网络安全教育在高职教育中的课程体系构建

杨凯
江西财经职业学院

摘　要：随着信息技术的飞速发展，网络安全问题日益凸显，对高职教育提出了新的挑战和要求。本文旨在探讨如何在高职教育中构建完善的网络安全教育课程体系，通过分析网络安全教育的重要性、现状以及面临的问题，提出了包括课程目标设定、课程内容设计、教学方法创新、师资队伍建设等方面的具体策略，以期提高大学生的网络安全意识和技能，培养适应新时代需求的高素质网络安全人才。

关键词：高职教育；网络安全教育；课程体系
【DOI】10.12252/j.issn.2096-6288.2025.05.036

引言

在数字化时代，网络已深度融入社会生活的各个领域，成为推动经济发展、社会进步的重要力量。然而，网络安全威胁也随之而来，如网络攻击、数据泄露、网络诈骗等事件频繁发生，给国家、社会和个人带来了巨大的损失。高职教育作为培养高素质人才的重要阵地，加强网络安全教育，构建科学合理的课程体系，对于提高大学生的网络安全素养，培养网络安全专业人才，维护国家网络安全具有重要意义。

一、高职教育中网络安全教育的重要性

（一）适应社会发展需求

随着互联网技术在各个行业的广泛应用，网络安全已成为保障行业稳定运行的关键因素。社会对网络安全人才的需求日益增长，不仅需要专业的网络安全技术人才，更需要具备网络安全意识和基本防护技能的复合型人才。高职教育通过开展网络安全教育，能够为社会培养大量适应时代需求的人才，推动网络安全产业的发展，促进社会的数字化转型。

（二）提升大学生网络安全素养

大学生是互联网的主要使用者，他们在学习、生活和社交中高度依赖网络。然而，部分大学生网络安全意识淡薄，对网络安全风险缺乏足够的认识，容易成为网络攻击的受害者。通过网络安全教育课程，能够帮助大学生了解网络安全的基本知识和技能，提高他们的网络安全意识和防范能力，使其在面对网络安全威胁时能够采取有效的应对措施，保护个人信息和合法权益。

（三）维护国家网络安全

网络安全是国家安全的重要组成部分，关系到国家主权、安全和发展利益。高职院校作为知识创新和人才培养的重要基地，肩负着为国家培养网络安全人才的重任。通过构建完善的网络安全教育课程体系，培养具有扎实专业知识和强烈爱国情怀的网络安全人才，能够为国家网络安全事业提供有力的人才支撑，增强国家在网络空间的竞争力和话语权，维护国家网络安全和信息安全。

二、高职教育网络安全教育现状分析

（一）课程设置情况

目前，部分高校已经意识到网络安全教育的重要性，在课程设置上有所体现。一些高校开设了网络安全相关的公共必修课或选修课，如“网络安全基础”“信息安全概论”等，向学生普及网络安全的基本知识。部分计算机科学与技术、信息安全等相关专业则设置了较为系统的网络安全专业课程，包括网络安全技术、网络安全管理、密码学等。然而，整体来看，网络安全教育课程在高校课程体系中的占比相对较低，课程内容的深度和广度也有待进一步拓展。

（二）教学方法与手段

在教学方法上，多数高校网络安全教育课程仍以传统的课堂讲授为主，教师通过讲解理论知识、展示案例等方式进行教学。这种教学方法虽然能够系统地传授知识，但学生的参与度较低，实践能力难以得到有效锻炼。在教学手段方面，一些高校利用多媒体教学工具辅助教学，如播放网络安全视频、展示安全工具的使用等，但缺乏创新性的教学手段，如虚拟仿真实验、在线学习平台等应用不够广泛，难以满足学生多样化的学习需求。

（三）师资队伍建设

网络安全教育对教师的专业素养要求较高，不仅需要教师具备扎实的网络安全理论知识，还需要具备丰富的实践经验和教学能力。然而，目前高校网络安全教育师资队伍存在一定的不足。一方面，部分教师是从计算机科学与技术等相关专业转型而来，对网络安全领域的知识掌握不够系统和深入；另一方面，具有企业实践经

验的“双师型”教师相对较少，难以将实际工作中的案例和经验融入教学中，影响了教学质量。

（四）实践教学环节

实践教学是网络安全教育的重要环节，能够帮助学生将理论知识转化为实际操作能力。然而，在实际教学中，实践教学环节相对薄弱。一些高校缺乏完善的网络安全实验室和实践教学平台，无法为学生提供真实的网络安全实践环境。部分实践教学内容与实际应用脱节，学生在实践中难以接触到最新的网络安全技术和工具，导致实践教学效果不理想。

