



网络信息安全 工程技术与应用分析

潘 霄 葛维春 全成浩 胡 博 吴克河 潘明惠◎著

- ◎ 系统总结了最新**网络信息安全**工程理论和研究成果。
- ◎ 汇集了国家重大**科技攻关项目**与信息安全示范工程的经验
- ◎ 全面介绍了**信息安全**的基本理论、基础知识和发展趋势
- ◎ 包含**安全系统设计**、**安全防护体系**、**身份认证**与**授权管理**系统
- ◎ 介绍了**风险评估**方法、**数据备份**与**灾难恢复**、网络信息安全等级保护

清华大学出版社



网络信息安全 工程技术与应用分析

----- 潘 霄 葛维春 全成浩 胡 博 吴克河 潘明惠◎著 -----

清华大学出版社
北 京

内 容 简 介

本书结合作者组织和参加国家重大科技攻关项目“电力系统信息安全示范工程”、国家 863 项目“电力二次系统安全防护体系研究”以及国网公司 SG186、SG-ERP 信息安全等级保护及保障体系工程的实践经验,本着力求反映信息安全技术的最新发展和理论与工程实践相结合的原则而编写。

全书共分为 10 章,主要包括国内外网络信息安全工程技术发展趋势、我国信息安全重大政策及发展方向、网络信息安全工程基本原理、网络信息安全工程技术领域基础知识及最新技术、网络信息安全风险评估方法与应用分析、网络信息安全系统设计与应用分析、网络信息安全防护体系及应用分析、网络信息安全身份认证与授权管理系统及应用分析、数据存储备份与灾难恢复技术及应用分析、网络信息安全等级保护及应用分析、互联网络空间安全战略与应用分析,以及在网络信息安全工程实践中成功的案例。

本书的突出特点是系统总结了运用最新网络信息安全工程理论和最新研究成果,组织和参加网络信息安全工程实践取得的成功案例。读者通过本书既可以学习网络信息安全工程理论和基础知识,互联网络空间安全战略及网络信息安全最新技术,也可以通过大量实例掌握网络信息安全工程组织、管理和技术实现方法。本书可作为高等院校、能源电力等行业的培训教材,也可以作为企事业单位从事信息安全工程工作的管理人员和工程技术人员的参考工具用书。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

网络信息安全工程技术与应用分析 / 潘霄等著. —北京:清华大学出版社, 2016

ISBN 978-7-302-43610-2

I. ①网… II. ①潘… III. ①计算机网络—安全技术—研究 IV. ①TP393.08

中国版本图书馆 CIP 数据核字(2016)第 077561 号

责任编辑:冯志强 薛 阳

封面设计:吕单单

责任校对:胡伟民

责任印制:杨 艳

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦 A 座 邮 编:100084

社总机:010-62770175 邮 购:010-62786544

投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn

质量反馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

印 刷 者:清华大学印刷厂

装 订 者:北京市密云县京文制本装订厂

经 销:全国新华书店

开 本:185mm×260mm 印 张:20.75 插 页:1 字 数:535 千字

版 次:2016 年 6 月第 1 版

印 次:2016 年 6 月第 1 次印刷

印 数:1~4000

定 价:49.00 元

产品编号:069001-01

This book is based on practical experience of organizing and participating in the major national scientific and technological project "Power System Information Security Demonstration project", the National 863 project "Power Secondary System Security Protection System Research" and the State Grid Corporation of SG186, SG-ERP of hierarchical protection of information security and the security system projects, and in principle of reflecting the latest development of information security technology and engineering practice.

This book contains 10 chapters. The main content is as follows: the domestic and international development trends of information security engineering technology, China's information security policy and the development direction of information security, the fundamental principle of information security engineering, the fundamental knowledge and the latest technology of information security engineering field, the design, application and analysis of information security system, identity authentication and authorization management system, data storage backup and disaster recovery system, network information security hierarchical protection, interconnection network space security strategy, and the successful cases in the network information security in engineering practice.

