档案管理中信息安全保护机制的优化研究

贺恩娅

重庆市垫江县五洞镇便民服务中心 重庆 408326

【摘　要】：档案管理中信息安全保护机制的优化研究，旨在分析和解决当前档案管理系统中存在的信息安全隐患。随着信息化进程的不断推进，档案管理面临着日益复杂的安全威胁。传统的安全防护机制已经无法有效应对现代信息技术带来的挑战。本文通过深入分析现有档案管理中的信息安全问题，提出了优化措施，包括技术手段、管理机制的改进，以及员工安全意识的提升。研究结果表明，综合运用多层次的保护机制能显著提高档案管理的安全性，为实现档案信息的长期安全保存提供理论依据和实践指导。

【关键词】：档案管理；信息安全；保护机制；优化；安全隐患

DOI:10.12417/3041-0630.25.24.036

在信息化时代，档案管理已成为各类组织的重要组成部分，保障档案信息的安全至关重要。现有的档案管理体系中，信息安全保护机制常常存在漏洞，无法应对日益复杂的安全威胁。随着技术的发展，信息泄露、篡改等问题越来越频繁，给档案管理带来了巨大挑战。因此，如何在传统档案管理基础上优化信息安全保护机制，已成为亟待解决的课题。本文将围绕这一问题展开，探索适应新形势的信息安全保护机制，提出切实可行的优化方案，旨在提升档案管理系统的整体安全性，并为行业提供参考。

1 现有档案管理信息安全保护机制的挑战

当前，档案管理系统在信息安全保护方面面临诸多挑战。随着信息化技术的迅速发展，档案管理中的信息安全问题愈加复杂，传统的保护机制已难以应对新的威胁。档案作为重要的历史、法律和文化载体，往往包含大量敏感信息，其安全性直接关系到国家、组织甚至个人的利益。很多档案管理系统在实际运行中，仍然依赖传统的防护措施，如纸质存档、单一密码保护等，这些方式缺乏足够的技术支撑，无法应对现代网络攻击的挑战。技术方面，很多档案管理系统未能及时跟上网络安全防护的技术更新，导致防护能力薄弱。网络攻击手段不断升级，恶意软件、病毒、勒索软件等威胁日益严重，而传统的安全防护方式无法有效预防这些风险。档案系统中大量使用的存储介质在信息传输过程中容易被窃取或篡改，尤其是存储在云平台和远程服务器中的档案，存在数据泄露的隐患。

在管理机制上，部分档案管理部门缺乏完善的信息安全政策和操作规范，安全防护措施落实不到位。尽管相关管理者已意识到信息安全的重要性，但在实际执行中，由于缺乏有效的监管与审核，很多安全漏洞未能及时发现和修复。特别是在档案人员的安全意识和技能方面，许多操作人员未经过专业的安全培训，导致管理过程中存在较大的人为疏忽，进一步加剧了安全风险。档案管理中存在的问题不仅仅是技术层面的薄弱，还包括管理上的松散。随着信息安全威胁的不断增多，现有的保护机制显得捉襟见肘，亟需进行优化和升级。

2 优化档案管理信息安全保护机制的策略

在优化档案管理信息安全保护机制方面，采用多层次、综合性的保护策略至关重要。技术手段的更新与升级是提升档案管理信息安全的关键。现有系统应引入先进的加密技术，确保数据存储和传输过程中的安全性。对于存储在云平台的档案，采用数据加密技术不仅能有效防止数据在传输过程中的泄露，还能保障文件在存储阶段的完整性。基于区块链的分布式存储技术可作为一种潜在的解决方案，利用其不可篡改的特性，可以为档案管理系统提供更高的安全保障。数字签名技术和身份验证技术的运用，也能够防止档案在流通过程中遭遇伪造或篡改的风险。

强化访问控制和权限管理是优化信息安全保护机制不可忽视的方面。通过实现细粒度的权限控制，确保只有授权人员能够访问特定档案信息，对于不同的岗位设置不同的访问权限，避免无关人员对档案内容的随意访问。角色基于访问控制（RBAC）模型和最小权限原则的实施，能够有效减少内部人员造成的安全威胁。与此并行的措施是监控与审计功能的加强，对每一次档案的访问、修改及删除操作进行详细记录并实时监控，确保对所有操作的可追溯性。一旦出现异常行为，系统应能够及时发出警报，并采取相应措施，如自动锁定用户账户或暂停访问权限。

