高职院校信息安全技术应用专业课程体系探究与实践

王　晶

（聊城职业技术学院，山东省聊城市，252000）

摘要：随着技术的不断发展，信息安全问题日益突出，对信息安全技术应用专业人才的需求也随之增长。作为一所培养技术技能型人才的高职院校，对信息安全技术应用专业的课程体系进行了深入探究并实践。本文将详细介绍我院在信息安全专业课程体系探究与实践过程中的一些经验，为其他同类职业院校提供借鉴和参考。

关键词：信息安全；课程体系；探究与实践

0 引言

随着技术的不断发展，信息安全已经成为当今社会的一大课题，涉及公民日常生活、企业运行和国家安全等方方面面。随着云计算、大数据、物联网、人工智能等技术的不断应用，信息安全面临的挑战也更加复杂。为了应对日益复杂的安全挑战，我们需要培养更多更高素质的技术技能型专业人才。信息安全技术应用专业是一个交叉学科，覆盖范围广，重在培养掌握信息安全基础理论、具备安全技术应用和系统安全运维能力，同时具有较高安全意识，遵守法律法规的高素质技术技能型人才。在当前环境背景下，我院对信息安全技术应用专业的课程体系构建进行了深入探究，以满足社会对人才的需求。

1 信息安全行业概述

1.1 信息安全行业现状

随着云计算、大数据、物联网、人工智能技术的发展普及，信息安全的重要性愈加突出。无论是防范病毒入侵、网络攻击、保护资产安全，还是确保系统运行稳定，都需要大量的专业人才。新技术的不断涌现，对信息安全提出了更高的要求。

1.2 人才需求分析

信息化程度越来越高，各行各业对信息安全的需求不断增长。无论是个人、单位、企业、机构都需要保障信息安全，防止个人隐私信息泄露、企业资产遭到破坏、网络攻击等事件的发生。因此，需要更多的信安专业人才。

在信息安全专业领域，需要从业者具备扎实的理论基础和较强的实践能力。例如交换机路由器配置、网络故障排除、防火墙配置、入侵监测、漏洞扫描与防护、web 安全防护、数据加解密、病毒入侵防范、程序设计、脚本编写、数据取证等。此外，从业者应熟悉相关法律法规，具备基本的职业素养、良好的团队协作精神和沟通能力。为了培养更多满足行业发展的专业人才，也为了更好地服务区域产业，我院在人才培养与专业建设方面不断探究与实践。

2 课程体系构建与实践

2.1 课程体系构建思路

课程体系构建整体思路如下：深入调研信息安全行业，走访多家具有代表性的知名企事业单位，根据应届生求职网、前程无忧、BOSS 直聘等多个求职网站的招聘信息，分析归纳总结调研数据，得出信息安全行业相关的典型工作岗位，并分析典型工作岗位所需要的专业能力。在此基础上结合高职院校的学情现状，构建了符合学生职业生涯发展规律的课程体系，包括有公共基础课、专业平台课、核心课、选修课共四部分，形成层次递进、内容互补的课程体系。对课程进行模块化设计，理论与实践相结合，完善实验实训环节，重在培养学生的动手操作能力和解决实际问题的能力。由于信安行业发展较快，在实施过程中，根据不断涌现的新技术、新标准、新要求，持续更新完善课程体系和课程内容，确保课程内容的实用性。

2.2 岗位能力分析

信息安全技术行业的典型工作岗位包括网络安全管理员、网络工程师、安全服务工程师、安全运维工程师、渗透测试工程师、资深安全顾问等。表 1 展示了其中 3 种典型工作岗位的能力要求。

2.3 课程体系构建

信息安全技术应用专业课程体系的构建综合考虑以上多方面因素，构建了满足学生职业发展和教育教学发展规律的课程体系，分为公共基础课、专业平台课、专业核心

课题名称：聊城职业技术学院科研项目重点课题《网络安全数字科技馆建设与实践研究》（编号：2021LZYR01）。

表 1 典型工作岗位及岗位能力分析

典型工作岗位	岗位能力要求
安全服务工程师	(1)良好的安全意识、较高的法律意识； (2)熟练掌握网络安全基础知识和专业技能，包括系统、应用安全等； (3)能够发现潜在风险并进行有效处理； (4)熟练掌握防火墙等设备的配置与调试，实现网络安全防护； (5)较高应急响应能力，熟悉应急响应流程，能快速响应并有效处理； (6)良好的团队协作和沟通能力
安全运维工程师	(1)良好的安全意识和法律意识； (2)扎实的网络基础知识； (3)良好的系统运维能力，包括网络设备、系统、数据库等； (4)具备良好的故障排查和问题解决能力； (5)能够对网络和系统日志进行深入分析，并及时处理问题
渗透测试工程师	(1)敏锐的安全意识，良好的职业素养； (2)熟练掌握渗透测试流程、方法，熟练使用主流渗透测试工具； (3)具备一定的编程和脚本编写能力，例如 Python、PHP 等； (4)良好的文档编写能力，能够编写渗透测试报告； (5)良好的团队协作和沟通能力； (6)独立思考、分析问题和解决问题的能力