The outstanding feature of this book is to systematically summarize the application of the latest network information security engineering theory and the latest research results, and the successful cases from the personal organization and participation in network information security engineering practice. Readers can not only learn the network information security engineering theory and the fundamental knowledge, interconnection network space security strategy and the latest technology of network information security, but also grasp the method of organizing and managing the network information security engineering through a large number of practical examples. It is a valuable reference which elaborates network information security technology and engineering application analysis. It can be used as the textbook for institutions of higher learning or training materials for energy and electric power enterprises, or as the reference book for management and technical personnels of enterprises and institutions engaged in information security engineering.

本书编写人员

著者 潘霄 葛维春 全成浩 胡博 吴克河 潘明惠

前言 潘明惠

第1章 绪论 葛维春、刘刚、周雨田、胡全贵

第2章 网络信息安全工程基本理论 全成浩、王漪、黎辉、杨大威、栾敬钊

第3章 网络信息安全工程基础知识 刘文娟、杨海峰、吴菲、陈力、王跃东

第4章 网络信息安全风险评估方法与应用分析 胡博、鲁顺、夏宗泽、祝榕岭

第5章 网络信息安全系统设计与应用分析 吴克河、李广野、潘洪建、苏畅、祁广源

第6章 网络信息安全防护体系及应用分析 孙刚、刘国威、张松、高海波、戚欣革

第7章 身份认证与授权管理系统及应用分析 杨万清、王泽宁、雷振江、潘宁、隋佳新

第8章 数据存储备份与灾难恢复技术及应用分析 杨轶、潘邈、吕旭明、张忠林、潘琪

第9章 网络信息安全等级保护及应用分析 陈文康、尹晓华、刘永昌、刘坤、金星

第10章 网络空间信息安全战略及应用分析 潘霄、刘凯、金昱、周英杰、张凤军

前 言

人类先后经历了农业革命、工业革命、信息革命。每一次产业技术革命，都给人类的生产、生活带来了巨大而深刻的影响。现在，以互联网为代表的信息技术日新月异，引领了社会生产的新变革，创造了人类生活新空间，拓展了国家治理新领域，极大地提高了人类的认识水平，人们认识世界、改造世界的能力得到了极大提高。互联网作为 20 世纪最伟大的发明之一，把世界变成了“地球村”。全世界进入互联网 3.0 万物互联时代，2015 年，全球网民数量已接近人口总数的一半。中国网民数量早在 2008 年就跃居全球第一，目前仍在快速增长中。截至 2015 年 6 月，中国网民规模已达 6.68 亿人，超过整个欧盟的总人口数量。互联网普及率为 48.8%，其中，农村网民规模达 1.86 亿，与 2014 年年底相比增加 800 万。“十二五”期间，互联网经济在中国 GDP 中占比持续攀升，2014 年达到 7%，占比超过美国。

自 2014 年 2 月中央网络安全与信息化领导小组成立以来，习近平主席就网络安全与信息化重要性，多次强调指出“没有网络安全，就没有国家安全”、“没有信息化，就没有现代化”、“现在人类已经进入互联网时代这样一个历史阶段，这是一个世界潮流，而且这个互联网时代对人类的生活、生产、生产力的发展都具有很大的进步推动作用”、“网络信息是跨国界流动的，信息流引领技术流、资金流、人才流，信息资源日益成为重要生产要素和社会财富，信息掌握的多寡成为国家软实力和竞争力的重要标志”、“网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进、统一实施。做好网络安全和信息化工作，要处理好安全和发展关系，做到协调一致、齐头并进，以安全促发展、以发展促安全，努力建久安之势、成长治之业”。

