计算机信息管理技术与计算机网络安全应用

刘　猛
天津赢大科技有限公司　天津　300384

摘　要：随着信息技术的迅速发展和广泛应用，计算机信息管理技术和计算机网络安全日益受到重视。本文简要回顾了计算机信息管理技术的发展历程，并探讨了其核心要点和关键技术。同时，文章分析了当前网络安全面临的挑战和威胁，以及信息管理技术在网络安全中的重要作用。最后，文章提出了促进信息管理与网络安全融合发展的策略与建议，以保障信息安全和促进信息化健康发展。

关键词：计算机；信息管理技术；网络安全应用

引言：在数字化时代的浪潮下，计算机信息管理技术与计算机网络安全应用显得至关重要。随着信息技术的迅猛发展和数字化转型的深入推进，企业和组织对高效、准确的信息管理需求日益迫切，同时网络安全威胁也层出不穷，对信息安全提出了更高的要求。本文旨在全面剖析计算机信息管理技术的核心要点与关键技术，并探讨其在网络安全领域的应用实践，旨在推动信息管理与网络安全的融合发展，确保信息安全与业务发展的双赢。

1 计算机信息管理技术概述

1.1 计算机信息管理技术的发展历程

计算机信息管理技术的起步可追溯到20世纪中期，当时主要为简单的数据处理与存储。随着计算机技术的飞速发展和普及，信息管理逐渐演变为一门集数据存储、处理、传输、分析和保护于一体的综合性技术。进入21世纪后，随着大数据、云计算、人工智能等技术的兴起，信息管理技术进一步革新，数据处理能力成倍增长，数据分析变得更为精确与复杂。

1.2 当前信息管理技术的核心要点与关键技术

当前信息管理技术的核心要点主要包括数据集成、数据存储、数据处理、数据分析和数据保护。关键技术则涉及以下几个方面：（1）数据库技术。作为信息管理的基础，数据库技术负责高效存储和检索数据，确保数据的完整性和一致性。（2）数据挖掘与分析。通过高级算法，从海量数据中提取有价值的信息，为决策提供支持。（3）数据可视化。将复杂的数据转化为直观的图形或图表，帮助用户更好地理解和分析数据。（4）数据安全与隐私保护。确保数据在传输、存储和使用过程中不被非法访问或篡改，保护用户的隐私[1]。

1.3 信息管理技术在企业和组织中的应用实例

（1）电子商务平台的数据管理。电子商务平台每天都会产生大量的交易数据、用户行为数据等。利用信息管理技术，企业可以对这些数据进行整合和分析，以了解用户的购物偏好、消费习惯等，从而为用户提供更加个性化的购物体验。同时，通过对交易数据的分析，企业还可以优化库存管理、提高供应链效率等。（2）金融机构的风险管理与决策支持。金融机构在处理大量的金融数据时，需要高效、准确的信息管理技术来支持。通过数据挖掘和分析，金融机构可以识别出潜在的风险点，及时采取风险控制措施。同时，信息管理技术还可以为金融机构提供决策支持，帮助其制定更加合理的投资策略和产品设计方案。（3）政府机构的公共信息管理。政府机构需要管理大量的公共信息，如公民个人信息、政府文件等。利用信息管理技术，政府机构可以实现对这些信息的高效存储、检索和共享，提高政务服务的效率和透明度。同时，信息管理技术还可以帮助政府机构监测舆情动态、分析社会热点问题等，为政策制定提供数据支持。

2 计算机网络安全现状与挑战

2.1 网络安全威胁的种类与特点

随着互联网的深入发展和普及，网络安全威胁日益增多，其种类和特点也变得更为复杂。常见的网络安全威胁主要包括：（1）恶意软件。包括病毒、木马、蠕虫等，它们通过各种途径传播，感染计算机系统，窃取、破坏或篡改数据，甚至占用系统资源，导致系统崩溃。（2）黑客攻击。黑客利用漏洞、木马、社会工程学等手段，非法侵入他人计算机系统，窃取机密信息，进行身份盗窃、网络诈骗等活动。（3）网络钓鱼。通过发送伪装成合法来源的电子邮件或网站，诱骗用户点击恶意链接或下载恶意附件，进而窃取用户的个人信息。（4）数据泄露。由于系统漏洞、人员失误或内部人员滥用权限等原因，导致敏感数据被非法获取或传播。（5）拒绝服

务攻击（DoS/DDoS）。通过大量请求拥塞目标服务器或网络的带宽，使其无法为正常用户提供服务。这些网络安全威胁的特点是：传播速度快、隐蔽性强、危害大、难以追踪。随着技术的发展，威胁手段还在不断演变，变得更加智能和复杂。

