0 8

2 11801 86.0000 00.0000 0000 0.0000 0.000 12.1330 6

模拟时间：2022 年 1 月 1 日 12:00:00 UTCG ~ 2022 年 1 月 2 日 12:00:00 UTCG。

步长：60s；

操作系统：Windows 10 x64

CPU：英特尔酷睿 i7-10700，CPU 架构：Comet Lake-S，核心主频：3.8GHz, 加速频率：5.1GHz，三级缓存大小：16M，8 核心 16 线程，125W 热设计功耗。

GPU：NVIDIA GeForce GTX 860M，具备 640 个 CUDA 核心，配备 4096MB 的显存容量。

表 1 仿真时间与加速比

数据组数	CPU 串行计算时间 (s)	CPU 并行计算时间 (s)	加速比
1	3.2	36.3	0.088
10	11.7	40.4	0.290
100	70.4	73.4	0.959
500	353.1	150.2	2.351
1000	738.7	187.9	3.931
5000	4206.6	550.3	7.644
10000	8560.3	901.1	9.500

（2）计算结果对比：

实验数据基于 NORAD 发布的双行轨道参数文件，共处理了 1000 颗卫星的数据。这些数据的覆盖范围按纬度划分为以下几组：-5° 至 5° ，-10° 至 10° ，-30° 至 30° ，-60° 至 60° ，以及 -90° 至 90° 。在正式发布的环境中，使用 SGP4 轨道模型对这些卫星的轨道进行了仿真分析，对比运算效率与加速比，如表 2 所示。

表 2 仿真时间与加速比

覆盖范围 / 纬度	CPU 串行计算时间 (s)	CPU 并行计算时间 (s)	加速比
-5~5	738.1	887.3	0.832
-10~10	968.5	1042.8	0.929
-30~30	4205.8	1535.5	2.739
-60~60	7120.3	1917.7	3.713
-90~90	13457.2	2265.2	5.941

由仿真结果可知，随着数据组数的增加，CPU 串行计算时间呈正比式增长，单 CPU 并行计算时间增长速度较缓慢。因为对于数据量较少时，CPU 并行需要线程池的初始化和线程的申请以及执行数据划分逻辑，所消耗的时间占总的计算时间大。因此对于数据量较小的计算使用 CPU 并行的效率比 CPU 串行耗时更多。当涉及到 SGP4 轨道模型的仿真，并且轨道数量超过 500 条时，为了提升仿真的效率，可以考虑采用 CPU 并行处理技术。但整体运行加速比随着数据量的变大而增大，但由于硬件条件的限制，其加速比上限将受限于 CPU 的核心数。

5 结语

本文提出了基于并行计算的星座覆盖分析系统设计方法，研究了任意多边形闭合区域的网格点划分方法、任意闭合区域的可见性计算方法、星座轨道并行计算处理方法以及星座覆盖并行计算处理方法，开发实现了基于并行计算的星座覆盖分析系统，并对上述方法进行了实验验证。实验结果表明当计算处理的数据量达到一定的规模后，采用并行计算的方法能够大幅减少数据处理的时间，为星座覆盖分析提供了高效的数据处理解决方案。

参考文献

[1] 韩蕾, 陈磊, 周伯昭. SGP4/SDP4 模型用于空间碎片轨道预测的精度分析[J].中国空间科学技术, 2004, 24(4):75-91.

[2] 刁宁辉, 刘建强, 孙从容,等. 基于 SGP4 模型的卫星轨道计算[J]. 遥感信息,2012, 27(4):56-71.

[3] 韦栋, 赵长印. SGP4/SDP4 模型精度分析[J]. 天文学报, 2009, 50(3):312-337.

[4] 吴金兰.多柔体系统约束方程的牛顿-拉斐逊算法研究.山西师范大学学报.2010,3,10.

[5] 丁永祥, 夏巨谌.任意多边形的Delaunay三角剖分.国家科技图书文献中心.1994-04-004.

[6] Kelso T S C. Validation of SGP4 and IS-GPS-200D Against GPS Precision Ephemerides[C]// 2007

[7] Hoots F R, Roehrich R L. Models for Propagation of NORAD Element Sets[J].Spacetrack Report, 1980.

[8] FELIX R H，RONALD L R. Space track report No.3-models for propagation of NORAD element sets[R].Peterson: Aerospace Defence Command，United States Air Force，1980：1-79.