信息技术的发展拓展了人类感知、处理、存储、传递的能力，为人类开拓了崭新的生存空间。这种能力渗透到各行各业，显示了任何人，在任何地方，任何时间，高效高速地完成计算、通信、控制的潜能，使人类进入了无限遐想的信息革命时代。中国工程院沈昌祥院士，在谈到信息时代网络安全的重要性时强调：网络已经成为继陆、海、空、天之外的国家第 5 大主权空间。正如美国著名未来学家托夫勒所预言：“计算机网络的建立与普及将彻底地改变人类生存及生活的模式，而控制与掌握网络的人就是主宰。谁掌握了信息，控制了网络，谁就将拥有整个世界”。网络安全关系到国家安全，控制网络空间，就可以控制一个国家的经济命脉、政治导向和社会稳定。由于互联网信息技术以几何级数爆炸式增长、与相关领域快速融合和治理规范的缺失，在国内和国际层面上，网络虚拟空间都潜藏着诸多风险，包括网络恐怖主义在内的种种不法行为和有害信息，给各国的主权安全、民生经济等带来了严峻的现实挑战。信息是我们所处时代人类社会发展的主要战略资源，网络信息安全危及国家的政治、军事、经济、文化、社会生活的各个方面，已成为影响国家

大局和长远利益的重大战略问题。网络信息安全保障能力是 21 世纪综合国力、经济竞争实力和生存能力的重要组成部分, 是世界各国在奋力攀登的制高点。

本书结合作者组织和参加国家重大科技攻关项目“电力系统信息安全示范工程”、国家 863 项目“电力二次系统安全防护体系研究”以及国家电网公司 SG186、SG-ERP 信息安全等级保护及保障体系工程的实践经验, 本着力求反映信息安全技术的最新发展成果, 以及理论与工程实践相结合的原则而编写。全书共分为 10 章: 第 1 章分析国内外网络信息安全工程技术发展趋势, 我国信息安全重大政策及发展方向; 第 2、3 章介绍网络信息安全工程技术基本理论、信息安全工程技术领域基础知识及最新技术; 第 4 章探讨网络信息安全系统设计与应用分析; 第 5 章阐述网络信息安全风险评估方法与应用分析; 第 6 章分析网络信息安全防护体系与应用; 第 7 章探讨网络信息安全身份认证与授权管理系统与应用分析; 第 8 章介绍数据存储备份与灾难恢复系统与应用分析; 第 9 章阐述网络信息安全等级保护与应用分析; 第 10 章分析互联网络空间安全战略与应用; 并介绍了在网络信息安全工程实践中成功的案例。

近年来, 互联网信息技术飞速发展, 在人们面前展示出一幅美好的画卷, 同时, 网络空间信息安全也受到严重的威胁, 党中央和国务院已将网络空间安全与信息化同时提升到国家战略。作者长期从事信息化与网络信息安全工程研究, 在国内外发表过大量文章、报告和培训讲课, 深深地感到我们与先进国家相比还有一定差距, 挑战与机遇并存, 希望与困难同在, 我们必须抓住机遇迎接挑战, 满怀希望战胜困难。

本书的突出特点是系统总结了最新网络信息安全工程理论和最新研究成果, 运用社会发展系统动力学原理, 组织和参加网络信息安全工程实践取得的成功案例。读者通过本书既可以学习网络信息安全工程理论和基础知识, 互联网络空间安全战略及网络信息安全最新技术, 也可以通过大量实例掌握网络信息安全工程组织、管理和技术实现方法, 是一本网络信息安全工程技术与应用分析的工具书。可作为高等院校、能源电力等行业培训教材, 也可以供企事业单位从事信息安全工程相关工作的管理人员和工程技术人员参考。

