网络安全专业的学生掌握了良好的网络技术交流技能,甚至部分学生具有一定的漏洞挖掘、渗透测试技能,但许多思政课智能平台的安全防护体系难以满足相关群体需求,表现出数据加密性较差、入侵检测响应滞后等问题。例如,平台内可以存储数据,如学生思想动态、学习行为等,并使用高强度算法,容易被学生借助技术手段获取,对学生隐私造成侵犯,甚至带来教学评价结果的失真。部分平台后台管理存在漏洞,容易被学生打破权限限制,进而调整教学内容,甚至干扰正常教学的开展,严重冲击正常的思政教学顺序。第二,人工智能和思政教学缺乏适配性。在当前思政课中,智能化教学资源包括虚拟仿真场景、AI课件等,均以通用思政理论作为核心,缺少与网络安全专业的融合。部分VR思政教学场景可以还原红色事件,虽然可以传递爱国精神,但尚未与网络安全领域相融合,容易出现技术和专业特色脱节问题,不利于激发学生的专业认同感。另外,人工智能技术发展与思政教学的相对稳定性具有矛盾,如果人工智能技术推出新应用形态,思政教师通常需要花费较多时间,探索合适的教学方式,容易造成技术滞后于教学所需,难以充分发挥智能教学价值。

(二) 教育主体层面:教师能力断层与AI信任困境凸显

基于人工智能时代背景,高校网络安全类专业思政教学面临的核心挑战是教育主体适配性,其表现在教师能力的差异、师生对人工智能存在的信任等方面。从教师能力视角出发,部分思政教学出现了能力短板,其一是缺乏信息技术应用技能。部分教师

缺少对人工智能技术的深层次认知,很难熟练使用大数据技术,难以精确分析学生思想,面对智能化教学的功能板块理解缺乏全面性,很容易造成技术工具的形式化,阻碍教学质量提高。如思政教师使用人工智能问答辅助系统时,由于不熟悉系统话术训练作用,很难结合网络安全专业学生情况调整问答库,进而造成系统无法解答学生提出的专业性问题,不利于发挥该工具价值。其二缺少网络安全专业知识。在网络安全类专业的思政课内,可以结合思政理论与专业知识,如教师讲述社会主义核心价值观,适当结合数据安全、网络空间等概念,但由于部分教师能力有限,很难精确把握专业和思政的结合部分,甚至可能造成专业概念解读误差的出现。

(三) 教育环境与文化层面:多元信息冲击与专业文化割裂

教育环境和文化具有复杂性,对网络安全类专业思政带来了挑战,其表现在信息冲击与专业文化割裂方面。面对信息环境内容,人工智能时代下学生掌握信息渠道表现出碎片化、多元化特点,许多网络平台内蕴含大量与思政教学相悖的观点,如网络安全技术无国界等,相关错误观点的出现,很容易对网络安全专业学生价值观念产生错误引导。同时,由于网络环境的复杂性,存在许多的虚假信息,这些信息容易推送给学生,表现出传播速度快、隐蔽性强特征,思政教师如果无法及时发现,容易大幅减弱思政教学实效性。在文化融合方面,当前校园文化与网络安全专业文化存在明显割裂,未能形成支撑思政课教学的协同文化氛围。校园思政文化活动缺乏专业特色,多数活动仍以“红色观影”“理论宣讲”等传统形式为主,未结合网络安全专业特点设计活动内容,如未开展“网络安全攻防演练中的思政教育”“AI技术伦理辩论赛”等特色活动,导致学生难以将思政教育与专业学习结合起来,参与活动的积极性较低。

三、人工智能时代网络安全类专业思政课教学实践创新策略

(一) 在技术层面构建安全稳定的智能化教育支持体系

人工智能时代背景下,技术成为促进思政改革的推动力。其中安全智能教育支持体系建设,可以构建良好技术环境,拓展教学方式,取得良好的教学质量,并加快网络安全技术和思政课的融合,推动协同育人的实现。^[4]在技术层面的创新环节,智能教学平台建设是核心之一。通过汇聚各种先进技术,有效满足思政教学需求。第一,智能教学平台需掌握资源整合作用,整理归纳思政理论知识,把握经典素材内容,如马克思主义著作等,并适当结合网络安全类专业,进行网络安全领域内容的收集,如红色资源、典型案例等,制作系统性、专业性教学资源库。例如,整理归纳我国网络安全领域专家面对关键技术突破相关奋斗故事,了解重大网络安全事故的处理,了解其中的英雄事迹,帮助学生了解思政理论知识,并熟悉网络安全行业信息,形成良好的专业认同感。