课和选修课四部分，下面对其中三部分进行详细介绍。

(1)专业平台课

专业平台课主要是面向信息安全技术应用、云计算技术应用、密码技术应用、大数据技术等计算机类专业的具有相近技能的一些基础性课程，平台课内容相对基础，易于掌握，主要目的是引导帮助大一新生了解所学专业，激发学生的专业兴趣，打好专业基础，为后续其他课程的学习做好准备。具体来说，专业平台课包括信息技术基础、程序设计基础、信创技术应用等 6 门课程，以下是部分内容。

1)信息技术基础：计算机体系架构，软件与硬件，操作系统，文档处理，电子表格处理，演示文稿制作，信息检索，音频、视频、图像的处理和制作，信息安全与隐私保护，前沿技术云计算、大数据、人工智能等新概念。

2)程序设计基础：数据类型与表达式，结构化设计(顺序结构、分支结构、循环结构)，数组，函数，指针，字符串，结构体与公用体，文件，综合项目(学生成绩管理系统)。

3) 计算机网络基础：网络的形成、发展、组成、拓扑结构，数据通信技术，OSI 参考、TCP/IP 参考模型，局域网，广域网技术与 Internet，网络应用(DNS、WWW、FTP、远程桌面、邮件服务等)，网络故障分析与排除。

4)网络安全概论：安全基础，威胁与攻击，安全技术/管理，相关法律法规。

5)数据库技术应用：数据库系统安装，数据库基础应用，SQL 基础应用，SQL 添加、删除、更新数据，查询数据，使用 SQL 语言管理数据库对象。

6)信创技术应用：信创技术概述，信创基础设施，信创应用软件开发，信创系统安全与管理，信创技术应用实践。

(2)专业核心课

信息安全技术应用课程体系的专业核心课是该专业的必修课程，课程内容不断增多，难度逐渐加深。该课程主要目的是使学生扎实掌握信息安全的理论知识，同时重点培养学生动手解决实际问题的专业技能。该部分课程紧紧围绕典型工作岗位能力要求，突出信安专业的特点和方向，同时注重课程的实践性和应用性，结合行业标准和认证，融入信息安全新知识和新技术，帮助学生掌握专业核心知识和技能，提高学生的职业竞争力。表 2 列出了专业核心课程的主要内容。

(3)专业选修课

专业选修课是对核心课程的补充，在核心课程的基础

课程名称	专业核心课程主要内容
Python 程序设计	Python 语言基础，Python 语言标准库和扩展库，Python 编程实践，Python 面向对象编程，Python 文件操作和异常处理，Python 网络编程和多线程编程
PHP 后端基础	PHP 面向对象编程，PHP 与 Web 开发，PHP 性能优化，PHP 扩展开发，PHP 安全实践，PHP 项目实践
服务器配置与管理(Windows)	Windows 服务器的概念和特性，服务器硬件和网络环境搭建，服务器的安装和配置，活动目录和域控制器，DNS 服务器，DHCP 服务器，文件和打印服务器，Web 服务器和 FTP 服务器
路由与交换技术	网络基础知识，IP 基础，交换机的工作原理、功能和配置，以太网卡、以太网帧、以太网交换机、VLAN 虚拟局域网技术、链路技术、STP 生成树协议，路由器原理、功能和配置、RIP 路由信息协议、OSPF、ACL、NAT、PPP 与 PPPoE
漏洞扫描与防护	漏洞扫描技术，漏洞分析，漏洞利用与防护，漏洞扫描工具，漏洞修补与加固，模拟攻击与防御演练，网络安全法规与道德规范
网络渗透与安全运维	网络安全概述，网络渗透测试，常见网络攻击手段，入侵检测与防御，日志分析与事件响应，安全运维实践，法律法规与道德规范
网络安全技术应用	网络安全基本概念，加密技术与应用，网络防御技术，应用安全技术，移动安全技术，网络安全工具，网络安全法律法规与道德规范，综合实践项目

表 2 专业核心课程主要内容

上延伸和拓展，扩展了学生的知识储备，协助学生发掘自己的潜能和特长，满足学生的多样化发展需求。选修课程的内容与核心课程的内容层层递进、紧密衔接，构成了完善的课程体系。以下对重点几门选修课内容进行介绍。