本书编著出版, 衷心感谢国家电网公司吴玉生总信息师、李向荣副总工程师、刘建明主任、王继业主任、吴杏平主任, 中国电力科学研究院周孝信院士、于尔铿老师、刘广一博士、赵君总经理、哈尔滨工业大学徐殿国院长、陈学允老师、柳焯老师、李志民老师, 中国科学院沈阳计算技术研究所李彤、王素香研究员等人多年来的关心帮助与支持。衷心感谢辽宁省电力有限公司有关部门、基层单位同志们的大力支持, 感谢国家科技部及国家商用密码管理办公室组织专家、教授的指导和帮助, 感谢辽宁省电力有限公司经济技术研究院、华北电力大学电力信息技术工程研究中心、为本书编辑出版发行给予的大力支持和帮助。由于时间仓促, 作者水平有限, 书中的内容难免有疏漏或不妥之处, 敬请读者批评与指教。

潘明惠

2016 年 1 月 16 日于沈阳

目 录

第 1 章 绪论	1
1.1 背景及意义	1
1.2 国内外网络信息安全发展简述	2
1.2.1 国际网络信息安全工程技术发展历程	2
1.2.2 我国网络信息安全发展历程及趋势	3
1.2.3 国际网络信息安全工程技术发展新趋势	4
1.2.4 我国电力信息安全工程技术发展的主要特点	6
1.3 2014 年以来我国网络信息安全的重大事件	9
1.3.1 网络安全与信息化已经上升为国家战略	9
1.3.2 网络信息安全法律法规体系日趋完善	9
1.3.3 网络信息安全国际合作全面展开	10
1.4 网络信息安全工程技术面临的新挑战	11
1.4.1 网络信息安全工程技术存在的问题	11
1.4.2 信息化新阶段的网络信息安全	12
1.4.3 信息安全工程技术主要研究方向	15
第 2 章 网络信息安全工程基本理论	17
2.1 信息化工程基本理论	17
2.1.1 社会发展系统动力学原理简化模型	17
2.1.2 信息化是人类社会发展的必然趋势	18
2.1.3 国家信息化定义及体系六要素	22
2.1.4 中国特色的信息化道路主要特征	25
2.1.5 信息化在企业生存发展中的地位与作用	26
2.1.6 信息化与工业化深度融合	28
2.2 网络信息安全工程基本原理	31
2.2.1 网络信息安全工程基本原理	31
2.2.2 网络信息安全工程基本策略	32
2.2.3 电力系统信息网络安全“三大支柱”	34
2.2.4 基于主动意识的信息网络安全综合防护	36
2.3 网络信息安全常用典型标准模型	38
2.3.1 OSI 开放系统互连参考模型	38

2.3.2	TCP/IP 参考模型	41
2.3.3	OSI 与 TCP/IP 参考模型应用差异	43
2.3.4	网络信息安全体系安全服务机制	44
第 3 章	网络信息安全工程基础知识	47
3.1	国家信息安全有关法律法规	47
3.1.1	国家安全法有关信息安全内容	47
3.1.2	中华人民共和国计算机信息系统安全保护条例	48
3.1.3	信息安全等级保护管理办法有关部分	49
3.1.4	加强工业控制系统信息安全有关管理规定	52
3.1.5	电力监控系统安全防护规定部分	54
3.1.6	中华人民共和国网络安全法（草案）部分	56
3.2	网络信息安全工程技术知识	59
3.2.1	抓住网络空间发展与网络信息安全机遇	59
3.2.2	网络强国必须强化掌控网络信息安全力	62
3.2.3	国家信息安全法规和保障体系框架设想	63
3.2.4	云计算、云数据中心及云安全	65
3.2.5	互联网与物联网及其主要特点	66
3.2.6	全球能源互联网及其关键技术	68
3.3	信息化工程最新应用技术	69
3.3.1	新一代移动通信技术的主要特点及应用情景	69
3.3.2	海量大数据及其主要特点	71
3.3.3	智慧城市的含义及其新技术	72
3.3.4	内存计算技术及其应用案例	74
3.3.5	智能电网及其主要特点	76
3.3.6	一种现代商业方法——电子商务	80
第 4 章	网络信息安全风险评估方法与应用分析	82
4.1	信息安全风险评估基础知识	82
4.1.1	信息安全管理实用规则 ISO/IEC27001	82
4.1.2	系统安全工程能力成熟模型	84
4.1.3	SSE-CMM 模型的应用范围和建议	85
4.1.4	信息安全风险评估的目的与范围	87
4.1.5	信息安全风险评估的主要流程	88
4.1.6	信息安全渗透测试技术能力	89
4.1.7	电力系统信息安全试验测试技术	91
4.2	信息安全风险评估实施方法	93