三、高职教育网络安全教育课程体系构建的目标与原则

（一）课程体系构建目标

课程体系构建致力于全方位培育学生，涵盖知识、能力与素质三个维度。知识层面，助力学生掌握网络安全基本概念、原理及技术，熟知网络安全法律法规与行业标准，洞悉常见网络安全威胁及防范手段；能力培养上，让学生具备网络安全系统设计、实施与运维能力，能运用所学知识技能处理实际网络安全问题，拥有网络安全漏洞检测修复以及事件应急处理能力；素质提升方面，着重提高学生网络安全意识与职业道德素养，培育创新思维和团队协作精神，使其契合网络安全行业发展需求，成长为富有社会责任感的高素质网络安全专业人才。

（二）课程体系构建原则

系统性原则：网络安全教育课程体系应涵盖网络安全的各个方面，包括网络安全基础、网络安全技术、网络安全管理、网络安全法律法规等，形成一个有机的整体。课程之间应具有合理的逻辑关系，由浅入深、循序渐进地进行设置，确保学生能够系统地掌握网络安全知识和技能。

实用性原则：课程内容应紧密结合实际应用，注重培养学生解决实际问题的能力。在教学过程中，引入大量真实的网络安全案例和项目，让学生在实践中学习和应用知识，提高学生对网络安全技术的实际操作能力和应对网络安全威胁的能力。

创新性原则：随着网络技术的不断发展，网络安全威胁也日益多样化和复杂化。因此，网络安全教育课程体系应具有创新性，及时跟踪网络安全领域的最新技术和发展动态，将前沿知识和技术融入课程教学中，培养学生的创新思维和创新能力，使其能够适应未来网络安全行业的发展变化。

个性化原则：不同专业、不同层次的学生对网络安全知识的需求存在差异。因此，在课程体系构建过程中，应充分考虑学生的个性化需求，设置多样化的课程模块，供学生根据自己的兴趣和专业方向进行选择。同时，在教学过程中，采用分层教学、个性化指导等方式，满足不同学生的学习需求。

四、高职教育网络安全教育课程体系的具体构建

（一）课程内容设计

网络安全基础课程，包括网络安全概论、计算机网络基础、操作系统安全等。网络安全概论主要介绍网络安全的基本概念、发展历程、面临的威胁和挑战等；计算机网络基础课程讲解计算机网络的体系结构、协议、拓扑结构等基础知识，为学生学习网络安全技术奠定基础；操作系统安全课程则重点讲解操作系统的安全机制、安全配置以及常见的操作系统安全漏洞与防范方法。

网络安全技术课程，涵盖网络安全攻防技术、密码学、网络安全检测与监控技术等。网络安全攻防技术课程详细介绍网络攻击的原理、方法和工具，以及网络防御的策略和技术，培养学生的网络安全攻防能力；密码学课程讲解密码学的基本原理、加密算法、数字签名等内容，使学生掌握密码技术在网络安全中的应用；网络安全检测与监控技术课程主要介绍网络安全漏洞扫描、入侵检测系统、防火墙等安全检测与监控工具的原理和使用方法，培养学生对网络安全状态的监测和分析能力。

网络安全管理课程，包括网络安全风险管理、信息安全管理体系、网络安全应急响应等。网络安全风险管理课程讲解网络安全风险评估的方法和流程，以及风险控制策略的制定和实施；信息安全管理体系课程介绍信息安全管理体系的建立、运行和维护，使学生了解如何通过管理手段保障网络信息安全；网络安全应急响应课程主要讲解网络安全事件的应急处理流程和方法，培养学生在面对网络安全突发事件时的应急处置能力。

网络安全法律法规课程，介绍国内外网络安全相关的法律法规，如《网络安全法》《数据安全法》《个人信息保护法》等，使学生了解网络安全领域的法律规范，增强学生的法律意识和合规意识，在今后的工作和生活中能够依法维护网络安全。

（二）教学方法创新

案例教学法：在教学过程中，引入大量真实的网络安全案例，如网络攻击事件、数据泄露事件等，通过对案例的分析和讨论，引导学生运用所学知识进行思考和

解决问题。案例教学法能够激发学生的学习兴趣，提高学生的分析问题和解决问题的能力，同时让学生了解网络安全实际应用中的复杂性和多样性。

项目驱动教学法：将课程内容分解为若干个项目，让学生以小组的形式完成项目任务。在项目实施过程中，学生需要综合运用所学的知识和技能，进行需求分析、方案设计、系统实现和测试等环节。项目驱动教学法能够培养学生的团队协作精神和实践能力，提高学生的综合素质和创新能力。