1）Web 防御技术：Web 概述，HTTP 与 HTTPS，网络嗅探工具，漏洞检测工具，漏洞实验平台 DVWA，SQL/XSS/CSRF 漏洞分析，任意文件下载漏洞，文件包含漏洞，任意文件上传漏洞，暴力破解，命令注入。

2）Linux 服务配置与安全管理：网络连接应用与管理，服务管理系统 Systemd 的应用与管理，安全子系统 SELinux 的应用与管理，DNS、DHCP 等服务器的应用与管理，Linux 操作系统的加固与安全管理。

3）网络信息安全管理：防火墙网络安全管理与策略，入侵检测系统，数据加密和认证技术，网络攻击与防御，隐私保护与法律法规，实战演练与案例分析。

4）网络协议分析：网络协议基础，协议分析仪，网络抓包工具，常见网络协议 TCP/IP 协议族、HTTP 协议、FTP 协议、DNS 协议、SMTP 协议等，报文格式、交互流程、工作原理和性能特点，协议设计与优化。

信息安全技术应用专业课程体系的构建遵循了基础性、通用性、科学性、实践性、可持续发展等原则，确保学生能够学以致用、学有所成，能够在未来的职业生涯发展中有足够的竞争力。通过对专业平台、专业核心、专业选修课程递进式的学习，学生能具备良好的职业道德、职业素养、创新意识和工匠精神，同时扎实掌握信息安全技术领域核心知识、技术、技能和方法，提高自己动手实践能力，以及就业竞争力，为未来职业生涯发展奠定良好基础。

3 教学实施与教学评价

3.1 教学实施

教学过程中，注重理论与实践的结合，采用多种教学方法，如案例分析、项目驱动、理论与实操相结合，提高学生学习的主动性，从而提高课堂质量，保证学习效率和学习效果。从企业和技能大赛引入实际项目案例，结合专业人才培养方案、课程标准，选取合适的项目内容引入课堂，让学生在实际案例中加深理解理论知识，提高实际动手操作能力。注重培养学生的安全意识，在课程内容中，增加相应的法律法规内容，引入一些典型案例。专任教师应定期进行企业实践，参加培训和学习，确保教学内容的前沿性和实用性。

3.2 教学评价

教学评价是教学过程中的重要环节，通过教学评价，教师可实时地了解学生的学习状况，并根据结果有针对性地调整教学过程。通过采用多种评价相结合的方式：期末考试、项目报告、实践操作等，从多个维度评估教师的教学效果和学生的学习成果。重视过程性考核，除了期末考试评价，注重学生在学习过程中的表现，如平时作业、课堂表现、小组合作、实操训练等。建立完善的反馈机制，及时反馈评价结果，学生可实时了解自己对知识的掌握程度。实践教学环节中，企业参与评价，从行业角度给出指导性意见。根据反馈的结果，及时进行内容的更新与调整，满足不断变化的学习需求，从而提高人才培养和教学教学质量。

4 结语

本文通过对信安行业的现状分析，对信息安全技术应用专业的课程有了更深入的思考。构建满足学生职业生涯发展和教育教学规律的课程体系，并不断更新完善，希望能为高职院校信息安全技术应用专业课程体系的构建与实践提供有益的思路和参考。未来，信安课程体系和教学内容也将持续改进更新，以适应人才培养的新要求。

参考文献

[1]余姜德,梁本来,冷令.专业群建设背景下高职信息安全专业课程体系构建研究[J].现代职业教育,2022(05):97-99.

[2]蔡东蛟.信息安全技术应用专业课程体系构建探讨[J].中国多媒体与网络教学学报(中旬刊),2021(09):173-175.

[3]杨鹏.新时期信息安全技术应用专业课程体系构建研究[J].陕西教育(高教),2023(08):44-46.

[4]韩武光.高职信息安全技术专业课程体系建设与实践[J].网络空间安全,2023,14(2):80-86.

[5]宋星月."双高"背景下信息安全专业群建设研究[J].甘肃科技,2022,38(05):51-54.

[6]马延奇,王俊飞.从专业到专业群：高职院校专业群建设的产业需求逻辑[J].中国职业技术教育,2021(8):11-15.

[7]唐成华,汪华登,王晶等.高校网络与信息安全专业群建设研究[J].实验科学与技术,2020(5):53-57.

[8]齐攀,庄越,陈玉琪等.高职信息技术专业群创 新性人才培养的新路径[J].中国职业技术教育,2020(32),69-73.