4.2.1	基于风险关系模型的安全风险评估方法	93
4.2.2	信息系统安全威胁的概念及分类	95
4.2.3	信息系统安全弱点的概念及分类	97
4.2.4	信息安全策略文档评估内容及方法	99
4.2.5	信息资产类别定义与划分	101
4.2.6	信息资产赋值确定安全属性方法	103
4.3	信息安全示范工程安全评估案例	106
4.3.1	信息安全策略文档内容分类与评估实用方法	106
4.3.2	信息系统安全评估白客渗透测试及应用分析	107
4.3.3	信息系统网络部分测试与安全评估方法	109
4.3.4	信息系统网络拓扑结构测试与应用分析	110
4.3.5	信息系统网络设备风险测试与应用分析	112
4.3.6	信息网络系统管理安全风险与应用分析	113
4.3.7	信息系统网络拓扑结构及设备安全策略建议	114
第5章	网络信息安全系统设计与应用分析	116
5.1	网络信息安全系统工程设计基础	116
5.1.1	网络信息安全系统总体框架模型	116
5.1.2	国内外信息化工程最佳实践模型	120
5.1.3	信息安全示范工程应用国际标准	122
5.1.4	网络安全方案整体规划、设计基本原则	123
5.1.5	网络信息安全管理体制设计应用案例	126
5.1.6	网络信息安全组织体系框架设计	127
5.2	信息安全防护分项目系统实用设计	128
5.2.1	企业信息安全策略体系文档结构设计	128
5.2.2	网络信息安全运行管理体系设计应用案例	130
5.2.3	网络信息安全鉴别和认证系统设计应用案例	131
5.2.4	网络信息安全访问控制系统设计应用案例	132
5.2.5	网络信息安全内容安全系统设计	133
5.2.6	网络信息安全数据冗余备份和恢复系统设计	134
5.2.7	网络信息安全审计和响应系统设计	136
5.3	辽宁电力系统信息安全应用示范工程实例	137
5.3.1	辽宁电力系统信息安全应用示范工程实例综述	137
5.3.2	辽宁电力系统信息安全应用示范工程实施历程	139
5.3.3	辽宁电力系统信息安全应用示范工程成果之一	141
5.3.4	辽宁电力系统信息安全应用示范工程成果之二	142
5.3.5	辽宁电力系统信息安全应用示范工程成果之三	144

5.3.6	辽宁电力系统信息安全应用示范工程成果之四	146
第6章	网络信息安全防护体系及应用分析	149
6.1	网络信息安全防护技术基本原理	149
6.1.1	信息系统安全主动防护技术原理	149
6.1.2	信息系统安全被动防护技术原理	151
6.1.3	网络信息安全防护体系的设计原则	152
6.1.4	防火墙系统的工作原理与主要功能	153
6.1.5	防病毒系统的工作原理与主要功能	154
6.1.6	入侵检测系统的工作原理与主要功能	157
6.1.7	漏洞扫描系统工作原理与主要功能	160
6.2	网络信息安全防护技术基础知识	161
6.2.1	国家工业控制系统发展历程与展望	162
6.2.2	我国工业控制系统信息安全重点及措施	163
6.2.3	电力监控系统安全防护含义及安全规范	164
6.2.4	电力监控系统安全防护体系的实施案例	166
6.2.5	电力监控系统安全防护重点与难点	167
6.2.6	电力监控系统安全防护大区划分	169
6.3	网络信息安全防护体系应用分析实例	170
6.3.1	网络信息安全防护主要技术措施	170
6.3.2	电网信息安全纵深防御最佳实践	174
6.3.3	部署统一分层管理的防火墙系统	175
6.3.4	统一防病毒策略和分布式管理防病毒系统	177
6.3.5	统一部署分层管理的入侵检测系统	178
6.3.6	集中部署分级管理的漏洞扫描系统	180
第7章	身份认证与授权管理系统及应用分析	182
7.1	密码学原理与系统设计规范	182
7.1.1	信息密码技术及基本原理	182
7.1.2	现代密码学加密算法与分类	183
7.1.3	基于公共密钥(PKI)的认证机制	185
7.1.4	网络信息安全认证系统设计规范	187
7.1.5	网络信息安全认证体系总体功能	188
7.1.6	辽宁电力PKI-CA认证系统设计与应用层次	190
7.2	信息系统PKI-CA/PMI基本理论	191
7.2.1	信息系统PKI-CA基本工作原理	191
7.2.2	信息系统PKI-CA结构及技术特点	192

