医院计算机信息管理系统维护技术

秦　豪　杨红霞*
宁夏医科大学总医院　宁夏　银川　750000

摘　要：医院计算机信息管理系统对医疗工作至关重要，本文聚焦系统维护技术，涵盖系统硬件、软件、安全及运维管理等多方面。硬件维护涉及服务器、终端设备和网络设备；软件维护包括操作系统、数据库和应用系统；安全维护包含数据、终端和网络安全；运维管理涉及流程、监控和容灾。通过全面且细致的维护，保障系统稳定运行，提升医疗服务效率与质量，为医院信息化建设提供坚实支撑。

关键词：医院计算机信息管理系统；系统维护技术；硬件维护；软件维护；安全维护

引言：在医疗信息快速发展的当下，医院计算机信息管理系统成为医疗工作高效开展的关键支撑。它涵盖患者信息管理、医疗业务流程、数据存储与共享等多个环节，对提升医疗服务质量、优化管理流程意义重大。然而，系统运行过程中面临硬件故障、软件漏洞、安全威胁等诸多挑战。因此，全面且深入地掌握系统维护技术，确保系统稳定、安全、高效运行，成为医院信息化建设的核心任务，也是保障医疗服务顺利进行的必然要求。

1 系统硬件维护技术

1.1 服务器维护技术

服务器作为医院计算机信息管理系统的核心支撑，其硬件组件的稳定运行是保障系统高效运转的基础。在日常维护工作中，需定期对服务器硬件组件进行全面巡检，涵盖处理器、内存条、硬盘、电源等关键部件，检查是否存在过热、松动、老化等潜在问题，并及时进行紧固、清洁或更换处理，以消除硬件故障隐患[1]。针对服务器性能参数，需根据系统实际运行负载情况进行动态调整，例如合理分配处理器资源、优化内存使用策略、调整磁盘读写参数等，确保服务器在不同业务场景下均能保持最佳性能状态。同时，服务器运行环境的稳定性对硬件寿命及系统可靠性具有重要影响，需对机房温度、湿度、洁净度等环境参数进行实时监测与调控，避免因环境因素导致服务器硬件损坏或性能下降。

1.2 终端设备维护技术

医用终端设备是医护人员与信息系统交互的关键界面，其运行状态的稳定性直接关系到医疗工作的效率与质量。需定期对医用终端设备进行全面检查，涵盖设备外观、接口连接、系统运行等多个方面，确保设备无损坏、无松动、无异常提示，保障设备正常运行。终端输入输出设备，如键盘、鼠标、显示器、打印机等，是医护人员操作信息系统的重要工具，需进行定期调试与保养。清洁设备表面灰尘，防止灰尘进入设备内部影响性能；检查接口连接是否牢固，避免因接触不良导致设备无法正常工作；调整设备参数至最佳状态，如显示器的亮度、对比度，打印机的打印质量等，以保障输入输出设备的正常工作。当终端设备出现故障时，需迅速且准确地定位故障原因。通过检查设备日志，分析其中记录的设备运行信息和错误提示；对错误提示信息进行深入剖析，结合以往经验判断可能的故障点；采用替换可疑部件的方式，逐步缩小故障范围，最终确定故障点并进行修复，恢复终端设备的正常运行。

1.3 网络设备维护技术

网络交换设备作为医院内部网络数据交换的枢纽，其配置与维护对网络通信的稳定性与效率具有决定性作用。需定期对网络交换设备进行配置检查与优化，确保设备端口配置正确、VLAN划分合理、路由策略有效，避免因配置错误导致网络通信故障。网络路由设备负责医院内部网络与外部网络的连接，其运行参数的管控对网络访问速度与安全性至关重要。需对路由设备的带宽分配、访问控制列表、防火墙策略等参数进行定期审查与调整，确保网络路由设备能够高效、安全地完成数据转发任务。同时，需对网络传输链路状态进行实时监测，通过部署网络监控系统，实时收集链路带宽利用率、丢包率、延迟等关键指标数据，及时发现并处理链路故障，保障网络传输的畅通无阻。

