 DOI: https://doi.org/10.12345/bdai.v7i3.38174

Research on Security Risk Assessment and Prevention Strategies for University Data Center Server Rooms

Tianzi Gu

Hubei Engineering University, Xiaogan, Hubei, 432000, China

Abstract

With the rapid development of information technology, university data center computer rooms have become crucial infrastructure for ensuring teaching, research, and management informatization. These facilities face various security risks, including physical security, network security, power safety, and environmental safety, which impact the efficiency of university information operations. This study conducts an in-depth analysis of the security risks in university data center computer rooms, evaluates potential risk sources, and proposes corresponding prevention and control strategies. The research demonstrates that mitigating security risks in university data center computer rooms requires a multi-dimensional approach, involving enhanced physical security measures, improved network security defenses, optimized power safety management, and intensified environmental monitoring. These measures aim to minimize safety hazards and ensure stable data center operations. This study provides both theoretical foundations and practical guidance for the security management of university data center computer rooms.

Keywords

university data center; server room security; risk assessment; prevention and control strategies; information security

高校数据中心机房安全风险评估与防控策略研究

谷田子

湖北工程学院，中国·湖北 孝感 432000

摘　要

随着信息技术的迅速发展，高校数据中心机房成为保障教学、科研和管理信息化的重要基础设施。数据中心机房面临着各种安全风险，包括物理安全、网络安全、电力安全和环境安全等，影响着高校的信息作效率。本文通过对高校数据中心机房的安全风险进行深入分析，评估其潜在风险源，提出相应的防控策略。研究表明，高校数据中心机房的安全风险防控需要从多维度入手，通过加强物理设施的安全防护、提升网络安全防范能力、优化电力安全管理、加强环境监测等措施，最大限度降低安全隐患，保障数据中心的稳定运行。本研究为高校数据中心机房的安全管理提供了理论依据与实践指导。

关键词

高校数据中心；机房安全；风险评估；防控策略；信息安全

1 引言

随着信息化建设的不断推进，高校数据中心机房作为信息技术的核心基础设施之一，其重要性日益突出。数据中心机房承载着大量关键数据和信息系统，是保障高校教学、科研、行政管理等各项工作的基础平台。然而，随着信息技术的发展，数据中心机房面临的安全威胁也日益严峻。物理安全、网络安全、电力安全、环境安全等多个方面的安全隐患若得不到有效防控，可能会造成数据丢失、服务中断、设备损坏等严重后果，影响高校的正常运作。因此，对高校数据中心机房的安全风险进行评估，并根据评估结果制定科学合理的防控策略，已成为高校信息化建设中的重要课题。本文将从数据中心机房的安全风险评估出发，分析当前存在的主要安全隐患，并结合实际情况，提出切实可行的防控策略，以期为高校数据中心的安全管理提供理论依据和实践指导。

【作者简介】谷田子（1996–），女，中国河南南阳人，硕士，从事人工智能研究。

2 数据中心机房安全风险分析

2.1 物理安全风险

数据中心机房的物理安全是保障其正常运作的基础。物理安全风险主要包括：未经授权的人员进入、设备遭遇自然灾害（如火灾、洪水、地震等）、设备失窃或破坏等。这些风险直接威胁到数据中心的基础设施与设备的完整性和安全性。为了降低物理安全风险，数据中心需要加强人员管理与监控，完善设备设施，采取有效的防火、防水、防盗等措施。

2.2 网络安全风险

网络安全是数据中心机房面临的另一大挑战。随着网

络攻击手段的不断升级，数据中心机房的网络安全风险愈发严峻。常见的网络安全威胁包括黑客攻击、病毒感染、数据泄露、拒绝服务攻击等。这些威胁不仅可能导致数据中心系统瘫痪，甚至可能导致数据泄露和重要信息的丢失。为了有效应对这些风险，数据中心必须强化网络安全措施，包括加强防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）等的建设，同时加强员工的网络安全意识教育，定期进行安全漏洞检测与修补。

2.3 电力安全风险

数据中心机房的电力安全直接关系到关键设备的持续运行，其风险主要源于电力供应中断、电力设备故障以及电磁干扰等多重因素。电力中断不仅会造成服务器停机，还可能引发数据损坏、系统崩溃，给业务连续性带来严重影响。为降低风险，数据中心需构建高可靠性的电力保障体系，通过配置 UPS 不间断电源、备用发电机及双路供电系统等措施实现电力冗余，确保在主电源失效时仍能维持稳定供电。此外，电力设备的日常巡检与周期性维护至关重要，包括对配电柜、变压器、蓄电池组及线路的运行状态进行监测，及时排查老化、过载或接触不良等隐患。电力系统的电磁干扰也需加以控制，可通过屏蔽、接地和合理布局来降低对精密设备的影响。通过完善的技术手段与管理措施，可显著提升数据中心电力系统的安全性与可靠性。

