高职院校智慧校园网络信息安全管理研究

王大萌[1]　王　欢[2]
（1. 黑龙江省网络空间研究中心，黑龙江 哈尔滨 150000；
2. 黑龙江建筑职业技术学院，黑龙江 哈尔滨 150000）

摘要：随着信息化进程的不断推进，高职院校智慧校园建设已成为教育现代化的必然选择，为学校管理与教学带来了极大的便利和提升。然而，在智慧校园建设的过程中，网络信息安全问题愈发凸显，成为制约高职院校发展的重要因素之一。本文旨在对高职院校智慧校园网络信息安全管理现状进行深入分析，并提出相应的管理体系构建策略，以期为高职院校网络信息安全管理提供有效的参考与指导。在信息化时代，保障高职院校网络信息安全，不仅关乎学校的稳定运行和师生的合法权益，更是对教育事业可持续发展的重要保障，因此，我们迫切需要加强对智慧校园网络信息安全管理的研究与实践。

关键词：高职院校；智慧校园；网络信息安全管理

一、高职院校智慧校园网络信息安全管理现状分析

（一）信息安全建设顶层设计不完善

在高职院校智慧校园建设中，信息安全往往被视为附属品而非核心要素，导致信息安全建设在顶层设计上缺乏系统性、整体性和前瞻性。这种设计缺陷表现为：首先，信息安全规划未能与智慧校园整体规划同步进行，信息安全建设往往滞后于智慧校园其他项目的实施，难以形成有效的安全防护体系。其次，信息安全建设缺乏统一的标准和规范，不同系统、不同平台之间的安全防护措施难以兼容，形成信息孤岛，降低了整体安全防护效果。最后，顶层设计中缺乏对新技术、新应用的安全风险评估机制，导致新技术、新应用在推广使用过程中可能带来未知的安全隐患。

（二）信息安全制度建设不健全

信息安全制度是保障智慧校园网络安全的重要基石，然而目前高职院校在信息安全制度建设方面存在明显不足。首先，信息安全责任体系不明确，缺乏具体的安全责任划分和追究机制，导致在发生安全事件时难以迅速定位问题、追究责任。其次，信息安全管理制度不完善，缺乏针对智慧校园特点的安全管理制度和操作规范，使得日常安全管理工作难以有效开展。再次，信息安全培训和教育机制缺失，师生员工的信息安全意识薄弱，缺乏基本的安全防范知识和技能，容易成为网络攻击的目标。最后，信息安全应急处置机制不健全，缺乏科学有效的应急预案和演练机制，无法在发生安全事件时迅速响应、有效处置，降低了智慧校园的安全防护能力。

（三）硬件设施和软件风险

在智慧校园的建设中，硬件设施是信息传输和存储的基础，而软件则是实现信息处理和智能管理的关键。然而，目前高职院校在硬件设施和软件系统方面普遍存在着较大的风险。一方面，部分高职院校在智慧校园建设初期，由于缺乏长远规划，导致硬件设施配置不足，无法满足日益增长的数据处理需求。这不仅影响了校园网络的运行效率，也为信息安全埋下了隐患。另一方面，软件系统的设计和开发往往缺乏足够的安全考虑，容易受到外部攻击和内部滥用。例如，一些高职院校的教务管理系统、学生信息管理系统等关键软件，由于缺乏有效的安全防护措施，经常发生数据泄露、系统瘫痪等安全事故。

（四）师生信息安全防范意识差

高职院校师生作为智慧校园的主要用户群体，其信息安全防范意识的高低直接关系到校园网络的安全稳定。然而，目前高职院校师生的信息安全防范意识普遍较为薄弱。一方面，由于缺乏系统的信息安全教育，部分师生对网络安全风险缺乏足够的认识，容易在不经意间泄露个人信息或敏感数据。例如，在使用公共无线网络时，不加密传输敏感信息，或在社交媒体上随意发布个人照片和行踪等。另一方面，部分师生对网络安全防护技能掌握不足，无法有效应对网络攻击和诈骗行为。例如，在面对钓鱼邮件、恶意软件等网络威胁时，往往缺乏辨别和应对的能力，容易上当受骗。

二、高职院校智慧校园网络信息安全管理体系构建策略

（一）建立信息安全管理制度

在高职院校智慧校园的建设中，网络信息安全无疑是重中之重。面对日益复杂的网络环境和不断更新的信息安全威胁，建立一套科学、高效、实用的信息安全管理制度显得尤为重要。这不仅是为了保障校园网络的正常运行和数据安全，更是为了维护学校的教学秩序和师生的个人权益。