2 系统软件维护技术

2.1 操作系统维护技术

作者简介：秦豪，男，1998年12月，硕士，研究方向：计算机。邮箱：qinhao0403@163.com

通讯作者：杨红霞，女，1987年3月，研究生，中级，计算机，邮箱：675639496@qq.com

服务器操作系统作为支撑医院业务运转的核心软件平台，补丁与版本管理是保障系统安全稳定运行的基石。定期对服务器操作系统进行安全补丁更新，能够及时修复已知漏洞，抵御潜在的网络攻击与恶意软件入侵，避免因系统漏洞导致的业务中断或数据泄露风险[2]。随着技术发展与应用需求变化，适时进行操作系统版本升级，引入新功能特性与性能优化，提升系统整体运行效率与兼容性。终端操作系统配置优化聚焦于提升用户使用体验与系统运行效能，针对不同科室、不同岗位的终端设备，依据实际业务需求调整系统参数，如关闭非必要系统服务、优化磁盘读写策略、调整网络连接设置等，减少系统资源占用，加快终端响应速度。操作系统进程与资源调度维护是确保系统稳定运行的关键环节，通过监控系统进程状态，及时发现并处理异常进程，避免进程冲突或资源耗尽引发系统崩溃，同时合理分配系统资源，保障关键业务进程获得充足资源支持，提升系统整体处理能力。

2.2 数据库维护技术

数据库存储结构优化管理是提升数据库性能与存储效率的重要手段。依据医院业务数据特点与访问模式，对数据库表结构、索引设计、分区策略等进行优化调整，减少数据冗余与碎片，提升数据读写速度与查询效率。数据库日志记录了数据库运行过程中的各类操作信息，定期进行日志清理与归档，能够释放存储空间，避免日志文件过大影响数据库性能，同时对重要日志进行妥善归档保存，便于后续审计与故障排查。数据库连接会话管理关乎数据库的访问安全与性能表现，通过监控数据库连接会话状态，及时发现并处理长时间未释放的连接会话，防止连接泄漏导致数据库性能下降或资源耗尽，同时对连接会话进行权限控制，确保只有授权用户能够访问数据库。

2.3 应用系统维护技术

医院业务应用模块版本更新是保持应用系统先进性与功能完整性的必要举措。根据医院业务发展需求、技术进步以及用户反馈，定期对应用系统进行版本升级，引入新功能模块、修复已知问题、优化用户界面，提升应用系统的适用性与用户体验。应用系统功能参数配置调整旨在满足不同科室、不同业务流程的个性化需求，依据实际业务场景对应用系统功能参数进行灵活配置，如调整业务流程节点、修改数据展示方式、设置权限控制规则等，确保应用系统能够精准匹配医院实际业务运作。应用系统异常交互处理是保障系统稳定运行的重要环节，建立完善的异常交互监测与处理机制，对应用系统运行过程中出现的异常交互行为进行实时捕获、记录与分析，定位问题根源并采取有效措施进行修复，避免异常交互对医院业务造成影响，确保应用系统持续稳定运行。

3 系统安全维护技术

3.1 数据安全维护技术

数据作为医院运营的核心资产，存储加密与脱敏处理是保障数据安全的第一道防线。通过采用先进的加密算法，对存储在数据库、文件服务器等位置的数据进行加密处理，确保即使数据被非法获取，也无法被轻易解密，从而有效保护患者隐私与医院敏感信息[3]。数据脱敏处理则针对特定业务场景，对敏感数据进行变形处理，如替换、遮蔽等，使得数据在保持可用性的同时，降低泄漏风险。数据访问权限分配与更新是数据安全管理的关键环节，根据医院组织架构与人员职责，为不同用户分配精细化的数据访问权限，确保用户只能访问工作所需的数据，避免数据越权访问。随着医院人员变动与业务调整，及时更新数据访问权限，确保权限分配的准确性与时效性。数据流转全流程防护则贯穿于数据的产生、传输、存储、使用与销毁等各个环节，通过部署数据安全防护系统，对数据流转过程进行实时监控与审计，及时发现并阻断数据泄露风险，确保数据在全生命周期内的安全性。

3.2 终端安全维护技术

终端作为医院信息系统的入口，其安全策略配置与更新至关重要。根据医院安全策略要求，为终端设备配置防病毒、防火墙、入侵检测等安全软件，并定期更新安全策略，以应对不断变化的网络威胁。终端恶意程序防范与清理是保障终端安全的重要措施，通过部署恶意程序检测与清除工具，对终端设备进行定期扫描与清理，及时发现并清除潜伏的恶意程序，防止其对终端设备与医院网络造成损害。终端安全接入控制则确保只有经过授权的终端设备才能接入医院网络，通过身份认证、访问控制等技术手段，对终端设备的接入请求进行严格审核，防止非法设备接入网络，从而保障医院网络的安全性。

3.3 网络安全维护技术

网络边界防护策略维护是构建医院网络安全屏障的基础。通过部署防火墙、入侵防御系统等网络安全设备，对医院网络边界进行严密防护，阻止外部非法访问与攻击。定期对网络边界防护策略进行审查与更新，确保策略的有效性与适应性。网络访问行为监测则对医院网络内的用户访问行为进行实时监控与分析，通过收集用户访问日志、网络流量等数据，发现异常访问行为，如频繁访问敏感资源、非法下载等，及时采取措施进行干预，

