网络安全等级保护下数据安全治理研究——现状与挑战

杨跃
西安医学院信息化处，陕西 西安 710021

摘　　要： 本文旨在探讨网络安全等级保护制度下的数据安全治理现状与挑战。随着互联网和大数据技术的飞速发展，数据安全问题日益凸显，给个人隐私、企业商业秘密以及国家信息安全带来了严重威胁。我国已建立网络安全等级保护制度，以提升网络安全水平，保障数据安全。然而，当前数据安全治理仍面临诸多挑战，如数据安全风险、法律法规实施力度不足、技术防护水平有待提高以及数据安全人才短缺等。本文通过分析现状与挑战，提出完善数据安全法律法规体系、强化数据安全治理体系建设、提高数据安全技术防护水平、加强数据安全人才培养以及增强全社会数据安全意识等对策建议，以期为从事数据安全治理行业人员提供有益参考。

关 键 词： 网络安全；等级保护；数据治理；数据安全治理体系

Research on data security governance under network security Level protection: Current Status and Challenges

Yang Yue
Information Department of Xi'an Medical University, Xi'an, Shaanxi 710021

Abstract: This paper aims to discuss the current situation and challenges of data security governance under the network security hierarchical protection system. With the rapid development of the Internet and big data technology, the problem of data security is becoming increasingly prominent, which brings serious threats to personal privacy, corporate business secrets and national information security. China has established a hierarchical protection system of network security to improve the level of network security and ensure data security. However, the current data security governance still faces many challenges, such as data security risks, the insufficient implementation of laws and regulations, the level of technical protection needs to be improved and the shortage of data security talents. This paper by analyzing the present situation and challenges, put forward the data security laws and regulations system, strengthen the data security management system construction, improve the level of data security technology protection, strengthen data security personnel training and enhance the whole society data security consciousness countermeasures, in order to provide personnel engaged in data security management industry reference.

Keywords: network security; level protection; data governance; data security governance system

一、引言

随着互联网、大数据、人工智能等新一代信息技术的飞速发展，数据已经成为国家基础性战略资源，网络安全和数据安全问题日益突出[1]。网络安全等级保护制度作为我国网络安全保障体系的核心制度，对于提升网络安全水平、保障数据安全具有重要意义。信息安全问题日益凸显，特别是数据安全问题已经成为我国网络安全领域面临的一大挑战。近年来，我国政府高度重视网络安全和信息安全，制定了一系列法律法规和政策文件，如《网络安全法》《信息安全技术网络安全等级保护基本要求》等，明确了网络安全等级保护制度[2]。在此背景下，研究网络安全等级保护下的数据安全治理具有重要的理论和实践意义。

本文首先分析了网络安全等级保护制度的基本概念和内涵，然后梳理了当前数据安全治理的研究现状，接着分析了网络安全等级保护下数据安全治理面临的挑战，最后提出了相应的对策和建议。

二、网络安全等级保护

（一）网络安全等级保护制度的背景与意义

随着信息技术的飞速发展，网络已经深入到我们生活的方方面面，网络信息系统已经成为国家安全、经济发展、社会稳定和公民权益的重要保障[3]。然而，网络信息系统面临着日益严重的安全威胁；如：黑客攻击、病毒感染、数据泄露等，给国家安全、公民权益和企业利益带来严重损害。因此，网络安全等级保护制度的实施，有助于提高我国网络信息系统的安全防护能力，降低网络攻击和信息安全风险[4]。

作者简介：杨跃（1992-2），男，汉族，陕西西安人，硕士，助理工程师
研究方向：网络安全、人工智能、数据挖掘与分析，邮箱：12979579391@qq.com

（二）网络安全等级保护制度的基本内容

等级划分：根据网络信息系统的业务特点、重要程度和可能面临的安全威胁，将其分为不同的安全等级，如一级、二级、三级等，级别越高，安全保护要求越严格[5]。

（1）基本要求：针对各个安全等级，制定相应的安全保护基本要求，包括组织管理、技术防护、安全审计、物理安全等方面，以确保网络信息系统在各个层面上都能得到有效保护。

（2）测评要求：为检验网络信息系统安全保护措施的有效性，制定测评要求，包括对安全管理、技术防护、安全事件响应等方面的检查和评估。

（3）安全设计技术要求：针对网络信息系统安全设计，提出相应技术要求，包括系统架构、软硬件选型、安全功能实现等方面，以确保系统在设计阶段就具备良好的安全性能。

（三）网络安全等级保护制度的实施与挑战

我国自实施网络安全等级保护制度以来，已经在网络安全保护方面取得了显著成效。然而，随着网络技术的不断发展和新型网络威胁的涌现，网络安全等级保护制度也面临着不断升级和完善的挑战[6]。

