

# 计算机技术在保障电子信息安全中的应用研究

## ——评《中国电子信息工程科技发展研究:计算机应用专题》

随着信息技术的飞速发展,计算机已经应用到社会的各个领域,为人们的生活和工作带来了极大便利。然而,计算机技术的广泛应用也带来了一系列信息安全问题,如信息泄露、数据篡改、网络攻击等。这些问题不仅给个人和企业带来巨大的经济损失,还可能危及到国家安全。因此,如何保障电子信息安全已经成为亟待解决的问题。

我国高度重视计算机的应用发展,大数据、人工智能、云计算、5G等新一代信息技术与国民经济及国家安全等领域深度融合,推动了各领域数字化转型与智能化升级,促进了相关新兴数字产业的快速发展。《中国电子信息工程科技发展研究:计算机应用专题》一书深入介绍了我国计算机应用发展现状,全书共6个章节。第1章介绍了计算机产业在全球各国的发展态势,包括计算机融入产业发展、助力产业智能化、助力抵御疫情及应用多元化。第2章阐述了我国计算机的发展现状,如“数字中国”战略的稳步推进、数字乡村的蓬勃发展、智慧教育的快速发展及应用技术的持续创新。第3章探讨了对我国计算机产业未来的展望,研判了发展方向,并提出了相应的建议举措。第4章重点研究了智能制造、数字抗疫、智慧远程医疗、智慧教育、智慧农业与数字乡村、电子商务、自动驾驶、数联网和人机融合等9个领域的技术热点和亮点,并提出了相关发展建议。第5章讲述了相关领域的年度热词。第6章介绍了该领域的相关指标。

编者指出,信息技术正在推动全球经济进入新时期,计算机技术逐渐成为变革经济发展模式的主导力量。计算机应用与产业融合的不断深入,推动了智能制造、自动驾驶、电子商务等新兴领域的飞速发展,助力各类实体抵御疫情风险。随着数字化、网络化、智能化为特征的信息化浪潮蓬勃兴起,大量关系国计民生的数据和个人数据逐渐进入互联网领域。这也带来了电子信息安全问题,需要引起高度重视。

笔者认为,计算机技术在保障电子信息安全方面具有重要作用,通过不断研究和应用计算机技术,可有效保障电子信息安全。具体来讲,主要是加强以下方面的技术。一是加密技术。加密技术是保障电子信息安全的重要手段之一。通过加密处理信息,可以使得未经授权的人员无法获取到原始信息。常用的加密技术包括对称加密算法和非对称加密算法。对称加密算法是指加密和解密使用相同密钥,如DES、AES等;非对称加密算法是指加密和解密使用不同密钥,如RSA、ECC等。二是数字签名技术。数字签名技术是一种用于验证信息完整性和身份认证的技术。通过数字签名处理信息后,可确保信息在传输过程中不被篡改,且可确认信息来源。目前,常用的数字签名技术含基于公钥的数字签名和基于私钥的数字签名。三是访问控制技术。访问控制技术是一种用于限制用户对系统资源的访问权限的技术。通过对用户进行身份认证和权限分配,可确保只有经过授权的用户才能访问系统资源。常用的访问控制技术包括基于角色的访问控制和基于属性的访问控制。四是入侵检测技术。入侵检测技术是一种用于发现和防止网络攻击的技术。通过分析网络流量可以发现异常行为并采取相应措施。目前,常用的入侵检测技术有基于签名的入侵检测和基于异常的入侵检测,来共同保障电子信息安全。五是安全审计技术。安全审计技术是一种用于记录和分析系统安全事件的技术。通过记录和分析系统安全事件,可发现潜在安全问题并及时采取相应措施。

总之,计算机技术在保障电子信息安全方面具有重要作用。通过应用加密技术、数字签名技术、访问控制技术、入侵检测技术和安全审计技术,可有效保障电子信息安全。然而,计算机技术在电子信息安全中仍然面临着许多挑战,需要不断进行研究和改进。加强计算机技术在电子信息安全中的应用和研究,可为解决电子信息安全问题提供有力支持,为构建安全、可信的信息社会做出贡献。

(周玉红/山东省社会信用中心/高级工程师)



书名:中国电子信息工程科技发展研究:计算机应用专题  
作者:中国信息与电子工程科技发展  
战略研究中心  
出版社:科学出版社  
ISBN:9787030730701  
出版时间:2022年9月  
定价:88元