信息安全与网络技术在高校中的应用探究

唐 超

（广州科技职业技术大学，广东 广州 510450）

摘要：在信息时代下，高校成为了信息传播和知识共享的中心枢纽，信息安全愈加重要。高校在学术研究、学生信息管理等方面广泛应用信息技术，信息安全问题日益凸显。基于此，本文针对信息安全与网络技术在高校中的应用展开研究，分析了信息安全与网络技术在高校中的应用重要性，阐述了信息安全与网络技术在高校中的应用原则，提出了具体的应用策略，旨在为高校制定应对复杂局面战略提供参考，促进高校的健康发展。

关键词：信息安全；网络技术；高校；应用探究

随着信息技术的飞速发展，高校作为知识传播与创新的重要场所，其信息化建设日益成为提升教育质量和管理效率的关键因素。然而，信息技术的应用也带来了诸多安全隐患，如数据泄露、网络攻击等，对高校的正常运行和师生的信息安全构成了严重威胁。因此，信息安全与网络技术在高校中的应用显得尤为重要。本文旨在探讨信息安全与网络技术在高校中的应用现状、原则及策略，以期为高校的信息安全管理和网络技术应用提供有益的参考。

一、信息安全与网络技术在高校中的应用重要性

在信息化时代背景下，信息安全与网络技术在高校中的应用显得尤为重要，不仅关乎学校的日常运营，更直接影响到教学、科研及管理的方方面面，表现在以下方面：

（一）有利于提高学校科研环境安全性

信息安全技术的有效应用，为高校的科研环境提供了坚实的保障，确保了科研数据的机密性与完整性。在科研过程中，大量的数据和信息需要被存储、传输和处理，而这些数据往往涉及学校的核心机密和研究成果，包括为发表的研究成果、与企业合作项目中的技术机密等。如缺乏对数据的有效保护，可能会造成信息泄露与丢失，对社会利益、学术诚信等产生不良影响。通过采用先进的信息安全技术，如数据加密、访问控制等，可以确保科研数据在传输和存储过程中的安全性，防止数据泄露或被恶意篡改，从而保护学校的科研成果和知识产权。比如采取主动防御技术能够有效检测网络流量，发展与组织潜在威胁，保障科研活动的稳定性。

（二）有利于推动学校教育管理智能化

网络技术为高校教育管理提供了全新的手段和工具。在现代技术支持下，高校教学管理主要依托信息系统进行，包括学生信息管理系统、考试管理系统等，这些系统中存在着大量的学生数据，包括学生学习资料、学生学习成绩等，若出现数据泄露，可能会影响整体的教学秩序和教育公平性。通过对信息安全和网络技术的应用，能够保障上述管理系统的安全性，减少不良影响，推动学校构建出安全、智能化的教育管理平台，进而实现对学生信息、教学资源、课程安排等方面的全面管理，提高管理效率和质量。网络技术可以为师生提供便捷的在线学习、交流和协作环境，促进教育资源的共享和优化配置。这些功能的实现，都离不开网络安全技术的支持，只有确保网络环境的稳定性和安全性，才能保障教育管理平台的正常运行和数据的准确性。

（三）有利于保障学校各项工作开展

信息安全与网络技术的应用，对于保障学校各项工作的顺利开展具有至关重要的作用。无论是教学、科研还是管理，都需要依赖稳定、安全的网络环境。通过加强网络安全管理，学校可以及时发现并处理潜在的网络威胁，确保网络环境的稳定性和安全性。例如通过应用强密码、双因素认证等方式，降低非法访问风向问题；通过检测用户行为，及时发展异常操作，避免数据非法修改等问题。此外，信息安全技术的应用能够为学校提供数据备份和恢复服务，防止因数据丢失或损坏而导致的工作中断，为学校的各项工作提供了有力的技术保障。信息安全和网络技术的应用，能够促使高校教学管理工作更加安全可靠地开展，有助于提升学生整体管理效率，为高等教育健康发展提供有效支持。

二、信息安全与网络技术在高校中的应用原则

高校亟需推进信息完全与网络技术的应用，但在实际应用应遵循一系列原则，以切实发挥技术的应用价值，主要体现在以下方面：

（一）全面性原则

全面性原则强调对学生信息、教育管理信息等所有关键数据的全面管理。这意味着高校需要建立一个覆盖全校范围的信息安全管理体系，确保从数据的收集、存储、处理到传输的每一个环节都得到有效的保护。该原则要求高校不仅要关注单个信息系统或网络的安全，还要从整体上考虑整个信息生态系统的安全性，确保所有信息资产都得到妥善管理。