防止潜在的安全威胁。网络异常流量识别与处置是应对网络攻击与故障的重要手段，通过部署流量监测与分析系统，对网络流量进行实时监测与分析，及时发现异常流量模式，如DDoS攻击、病毒传播等，并采取流量清洗、阻断等措施进行处置，确保医院网络的稳定运行。

4 系统运维管理技术

4.1 运维流程管理技术

系统运维任务规划与分配是保障运维工作有序开展的基础。依据医院业务系统的运行特点、重要程度以及维护周期，对各类运维任务进行科学规划，明确任务目标、执行时间与责任人员[4]。通过合理分配运维资源，确保关键业务系统的运维任务得到优先处理，避免因任务堆积或资源分配不均导致系统故障处理延误。运维工单处理流程执行是规范运维操作、提升运维效率的关键环节。建立标准化的运维工单处理流程，从工单提交、审核、分配、处理到反馈，每个环节都设定明确的操作规范与时间节点。运维人员按照流程要求执行工单任务，确保问题得到及时、有效的解决，通过工单记录详细的处理过程与结果，为后续运维工作提供参考依据。运维文档更新与归档是运维知识积累与传承的重要手段。随着医院业务系统的不断升级与优化，运维文档需及时更新，记录系统配置信息、维护操作步骤、故障处理方法等内容。将更新后的运维文档进行妥善归档保存，形成完整的运维知识库，方便运维人员随时查阅与学习，提升运维团队整体技术水平。

4.2 系统监控管理技术

硬件设备运行状态监控是保障系统稳定运行的物质基础。通过部署专业的硬件监控工具，对服务器、存储设备、网络设备等硬件设备的运行状态进行实时监测，包括设备温度、电压、风扇转速、磁盘使用情况等参数。及时发现硬件设备异常状态，如温度过高、磁盘故障等，提前采取措施进行维修或更换，避免硬件故障引发系统崩溃。软件系统运行参数监控聚焦于软件层面的性能表现。对操作系统、数据库、应用系统等软件系统的关键运行参数进行监控，如CPU使用率、内存占用率、数据库连接数、应用系统响应时间等。通过分析这些参数变化趋势，及时发现软件系统性能瓶颈，如内存泄漏、数据库查询效率低下等问题，为软件系统优化提供数据支持。网络链路传输状态监控是保障网络通信畅通的关键。对医院内部网络链路以及与外部网络连接的传输状态进行实时监测，包括网络带宽使用情况、数据包丢失率、网络延迟等指标。及时发现网络链路故障或拥塞问题，快速定位故障点并采取措施进行修复，确保网络通信稳定可靠。

4.3 系统容灾维护技术

备份策略制定与执行是容灾维护的核心环节。根据医院业务系统数据的重要性与更新频率，制定科学合理的备份策略，确定备份周期、备份方式与备份存储位置。定期执行备份任务，确保业务数据得到及时、完整的备份，避免因数据丢失导致业务中断。备用系统切换流程维护是保障在主系统出现故障时能够快速恢复业务的关键。制定详细的备用系统切换流程，明确切换条件、切换步骤与责任人员。定期组织演练，确保运维人员熟悉切换流程，在主系统故障时能够迅速、准确地将业务切换至备用系统，减少业务中断时间[5]。容灾环境定期校验是确保容灾系统有效性的重要措施。定期对容灾环境进行全面校验，包括硬件设备、软件系统、网络连接等方面，验证备用系统是否能够正常启动与运行，数据是否能够成功恢复。通过定期校验及时发现容灾环境存在的问题并进行修复，确保在需要时容灾系统能够发挥预期作用。

结束语

医院计算机信息管理系统维护是一项长期且复杂的工作，涉及硬件、软件、安全及运维管理等多个层面。通过科学有效的维护技术，可及时发现并解决系统运行中的问题，降低故障发生率，保障系统稳定运行。这不仅有助于提升医院的工作效率和服务质量，还能增强医院应对各种风险的能力。持续优化系统维护策略，是推动医院信息化不断发展的重要保障。

参考文献

[1]郑矗.医院计算机信息管理系统维护技术分析[J].IT经理世界,2025,28(9):234-236.

[2]周小程.医院计算机信息管理系统的维护技术研究[J].大众科技,2021,23(10):22-25.

[3]李大伟.计算机网络技术在医院信息管理系统中的应用[J].数字技术与应用,2021,39(7):59-61.

[4]邓博.基于医院计算机信息管理系统的维护技术研究[J].电脑爱好者（校园版）,2022(1):19-21.

[5]李琳,张晓青.医院计算机信息管理系统的维护策略研究[J].信息技术时代,2024(11):144-146.