首先，要明确信息安全管理的目标与原则。高职院校的信息安全管理工作应以保障教育教学的正常开展为核心目标，确保校园网络的安全稳定。在具体实践中，应遵循预防为主、综合治理的原则，通过技术手段和管理措施相结合，构建起多层次的安全防护体系。例如，可以设定明确的安全管理目标，如实现零安全事故、确保师生个人信息不泄露等，并制定相应的安全管理原则，如最小权限原则、数据备份原则等，为具体的安全管理工作提供指导。其次，要完善信息安全管理的组织架构和职责分工。高职院校应成立专门的信息安全管理机构，明确各部门的职责和协作机制。例如，可以设立信息安全管理中心，负责全面规划、组织、协调和监督校园网络的安全管理工作。同时，各教学单位、行政部门和技术支持部门也应明确自身在信息安全工作中的职责，形成齐抓共管的良好局面。通过完善组织架构和职责分工，可以确保信息安全管理工作的高效运行。最后，要制定具体的信息安全管理制度和操作规程。这些制度和规程应涵盖网络安全、数据安全、应用安全等各个方面，如网络访问控制制度、数据备份恢复制度、安全事件应急处理规程等。这些制度和规程的制定应充分考虑高职院校的实际情况和需求，确保既符合法律法规的要求，又具有可操作性。同时，还应定期对制度和规程进行审查和更新，以适应不断变化的网络安全环境。

（二）及时更新软硬件设施

随着信息技术的飞速发展，高职院校智慧校园的建设日新月异，网络信息安全所面临的挑战也日益严峻。在这个背景下，及时更新软硬件设施成为了维护智慧校园网络信息安全不可或缺的一环。而及时更新软硬件设施的重要性，这是构建高效信息安全管理体系的关键所在。

首先，及时更新硬件设施是保障网络信息安全的基础。高职院校的网络硬件设施，如服务器、路由器、交换机等，是支撑智慧校园正常运行的基石。这些设备一旦老化或出现故障，不仅会影响网络的稳定性和速度，还可能成为安全漏洞的源头。因此，

我们必须密切关注硬件设施的运行状态，及时发现并更换老化或损坏的设备。例如，当发现服务器性能下降，影响到了校园内各个应用系统的正常运行时，我们应迅速评估并采购性能更强大的新服务器，确保校园网络的稳定运行和数据安全。其次，软件系统的更新同样至关重要。软件系统是高职院校智慧校园网络信息安全的核心组成部分，包括操作系统、数据库、防火墙等。随着软件技术的发展和网络安全威胁的不断演变，软件系统也需要不断更新以应对新的安全挑战。我们应定期评估现有软件系统的安全性和稳定性，及时安装最新的安全补丁和升级版本。例如，当发现校园内使用的防火墙软件存在已知的安全漏洞时，我们应迅速采取行动，下载并安装官方发布的安全补丁，以弥补安全漏洞，防止潜在的网络攻击。最后，软硬件设施的更新需要与学校的发展规划相协调。高职院校在更新软硬件设施时，不能盲目追求最新技术或高端设备，而应根据学校的发展需求和财务状况进行合理规划。我们应与学校的其他部门密切沟通，了解他们的需求和意见，确保更新的软硬件设施能够满足学校整体发展的需求。同时，我们还应关注软硬件设施的生命周期和成本效益，选择性价比高的产品，为学校节约资金并避免资源浪费。

（三）充分利用计算机信息安全技术

随着信息技术的飞速发展，高职院校智慧校园的建设日益深入，网络信息安全问题也日益凸显。作为高职院校信息安全管理负责人，我深知在构建智慧校园网络信息安全管理体系时，必须充分利用计算机信息安全技术，以确保校园网络的稳定运行和数据安全。

首先，要充分利用防火墙技术。防火墙是网络安全的第一道防线，它能够有效隔离内外网络，阻止未经授权的访问。我们在构建智慧校园网络时，要精心设计和配置防火墙，确保它能够识别并过滤掉恶意访问和攻击。例如，我们可以采用状态监测防火墙，它不仅能够检查数据包的来源和目的地址，还能分析数据包的内容，从而更加精准地识别出潜在的威胁。其次，要利用入侵检测与防御系统（IDS/IPS）。入侵检测系统能够实时监控网络流量，发现异常行为并及时报警，而入侵防御系统则能够在检测到攻击时主动采取措施，阻止攻击行为。我们在高职院校智慧校园中部署 IDS/IPS，可以实现对网络攻击的快速响应和有效防御。比如，当检测到某个 IP 地址在短时间内发出大量异常请求时，IDS/IPS 可以立即切断该 IP 地址的访问权限，从而避免潜在的危害。最后，要充分利用数据加密技术。数据加密是保护数据在传输和存储过程中不被窃取或篡改的重要手段。在智慧校园中，我们要对敏感数据进行加密处理，确保即使数据在传输过程中被截获，也无法获得其真实内容。例如，我们可以采用 AES 或 RSA 等加密算法，对师生的个人信息、成绩数据等重要信息进行加密存储和传输，从而有效保护数据的安全。