2.2 国内外网络安全事件案例分析

（1）“棱镜门”事件：该事件揭露了美国国家安全局（NSA）通过网络入侵手段，长期、系统地窃取全球范围内的敏感信息。这起事件引发了全球对网络安全和国家信息安全的深思。（2）WannaCry勒索病毒事件：该病毒通过漏洞传播，对全球范围内的计算机系统进行攻击，导致数据被加密并索要赎金。事件造成了严重的经济损失和社会影响，凸显了网络安全威胁的严重性。（3）某大型电商数据泄露事件：该事件由于系统漏洞和内部人员疏忽，导致大量用户数据泄露。事件对电商的声誉和信任度造成了严重损害，也引发了用户对个人信息安全的担忧。

2.3 网络安全面临的挑战与问题

（1）技术发展带来的挑战：随着云计算、大数据、物联网等新技术的普及，网络安全边界变得模糊，数据流动更加复杂，给网络安全管理带来了新的挑战。（2）人员意识和技能不足：许多企业和组织对网络安全重视不够，员工缺乏足够的安全意识和技能，容易成为网络攻击的目标。（3）法律法规和监管体系不完善：当前网络安全法律法规还不够完善，监管体系也存在不足，导致一些网络安全事件难以得到有效的追责和处理。

3 计算机信息管理技术与网络安全的融合

3.1 信息管理与网络安全的内在联系

信息管理与网络安全之间存在深刻的内在联系，这两者的交融使得信息的保护和利用达到一个更高的水平。深入理解这种联系，对于构建一个安全、高效的信息系统至关重要。（1）信息管理是网络安全的前提和基础。信息管理涵盖了信息的收集、整理、存储、传输和使用等各个环节。在每一个环节中，都需要有相应的安全措施来确保信息的安全。例如，在信息的存储阶段，需要采用加密技术、访问控制等手段来保护数据的机密性，防止未经授权的访问。在信息的传输过程中，需要使用安全协议、防火墙等工具来确保数据的完整性和可用性，防止数据在传输过程中被篡改或丢失。没有完善的信息管理，网络安全就无从谈起。（2）网络安全是信息管理的必要保障。在一个开放的网络环境中，信息面临着来自各方面的威胁，如黑客攻击、病毒传播、恶意软件等。这些威胁不仅可能导致信息的泄露，还可能造成系统的崩溃，给组织带来重大的损失。因此，必须有强大的网络安全措施来预防和应对这些威胁，确保信息的安全。这包括定期的系统更新、病毒查杀、漏洞修复等措施，以及应对突发事件的应急预案[2]。（3）信息管理与网络安全相互促进，共同推动信息技术的发展。随着信息技术的不断进步，信息管理和网络安全的技术手段也在不断更新和完善。同时，信息管理和网络安全在实践中的融合应用也推动了二者的相互发展和进步。例如，通过引入先进的数据挖掘和分析技术，可以更有效地发现网络安全威胁，提高信息管理的效率和质量。反过来，加强信息安全管理也可以推动网络安全技术的进步，如更高级的加密算法、更安全的传输协议等。

3.2 信息管理技术在网络安全中的应用实践

随着信息技术的飞速发展，网络安全逐渐成为全球关注的焦点。在这个背景下，信息管理技术的运用成为了网络安全保障的重要一环。这些技术的应用不仅提升了网络安全的防护能力，也进一步推动了信息管理技术的发展和创新。（1）数据库安全技术是信息管理技术在网络安全领域的重要应用之一。数据库是企业和组织存储和管理核心数据的关键场所，因此其安全性至关重要。数据库加密技术通过对敏感数据进行加密，确保数据在存储和传输过程中不被非法访问。访问控制技术则通过设定权限，限制不同用户对数据库的访问和操作，防止未经授权的数据访问和篡改。审计追踪技术则能够记录数据库的操作日志，帮助管理人员及时发现异常行为并进行应对。（2）数据挖掘与分析技术在网络安全领域也发挥着重要作用。通过对网络流量、用户行为等大量数据的挖掘和分析，可以识别出潜在的安全威胁和异常行为，为安全预警和响应提供有力支持。这种技术的应用能够及时发现网络攻击的迹象，帮助企业和组织采取有效措施进行防范和应对。（3）数据备份与恢复技术是信息管理技术在网络安全领域的又一关键应用。在遭受攻击或故障时，能够及时恢复数据是减少损失、保障业务正常运行的关键。建立完善的数据备份与恢复机制，能够确保数据的可靠性和完整性，为企业在网络安全事件中的快速恢复提供有力保障[3]。（4）身份认证与访问控制技术也是信息管理技术在网络安全领域的重要应用。通过采用多因素认证、角色基于访问控制等机制，可以确保只有合法的用户才能访问敏感信息。这种技术的应用能够有效防止非法访问和恶意攻击，保护企业和组织的信息资产安全。

