大数据背景下高校网络信息安全防护策略研究

唐 超

（广州科技职业技术大学，广东 广州 510450）

摘要：随着信息技术的快速发展和广泛应用，高校的网络环境变得日益复杂。大数据背景下，高校网络信息安全面临着前所未有的挑战，严重影响了高校的教学、科研以及管理工作的正常开展。基于此，本文探讨了大数据时代下高校网络信息安全防护的有效策略，旨在通过技术手段与管理措施的结合，构建更加安全、可靠的高校网络环境，为师生提供更好的信息服务和支持。

关键词：大数据；高校；网络安全防护

一、高校网络信息安全防护面临的问题

（一）网络防护技术落后

在大数据时代，当前高校网络系统普遍采用的是传统的防火墙、入侵检测系统等安全措施，这些技术在一定程度上能够抵御一些常见的网络攻击，但面对日益复杂和隐蔽的新型威胁，其效果显得捉襟见肘。随着黑客技术的不断进步，攻击手段也更加多样化和智能化，传统的安全防护技术难以及时发现和应对这些高级威胁。此外，高校网络通常拥有大量的终端设备和用户，包括教职员工、学生、访客等，这些设备和用户的行为模式各不相同，增加了网络管理的难度。传统的安全防护技术通常难以适应这种高度动态的网络环境，就这导致高校在面对日益严峻的网络安全形势时无法实时监控和响应各种安全事件。

（二）数据隐私保护不足

随着信息技术的迅速发展，高校的教育、科研、管理等多方面均高度依赖网络系统，这使得大量敏感信息存储于网络平台之上，这些信息的存储和传输过程中的安全问题成为高校网络信息安全防护中的一大难题。一方面，高校在数据收集、存储、使用等环节缺乏统一的标准和规范，导致数据隐私保护存在诸多漏洞。不同部门之间的数据共享机制不健全，数据权限管理不严格，使得敏感信息在内部流通过程中容易被泄露。另一方面，高校在数据隐私保护方面的法律法规意识较为薄弱，缺乏相应的法律保障。尽管国家出台了一系列关于个人信息保护的法律法规，但部分高校在实际操作中未能严格遵守。部分高校对数据隐私保护的重视程度不够，缺乏专门的法律团队进行指导和监督，导致在数据处理过程中存在诸多法律风险。

（三）网络安全管理工作落实不到位

一方面，网络环境的开放性与共享性，虽然促进了信息交流与资源共享，但同时也增加了网络安全隐患，使得安全防护难度显著提升。高校内部网络安全管理制度不够健全，部分高校对网络安全重视程度不足，缺乏明确的网络安全管理政策和操作流程，导致网络安全防护措施难以有效落实。另一方面，高校内部网络设备更新换代周期长，许多老旧设备存在安全漏洞，但因资金投入不足，设备更新不及时，导致网络安全防护能力长期处于较低水平。此外，网络安全防护设备的配置与管理不合理，安全策略设置不当，导致安全防护效果大打折扣。

二、大数据背景下高校网络信息安全防护策略

（一）建立完善的网络入侵检测屏障

现代网络入侵检测技术不仅依赖于传统的签名匹配方法，更加强调行为分析和异常检测。例如，基于机器学习的入侵检测系统能够通过分析网络流量模式，自动识别出异常行为，从而提高检测的准确性和效率。该系统能够学习网络中的正常流量特征，一旦发现偏离正常模式的行为，即可触发警报，提醒管理员采取相应措施。某高校在网络中心就部署了一套基于机器学习的入侵检测系统，成功拦截了多次来自外部的 DDoS 攻击，保护了校园网络的稳定运行。此外，高校还应建立多层次的入侵检测屏障。在校园网的边界，可以部署防火墙和入侵防御系统（IPS），对进出流量进行实时监控和过滤，防止恶意流量进入内部网络。在内部网络中，通过部署主机入侵检测系统（HIDS），对关键服务器和终端设备进行监控，及时发现并阻止内部威胁。为了确保入侵检测系统的有效运行，高校还需建立健全的安全管理机制，注重对系统的更新和维护，确保入侵检测系统能够识别最新的威胁。同时，加强安全审计，对入侵检测系统生成的日志进行分析，及时发现潜在的安全隐患。例如，某高校通过建立安全审计团队，定期对入侵检测日志进行审查，发现并修复了多个潜在的安全漏洞，进一步增强了网络的安全性。如此，通过采用先进的入侵检测技术、建立多层次的防护体系以及健全安全管理机制，高校可以显著提升网络的安全防护能力，为师生提供一个安全、稳定的学习和工作环境。

（二）针对信息数据安全防护制定统一标准

在大数据背景下，高校网络信息数据的多样化和复杂化要求我们必须建立一套统一的信息数据安全防护标准，以确保数据的完整性、可用性和保密性。这就需要高校对现有数据进行分类分级，对数据的采集、存储、传输和使用等环节进行全面规范，以确保每个环节都符合安全要求。

其一，高校需要根据数据的重要性和敏感度，将其分为不同的等级，如公开数据、内部数据和机密数据等。针对不同等级的数据，制定相应的访问权限和操作规范，确保数据的安全。例如，对于公开数据，可以设置较低的访问权限，方便师生查询；对于

