

医院计算机中心机房的安全建设研究

高 鲁 党 伟*

宁夏医科大学总医院信息中心 宁夏 银川 750001

摘 要：随着医疗信息化的快速发展，医院计算机中心机房的安全建设显得尤为重要。本文旨在探讨当前医院计算机中心机房安全建设中存在的问题，并提出相应的解决方案。通过文献综述分析，本文详细阐述了物理安全、网络安全、数据安全和人员安全等方面的问题，并提出了具体的安全建设措施。研究表明，加强医院计算机中心机房的安全建设不仅能够保障医疗信息系统的稳定运行，还能有效防止数据泄露和网络攻击，对提升医院整体信息化水平具有重要意义。

关键词：医院计算机中心机房；安全建设；物理安全；人员安全

引言

随着医疗信息化的深入发展，医院计算机中心机房作为医疗信息系统的核心枢纽，其安全建设的重要性日益凸显。当前医院计算机中心机房在物理安全、网络安全、数据安全和人员安全等方面仍存在诸多问题，这些问题不仅影响了医疗信息系统的稳定运行，还可能引发严重的数据泄露和网络攻击事件^[1]。因此，研究医院计算机中心机房的安全建设问题，提出有效的解决方案，具有重要的现实意义。

1 当前医院计算机中心机房安全建设存在的问题

1.1 物理安全问题

(1) 机房环境控制不足。医院计算机中心机房对环境的要求极高，包括温度、湿度、灰尘、电磁干扰等。许多医院的机房环境控制设备老化，缺乏定期维护，导致机房环境不稳定。例如，温度过高可能导致服务器过热，湿度不当可能引发设备短路，灰尘积累可能影响设备的正常运行。

(2) 门禁系统不完善。机房的物理访问控制是防止未经授权人员进入的关键。许多医院的门禁系统存在漏洞，如门禁卡管理不严、门禁系统老化、监控摄像头覆盖不全等。这些问题使得机房容易受到物理入侵，增加

了数据泄露和设备损坏的风险。

(3) 防火设施不健全。机房内的电气设备众多，火灾风险较高。许多医院的机房防火设施不健全，灭火器材过期、烟雾报警系统失灵、防火隔离措施不到位等问题普遍存在。一旦发生火灾，可能导致严重的数据丢失和设备损坏。

1.2 网络安全问题

(1) 网络架构设计不合理。许多医院的网络架构设计缺乏层次性和隔离性，导致内外网之间的边界模糊，容易受到外部攻击。例如，内网和外网未进行有效隔离，可能导致外部攻击者通过互联网直接访问医院的核心数据。

(2) 防火墙和入侵检测系统配置不当。防火墙和入侵检测系统是保障网络安全的重要屏障。许多医院的防火墙配置过于宽松，允许不必要的端口和服务开放，入侵检测系统未能及时更新规则库，导致无法有效识别和阻止恶意攻击^[2]。

(3) 数据传输安全问题。医院在数据传输过程中，往往忽视了加密和认证机制的使用。例如，患者的电子病历、检验报告等敏感信息在传输过程中未进行加密，容易被窃取或篡改，导致信息泄露和医疗事故。

1.3 数据安全问题

(1) 数据备份不完善。数据备份是防止数据丢失的重要手段。许多医院的数据备份策略不完善，备份频率低、备份介质老化、备份数据未进行定期验证等问题普遍存在。一旦发生数据丢失，可能导致无法恢复，影响医院的正常运营。

(2) 数据加密不足。医院存储的大量敏感数据，如患者的个人信息、医疗记录、财务数据等，未进行有效的加密保护。这使得数据在存储和传输过程中容易受到

第一作者简介：名字：高鲁1989年3月，性别男，学历：本科，职称：初级，研究方向：计算机，通讯地址：宁夏银川市兴庆区胜利南街804号 宁夏医科大学总医院信息中心 电话：18395210297 邮箱：709847965@qq.com

第二作者：党伟(出生年月1994.1)，性别男，学历：大学本科，职称初级，通讯地址：宁夏银川市兴庆区胜利南街804号 宁夏医科大学总医院信息中心，邮编750001

通讯作者同二作

攻击,增加了数据泄露的风险。

(3) 权限管理混乱。医院的信息系统中,用户权限管理混乱,存在权限分配不合理、权限审计不严格等问题。例如,一些非授权人员可能拥有过高的权限,能够访问和修改敏感数据,增加了数据泄露和篡改的风险。

1.4 人员安全问题

(1) 安全意识薄弱。医院的信息化建设往往重视技术设备的投入,而忽视了人员的安全意识培训。许多医院员工对信息安全的重要性认识不足,缺乏基本的安全操作规范,容易在日常工作中无意中泄露敏感信息或引入安全漏洞^[3]。