（1）技术防护水平有待提高：随着网络技术的不断发展，新型网络攻击手段不断涌现，我国在部分领域的技术防护水平仍需提高。

（2）数据安全人才短缺：网络安全等级保护制度的实施需要大量专业人才的支持，当前我国在网络安全人才培养方面仍存在一定程度的短缺。

（3）全社会数据安全意识不足：网络安全等级保护制度涉及到的不仅仅是技术问题，更是意识问题。当前我国全社会数据安全意识仍需提高。

（四）网络安全算法

网络安全是当今数字化时代中至关重要的一个领域，它涉及到保护计算机系统、网络和数据免受未经授权的访问、攻击和破坏。而网络安全算法则是网络安全的核心，它通过一系列复杂的数学和逻辑运算，实现了对网络攻击的检测、防御和响应。网络安全算法的重要性体现在以下几个方面：

（1）数据保护：随着大数据时代的到来，企业和个人的数据信息面临着前所未有的威胁。网络安全算法可以通过加密、哈希等手段，保护数据的完整性和机密性，防止数据泄露和篡改。

（2）身份认证：在网络世界中，身份认证是确保安全的第一步。网络安全算法可以通过多因子认证、生物识别等技术，实现对用户身份的准确识别和验证，防止恶意用户冒充合法用户进行攻击。

（3）入侵检测：网络攻击者常常通过各种手段隐藏自己的身份和行为，入侵检测算法可以通过分析网络流量、日志等信息，发现异常行为，及时发现和阻止网络攻击。

（4）防火墙和入侵防御：网络安全算法可以用于设计和实现防火墙和入侵防御系统，通过过滤和阻止恶意流量，保护网络和系统的安全。

网络安全算法的应用主要包括以下几个方面：

（1）加密算法：加密算法是网络安全的基础，它可以通过将数据转换为密文，保护数据的机密性和完整性。常见的加密算法包括对称加密、非对称加密和哈希算法等。

（2）认证算法：认证算法用于验证用户的身份和数据的来源，确保用户和数据的合法性。常见的认证算法包括数字签名、证书认证和生物识别等。

（3）安全协议：安全协议是一系列规则和协议，用于在网络中实现安全通信。常见的网络安全协议包括 SSL/TLS、IPSec 和 SSH 等。

（4）入侵检测和防御算法：入侵检测和防御算法用于检测和阻止网络攻击。常见的入侵检测和防御算法包括基于特征的检测、基于行为的检测和基于机器学习的检测等。

（5）安全分析和风险评估算法：安全分析和风险评估算法用于评估网络和系统的安全性和风险。常见的安全分析和风险评估算法包括威胁建模、漏洞扫描和风险评估等。

网络安全算法是网络安全的核心，它通过一系列复杂的数学和逻辑运算，实现了对网络攻击的检测、防御和响应。在当今数字化时代，网络安全算法的重要性日益凸显，它涉及到数据保护、身份认证、入侵检测和防火墙等方面。网络安全算法的应用广泛，包括加密算法、认证算法、安全协议、入侵检测和防御算法以及安全分析和风险评估算法等。只有通过不断研究和创新网络安全算法，才能有效地保护网络和数据的安全，确保数字化时代的稳定和繁荣。

三、数据安全治理研究现状及算法

（一）研究现状

随着信息技术的快速发展，数据已经成为国家、企业和个人重要的资产。然而，数据的安全问题也日益突出，数据的泄露、篡改、丢失等问题频发，给个人隐私、企业运营和国家安全带来了严重的威胁[7]。可以从以下几个方面进行概述：

（1）管理体系和政策法规

数据安全治理需要建立完善的管理体系和政策法规。在管理体系方面，企业需要建立数据安全管理组织架构，明确数据安全责任和义务，制定数据安全策略和流程，建立数据安全培训和考核机制等。政策法规方面，国家需要制定相关法律法规，明确数据保护的基本要求和标准，建立数据安全监管机制，加强对数据安全违法行为的处罚力度。

（2）技术手段和防护措施

数据安全治理需要利用先进的技术手段和防护措施来保护数据的安全。目前，加密技术、访问控制技术、安全审计技术、数据脱敏技术等技术手段在数据安全治理中得到了广泛应用。

（3）数据安全评估和监控

数据安全治理需要建立数据安全评估和监控机制，定期对数据安全进行检查和评估，发现数据安全风险和漏洞，及时采取措施进行整改和修复。目前，数据安全评估方法和技术主要包括安全风险评估、数据资产评估、安全能力评估等[9]。

（二）数据安全治理算法

数据治理是指对组织中的数据进行管理、监督和控制的过

程，以确保数据的质量、可靠性、安全性与合规性。在当今大数据时代，数据治理算法成为了数据治理的核心，它通过一系列复杂的数学和逻辑运算，实现了对数据的质量评估、清洗、转换和分析[8]。数据治理算法的重要性体现在以下几个方面：

（1）数据质量评估：数据治理算法的核心任务之一是对数据的质量进行评估。通过数据质量评估算法，可以识别出数据中的错误、不一致和缺失等问题，为数据清洗和转换提供依据。

（2）数据清洗：数据清洗是数据治理的重要环节，它通过对数据进行过滤、填充、转换等操作，提高数据的准确性和可靠性。数据清洗算法可以根据数据质量评估的结果，自动地对数据进行清洗和修正。

