高校数字校园网络信息安全保障体系建设

文◆西北师范大学网络安全与信息化办公室　马　威

引言

随着科技的快速发展，高校网络环境变得越来越复杂，敏感数据量的激增使网络安全问题尤为突出。高校数字校园网络信息安全保障不仅关系到个人隐私和学术诚信的保护，还涉及教育资源的安全使用和管理。高校作为知识和创新的重要源泉，应保障其网络系统的完整性、可靠性和安全性。然而，面对越来越多样化的网络威胁，如黑客入侵、木马病毒等网络攻击行为，对数字化校园网络的安全造成了较大的影响，传统的网络安全措施已经难以满足需求。因此，探索计算机信息安全技术在高校网络安全中的应用变得尤为重要，如防火墙技术、数据加密技术、入侵检测系统以及定期安全漏洞评估等。除此之外，随着大数据、云计算和人工智能等现代技术的应用，高校网络安全面临的挑战也在不断演变，要求高校校园网络管理在维护网络安全的同时，应不断提高水平和升级计算机信息技术的应用。

1 数字校园网络信息安全概述

1.1 数字校园网络

数字校园网络是以高度发达的计算机网络为核心技术，将信息和知识资源进行共享的新型教育、学习方式和研究环境。数字校园网络强调合作、分享和传承的精神，并通过网络化、数字化和智能化的有机结合，为学习者提供适应其个性化成长和发展需求的学习环境以及自主选择多种媒体组合的学习资源。为了实现这一目标，校园网建设应考虑基础设施建设、网上管理、教学软件开发和有关人员培训 4 项内容。

1.2 信息安全

信息安全主要是保障网络中存储的信息不被泄露或损坏，避免网络数据在实际操作过程中受到外界的恶意软件攻击，避免造成网络信息资料泄露、丢失或破坏。数字化网络主要应用在网络服务器上，保证服务器和网络系统的稳定性，确保网络系统中的信息具有真实性和完整性，简单来讲就是对数字化网络的软件和硬件进行保护，保障操作和存储安全[1]。

1.3 高校数字校园网络信息安全的意义

在校园中合理利用数字化网络，能够有效提升学校的整体形象，维护学校利益。由于学校每年有大量的学生入学，学校需要收集学生信息，并存储在校园网络系统中，故应确保高校数字校园网络系统的安全性，充分保障学生的相关数据不被泄露和丢失。同时，学校积累的大量教学数据以及办公室应用软件等各类信息都将存储在校园网络中，有效促进高校未来的发展。例如，高校根据相关的数据积累提供相应的教学方案，有利于丰富学校的教学内容。

2 高校数字校园网络信息安全存在的问题

2.1 用户安全意识薄弱

由于计算机技术和网络信息安全的复杂性，用户在日常使用中缺乏安全认识和技术理解，构成了潜在的威胁，导致用户的个人信息（如身份证号、手机号码、学号和工号等）和涉密内容被发布到网络上。一旦被恶意用户利用，将会给个人甚至组织带来严重的安全风险。首先，在信息发布方面，未对发布的内容进行严格把关，无意间公开了敏感信息，使自己陷入被攻击的风险中。尤其在当前的大数据时代，一旦信息

【作者简介】马威（1980—），男，甘肃酒泉人，本科，工程师，从事计算机网络安全运维及软件开发工作。

进入网络，几乎无法完全清除[2]。其次，在使用计算机时，由于对系统程序的不理解或错误操作，导致误删重要的系统文件。例如，一些用户在遇到计算机问题时，采取极端的方法如格式化硬盘，不仅导致大量重要数据丢失，还会引发更严重的系统问题。最后，在应用系统程序的安装和更新方面，存在着诸多安全风险。用户在下载和安装新的应用程序时，忽视对应用程序的安全性检查。例如，用户从非官方或者不安全的来源下载软件，使计算机暴露于各种恶意软件和病毒的攻击之下。

