

# 网络视域下高校安全管理探究

李海伦

河北师范大学, 河北 石家庄 050024

DOI:10.61369/EDTR.2025120007

**摘要：** 随着信息技术的发展, 网络安全问题逐渐显现, 在高校这种信息密集型、技术高度依赖的视域下, 网络安全教育管理就显得尤为重要。本研究从网络视域下的高校安全管理入手, 分析当前高校安全管理存在的问题, 探究问题背后的具体原因。在此基础上, 从管理核心要素出发, 提出提高高校网络安全教育管理策略, 以期所高校安全管理提供理论依据和实践指导, 真正实现网络视域下的安全管理目的。

**关键词：** 高校管理; 网络安全; 安全教育; 管理策略; 信息技术

## An Exploration of Security Education Management in Higher Education Institutions in the Context of Networked Learning

Li Hailun

Hebei Normal University, Shijiazhuang, Hebei 050024

**Abstract:** With the advancement of information technology, cybersecurity issues have gradually become apparent. In the context of universities, which are information-intensive and highly reliant on technology, cybersecurity education and management have become particularly crucial. This study begins with the analysis of cybersecurity education and management in universities from a network perspective, examines the existing problems in current university cybersecurity education and management, and explores the specific reasons behind these issues. Based on this foundation, it proposes strategies to improve university cybersecurity education and management, with the aim of providing theoretical support and practical guidance for university cybersecurity education and management, ultimately achieving the goal of cybersecurity management within the context of the network.

**Keywords:** university management; cybersecurity; security education; management strategies; information technology

在数字化时代背景下, 信息网络的普及在促进社会发展、教育改革的同时也产生一些新问题。高校是人才培养、科技创新的主阵地, 高校网络环境的安全关系到教学、科研和师生的日常生活。由于网络技术的发展, 高校网络安全管理工作复杂程度不断提高, 传统的网络安全教育和管理方法已难以解决新的安全威胁。为提高高校安全管理水平, 需对目前存在的问题进行深入分析, 寻求新的管理模式、教育策略。本研究通过对现有的管理体系不足之处进行分析, 提出切实可行的管理策略, 促进高校安全管理创新与发展。

### 一、网络视域下高校安全管理面临的问题

#### (一) 高校网络信息环境呈现多样化特征

伴随着信息技术的迅猛发展, 大数据、云计算、人工智能等技术不断普及, 网络环境的复杂性不断加剧。高校是信息密集型单位, 往往隐藏着不少网络安全隐患, 部分高校网络信息系统的规模大、结构复杂, 传统的防护方式已经难以有效应对复杂的网络攻击, 间接引发数据泄露、病毒入侵、恶意软件等问题, 而高校在网络信息安全方面的防护措施相对落后, 无法真正做到全方位防护<sup>[1]</sup>。在网络犯罪手段不断升级的情况下, 现有的网络防护

技术已难以适应日益复杂的网络信息。高校网络安全的管理和防护措施必须跟上时代的发展, 来应对这些不断变化的潜在威胁。

#### (二) 高校师生网络安全意识仍有提升空间

网络安全问题开始显现, 但部分高校师生的网络安全意识普遍不高, 一些师生在使用网络时没有对潜在的网络安全风险采取科学有效的防范, 甚至在思想存在一定侥幸心理, 对于网络安全问题的重视度不足。高校师生时常出现不重视密码管理、随意下载不明软件、忽视个人隐私保护等行为, 这些行为不但会导致个人信息泄露, 甚至会给校园网络造成隐患。虽然部分高校已经开展了一定安全教育活动, 但从整体防护效果来看, 依然没有达到

既定要求，教师和学生的防护行为和理念存在偏差。

### （三）高校安全管理体制与技术支撑有待完善

大部分高校都已经投入到了网络安全工作上，但不可否认依然有小部分高校的安全管理体制、技术手段存在缺陷，部分高校网络安全管理体制不健全，大部分网络防护设施陈旧，难以有效应对现代网络安全威胁。尤其是对老旧的信息管理系统来说，其防护能力不能满足快速发展的网络安全要求，造成网络安全事件频发。除此之外，很多高校的网络安全管理责任划分不清，没有专门的管理部门，网络安全工作只依靠信息中心或者保卫部门的常规管理，缺少全校范围内的综合协调和高效统筹。

### （四）高校安全教育与日常管理协同程度不足

网络安全教育与日常管理工作脱离，已成为高校普遍存在的问题之一，纵观我国不少高校的网络安全教育，均停留在理论层面，缺少系统的培训与实践活动，教师和学生对于网络安全防护的相关知识并不完善，难以落实到日常的学习和生活中<sup>[2]</sup>。此外，网络安全教育与校园日常管理缺乏紧密对接，不能形成全面、深入的管理模式，造成安全教育的效果不能落实。部分高校的网络安全管理缺乏延续性，安全教育的内容与形式难以满足师生的实际需求，部分教师对于安全教育管理的重视程度不足，无形中影响到日常的行为，进而间接反映到安全教育管理中。日常管理工作中缺少网络安全教育的支持，不能通过持续性活动来提高师生的安全意识。如何将网络安全教育同日常管理有机结合，形成贯穿全程的教育和管理机制，成为有效提升高校网络安全管理的思路。