 DOI: https://doi.org/10.12349/iser.v6i9.7442

Research on network information security management in enterprise informatization construction

Lei Yang

Inner Mongolia Civil Aviation Airport Group Co., Ltd. Hohhot Branch, Hohhot, Inner Mongolia, 010000, China

Abstract

With the accelerated digital transformation and widespread adoption of information technology, enterprise informatization has become a critical pathway to enhance competitiveness. However, the escalating cybersecurity threats have made information security management a major challenge that enterprises must confront. Starting from the practical needs of enterprise informatization, this study provides an in-depth analysis of the importance of network information security management. It systematically explores six key security management strategies: technical protection, institutional norms, personnel training, risk control, technological innovation, and supply chain management. The research reveals that establishing a multi-layered and comprehensive security protection system forms the foundation for ensuring enterprise information security. Moreover, the organic integration of technical measures and management practices is crucial for enhancing security effectiveness.

Keywords

enterprise informatization; network security; information security management

企业信息化建设中的网络信息安全管理研究

杨蕾

内蒙古自治区民航机场集团有限责任公司呼和浩特分公司，中国 · 内蒙古 呼和浩特 010000

摘　要

随着数字化转型进程的加速推进和信息技术的广泛应用，企业信息化建设已成为提升竞争力的关键途径，然而网络安全威胁的日益严峻使得信息安全管理成为企业必须面对的重大挑战，本研究从企业信息化建设的实际需求出发，深入分析了网络信息安全管理的重要性，系统探讨了包括技术防护、制度规范、人员培养、风险管控、技术创新和供应链管理在内的六大安全管理策略，研究发现，构建多层次、立体化的安全防护体系是保障企业信息安全的基础，而将技术手段与管理措施有机结合则是提升安全防护效能的关键。

关键词

企业信息化；网络安全；信息安全管理

1 引言

在全球数字经济蓬勃发展的背景下，企业信息化建设已经从可选项转变为必选项，成为企业保持市场竞争优势的重要支撑，但与此同时，网络攻击手段的不断升级、数据泄露事件的频繁发生，以及各类安全威胁的层出不穷，使得网络信息安全问题日益凸显，成为制约企业信息化健康发展的关键因素，如何在推进信息化建设的同时确保网络信息安全，已经成为企业管理者必须深入思考和着力解决的核心问题，基于此，本文将从企业信息化建设的现实需求出发，全面剖析网络信息安全管理的重要性，并提出切实可行的管理策略，以期为企业构建安全可靠的信息化环境提供理论指导和实践参考。

2 企业信息化建设中的网络信息安全管理重要性

2.1 确保核心业务数据安全，防范机密信息泄露风险

企业在信息化建设过程中产生和积累的海量数据已成为其最宝贵的资产之一，这些数据涵盖了客户资料、财务信息、研发成果、战略规划等核心商业机密，一旦发生泄露将给企业带来难以估量的损失，网络信息安全管理的首要任务便是为这些关键数据筑起坚固的防护屏障，防止内部人员的恶意窃取和外部黑客的非法入侵 [1]。在当今复杂多变的网络环境中，数据泄露的途径日趋多样化，既包括传统的网络攻击手段，也涉及社会工程学等新型威胁方式，因此企业必须建立全方位的数据安全防护机制，从数据的产生、传输、存储到使用的各个环节实施严格管控，确保核心业务数据始终

【作者简介】杨蕾（1987–），女，中国甘肃隆德人，本科，工程师，从事网络信息安全研究。

处于安全可控的状态之下。

2.2 维护系统运行稳定性，保障企业运营连续性

信息系统的稳定运行是企业正常开展各项业务活动的基础保障，而网络安全事件往往会导致系统崩溃、服务中断等严重后果，直接影响企业的生产经营活动。勒索软件攻击、分布式拒绝服务攻击等恶意行为可能使企业的核心业务系统陷入瘫痪，造成订单处理延误、生产线停工、客户服务中断等一系列连锁反应，进而导致经济损失和声誉受损，强化网络信息安全管理能够有效预防和抵御各类网络攻击，确保企业信息系统的高可用性和业务连续性。此外，完善的安全管理体系还能够帮助企业建立快速响应和灾难恢复机制，即使在遭受攻击的情况下也能够迅速恢复系统运行，将损失降至最低，从而为企业的稳健发展提供坚实保障。