3.3 网络安全策略在信息管理中的体现

网络安全策略在信息管理中发挥着至关重要的作

用，它为组织提供了一个清晰、全面的安全框架，确保了信息的完整性、可用性和保密性。（1）网络安全策略为信息管理提供了明确的安全目标和指导原则。一个完善的网络安全策略会明确指出组织在信息管理过程中应达到的安全标准，为信息管理人员提供了明确的方向。这确保了所有与信息管理相关的活动都能够围绕这些目标进行，从而提高了整体的安全水平。（2）网络安全策略为信息管理提供了全面的安全保护措施。这些措施不仅覆盖了物理安全，如设备安全、数据存储设施的安全等，还包括了网络安全和应用安全。例如，策略中会明确如何防止未经授权的访问、如何对敏感数据进行加密、如何检测和应对恶意软件等。这些措施确保了信息从产生到存储、处理、传输到最终销毁的整个生命周期都能够得到有效的保护。（3）网络安全策略还为信息管理提供了持续的安全监控和改进机制。网络安全是一个持续的过程，需要定期评估和审计信息安全状况，及时发现和解决潜在的安全隐患。网络安全策略要求组织建立相应的监控机制，确保能够实时了解网络的安全状况，并在发现问题时迅速采取措施进行解决。同时，策略还鼓励组织进行持续的创新和改进，以适应不断变化的网络安全威胁[4]。

4 融合发展的策略与建议

在当前信息化、网络化日益普及的背景下，计算机信息管理技术与网络安全的融合发展成为确保信息安全、促进信息化健康发展的关键。针对这一融合发展的需求，本文提出以下策略与建议。（1）提升信息安全意识，强化人员培训。人是信息安全的第一道防线，因此提升信息安全意识至关重要。组织应加强对员工的信息安全教育和培训，提高他们对信息安全重要性的认识，掌握基本的信息安全知识和技能。同时，要建立健全的信息安全文化，使员工在日常工作中能够自觉遵守信息安全规定，主动防范和报告安全事件。（2）加强技术研发与创新，完善信息安全体系。技术创新是推动信息管理与网络安全融合发展的关键。应加大对信息安全技术研发的投入，推动技术创新，提升信息安全防护能力。同时，要完善信息安全体系，整合现有的信息管理和网络安全技术，形成一套完整、高效的信息安全解决方案。此外，还应加强与高校、科研机构等的合作，共同推进信息安全技术的研发和应用。（3）制定严格的法律法规，加大监管力度。法律法规是保障信息安全的重要手段。应制定和完善信息安全管理相关的法律法规，明确各方责任和义务，加大对违法行为的处罚力度。同时，要加强监管力度，建立健全的信息安全监管机制，对各类信息安全事件进行及时、有效的处置。此外，还应加强与国际社会的合作，共同应对跨国信息安全挑战。（4）促进产学研用深度融合。要实现信息管理与网络安全的融合发展，需要促进产学研用的深度融合。企业、高校和科研机构应共同建立合作平台，加强信息安全技术研发和人才培养。同时，应积极推广先进的信息安全技术和应用，推动信息安全产业的发展。

结束语

在计算机信息管理技术与计算机网络安全应用的研究之旅即将画上句号之际，我们不禁为这一领域的快速发展和广泛应用而感叹。随着技术的不断进步，信息管理与网络安全的结合将更加紧密，对维护信息安全和推动信息化建设的作用将愈发显著。展望未来，我们坚信，通过不断的研究与实践，我们能够构建一个更为安全、高效、可靠的信息管理体系，为各行各业的发展提供坚实的支撑。让我们携手前行，共创信息安全新篇章，迎接信息化社会的美好未来。

参考文献

[1]马骞.计算机信息管理技术在网络安全的应用[J].网络安全技术与应用,2020(02):14-15.

[2]胡恒金.论计算机信息管理技术在网络安全技术中的应用[J].网络安全技术与应用,2020(06):122-124.

[3]杨丽丽.网络安全中计算机信息管理技术的应用[J].黑龙江科学,2019,10(04):54-55.

[4]张建超.计算机信息管理技术与计算机网络安全应用[J].信息记录材料,2019,20(05):139-140.