2.2 网络安全防护措施不完善

数字校园的发展离不开网络安全防护措施地完善和升级。现阶段，高校网络信息安全防护措施仍存在一些不足之处，主要表现在以下方面。第一，安全管理制度落实不到位。大多数高校在进行网络信息安全管理时，虽然制定了相关制度和规定，但在实际操作中并没有真正落实到位。第二，缺乏科学的信息技术保障。数字校园的发展需要应用先进的信息技术手段，但当前许多高校在进行网络信息安全建设时，由于技术力量薄弱、资金投入不足，存在网络信息安全技术手段落后、系统功能不完善等问题。而且，在实际应用过程中，部分高校对信息技术保障不够重视，导致许多设备无法发挥其应有的作用。第三，缺乏足够的人力和物力保障。高校在进行网络信息安全建设时，没有配备专门的安全维护人员进行定期维护和管理，导致设备设施被损坏或者受到病毒侵害后无法及时发现并得到妥善修复和处理[3]。

2.3 网络安全管理体系不完善

现如今，高校对信息网络质量的要求越来越高，网络安全管理的工作量持续加大，任务持续增多。适逢院校改革，网络管理人员流动性较大，网络新技术、新平台、新手段不断更新迭代，对于网络管理人员的要求越来越高。然而，高效数字校园网络安全管理体系仍然不完善。一方面，高校对硬件系统的安全管理，没有消除硬件层面的隐患。例如，硬件设备兼容性差、性能不足、售后服务保障不到位。局限于顶层规划和资金等原因，硬件系统更新比较缓慢，无法满足未来信息化智能化建设需求。另一方面，由于软件本身存在安全漏洞，导致软件系统存在安全隐患。对于不同网络信息系统，存储在数据库中的隐私和敏感信息，没有对于不同身份人员设置严格的访问权限。同时，高校业务众多，各个业务单位都有各自的业务系统，经常出现网络安全管理工作开展不到位的现象，故无法形成统一的网络安全管理体系。

2.4 数字校园网络设备维护能力不足

网络设备在使用过程中存在较多安全隐患，应及时进行维护与更新。目前，高校网络设备主要有服务器、交换机、路由器、防火墙、无线接入点等，由不同的供应商生产制造，且不同厂家产品的技术水平参差不齐，难以保障所有设备的安全性和稳定性[4]。在这种情况下，高校应投入大量人力和物力对设备进行维护和更新，这就导致其资金投入与维护成本增加。同时，高校网络设备种类繁多、数量庞大，高校管理和维护工作大多采用人工管理、分散式管理和集中式管理等方式，因此，不仅增加了高校网络信息安全工作的难度，还造成了人力资源浪费。

3 高校数字校园网络信息安全保障体系建设措施

3.1 完善网络安全规章制度，建立网络安全责任管理体系

高校信息化建设工作必须实现与网络安全建设工作的协调一致，共同发展，积极建立并不断完善网络安全规章制度，确保网络安全工作有章可循。具体规章制度地制定可以参照网络安全法的相关内容，并结合高校信息网络的实际运行情况，制定与实际发展相符的管理制度，确保各部门能够科学地推进信息化建设工作，应用规范化的信息系统。另外，在数字化建设工作中，应建立网络安全责任管理体系，实行网络系统的责任制，即岗位有专人负责，对岗位相关人员进行专业知识和技能水平培训，及时更新岗位人员的专业知识，与现代数字技术的发展保持同步，并制定相应的考核制度和责任制度，在提高岗位工作人员责任心的同时，提高岗位工作效率[5]。

3.2 严格执行网络安全等级保护制度，实现信息系统安全防护

在高校数字化建设中，应用信息系统作为重要的资产组成，不仅要满足信息系统的功能以及性能的需求，还要增加其安全性和可靠性。高校内部服务器的所有应用信息系统，应由专业技术人员设置防火墙，并开展对外服务内容，对于没有在校内服务中中的系统，严禁其对外开放；对于没有信息系统负责人的应用系统，应严禁对外开展上网服务，从根本上确保网络安全性。此外，高校中的所有信息应用系统，必须严格遵守网络安全等级保护制度，所有的信息应用系统必须进