2.3 满足合规监管要求，规避法律责任和经济损失

随着各国对数据安全和隐私保护的重视程度不断提升，相关法律法规日趋严格和完善，对企业的网络信息安全管理提出了更高要求，欧盟《通用数据保护条例》、中国《网络安全法》《数据安全法》等法规的实施，明确规定了企业在数据收集、处理、存储等方面的合规义务，违反相关规定将面临巨额罚款和法律制裁 [2]。企业必须建立符合监管要求的安全管理体系，确保在数据处理的全生命周期中严格遵守相关法律法规，这不仅是企业履行社会责任的体现，更是避免法律风险和经济损失的必要举措。同时，良好的安全合规管理还能够提升企业的市场信誉和客户信任度，为企业赢得更广阔的发展空间和更多的商业机会，成为企业核心竞争力的重要组成部分。

3 企业信息化建设中的网络信息安全管理策略

3.1 构建多层次技术防护体系，实现纵深安全防御机制

企业应当采用纵深防御的理念构建多层次的技术防护体系，形成从网络边界到核心数据的立体防护架构，在网络边界层面部署高性能防火墙、入侵检测系统和入侵防御系统，实时监控和阻断外部威胁，在网络内部实施网络分段和访问控制，将不同安全级别的系统和数据进行隔离，防止威胁的横向扩散，针对终端设备部署终端安全管理平台，统一管理防病毒软件、主机防火墙和设备准入控制，确保每一个接入点的安全性。

在应用层面实施 Web 应用防火墙、数据库审计系统等专业防护措施，对应用程序的输入输出进行严格检查，防范 SQL 注入、跨站脚本等常见攻击，同时部署数据防泄露系统，对敏感数据的流转进行全程监控和管控，防止内部数据的非授权外传，在数据层面采用加密技术对重要数据进行加密存储和传输，确保即使数据被窃取也无法被解读利用。

3.2 建立完善制度规范体系，强化安全管理标准化程度

制度建设是网络信息安全管理的基础工作，企业需要建立涵盖组织架构、岗位职责、操作流程、应急预案等各个方面的完整制度体系，首先明确安全管理的组织架构和责任分工，设立专门的信息安全管理部门或安全管理委员会，明确各级管理人员和技术人员的安全职责，建立自上而下的安全责任体系，确保安全管理工作有人抓、有人管、有人负责 [3]。

制定详细的安全操作规程和管理流程，包括账号管理、权限分配、数据备份、系统维护、安全审计等各项日常工作的标准化操作程序，每一项操作都应有明确的执行步骤、审批流程和记录要求，避免因操作不当造成的安全隐患，建立安全事件分级分类标准和应急响应预案，明确不同级别安全事件的处置流程和责任人，确保在安全事件发生时能够快速、有序地进行处置。

3.3 加强人员安全意识培养，提升全员网络安全防护能力

人是网络安全防护体系中最关键也是最薄弱的环节，企业必须高度重视员工安全意识的培养和安全技能的提升，建立分层分类的安全培训体系，针对不同岗位、不同层级的人员制定差异化的培训方案，对于普通员工重点培训基础安全知识、安全操作规范和常见威胁识别方法，对于技术人员则加强专业安全技能和最新攻防技术的培训，对于管理人员着重培养安全管理理念和决策能力。

创新培训方式方法，采用案例分析、模拟演练、在线学习等多种形式开展培训活动，特别是通过真实案例的剖析让员工深刻认识到安全威胁的严重性和防护的必要性，定期组织钓鱼邮件测试、社会工程学演练等实战化训练，检验员工的安全意识水平和应对能力，对于测试中暴露出的问题进行针对性的强化培训，营造浓厚的安全文化氛围，通过安全知识竞赛、安全主题活动、安全标语宣传等方式，让安全意识深入人心，成为企业文化的重要组成部分。

3.4 实施动态风险评估管控，建立预警响应处置联动机制

风险管理是网络信息安全管理的核心环节，企业需要建立动态的风险评估和管控机制，持续识别、评估和应对各类安全风险，构建全面的资产台账和风险清单，对企业的信息资产进行分类分级管理，明确各类资产的重要程度和面临的主要威胁 [4]，采用定性和定量相结合的方法进行风险评估，综合考虑威胁发生的可能性和影响程度，确定风险等级和优先处置顺序。

部署安全态势感知平台，整合各类安全设备和系统的日志信息，运用大数据分析和人工智能技术进行威胁检测和行为分析，实现对安全风险的实时监测和预警，建立分级分类的预警机制，根据威胁的严重程度和紧急程度采取不同的响应措施，对于高危威胁立即启动应急响应流程，对于中低风险制定整改计划并限期完成，构建安全运营中心，配备专业的安全分析人员进行 7×24 小时的安全监控和事件处置。

建立与外部安全机构的合作机制，及时获取最新的威胁情报和漏洞信息，提前做好防范准备，定期开展渗透测试、