3 高校数据中心机房安全防控策略

3.1 完善物理安全防控措施

高校数据中心机房的物理安全管理是整体安全体系的基础，其核心在于通过科学的管理制度和硬件防护手段最大限度降低外部侵害与环境因素带来的安全威胁。人员出入控制是物理安全的首要环节，通过门禁系统、生物识别技术、全天候监控与巡查制度，可有效保障机房区域的封闭性和管理的可追溯性。在设施建设方面，应选用耐火材料、设置自动灭火系统和防水结构，使机房具备应对突发火灾、水患等环境风险的能力。同时，对机柜、供配电设备等关键设施进行牢固加固，可提升其在地震、振动或意外冲击中的稳定性。定期的设施检测与安全评估也十分必要，通过持续监测环境状态与结构安全状况，使潜在风险得到及时处置。完善的物理安全防控体系能够为数据中心的安全运行提供可靠屏障，保障设施在长期运维中的完整性与可靠性。

3.2 加强网络安全防护

网络安全是数据中心机房运行中最具复杂性和持续性挑战的安全领域，其威胁既来源于外部攻击，也可能源于系统漏洞与人员误操作。构建稳固的安全防护体系需依托多层级安全技术，通过防火墙、入侵检测系统和入侵防御系统形成多维度网络隔离与实时监测机制，使异常访问与恶意流量能够被及时识别和阻断。数据在传输与存储过程中面临泄露与篡改风险，加密技术的应用可在协议层与应用层提供双重保护，使敏感信息在跨设备、跨网络流动时保持高度安全性。定期漏洞扫描、安全审计与渗透测试有助于发现系统中的薄弱环节，并通过补丁更新与配置优化消除隐藏风险。同时，网络安全治理还依赖组织层面的文化建设，通过定期培训、案例分析与安全制度宣贯，使技术人员和管理人员形成稳定的安全意识，从而减少人为因素导致的安全隐患。多方协同作用可确保数据中心机房在复杂网络环境中保持稳健运行。

3.3 优化电力安全管理

电力系统是支撑数据中心持续运行的关键基础，其稳定性直接影响计算与存储设备的可靠度。为构建高可靠电力保障体系，应在制度、技术与监测三方面进行系统化管理。通过制定电力运行规范与维护计划，可确保电力设备在生命周期内维持良好状态。备用电源系统是电力安全的重要组成部分，UPS 与应急发电机能够在主电源中断时迅速切换供电，避免设备因断电而造成数据损坏或系统停机。同时，电力线路、配电柜、变压器及储能电池等关键部件需定期检测，关注老化程度、负载情况及连接稳定性，以减少潜在故障发生的可能。电力监控系统能够实现实时数据采集与状态分析，使电压波动、温升异常等问题得到及时预警，有助于提前采取措施，避免扩大为系统性故障。通过完善的电力管理策略，可为数据中心的稳定运维提供坚实保障，使各类业务在高负载条件下仍能保持连续与可靠。

4 数据中心机房环境安全风险与防控策略

4.1 温湿度控制

温湿度控制是维持数据中心机房环境稳定的重要环节，其作用不仅关系到设备运行的可靠性，也影响能源利用效率与运维成本。电子设备在温湿度波动环境中容易出现性能下降、部件老化或短路氧化等问题，因此必须依托精确监测与动态调节实现环境稳定。现代机房普遍采用智能监控系统，通过传感器实时采集各区域温湿度数据，并依据负载变化自动调节制冷模式，以保障设备在适宜条件下运行。为提升散热效果，可结合冷热通道分离、机柜封闭等技术减少热点生成，提高冷量利用率。空调系统的维护同样关键，需要定期清洁滤网、检查制冷剂与运行状态，确保持续高效运转。在温度高企或负载增加的阶段，应启动应急预案，通过冗余制冷设备或临时散热措施确保关键业务不中断，从而提升机房整体运行的安全性与稳定性。

4.2 火灾防控

火灾是数据中心最具破坏性的环境威胁之一，其隐患可能来自线路老化、设备过载、静电积聚及外部因素。火灾不仅会导致设备损毁，还可能造成数据丢失与业务中断，因此需构建高度严格的防控体系。机房建设应采用阻燃材料并科学规划电缆敷设，使绝缘、防燃与散热性能符合要求。技术层面的火灾预警与灭火设备至关重要，烟雾探测器、空气采样系统及自动灭火装置能够在火灾初期迅速识别异常，