## 二、网络视域下高校安全教育管理的关键要素

### （一）组织管理结构的完善与优化

高校要建立跨部门的协作机制，保证信息的共享和交流通畅。教务处、网络中心、保卫处等涉及网络安全的各部门要定期召开协调会议，及时解决安全管理中出现的问题。明确安全责任的划分，使各个部门各司其职、互相配合，提高整体的安全防护水平。另外学校应设立专门的网络安全管理部门，保证网络安全管理有专门的负责人和全职工作人员，责任明确、目标清晰，形成合力，共同推进校园网络安全工作。

### （二）安全教育的系统性与长期性

网络安全教育不能停留在应急响应的短期阶段，应逐步形成系统化的教育体系，高校可制订出长期的网络信息安全教育规划，将网络信息安全教育融合到各种课程体系中，实现新生入学到毕业的全程教育。网络安全教育不能只停留在课堂教学中，还应采用实践性教学、模拟演练等形式来提高师生实际操作的能力，保证安全防范措施得以执行。学校应定期对安全教育内容进行更新，使它跟得上网络技术的发展，保证教育体系始终处于前沿，保证每一位师生都掌握最新的安全知识和技能。

### （三）技术支持与管理手段的结合

高校要充分利用已有的网络安全技术，将技术手段同管理措施结合起来，通过入侵检测系统、数据加密技术、网络防火墙等

先进的技术手段加强网络安全防护，使技术手段与日常管理互相配合<sup>[3]</sup>。定期开展安全审计、漏洞扫描并预测、监控潜在风险，会使校园网络安全水平得到很大的提高。学校应建立完善的网络安全事件响应机制，保证安全事件发生时可迅速采取措施，及时止损，减少不必要的损失。依靠技术和管理的完美融合来保证网络安全管理的全面性和高效性。

### （四）师生的参与度与安全文化建设

提高师生的参与度是提高网络安全管理水平的重要保证，高校应通过举办网络安全宣传活动、讲座、培训等方式提高师生的网络安全意识。同时还要重视校园安全文化创建，促使师生在日常学习、工作中自觉担负起安全责任，创建起全员参与、全程覆盖的网络安全管理方式。通过组织网络安全知识竞赛、专题讲座、模拟应急演练等各种安全文化活动，提高师生对网络安全的重视程度，促使师生养成良好的网络安全行为习惯，真正做到“人人有责，人人参与”。

## 三、提升网络视域下高校安全教育管理的策略

### （一）加强网络安全技术和防护体系的建设

随着信息技术的发展，高校网络安全隐患日趋显现，为解决上述问题，首先要加强高校网络安全基础设施建设，加大校园网络防护系统投入，构建全方位的网络安全防护体系。从具体实施角度分析，高校可充分利用安全技术，即入侵检测与防御系统（IDS/IPS）、数据加密技术、身份认证机制等来提高整个网络的安全性<sup>[4]</sup>。学校应定期对信息系统进行扫描、审计，发现并修复安全漏洞。可同第三方安全公司合作定期开展渗透测试和红蓝对抗演练，模拟网络攻击的情形，找到并消除高校的隐患。上述措施可有效提高网络系统防护能力，保证校园网络稳定、安全。

除技术手段外，高校还需加强网络安全管理制度建设，制定完善有关管理政策、操作规范，使技术手段和管理措施互相配合。学校可设立专门的网络安全管理机构，统一管理全校的网络安全工作，按照不同网络应用场景制定差异化的管理方案。网络安全责任要落实到每个部门和岗位，形成闭环管理模式，避免出现漏洞。另外，学校要定期开展网络安全教育与培训，对信息系统维护人员、教师、管理人员开展网络安全意识及应急处理能力的培训，定期安全演练和技术提升可提高对于复杂的网络攻击的应对能力。

### （二）提高师生网络安全意识并强化日常管理

提高师生网络安全意识是高校网络安全管理取得成功的关键内容，高校应通过多种措施提高师生对网络安全问题的关注度，调动师生参与网络安全管理的积极性。高校可借助校园网、电子邮件、微信公众号等途径定时公布网络安全知识及最新网络安全信息，使师生掌握常见的网络安全威胁（勒索病毒、钓鱼邮件、数据泄露等）和防护方法<sup>[5]</sup>。安全提示和知识普及工作可提高师生在网络日常使用中的警觉性，降低网络安全事件发生的概率。尤其在网络信息高速发展的当下，教师和学生必须警惕信息安全，充分学习网络安全知识，了解相关风险，在日常学习和生活中学以致用。