(2) 安全管理机制不健全。医院的安全管理机制不健全,缺乏明确的安全责任分工和应急响应机制。例如,安全事件发生后,缺乏有效的追溯和处理机制,导致问题无法及时解决,甚至可能引发更大的安全风险。

2 医院计算机中心机房安全建设的基本要求

2.1 场地选择与室内装饰

(1) 场地选择。机房场地的选择是安全建设的第一步。应选择一个相对独立的空间,以减少外界环境对机房设备的干扰。机房应远离粉尘、油烟、易燃易爆及腐蚀性场所,这些环境因素不仅会影响设备的正常运行,还可能引发安全事故。机房应尽量避免磁场地区,磁场干扰可能导致数据丢失或设备故障。

(2) 室内装饰。在室内装饰方面,应采用钢化玻璃作为分隔材料,以提高机房的防火性能和美观度。钢化玻璃具有较高的强度和耐热性,能够在火灾发生时有效延缓火势蔓延。同时,机房应安装防火防盗门窗,确保在紧急情况下能够迅速疏散人员并保护设备安全。双层密闭窗的设计可以有效隔绝外界噪声和灰尘,为机房提供一个安静、清洁的工作环境^[4]。

2.2 电力系统要求

(1) 稳定的电力系统。稳定的电力供应是机房设备正常运行的基础。电力系统的稳定性直接影响到服务器、网络设备等关键设备的运行状态。任何电力波动或中断都可能导致数据丢失、系统崩溃,甚至设备损坏。因此,机房应配备稳定的电力系统,确保在任何情况下都能提供持续、稳定的电力供应。

(2) 专线供电与双路备份系统。为了进一步提高电力系统的可靠性,机房应采用专线供电与双路备份系统。专线供电可以避免与其他用电设备共享电源线路,减少电力波动和干扰。双路备份系统则可以在主电源出现故障时,自动切换到备用电源,确保机房设备的持续运行。这种设计不仅提高了电力系统的可靠性,还为机

房提供了更高的安全保障。

2.3 防雷措施

(1) 雷电对机房设备的威胁。雷电是机房设备面临的主要自然威胁之一。雷电产生的强大电流和电磁场可能直接损坏机房设备,或通过电力线路引入机房,造成设备故障和数据丢失。因此,防雷措施是机房安全建设中不可或缺的一部分。

(2) 避雷针与防雷器的安装及其作用原理。为了有效防范雷电威胁,机房应安装避雷针和防雷器。避雷针通过引导雷电电流进入地面,减少雷电对机房建筑的直接冲击。防雷器则安装在电力线路和通信线路上,能够在雷电发生时迅速将过电压引入地面,保护机房设备免受雷电损害^[5]。

(3) 防雷、接地技术检测的要求。防雷系统的有效性需要定期检测和维护。机房应定期进行防雷、接地技术的检测,确保避雷针、防雷器等设备处于良好工作状态。检测内容包括接地电阻的测量、防雷器的性能测试等,以确保防雷系统能够在雷电发生时发挥应有的保护作用。

3 医院计算机中心机房安全建设的具体措施

3.1 消防系统设计与施工

(1) 消防报警器与手提式灭火器的配置

在医院计算机中心机房的安全建设中,消防系统的完善是首要任务。机房内应配置高灵敏度的消防报警器,这些报警器能够实时监测机房内的烟雾和温度变化,一旦检测到异常,立即发出警报,提醒工作人员及时采取措施。手提式灭火器的配置也是必不可少的,它们应放置在机房的各个关键位置,以便在火灾初期能够迅速进行灭火操作,防止火势蔓延。

(2) 二氧化碳灭火系统及其感烟、感温探测器的设置

为了更有效地应对火灾,机房应安装二氧化碳灭火系统。这种系统能够在火灾发生时迅速释放二氧化碳,降低机房内的氧气浓度,从而达到灭火的目的。同时,为了确保灭火系统的有效性,机房内还应设置感烟和感温探测器,这些探测器能够精确监测火灾的早期迹象,为灭火系统提供及时的启动信号^[6]。

3.2 监控系统设计与实施

(1) 远程报警提示与短信报警提示系统的结合

在监控系统的设计中,远程报警提示和短信报警提示系统的结合是提高机房安全性的重要手段。远程报警提示系统能够在机房出现异常情况时,通过网络将警报信息实时传输到相关人员的终端设备上,确保他们能够第一时间了解情况并采取相应措施。而短信报警提示系统则能够在网络故障或其他原因导致远程报警失败时,

