

数字化档案系统中档案信息安全防护措施研究

康璐雯

会理市城南街道办事处 四川 凉山 615100

【摘要】：在数字化档案系统中，档案信息的安全防护是一个重要的课题。随着信息技术的发展，传统档案管理逐渐向数字化转型，信息安全风险也随之上升。因此，在数字化进程中，如何有效防护档案信息的安全性成为亟待解决的问题。本文通过对数字化档案系统中档案信息安全防护措施的研究，分析目前存在的安全隐患，并提出有效的技术和管理对策，以确保档案信息的完整性、机密性和可用性。

【关键词】：数字化档案系统；信息安全；安全防护措施；数据保护；网络安全

DOI:10.12417/2811-0528.26.01.020

引言

随着信息化浪潮的到来，各行各业开始逐步实现档案资料的数字化转型。数字化档案系统有效提高了档案管理的效率和准确性，但同时也面临着网络攻击、数据泄露和信息丢失等安全挑战。因此，在数字化进程中，如何有效防护档案信息的安全性成为亟待解决的问题。本文重点研究数字化档案系统中信息安全的主要威胁，并探讨相应的防护措施。

1 档案信息安全风险分析

1.1 常见的安全威胁

随着网络技术的进步和网络环境的复杂化，黑客攻击已成为档案信息的主要威胁之一。攻击者可以通过各种技术手段渗透到数字化档案系统中，窃取、篡改甚至删除重要数据。这种威胁不仅损害数据的完整性和机密性，还可能导致大量机密信息外泄，给组织带来难以估量的损失。数据泄露主要发生在系统的薄弱环节，如通信过程、储存位置或数据备份中。数据泄露可能因为不当的数据管理策略、未加密或低安全级别的存储设备而发生。一旦档案信息被泄露，不仅会导致敏感信息落入不法分子手中，还可能破坏个人隐私、组织声誉以及客户信任。信息丢失通常是由于系统故障、自然灾害、或人为因素引起的。这种风险尤其严重，因为它可能导致无可挽回的重要数据消失。自动化备份与恢复措施不充分，或者灾难恢复计划不完整，都会加大信息丢失的风险。此外，信息丢失还可能因为操作人员缺少培训而误删重要文件或错误配置安全设置所导致。

1.2 内部安全隐患

除了外部威胁，内部安全隐患同样对档案信息的安全构成巨大威胁，人为因素是许多安全漏洞的根源。即使是最完善的系统，如果操作人员缺乏足够的安全意识和技能，仍可能导致严重的安全事件。例如，员工可能由于缺少安全意识而点击恶

意链接、处理敏感信息时不遵循保密协议，或者在离开工作岗位时未锁定工作终端，这些都有可能导致信息泄露或系统感染恶意软件。权限管理的薄弱会导致超出必要范围的信息访问，增加信息被滥用的风险。窃取或误用权限的人员可能访问敏感数据或系统功能，从而造成信息损失或系统破坏。在许多组织中，权限分配不合理、细化管理不足以及缺乏定期审查，都是常见的问题。即使拥有完善的技术措施，不当或疏忽的权限管理仍可能对信息安全构成威胁。

2 档案信息安全防护措施

2.1 技术性措施

在数字化档案系统中，应用先进的技术性措施对信息安全进行防护是至关重要的。首先，数据加密技术作为保护档案数据的一项核心技术，通过使用加密算法对数据进行加密，即使数据被非法获取，攻击者也难以解读。现代的加密方法如 AES（高级加密标准）和 RSA（Rivest-Shamir-Adleman）算法等，可以提供不同强度和类型的保护，适用于静态数据和动态数据。加密不仅用于存储在硬盘上的数据，还用于在网络上传输的数据，确保信息在交换过程中不被窃听或篡改。此外，防火墙与入侵检测系统（IDS）是另一项关键技术，通过阻止非授权访问并实时监控网络流量来检测并响应潜在的威胁。这些系统可以配置为识别异常活动，如未经授权的访问尝试或数据流突然增加，触发警报以启动进一步调查。云存储安全也是如今备受关注的技术领域，随着越来越多的档案数据迁移到云平台，必须确保云服务提供商实现了严格的安全措施，包括身份验证、加密、数据分区以及连续监控，以防止数据泄露和损失。