行备案、复评等，不断提高应用系统在应用方面的安全性和可靠性，推动高校数字化建设工作有序开展。

3.3 优化防火墙设置

防火墙是计算机的第一道屏障，因此，必须具有良好的性能，检测扫描各种问题和病毒，有效保护网络信息安全。首先，优化防火墙设置是进行信息保护的第一步。在日常生活中，学校和政府的办公部门或老师专用的计算机会连接公用的内网，为了方便各种信息资源的共享和传播，不仅需要对内网进行保护，还需要对外网给予同样的重视。内网和外网的作用不同，在管理中应将内网和外网分隔开。由于不法分子利用互联网的漏洞，如果外网和内网没有明确的界定，那么将会通过外网漏洞进入内网，造成数据丢失。在此情形下，为了防止网络信息泄露，应充分体现防火墙的重要性。其中，优化防火墙设置对网络信息保护具有重要作用。因此，对防火墙进行科学、合理设置，优化防火墙结构，有利于防止各种病毒地攻击[6]。

3.4 应用病毒防范技术

高校将大量数据存储到校园网络数据库中，在管理过程中应加大安全管理力度，提升网络系统的安全系数，避免校园网络中的庞大数据受到病毒入侵。目前，计算机网络中的黑客、木马、病毒种类繁多，随着技术的进步病毒也在不断地升级。病毒入侵校园网络后，会对校园网络造成严重影响，导致校园网络中的信息丢失损毁，甚至破坏计算机系统致使无法正常运行。另外，病毒预防和查杀在计算机网络安全中发挥重要作用。高校网络系统在进行安全管理过程中采用的技术手段不断进步。例如，购买和安装正版杀毒软件、定期全盘安全扫描、实时更新病毒数据库信息以及设置安全防火墙，实现对校园网络的安全管理。针对访问非法网站或者不正规的网站下载数据时，应限制非法访问，对下载不合理的信息资源时应实现自动屏蔽，实现对校园网络安全管理的有效防范。

3.5 数据加密安全技术

在校园网络中，数据加密安全技术是防御黑客攻击的主要手段。目前，在校园网络中，加密安全技术主要分为传输加密技术和存储加密技术两种。传输加密技术主要使用的方式有链路加密、节点加密和端到端加密。利用 OSI 参考模型各层次，控制对加密方式的选取，选取合适的加密方式有效实现传输数据的安全，阻止信息数据受到攻击。存储加密技术是针对计算机硬盘中存储的数据信息进行加密的方式，能够确保即使黑客入侵盗取了数据，也会因为没有正确的解密方式，黑客无法获取真实的数据信息。

3.6 加强校园网络信息数据安全规范管理

在高校数字校园环境下，应加强对数据安全的规范管理，不仅能够提高学校的管理效率，还能够充分保证网络信息安全。首先，高校应从多个方面入手，对网络设备、系统软件和系统平台等进行管理。其次，高校应制订网络信息安全应急预案，在出现突发事件时能够及时、有效地处理问题。再次，应对用户进行严格管理，对用户的使用权限进行严格限制。如果用户出现违规操作，那么会面临严重惩罚。最后，高校应定期开展安全培训活动，增强师生的安全意识。

结语

在数字化时代的教育环境中，高校计算机网络信息安全问题引起了广泛关注。对于高校而言，做好计算机网络信息安全防护具有重要意义，不仅直接影响教学和科研的正常进行，还关系到师生的个人信息安全。因此，持续关注和改进网络安全防护措施是推进高校数字化建设的重要保障。只有这样，才能在全面推进数字化教学和科研的同时，保障高校数字校园网络环境的安全性和可靠性。

引用

[1] 宁顺政.探究高校网络信息安全与防护策略[J].中国新通信,2022,24(19):113-115.

[2] 王涛,赵耀军.高校网络信息安全防护管理的策略探讨[J].无线互联科技,2023,20(3):142-145.

[3] 张旭鹏,魏建兵.高校学生网络信息安全意识提升的四维路径[J].信息与电脑(理论版),2023,35(17):208-210.

[4] 李江灵.数字经济时代高校网络信息安全防护研究[J].互联网周刊,2023(24):71-73.

[5] 朱斌勇.大数据环境下高校校园网络信息安全隐患与防护措施[J].网络安全技术与应用,2024(3):76-78.

[6] 郭倩,张桦,何岚岚.高校数字校园网络信息安全保障体系建设[J].数字技术与应用,2022,40(3):224-227.