通过联动机制关闭电源、释放灭火介质或发出警报，将风险控制在最小范围。为确保系统长期可靠运行，应实行定期巡检，对探测器灵敏度、联动系统和灭火装置压力等进行校验。人员培训同样不可忽视，通过演练与案例学习提升应急判断与处置能力，使数据中心具备更强的火灾防控与自我保护能力。

4.3 水灾防控

水灾对数据中心具有突发性强、扩散迅速和破坏难以修复的特点，其风险既可能由内部管线渗漏引起，也可能源于自然灾害或外部基础设施故障。为确保机房安全，需要构建系统化的水灾防控体系。在设计阶段，应综合评估地势、排水能力与防水结构，通过架空地板、防水门和密封墙体等措施提升整体防护等级。为实现内部风险的早期识别，可在关键位置安装水浸传感器，并依托信息化平台实现自动预警与联动处置，使维护人员能够在最短时间内控制渗漏扩散。排水设施、水循环设备与空调冷凝系统等需纳入常规巡检范围，通过定期维护降低故障可能性。对地势较低或极端天气频发地区的数据中心，还应建立水灾风险评估与应急预案，采取如设备上架高度调整、重要数据异地备份和断电保护等措施，实现水灾风险的前瞻治理与全方位防护。

5 高校数据中心机房安全管理体系建设

5.1 安全管理制度建设

数据中心机房的安全管理离不开制度体系的支撑。高校在推进机房建设与运维的过程中，应构建结构清晰、责任明确且具有可执行性的安全管理制度，以确保各环节均处于受控状态。制度内容不仅应围绕人员准入、岗位权限、设备操作规程、环境监控要求等方面进行系统设计，还需形成完整的应急响应机制，使管理活动在异常情况下能够迅速进入预案流程，减少风险扩散的可能性。与此同时，制度建设应强调动态更新，根据技术发展、运行经验及风险评估结果进行周期性的修订，使其持续适应新的管理需求。为确保制度真正落地，高校应强化制度执行的监督机制，通过审计、检查与反馈环节形成闭环管理。

5.2 信息化管理手段

随着信息技术的持续演进，信息化手段在数据中心机房的安全管理中发挥着愈发显著的作用。高校在构建数字化运维体系时，应充分利用物联网、人工智能及大数据分析等新兴技术，实现机房的可视化、精细化与智能化管理。通过部署多类型传感器，可对温湿度、供配电状态、消防系统、设备运行参数等关键要素进行实时采集，使管理人员能够及时掌握运行态势，避免因环境波动或设备异常引发安全事故。在此基础上，大数据分析模型能够对运行记录进行趋势挖掘与健康度评估，提前识别潜在风险，实现从“事后处理”向“事前预警”转变，并显著提升决策的科学性。此外，信息化平台的构建有助于形成统一的资源管理与调度体系，使巡检记录、维护日志、工单流程等实现自动归档与智能分析，提高安全管理活动的透明度与执行效率，推动机房管理向数字化治理模式迈进。

5.3 安全文化建设

安全文化在数据中心机房的安全保障体系中具有基础性意义，其作用不仅体现在规范行为和统一价值观方面，也直接影响制度执行力度与安全技术运行水平。高校在推进机房安全管理过程中，应通过持续的宣传教育、典型案例剖析、岗位自查机制及正向激励措施，使安全理念成为员工自觉遵守的行为准则。安全文化的塑造需要组织层面的制度引导，也需要日常工作中的情境熏陶，使风险意识和责任意识内化为全体人员的职业素养。

6 结语

高校数据中心机房作为信息化建设的重要基础设施，其安全性关系到高校各项工作的正常进行。本文通过对数据中心机房面临的各类安全风险进行分析，并提出相应的防控策略，旨在为高校数据中心的安全管理提供理论支持和实践指导。随着信息技术的不断发展，数据中心的安全防护工作面临着越来越多的挑战，未来需要不断加强技术手段与管理措施的结合，提升数据中心机房的安全保障能力，确保其持续稳定运行。

参考文献

[1] 王应求.高校校园网数据中心安全防护体系建设分析[J].信息与电脑(理论版),2022,34(06):221-223+250.

[2] 谢超群.高校数据中心云原生平台安全风险研究[J].网络安全技术与应用,2022,(01):79-80.

[3] 王晓震,金培莉,陈瑛,等.高校数据中心数据安全风险分析及对策研究[J].北京联合大学学报,2021,35(03):53-59.

[4] 李鑫,张琴.高校数据中心安全运维实践研究[J].山西大同大学学报(自然科学版),2022,38(04):33-37.

[5] 孙利宏.高校云计算数据中心网络安全问题与防护措施研究[J].科技视界,2019,(05):231-232.