2.2 管理性措施

为了支持技术性措施，强有力的管理性措施同样不可或缺。首先，通过完善权限管理来控制访问权限是基本的安全策略。每个用户的访问权限应根据其工作职责进行严格规定，并

通过持续的监控和期审来确保权限的合理性和及时调整,防止权限扩散和滥用。此外,定期安全审计是维持系统安全的良好实践。安全审计可以检查系统中的安全政策和措施是否有效运行,是否符合最新的安全标准和法规要求。通过审计发现的漏洞和薄弱环节能够及时修复,从而不断提高系统的安全性和稳健性。最后,员工安全意识培训对减少人为失误和提高整体安全系数起到关键作用。通过定期举行培训和讲座,提高员工对信息安全风险的认识和防范能力,使他们了解最新的安全威胁和如何避免成为攻击目标是必不可少的。通过技术与管理相结合的双重防护策略,档案信息安全可以得到更全面和有效的保障。

3 法律与政策支持

在保护数字化档案系统中档案信息安全方面,法律法规起到了基础性和指导性的作用。数据保护法律法规确立了信息保护的基本原则和具体要求。例如,《通用数据保护条例(GDPR)》和各国制定的数据隐私法规,为数据处理和储存设定了严格的标准。这些法律要求组织确保其处理的数据安全,并规定了数据泄露的严重后果和相应的惩罚措施。这为档案信息的保护提供了法律依据,促使组织在信息管理中采取更科学和严谨的措施,对信息的收集、存储、处理和传输实行更有效的监督与控制。此外,政府和组织的政策指导在信息安全治理中也扮演着重要角色。各国政府和行业协会均有制定相关政策,以推动和规范档案信息的安全管理。这些政策通常包括应急响应机制、行业最佳实践指南以及教育和培训计划等,目的在于提高组织对潜在风险的识别和应对能力。通过这些指导,组织可以更好地理解政策要求,制定适合自身发展和管理体系的信息安全策

略,确保在合规的同时实现信息安全的最大化。

4 未来发展方向

随着信息技术的飞速进步和网络环境的日益复杂,档案信息安全的保护需要不断创新。智能安全监控系统是未来研究的一个重要方向。这类系统利用人工智能和机器学习技术,能够实时监控和分析网络环境中的异常行为和潜在威胁,自动调整安全策略以预防和响应安全事件。这不仅提高了安全事件发现的及时性,也降低了人为监控的失误率。智能化的安全体系可以根据多维数据分析动态更新安全协议和策略,以应对不断变化的攻击手段和复杂的网络环境。区块链技术在档案安全中的应用也是值得关注的前沿领域。区块链因其去中心化、不可篡改和可追溯的特点,被认为在档案信息的验证、加密和存储中具有巨大潜力。通过区块链技术,档案数据可以记录在一个安全的分布式账本中,任何数据的更改都需得到共识验证,防止了未经授权的数据篡改和丢失。此外,区块链技术还能为档案提供透明的访问控制和登录管理,为档案信息提供多维度的安全保障,这将为未来的档案管理带来新的机遇和解决方案。

5 结语

数字化档案系统的安全性关系到整个信息管理架构的稳定性与可靠性。通过实施有效的安全防护措施,结合技术与管理的双重手段,可以大幅度降低档案信息被不当获取、篡改或删除的可能性。未来,随着技术的不断进步和政策的日益完善,数字化档案系统的信息安全将达到一个更高的水平,为档案管理的现代化提供强有力的保障。档案管理者应不断更新知识,提升技术水平,以应对不断演变的安全挑战。

参考文献:

- [1] 戴秀文.网络边界改变下档案信息安全防护体系的变革措施[J].机电兵船档案,2020,(03):78-80.
- [2] 贾丽娜.医院电子档案管理与档案信息的安全防护措施[J].办公室业务,2020,(10):96-97.
- [3] 王滨娜.谈档案信息安全管理中的防护策略和保密措施[J].兰台世界,2012,(23):64-65.
- [4] 阎立明.数字化时代档案安全防护——评《信息安全视域下高校档案管理研究》[J].中国科技论文,2020,15(09):I0017-I0017.
- [5] 李禹静.档案信息化的安全风险及防护措施研究[J].移动信息,2025,47(07):212-214.
- [6] 吴育良,车宇辉,王琳.数字化人事档案管理系统信息安全设计研究[J].兰台内外,2024,(22):25-27.