机密数据，则需要设置严格的访问权限，仅限特定人员访问，并记录访问日志，以便追踪和审计。其二，高校应建立统一的数据采集标准，明确数据来源的合法性，确保数据的真实性和可靠性。例如，通过签订数据采集协议，明确数据提供方的责任和义务，确保数据来源合法。其三，高校应建立统一的数据存储标准，确保数据的安全存储。例如，高校可以利用加密技术对敏感数据进行加密存储，防止数据泄露。同时，建立健全数据备份和恢复机制，定期对数据进行备份，并在数据丢失或损坏时能够快速恢复，确保数据的连续性和完整性。其四，高校应建立统一的数据传输标准，确保数据在传输过程中的安全。例如，采用安全传输协议（如 HTTPS、TLS 等），对数据进行加密传输，防止数据在传输过程中被截获或篡改。同时，建立数据传输监控机制，对数据传输过程进行实时监控，及时发现并处理异常情况，确保数据传输的安全性。其五，高校应建立统一的数据使用标准，确保数据在使用过程中的安全。例如，完善数据使用记录制度，记录数据的使用情况，便于追踪和审计。

（三）提升技术操作人员专业素质和安全意识

在大数据时代，高校网络信息安全不仅依赖于先进的技术设备，还与技术操作人员的专业素质和安全意识密切相关。技术操作人员是高校网络安全防护的第一道防线，他们的专业技能和安全意识直接决定了网络安全防护措施的有效性。因此，提升技术操作人员的专业素质和安全意识成为了高校网络信息安全防护中不可或缺的一环。

技术操作人员的专业素质提升，可以通过定期组织培训来实现。例如，北京某高校与网络安全公司合作，定期为技术操作人员举办网络安全知识讲座和技术交流会，帮助技术操作人员及时了解网络安全领域的最新动态，通过经验分享，提升团队整体的应急响应能力。此外，该高校还通过模拟真实网络攻击场景，组织技术操作人员进行实战演练，以提高他们在面对真实网络威胁时的应对能力。除了专业技能的提升，安全意识的培养同样重要。高校可以开展网络安全教育活动，提高技术操作人员对网络安全重要性的认识。上海某高校在这方面做出了积极探索，该校制作了网络安全宣传手册，内容包括常见的网络安全威胁、预防措施等，分发给技术操作人员，帮助他们树立正确的网络安全观念。提升技术操作人员的专业素质和安全意识，还需要建立有效的激励机制。高校可以将网络安全工作纳入绩效考核体系，对于表现突出的技术操作人员给予物质和精神上的奖励，以此激发他们的工作热情和责任感。同时，对于因疏忽大意导致网络安全事故的技术操作人员，应给予相应的惩罚，以此警示全体人员，提高整体的安全意识。由此，提升技术操作人员的专业素质和安全意识需要高校从培训、教育、激励等多个方面入手，构建一个全面的提升体系。这不仅有助于提高高校网络信息安全防护水平，还能够促进技术操作人员个人能力的发展，为高校网络安全建设提供坚实的人才保障。

（四）健全网络信息安全防护建设

1. 加强机房的安全建设

加强机房的安全建设，可以有效防止物理层面的安全威胁。机房作为存储和处理数据的核心场所，其安全性直接关系到整个网络系统的稳定运行。因此，高校应定期对机房进行安全检查，确保环境温度、湿度等条件符合标准，防止因环境因素导致设备故障。同时，机房的物理安全防护措施也需得到重视，如安装监控摄像头、门禁系统等，确保只有授权人员才能进入机房，防止非法入侵。例如，某高校在机房安全管理方面，采用了先进的门禁系统和 24 小时监控，有效保障了机房的安全。

2. 完善校园网络建设

校园网络是高校教学、科研和管理的重要支撑，其安全性和稳定性直接影响到师生的工作和学习。高校应定期对网络设备进行维护和升级，确保网络的高效运行。同时，校园网络的拓扑结构也需合理规划，避免因网络设计不合理导致的安全漏洞。例如，某高校在校园网络建设中，采用了多层次的网络架构，通过划分不同的网络区域，实现了对不同用户群体的精细化管理，提高了网络的安全性。

3. 建立安全事件应急响应机制

高校应制定完善的安全事件应急预案，明确各环节的责任和流程，确保在安全事件发生时能够迅速响应，减少损失。同时，高校还应积极组织安全演练，提高师生的安全意识和应急处理能力。例如，上海某高校成立了安全事件应急响应小组，该小组由网络安全专家、IT 技术人员和管理人员组成，负责处理校园内的各类安全事件。2019 年，该高校发生了一起黑客攻击事件，应急响应小组迅速启动应急预案，通过技术手段迅速定位攻击源，及时切断了攻击路径，成功阻止了攻击的进一步蔓延，确保了校园网络的安全。

三、结束语

总之，本文对当前高校网络信息安全防护现状进行了深入分析，指出当前高校网络信息安全存在的主要问题，如网络防护技术落后、数据隐私保护不足、网络安全管理措施落实不到位等，并以此提出了建立完善的网络入侵检测屏障、针对信息数据制定统一标准、提升技术操作人员专业素质和安全意识、健全网络信息安全防护建设等策略，对提升高校网络信息安全水平具有重要意义，有助于推动网络信息安全领域的整体进步。

参考文献：

[1] 马航航 . 高校校园网网络安全态势感知建设方案 [J]. 甘肃科技，2020（17）：10-12.

[2] 张泽 . 高校计算机网络信息安全及防护对策 [J]. 信息系统工程，2023（6）：76-79.