（四）设计应用系统接入申请表

在构建高职院校智慧校园网络信息安全管理体系的过程中，应用系统接入是至关重要的一环。为了确保校园网络的安全稳定，防止未经授权或存在安全隐患的应用系统接入网络，设计一份科学、合理、严谨的应用系统接入申请表显得尤为重要。

首先，这份申请表应包含基本的应用系统信息。例如，申请接入的应用系统名称、版本号、开发商信息、预计接入时间、预计服务范围等。这些信息有助于安全管理团队对申请接入的应用系统进行初步了解，为后续的安全评估提供基础数据。其次，安全性能评估是申请表的核心部分。在这一部分，需要详细列出应用系统的安全特性，如是否具备数据加密传输功能、是否有完善的用户身份认证机制、是否存在已知的安全漏洞等。此外，还应要求申请方提供应用系统的安全测试报告或相关认证，以确保其满足校园网络的安全标准。再次，申请表还应涉及应用系统的维护与管理计划。这包括应用系统的日常运维流程、应急预案、定期更新计划等。这些计划的详细程度和执行情况，将直接影响应用系统在接入后的稳定性和安全性。最后，申请表应包含申请方的承诺与法律责任声明。申请方需明确承诺遵守校园网络信息安全管理的相关规定，对因应用系统问题导致的网络安全事件承担相应的法律责任。这一部分的设置，旨在强化申请方的安全意识和责任感，确保其在应用系统的开发、运营、维护过程中始终将安全放在首位。

（五）全面提升师生信息安全意识

信息安全不仅仅是技术层面的问题，更是关乎每一个校园成员的行为习惯与意识素养。因此，我们需要通过一系列的策略和活动，全面提升师生的信息安全意识。

首先，开展信息安全教育培训。通过定期组织信息安全培训课程，向师生普及网络安全知识，包括密码安全、防范网络诈骗、保护个人信息等。例如，可以邀请信息安全专家来校进行讲座，用生动的案例和深入浅出的语言，让师生们认识到网络安全的重要性。同时，也可以制作信息安全教育视频或手册，方便师生随时随地学习。其次，举办信息安全实践活动。理论知识的学习是必要的，但实践操作同样重要。可以组织师生参与网络安全攻防演练，模拟真实的网络攻击场景，让师生们亲身体验到信息安全的紧迫性。最后，加强信息安全监管。提升师生信息安全意识不仅需要教育和引导，还需要有效的监管。学校可以建立信息安全监管机制，对师生的网络行为进行监控和管理。对于违反信息安全规定的行为，应及时进行纠正和处理，以儆效尤。同时，还应建立信息安全事件应急处理机制，一旦发生信息安全事件，能够迅速响应、有效处置。

三、结语

智慧校园建设是高职院校迈向现代化、信息化的必由之路，而网络信息安全则是其发展过程中不可或缺的重要环节。通过对高职院校智慧校园网络信息安全管理现状的深入分析，我们发现了诸多存在的问题与挑战。然而，面对挑战，我们不应束手待毙，而是应该积极探索有效的解决途径。本文提出的管理体系构建策略，旨在强化高职院校网络信息安全管理，提升师生的信息安全意识，从而确保智慧校园建设的顺利推进和高效运行。相信随着这些策略的落实与完善，高职院校的网络信息安全管理将迎来新的里程碑，为教育事业的持续发展注入更强劲的动力。

参考文献：

[1] 李晨燕 . 高职院校智慧校园网络信息安全管理分析 [J]. 产业与科技论坛，2021，20（12）：274-275.

[2] 张双喜 . 基于高职院校智慧校园网络与信息安全的探讨 [J]. 内蒙古煤炭经济，2020（09）：211-212.

[3] 陈庆惠，王秀芳 . 浅谈高职院校智慧校园网络与信息安全管理 [J]. 网络安全技术与应用，2019（01）：72+79.

[4] 钟玲 . 高职院校校园网络信息安全的防护与管理 [J]. 电子技术与软件工程，2018（14）：197.

本文系中国校园健康行动 . 教育教学研究成果项目：《校园网络安全管理问题及对策研究研究（编号：EDU0586）》阶段性成果