在此基础上,学校应举办专题讲座、网络安全周、知识竞赛等活动来提高师生的网络安全意识与技能。高校可邀请网络安全专家讲解网络安全案例,分析典型的网络安全事件来提高师生对网络安全的认识和重视。此外,学校还可根据不同师生群体设计网络安全课程与培训。对新生进行基础的网络安全知识普及,对教师和科研人员重点讲解科研数据保护、学术不端问题。依靠针对性的教育内容来提高师生的网络安全素养,使师生在生活和工作中自觉遵守网络安全规范,最大限度避免网络攻击、数据泄露等。

### (三) 完善高校安全管理体制与技术手段的对接

高校网络安全管理体制的完善,是提高高校网络安全教育和管理效果的关键前提,高校应设立网络安全管理机构,明确该机构的职责和责任,保证网络安全工作有专人负责。管理机构可由信息中心、保卫处、教务处等单位的代表组成,定期召开会议就网络安全有关事务进行商议,协调各个部门的网络安全管理工作。另外该机构还需要对各个部门的安全责任予以明确,定期开展网络安全管理政策及措施的落实情况检查,保证责任落实到位,保证全校网络安全工作步调一致。

此外,高校应加强技术手段的应用,使技术与管理深度融合。学校可引进大数据分析技术、人工智能辅助监控技术、智能入侵检测系统等先进的网络安全技术,提高校园网络的实时监控能力。此外,学校应将技术手段与管理流程结合起来,利用技术手段对校园网络的安全状况进行实时监控,及时发现异常行为并加以处理。系统发现某个设备或用户行为异常时,可自动发出警报并采取措<sup>[6]</sup>。运用智能化技术提升校园网络的安全性,给师生营造更加安全的网络环境。不仅如此,学校应持续加强对网络安全数据的管理,结合完善的数据防泄露机制来保证师生个人信息和科研数据的安全。在数据存储和传输时可采用加密技术,避免没有权限的人获取数据。学校应定期开展数据安全审计工作,保证数据保护措施的有效性和完整性。学校要健全安全事件应急

响应机制,一旦发生安全事件可立即启动应急响应程序,迅速处置网络安全事件,减少损失。管理者应制定一套行之有效的应急响应预案,系统整理可落实到应急措施,并通过校内各类平台发放,让教师和学生了解到网络安全事件的危害,在日常的学习和生活中加以防范,将网络安全防护措施落到实处。

### (四) 增强安全教育与日常管理工作的协同效应

提高网络安全管理效果要依靠安全教育和日常管理互相配合,保证教育和管理互相配合,形成教育合力。学校应将网络安全教育与日常工作相结合,在日常管理中渗透安全教育。学校新生入学时可开展安全教育培训、发放安全手册等手段,使新生掌握校园网络使用规定及安全防范措施。学校在日常管理中应定期对各个部门、学院的网络安全状况进行检查,发现问题及时处理。学校应在学校内设置安全检查点,即图书馆、宿舍楼等人流流量较大的地方,定期进行网络安全检查,保证网络安全措施的落实。

在此基础上,学校还需创建全员参与的网络安全文化,形成强有力的安全文化氛围。为调动师生参与网络安全的积极性,学校可制定激励政策,评选网络安全优秀个人和团队,用奖励的形式来激励师生积极参与网络安全工作。学校应加强同外部网络安全机构之间合作,定期开展网络安全技术交流与合作研究,共享安全信息,全面提高师生的网络安全责任感,校园网络安全水平随之提升。

## 四、结语

在网络视域下,高校安全管理的问题逐渐显现,但通过管理体制、科学的教育方法、技术手段和全员参与,可全面提高高校网络安全管理水平。通过对相关问题的剖析,本研究为高校网络安全教育管理提供行之有效的解决措施,为创建更安全、稳定的网络环境提供实践样本。

## 参考文献

- [1] 郭少军,郑凤.“三全育人”视域下高校网络安全教育体系建设研究[J].大学,2025(16):4-7.
- [2] 胡皓月.“大思政”视域下大学生网络素养现状分析与提升对策[J].教书育人(高教论坛),2024(21):61-67.
- [3] 姜晓甜.网络思政育人视域下高校意识形态安全教育现状[J].中文科技期刊数据库(全文版)教育科学,2022(11):3.
- [4] 吕洋.浅谈基于大数据环境下高校网络空间安全防护策略——以白城师范学院为例[J].科学大众:科技创新,2020.
- [5] 李兆亮.人工智能技术在校园安全风险治理中的创新实践与融合应用研究[J].信息与电脑,2025,37(10):28-30.
- [6] 尹能民.“互联网+”背景下高职院校加强公共安全教育的策略分析[J].品位·经典,2024(1):103-106.