（二）自适应原则

自适应原则强调网络安全措施的自适应性。随着网络技术的不断发展和网络威胁的不断演变，高校需要确保其网络安全措施能够灵活应对各种新的挑战，定期评估其网络安全策略的有效性，并根据最新的威胁情报和技术发展进行必要的调整。该原则要求高校具备一种动态、灵活的安全管理思维，能够迅速适应不断变化的网络环境。

（三）平衡性原则

平衡性原则关注可访问性和安全性之间的平衡。在保障信息安全的同时，高校还需要确保师生能够便捷地访问和使用各种信息系统和资源，在安全性和易用性之间找到一个合理的平衡点，既要防止未经授权的访问和数据泄露，又要确保师生能够高效地使用信息系统进行学习和工作。该原则要求高校在设计和实施信息安全措施时，充分考虑用户的需求和体验，确保安全措施既有效又实用。

三、信息安全与网络技术在高校中的应用策略

（一）完善网络技术治理框架，制定信息安全管理策略

在应用信息安全与网络技术过程中，高校应制定出全面的信息安全策略，以有效保护敏感数据，促进高校学术发展，维护高校教学管理秩序。首先，搭建网络技术治理框架。高校应构建出全面系统的网络技术治理框架，涵盖网络基础设施的规划、建设、运营、维护以及安全防护等多个方面，明确出各级管理部门的职

责和权限，确保网络技术的规范化和标准化管理；注重技术创新和持续改进，以适应不断变化的网络环境与技术发展趋势。在制定框架过程中，高校应注重确保网络架构的合理性，保证网络的高可用性和可扩展性；合理选择网络设备配置，选用安全可靠、性能稳定的设备，并合理配置以优化网络性能；建立网络安全防护体系，引进防火墙、入侵检测系统、安全审计系统等，以有效防范网络攻击和数据泄露等风险。其次，制定安全管理策略。信息安全策略是保障高校信息安全的关键。高校应结合自深深灰机情况，制定出全面、切实可行的管理策略，覆盖信息资产分类、保护级别制定、访问控制等内容，确保数据的有效保护。比如注重识别与评估信息资产，明确出那些信息时重要的或者敏感的，针对不同类别采取个性化保护措施；实施访问控制机制，采取身份认证、权限管理等手段，确保只有合法用户才能访问敏感信息；制定数据备份与恢复计划，确保数据在丢失或损坏时能够迅速恢复；建立应急响应机制的建立，包括应急预案的制定、演练和持续改进，以应对可能发生的网络安全事件。通过上述措施，高校能够强化对潜在威胁的防御，减少不良危害的侵蚀，有效提升信息安全防护能力，为师生提供安全、稳定的网络环境。

（二）强化安全审计评估工作，定期筛查网络威胁问题

为强化信息安全与网络技术的应用，高校应开展安全审计评估工作，筛查网络威胁问题，及时发现并消除潜在的安全隐患，确保网络环境的安全稳定。首先，进行安全审计评估。安全审计评估是检验高校网络安全措施有效性的重要手段。高校应建立健全的安全审计机制，定期对网络系统进行全面的审计评估，包括对网络架构、安全策略、系统配置、用户权限、数据保护等多个方面的审查。通过审计，高校可以发现安全配置不当、权限管理混乱、数据泄露风险等问题，为后续的整改工作提供依据。在此过程中，高校可与第三方安全评估机构建立合作，由第三方评估机构进行网络安全状况评估。第三方机构有着丰富的安全经验和专业知识，能够发现高校自身难以察觉的安全漏洞和隐患，为高校提供更具针对性的安全建议和改进措施。其次，设置常态化定期筛查机制。网络威胁是不断变化的，高校应建立常态化的网络威胁筛查机制，包括定期对网络流量、系统日志、安全事件等进行分析，发现异常行为和潜在威胁。高校应密切关注网络安全领域的最新动态和威胁情报，及时调整和完善安全策略，比如针对新出现的网络攻击手段或漏洞，应迅速采取相应的防护措施，确保网络安全防护的及时性和有效性。在筛查工作中，高校能够及时发展并阻断恶意攻击、病毒传播、数据泄露等安全事件，确保网络环境的稳定和安全。最后，制定安全事件处理和应急预案。在实际应用中，高校应对可能发展的安全事件制定相应的应急预案，针对不同情况设置针对性应急处理措施。高校可建立相应的安全事件处理机制，建设专门的管理团队，针对网络入侵、恶意软件感染等事件进行技术处理，采取措施消除安全隐患，制定详细实施方案，以减少损失，保护网络安全。