（3）数据转换：数据转换是指将数据从一种格式或结构转换为另一种格式或结构的过程。数据转换算法可以根据业务需求和数据用途，将数据进行重新组织和整合，使其更好地满足业务需求。

（4）数据分析：数据分析是指对数据进行统计、挖掘和分析，以提取有用信息和洞察。数据治理算法可以通过对数据进行预处理和特征提取，提高数据分析的准确性和效率。

数据治理算法的应用主要包括以下几个方面：

（1）数据质量评估算法：数据质量评估算法用于对数据进行质量评估，识别数据中的错误、不一致和缺失等问题。常见数据质量评估算法包括统计方法、机器学习方法和专家系统等。

（2）数据清洗算法：数据清洗算法用于对数据进行清洗和修正，提高数据的准确性和可靠性。常见数据清洗算法包括填充算法、转换算法和去重算法等。

（3）数据转换算法：数据转换算法用于将数据进行重新组织和整合，使其更好地满足业务需求。常见数据转换算法包括映射算法、编码算法和聚合算法等。

（4）数据分析算法：数据分析算法用于对数据进行统计、挖掘和分析，以提取有用信息和洞察。常见数据分析算法包括统计分析算法、机器学习算法和数据挖掘算法等。

数据治理算法是数据治理的核心，它通过一系列复杂的数学和逻辑运算，实现了对数据的质量评估、清洗、转换和分析。在当今大数据时代，数据治理算法的重要性日益凸显，它涉及到数据质量评估、数据清洗、数据转换和数据分析等方面。数据治理算法的应用广泛，包括数据质量评估算法、数据清洗算法、数据转换算法和数据分析算法等。只有通过不断研究和创新数据治理算法，才能有效地提高数据的质量和管理水平，为组织的决策和业务发展提供有力支持。

四、网络安全等级保护下数据安全治理面临的挑战

网络安全等级保护制度下，数据安全治理面临诸多挑战。首先，法律法规和标准体系尚不完善，部分企业和机构对法律法规的理解和执行力度不足。其次，数据安全技术和防护能力有待提高，尤其是面对新兴技术如人工智能、大数据、云计算等，现有的防护体系难以应对复杂的网络攻击手段[10]。此外，数据安全人才短缺，尤其在关键技术领域，如数据加密、安全存储、安全审计等，专业人才储备不足。

五、对策与建议

（一）加强技术研发与创新

面对不断演变的安全威胁，我们需要加强网络安全技术的研发与创新。投入更多资源进行安全技术研发，同时也可以设立专项资金支持网络安全技术的研究。

（二）提高数据安全治理能力

加强对企业数据安全治理能力的培养和提高。通过组织数据安全培训、研讨会和论坛等形式来实现，邀请法律、技术专家和企业代表分享经验和最佳实践。

（三）强化数据安全监控与预警

为了及时发现和应对数据安全威胁，政府和企业应强化数据安全监控与预警能力。这可以通过建立数据安全监控中心、采用先进的数据安全检测技术等手段来实现。

六、结论

网络安全等级保护下的数据安全治理是一项系统性、综合性的工作，需要政府、企业和个人共同努力。面对当前的挑战，我国应加强数据安全技术研发与应用，完善数据安全管理机制，落实数据安全法规与政策，平衡数据安全与隐私保护，不断提高数据安全治理水平，以确保网络空间的安全与稳定。

本文针对网络安全等级保护下的数据安全治理进行了研究，总结出现状与挑战，并提出了相应的对策和建议。

参考文献：

[1] 孙远运. 建立铁路网络空间安全治理新格局的实践探索［J］. 铁路计算机应用，2021，30（11）：1-4.

[2] 刘爱娇，孙越洋. 深化公安改革促进网络安全等级保护工作的思考［J］. 网络安全技术与应用，2021（5）：149-152.

[3] 马力，祝国邦，陆磊.《网络安全等级保护基本要求》（GB/T 22239—2019）标准解读［J］. 信息网络安全，2019（2）：77-84.

[4] 赵少飞. 浅谈等保测评中企业面临的安全风险和应对措施［J］. 网络安全技术与应用，2022（10）：98-99.

[5] 马玉州. 等保2.0时代普通高校等级保护工作实践［J］. 网络安全技术与应用，2021，247（7）：97-98.

[6] 吴宝琦，李若琛. 信息网络安全等保建设的思考［J］. 信息系统工程，2023（1）：125-127.

[7] 王国丽. 论网络安全等级保护的演变及主要变化［J］. 数字通信世界，2022（2）：91-93.

[8] 张炜，宋海萍，袁博. 等保2.0要求下的城轨云内部管理网信息系统安全管理工作的思考［J］. 网络安全技术与应用，2022（9）：113-114.

[9] 陈广勇，祝国邦，范春玲.《信息安全技术网络安全等级保护测评要求》(GB/T28448 - 2019）标准解读［J］. 信息网络安全，2019(7) :1 - 7

[10] 李越，张振川，林川倩. 网络安全等级保护下数据安全治理初探［J］. 铁路计算机应用，2023，32(2) :78 - 81.