管理制度的优化同样不可忽视。档案管理人员的安全意识提升和专业技能培训是加强信息安全管理的基础。通过定期的安全培训和演练，提高档案管理人员对于信息安全威胁的敏感性，并且提升其应对突发安全事件的能力。同时，档案管理体系应制定完善的信息安全应急预案，确保在发生安全事件时，能够迅速响应并采取有效措施进行应急处置，最大限度减少损失。定期进行安全漏洞扫描和风险评估，及时发现系统中的薄

弱环节，并进行修补和升级，是保障系统长期稳定运行的重要措施。

技术手段和管理制度的双重优化，将为档案管理系统提供更加坚实的安全保障。而为了确保这些措施的有效实施，还需要一个强有力的监督机制，通过组织内部的安全评估和外部审计的方式，确保信息安全保护措施得到贯彻执行，形成多方联动的防护网络。通过这一系列策略的实施，可以显著提升档案管理系统的信息安全水平，为档案的安全管理和长久保存提供坚实的基础。

3 优化方案的实施与效果评估

在实施优化方案时，首先需要确保技术措施的顺利落地和更新。信息安全保护技术的集成不仅仅是对现有系统的简单升级，而是要进行全面的技术架构重构。将加密技术、身份验证机制、访问控制系统等核心技术进行整合，形成一个统一的安全防护网络。在档案管理系统中部署多层次防护措施时，关键技术如数据加密、身份验证和访问控制应紧密结合，确保不同层级的安全措施能够协调运作。技术实施的过程中，还需进行严格的测试，验证加密、备份和访问控制等功能的有效性，确保其在面对各种潜在威胁时能够发挥作用。系统的管理和操作人员需要接受专业的安全培训。这不仅限于对新技术的学习，还包括对新实施的安全管理制度的熟练掌握。通过定期培训、模拟演练等方式，强化管理人员的安全意识和应急处理能力，确保在安全事件发生时能迅速响应并采取正确措施。对档案管理人员进行全面的安全防护教育，帮助其理解新的安全策略和技术，提升整体档案管理的安全性。

评估优化方案效果的关键在于持续的安全监控和定期的审计评估。通过对优化后的系统进行定期安全检查和漏洞扫描，能够及时发现潜在的安全隐患，并采取针对性措施加以修补。实施实时监控机制，对每一项档案的存取、修改及删除操作进行跟踪，确保所有操作可追溯并且符合安全规范。定期的系统评估报告和第三方审计，可以提供客观、专业的安全性反馈，帮助发现问题并进行调整。效果评估不仅仅是对技术层面的考量，更要综合考虑管理流程的改进和人员的响应能力。通过对实际操作过程中出现的安全问题和管理漏洞进行深入分析，评估优化方案是否真正起到提高档案信息安全的作用。评估结果应当反馈到系统优化和管理措施的进一步完善上，形成一个闭环反馈机制，确保档案管理系统在各个环节中都具备高效的安全防护能力。

4 结语

通过对档案管理信息安全保护机制的优化研究，提出的技术和管理措施有助于提高档案管理系统的安全性。多层次的防护体系、严格的访问控制、完善的人员培训以及持续的安全监控，都能够有效应对当前档案管理面临的安全挑战。实施这些优化方案后，能够显著降低信息泄露、篡改等风险，保障档案的长期安全保存。随着技术不断进步和管理机制的持续完善，档案管理信息安全将在更高水平上得到保障，为社会各界提供可靠的信息保护服务。

参考文献：

[1] 张华,王晓.基于大数据的档案管理信息安全保护策略研究[J].信息安全研究,2023,9(2):56-63.

[2] 李强,赵云.信息化时代档案管理中的信息安全挑战与对策[J].信息技术与信息化,2022,35(5):74-80.

[3] 刘旭东,陈晓.云计算环境下档案管理信息安全防护机制优化[J].云计算与大数据,2021,10(1):45-52.