虚拟仿真实验教学法：利用虚拟仿真技术，搭建网络安全实验环境，让学生在虚拟环境中进行网络安全实验操作。虚拟仿真实验教学法能够为学生提供安全、便捷的实验平台，让学生在模拟的网络安全场景中进行实践操作，提高学生的实际动手能力和应对网络安全威胁的能力。同时，虚拟仿真实验教学法还能够降低实验成本，提高实验教学的效率和质量。

线上线下混合式教学法：充分利用互联网技术，开展线上线下混合式教学。线上教学通过在线课程平台，为学生提供丰富的学习资源，如教学视频、电子教材、在线测试等，学生可以根据自己的学习进度和需求进行自主学习。线下教学则采用课堂讲授、小组讨论、实验教学等方式，加强师生之间的互动和交流，及时解决学生在学习过程中遇到的问题。线上线下混合式教学法能够充分发挥线上教学和线下教学的优势，提高教学效果。

（三）师资队伍建设

加强教师培训，定期组织教师参加网络安全领域的培训和学术交流活动，鼓励教师参加企业实践，提升教师的专业素养和实践能力。通过培训，使教师能够及时了解网络安全领域的最新技术和发展动态，将前沿知识和实践经验融入教学中。

引进“双师型”教师，积极引进具有企业网络安全工作经验的“双师型”教师，充实师资队伍。“双师型”教师能够将实际工作中的案例和经验带入课堂，使教学内容更加贴近实际应用，提高教学质量。同时，“双师型”教师还能够指导学生开展实践项目，培养学生的实践能力和职业素养。

建立教师团队，组建由不同专业背景、不同研究方向的教师组成的网络安全教育教师团队，开展团队教学和科研活动。教师团队可以共同探讨教学方法和课程内容的优化，合作开展科研项目，提高教师的教学水平和科研能力。同时，教师团队还能够为学生提供更加全面的指导和服务，促进学生的全面发展。

（四）实践教学环节强化

建设网络安全实验室，加大对网络安全实验室的投入，购置先进的网络安全实验设备，如网络安全攻防设备、漏洞扫描设备、入侵检测设备等，搭建完善的网络安全实验环境。网络安全实验室应能够支持网络安全基础实验、网络安全技术实验、网络安全管理实验等各类实验教学活动，为学生提供良好的实践平台。

开展校企合作，加强与网络安全企业的合作，建立校外实习实训基地。通过校企合作，为学生提供实习机会，让学生在企业实际工作环境中接触最新的网络安全技术和项目，提高学生的实践能力和就业竞争力。同时，校企合作还可以促进学校与企业之间的人才交流和技术合作，推动网络安全教育与产业需求的深度融合。

组织网络安全竞赛，积极组织学生参加各类网络安全竞赛，如“强网杯”“护网杯”等。网络安全竞赛能够激发学生的学习兴趣和创新精神，提高学生的网络安全实践能力和团队协作能力。通过竞赛，学生可以与其他高校的学生进行交流和切磋，了解自己在网络安全领域的水平和差距，进一步明确学习目标和方向。

结语

网络安全教育在高职教育中具有重要的地位和作用，构建科学合理的课程体系是提高大学生网络安全素养、培养网络安全专业人才的关键。通过明确课程体系构建的目标与原则，从课程内容设计、教学方法创新、师资队伍建设、实践教学环节强化等方面入手，构建完善的网络安全教育课程体系，并采取有效的保障措施，能够提高网络安全教育的教学质量，培养出适应新时代需求的高素质网络安全人才，为国家网络安全事业的发展提供有力的人才支撑。

参考文献

[1] 王雨萌．高校网络安全教育课程体系建设路径探索 [J]．山西青年，2024,(23):178-180.

[2] 金磊．高职院校加强网络空间安全专业建设的必要性分析 [J]．网络安全技术与应用，2022,(04):89-90.

[3] 周恒洋，邹浩．“三全育人”视域下大学生网络安全教育探析 [J]．学校党建与思想教育，2022,(02):73-75.

[4] 靳家宝，杨嵘灏．大学生网络安全教育的作用途径研究 [J]．教育现代化，2019,6(83):238-239.