第二,在平台内设置人工智能交流版块,巧用智能问答、自然语言处理等技术,方便学生获得实时辅导与交流服务。当学生

在知识学习遇到问题后，巧用智能问答方式，及时快速的解答问题。^[6]同时，平台能够设置在线交流区域，灵活使用人工智能技术，实时分析与引导学生交流内容，避免偏离教学目标，切实提升互动效果。另外，平台还需拥有学习过程的追踪、评价功能，可以借助大数据技术，整理学生学习进度、作业完成状况等，了解学生知识学习成效，开展客观公正的评价，适当结合评价结果，使学生获得个性化学习建议，有效改善知识学习方式，提升课堂教学质量。

第三，面对智能化教学平台的建设，需看重平台的网络安全防护。基于网络安全类专业学生具有的探索技能，平台内蕴含许多教学数据、学生信息，当平台出现安全漏洞后，容易带来数据泄露、平台遭受攻击等问题，不仅影响到正常教学，还可能威胁到学生信息安全。基于此，高校的网络安全类人才培养可以引进先进网络安全技术，如漏洞扫描、访问控制以及数据加密等技术，进行平台的全方位安全防护。^[6]例如，面对平台蕴含的教学数据、学生信息开展加密存储，有效避免数据泄露问题的出现。同时，可以设置严格访问权限，当教师、学生得到授权后，才可以有效访问相关资源、功能，避免出现未授权访问。另外，积极渗透隐私计算技术。联邦学习框架是新兴分布式机器学习技巧，其核心在于保障原始数据，并适当分散各参与方数据源，开展良好的模型训练，切实提高模型的性能，从而有效完成教学数据分析活动。例如，高校可以结合智能测评系统，设置隐私技术板块，保障学情分析活动的开展，避免泄露学生信息。其中隐私技术可以保障学生隐私，并深层次分析和使用数据，切实提升教学质量，取得良好的课程思政成效。

（二）在教育主体层面构建人机协同机制

在实际的人机协同机制内，教师通常处于主导，其角色、能力需适应人工智能时代需求，并开展适当转变与提高。第一，教师需要由传统知识讲述者转变为引导者、组织者。在思政课程的教学环节，教师不仅需要重视知识讲解，还可以灵活使用人工智能技术，整理与分析学生需求、思想动态等，并结合学生情况，制定科学合理的教学计划，鼓励学生参与学习，形成良好的自学和批评思维技能。^[7]例如，教师通过分析智能化教学平台收集的学生学习数据，发现部分学生对网络安全伦理问题存在困惑，就可以组织专题讨论课，引导学生围绕网络安全伦理案例进行深入讨论，帮助学生树立正确的网络安全伦理观念。第二，教师需要不断提升自身的信息技术应用能力和跨学科整合能力。人工智能技术的快速发展要求教师能够熟练掌握智能化教学平台和教学工具的使用方法，将人工智能技术与思政课教学内容有机结合起来。同时，网络安全类专业思政课具有较强的专业性和交叉性，需要教师具备一定的网络安全专业知识，能够将思政教育与网络安全专业知识深度融合，在教学过程中准确把握专业知识与思政元素的结合点，实现“润物细无声”的育人效果。^[8]例如，教师在讲解马克思主义实践论时，可以结合网络安全实践教学环节，引导学生认识到理论与实践相结合的重要性，培养学生的实践能力和创新精神。第三，教师还应注重自身的师德师风建设，以高尚的道德情操和人格魅力影响学生，成为学生健康成长

的榜样。在网络安全领域，教师的职业道德和伦理素养对学生具有重要的示范作用，教师应严格遵守网络安全法律法规和职业道德规范，在教学和科研活动中坚守底线，为学生树立良好的职业榜样。