通过短信的方式将警报信息发送给相关人员，确保警报信息的传递不受阻碍。

(2) 防盗监控、网络监控、温度监控、湿度监控等系统的应用

为了全面保障机房的安全，防盗监控、网络监控、温度监控和湿度监控等系统的应用是必不可少的。防盗监控系统能够实时监测机房的出入口和重要区域，防止未经授权的人员进入。网络监控系统则能够监测机房内网络设备的运行状态，及时发现并处理网络故障。温度和湿度监控系统则能够确保机房内的环境参数始终处于最佳状态，防止因环境因素导致的设备故障。

3.3 系统安全建设

(1) 防火墙建设、内外网隔离系统与病毒库的重要性

防火墙建设：防火墙是医院计算机中心机房安全的第一道防线，它通过分析进出网络的数据包，按照事先设定的安全规则来决定是否允许数据包通过^[7]。防火墙能够有效地阻止未经授权的访问，防止外部攻击者进入内部网络，保护机房内的重要数据和业务系统。**内外网隔离系统：**为了进一步提高系统的安全性，需要实现内外网的严格隔离。这通常通过物理隔离或逻辑隔离的方式实现，确保内部网络的数据和业务流程不会受到外部网络的干扰和威胁。内外网隔离系统有助于防止内部敏感信息泄露给外部，同时也能够抵御外部网络中的病毒、木马等恶意软件的入侵。**病毒库的重要性：**病毒库是防病毒系统的重要组成部分，它包含了已知病毒的特征码和相关信息。防病毒系统通过定期更新病毒库，能够及时发现并清除机房内的病毒和恶意软件，保障系统的正常运行和数据的安全。

(2) 防火墙在机房安全建设中的屏障作用

防火墙作为机房安全建设中的核心组件，其屏障作用主要体现在以下几个方面：**访问控制：**防火墙通过设定安全策略，对进出网络的数据包进行严格的访问控制，确保只有合法的用户和数据才能通过。**入侵检测与防御：**防火墙具备入侵检测和防御功能，能够及时发现并阻止网络攻击行为，如DDoS攻击、SQL注入等。**日志审计：**防火墙能够记录所有进出网络的数据包信息，为安全审计和故障排查提供重要依据。

(3) 建立完善的防毒库体系

建立完善的防毒库体系是保障机房系统安全的重要措施之一。这包括以下几个方面：**定期更新病毒库：**确保防病毒系统能够及时获取最新的病毒特征码和相关信息，提高病毒检测和清除的准确性。**多层防御：**在机房

内部署多个防病毒软件，形成多层防御体系，提高系统的整体安全性。**应急响应机制：**建立完善的病毒应急响应机制，一旦发现病毒入侵，能够迅速启动应急预案，隔离并清除病毒，防止其扩散。

3.4 空调系统设计与维护

(1) 机房环境质量对设备与人员的影响。机房环境质量对设备和人员的影响不容忽视。过高的温度和湿度可能导致设备性能下降、故障率增加，甚至引发火灾等安全事故。同时，恶劣的机房环境也会影响人员的工作效率和健康。因此，必须高度重视机房环境质量的控制。

(2) 健康、节能的空调系统的设计与实施。为了保障机房环境质量的稳定，需要设计并实施健康、节能的空调系统。这包括以下几个方面：**精确控制：**采用先进的温湿度控制系统，实现对机房环境质量的精确控制，确保设备在最佳状态下运行。**节能设计：**采用高效节能的空调设备和控制技术，降低能耗，减少运行成本。**空气净化：**在空调系统中加入空气净化装置，过滤掉空气中的尘埃、细菌等有害物质，保障机房内的空气质量。**定期维护：**定期对空调系统进行维护和保养，确保其正常运行和性能稳定。这包括清洗过滤器、检查制冷剂、调整温湿度设定等。

结论：本文通过对当前医院计算机中心机房安全建设中存在的问题进行深入分析，提出了一套全面、系统的安全建设方案。研究表明，加强医院计算机中心机房的安全建设不仅能够保障医疗信息系统的稳定运行，还能有效防止数据泄露和网络攻击，对提升医院整体信息化水平具有重要意义。

参考文献

- [1]朱政.论医院计算机网络技术的安全威胁及对策[J].电子元器件与信息技术,2024,8(09):257-260.
- [2]李军强.计算机网络技术在医院信息化建设中的实践探究[J].电子元器件与信息技术,2024,8(08):178-180.
- [3]邓玲.智慧医院数据中心机房设计与规划研究[J].数字通信世界,2024,(08):110-112.
- [4]王何娟.医院计算机信息管理系统维护策略研究[J].科技风,2022,(13):47-49.
- [5]徐大志.医院信息化建设中的网络安全分析与防护[J].长江信息通信,2022,35(03):185-187.
- [6]梁猛.医院计算机信息系统的风险管理分析[J].电子技术,2021,50(12):132-133.
- [7]张文强,王翠花.医院双中心机房虚拟化网络的设计[J].中国新技术新产品,2023,(06):34-37.