（三）促进软硬件技术更新优化，保障信息技术安全管理

随着科学技术的不断发展，网络威胁技术不断复杂，高校应紧跟技术潮流，不断促进软硬件技术的更新优化，以确保信息技术安全管理的持续有效。就目前而言，高校常用的信息安全和网络技术包括以下内容：一是防火墙和 IDS（入侵检测系统）。防火墙作为网络安全的第一道防线，通过制定严格的访问控制策略，有效阻止未经授权的访问和数据泄露。IDS 能够实时监测网络流量，及时发现并报告潜在的入侵行为，为高校提供实时的安全预警和响应能力。二是安全 WiFi 网络。通过采用 WPA3 等最新的无线安全标准，结合 MAC 地址过滤、访客网络隔离等技术，高校可以确保无线网络的安全性和稳定性，为师生提供便捷的无线接入体验。三是 SSL/TLS。通过部署 SSL/TLS 证书，高校可以确保敏感数据（如用户密码、交易信息等）在传输过程中的安全性和完整性，有效防止数据被窃取或篡改。根据上述软件系统，学校应加强对软硬件技术的更新与优化，主要采取以下措施：一是定期评估与更新。高校应定期对现有的软硬件系统进行评估，根据评估结果及时更新或升级系统，以确保其安全性和稳定性；对已过期的安全补丁或软件版本，应尽快进行更新，以避免潜在的安全漏洞。二是引进新技术。高校应积极引入新技术以提升网络安全防护能力，例如采用 AI 和机器学习技术来增强入侵检测系统的准确性和效率；利用区块链技术来确保数据的不可篡改性和透明度；采用安全管理软件和硬件设备监测和防御各种网络威胁，采用虚拟技术对网络进行隔离与保护。三是加强相关培训。高校应加强师生对信息安全的认识和培训，面向师生采取安全培训、模拟演练等手段，切实提升师生的安全意识和应急处理能力，确保他们在面对网络安全威胁时能够迅速作出正确的反应。同时，注重组建一支具有网络安全专业知识和管理经验的网络管理团队，通过专业知识培训，不断提高管理人员的网络防护能力和处理能力，保障网络安全运行。通过上述措施的实施，学校能够不断提升自身的网络安全防护能力，为师生提供安全、可靠的信息化服务。

四、结语

综上所述，信息安全与网络技术在高校中的应用，对提升学校科研环境的安全性、推动教育管理智能化以及保障学校各项工作的顺利开展具有不可替代的作用。在实际应用中，高校应采取相应的策略，通过完善网络技术治理框架，强化安全审计评估工作，促进软硬件技术的更新优化等，有效应对信息安全挑战，保障师生的信息安全和学校的正常运行。随着信息技术的不断激怒，高校应强化对信息安全和网络技术应用的挽救，为自身健康发展提供有力支撑。

参考文献：

[1] 吴曼，谭淑琴，李明，等 . “政产学研金服用”协同视域下高校数字图书馆信息共享服务探究 [J]. 中国高校科技，2023(11)：70-74.

[2] 冯艳，赵子建，梁华伟，等 . 数字技术赋能智慧体育校园建设的行动路径研究 [C]// 中国体育科学学会 . 第十三届全国体育科学大会论文摘要集——专题报告（学校体育分会）. 郑州大学；河南理工大学；，2023：3.

[3] 郑小辉，郭金涛 . 云计算环境下网络信息安全技术发展分析 [J]. 数字通信世界，2024（08）：119-121.

[4] 唐鹏，冯德万，杨应志 . 新时代高校样板支部对标“七个有力”的建设逻辑——以中共重庆安全技术职业学院网络与信息安全系党支部为例 [J]. 办公室业务，2023（13）：72-76.

[5] 董敏 . 计算机信息安全技术在高校校园网络中的应用 [J]. 数字通信世界，2023（12）：138-140.

[6] 尉冀超，白媛慧，马越 . 基于物联网技术的智能电网网络信息安全分析 [C]// 中国电力设备管理协会 . 全国绿色数智电力设备技术创新成果展示会论文集（二）. 国网宁夏电力有限公司石嘴山供电公司；，2024：3.