（三）在教育环境与文化层面构建智能文化治理体系

教育环境、文化潜移默化的影响到学生思想意识与行为。基于人工智能时代背景，智能文化治理体系的建设，有助于构建健康且具有专业特色的教育环境，并营造良好的文化氛围，为思政教学的开展创建外部条件，切实提升思政教学实效性、影响力。智能化校园文化环境建设，有助于搭建智能文化治理体系。^[9]校园文化属于隐性资源，关系到学生成长。高校可以灵活使用人工智能技术，构建智能化环境，并将思政元素、网络安全专业与校园各角落的融入，促进思政教学的顺利开展。例如，高校可以利用公共场所，包括图书馆、教学楼以及宿舍等，设置智能显示屏，灵活使用人工智能技术，结合差异化场所与时间段，推送多样化思政与网络安全知识。其中在教学楼显示屏内，能够推送国家政策、网络安全动态等，鼓励学生在上下课途中获取相关信息。在图书馆显示屏，能够及时推送思政典籍、网络安全技术等内容，并帮助学生丰富阅读知识。在宿舍显示屏内，可以推送网络防护知识、思政主题等内容，切实提升学生网络安全意识，提高其参与思政的热情。^[10]另外，人工智能技术的使用，有助于搭建校园虚拟空间，包括虚拟思政教学、虚拟网络博物馆等。学生还可以登录虚拟文化空间，随时参观学习，突破时间、空间限制。虚拟思政基地能够模拟红色基地，如延安、井冈山等，使学生参与虚拟环境，有效接受红色教育，传承红色基因。虚拟网络博物馆还能够展示网络安全历程、重大网络安全事件等，方便学生认识网络安全文化，形成良好的专业认同感。

（四）构建过程+结果多元评价，突出素养导向

将过程性评价贯穿教学始终，综合考核学生的课堂参与、实践表现与日常素养：一是课堂参与评价，通过记录学生在讨论、辩论、案例分析中的发言质量，评估其思政思维能力。二是实践表现评价，针对虚拟仿真实践、项目式学习等实践环节，制定“技术能力+思政素养”双维度评价标准，如在校园AI安全防护系统开发项目中，不仅评价技术方案的合理性，还评价学生在项目中体现的伦理意识、团队协作精神与责任担当。三是日常素养评价，通过观察学生在网络行为中的表现（如是否遵守网络道德、是否积极参与网络安全宣传活动）、在线讨论中的观点表达，评估其思政素养的日常养成。改革期末考试形式，避免单一的理论笔试，采用“理论考核+实践考核+素养展示”的综合考核方式。

四、结束语

综上所述，基于数字经济的不断发展，网络安全威胁不断提升，高校作为高素质人才培养的主要场所，需要重视网络安全类课程调整，促进专业技能和思政教学的融合，切实提升育人效果。人工智能技术具有数据驱动、智能交互特点，有助于打破传统教学限制，有效创新育人活动。通过发挥前沿技术作用，可以

构建协同育人模式，真正实现技术训练、价值引领的统一，培养出具有综合素质的网络安全类人才。高校通过开展人机协同机制研究，可以探索人工智能在价值引导、情感培养等领域的应用，加快高等教育的创新发展。

参考文献

[1] 崔晨, 周胜利, 阮琳琦. 大数据时代网络安全专业课程中思政教育融合与创新研究 [J]. 网络安全技术与应用, 2024, (10): 96-98.

[2] 刘云恒, 吴玉强. 新工科背景下网络安全与执法专业课程思政教学指南构建研究 [J]. 网络安全技术与应用, 2024, (09): 116-118.

[3] 沈碧婷. 高职卫生信息管理专业计算机网络与网络安全课程思政研究与探索 [J]. 现代商贸工业, 2024, 45(13): 233-235.DOI: 10.19311/j.cnki.1672-3198.2024.13.080.

[4] 张晓航, 闫玺玺. 网络信息安全专业课程思政教学实践——以防火墙与入侵检测课程为例 [J]. 焦作大学学报, 2024, 38(02): 93-96.DOI: 10.16214/j.cnki.cn41-1276/g4.2024.02.003.

[5] 杜春来. 课程思政融入信息安全专业课程《软件安全》的教学实践 [J]. 数字技术与应用, 2023, 41(10): 37-39.DOI: 10.19695/j.cnki.cn12-1369.2023.10.09.

[6] 郭向民, 王群. 网络安全与执法专业课程思政教学探索 [J]. 计算机教育, 2023, (07): 73-77.DOI: 10.16512/j.cnki.jsjy.2023.07.008.

[7] 贾春福, 哈冠雄, 李瑞琪, 等. 信息安全数学基础课程思政教学实践 [J]. 计算机教育, 2023, (06): 52-55.DOI: 10.16512/j.cnki.jsjy.2023.06.010.

[8] 张艳苏, 杨晨影, 田俊静, 等. 公安院校“数据库原理”课程思政研究 [J]. 中国人民警察大学学报, 2023, 39(02): 84-87.

[9] 李莉, 宋亚奇. 网络安全课程思政元素提炼与融入教学设计 [J]. 教育教学论坛, 2023, (01): 133-136.

[10] 冯斌, 冯玲, 段西强, 等. 网络安全技术课程思政教学探索与实践 [J]. 软件导刊, 2022, 21(11): 182-187.