7.2.3	信息系统 PKI-CA 系统主要功能	194
7.2.4	信息系统 PMI 基本工作原理	196
7.2.5	信息系统 PMI 系统结构及主要特点	198
7.2.6	信息系统 PKI 与 PMI 主要关联分析	200
7.3	示范工程 PKI-CA/PMI 系统与应用分析	201
7.3.1	辽宁电力 PKI-CA 总体安全体系工程实施	201
7.3.2	基于 PKI-CA 的应用系统升级改造	205
7.3.3	辽宁电力 PMI 授权管理系统的建设工程	207
7.3.4	辽宁电力 PKI-CA 系统的升级和扩建工程	207
7.3.5	辽宁电力 PMI 授权管理系统与应用分析	210
7.3.6	基于 PKI/PMI 的应用系统升级改造	212
7.3.7	辽宁电力 PKI-CA/PMI 系统应用成果	215
第 8 章	数据存储备份与灾难恢复技术及应用分析	219
8.1	数据存储备份与灾难恢复基础知识	219
8.1.1	企业数据环境建设基本概念	219
8.1.2	数据管理 5 项基础标准	220
8.1.3	4 类数据环境基本含义	222
8.1.4	数据仓库及其主要特点	223
8.1.5	数据存储备份基本概念	225
8.1.6	系统灾难恢复基本概念	226
8.1.7	根据信息系统影响程度定义灾难	228
8.2	存储备份与灾难恢复技术	230
8.2.1	数据存储与备份技术	230
8.2.2	数据库热备份应用技术	232
8.2.3	信息网络系统的高可用性技术	235
8.2.4	存储网络-数据访问的基础设施	238
8.2.5	数据块和文件访问	239
8.2.6	弹性存储网络应用与管理	242
8.3	存储备份与灾难恢复技术应用分析	244
8.3.1	企业数据备份策略选择	245
8.3.2	灾难恢复计划方式选择	247
8.3.3	数据备份及灾难恢复现状分析	248
8.3.4	一期数据备份及灾难恢复系统主要功能	250
8.3.5	一期数据备份与灾难恢复系统架构选择	251
8.3.6	二期数据备份与灾难恢复系统建设成果	255

第9章 网络信息安全等级保护及应用分析	258
9.1 网络信息安全等级保护基本概念	258
9.1.1 信息安全等级保护基本含义	258
9.1.2 信息安全等级保护政策体系	260
9.1.3 信息安全等级保护标准体系	261
9.1.4 不同保护等级信息系统的基本保护要求	263
9.1.5 国家等级保护对电力行业新要求	264
9.1.6 电力工业控制系统测评目的和意义	266
9.2 网络信息安全等级保护技术基础	267
9.2.1 等级保护纵深防御体系总体架构	267
9.2.2 信息安全等级保护纵深防御体系设计	268
9.2.3 安全产品测评与事件调查取证能力	270
9.2.4 信息内外网逻辑强隔离装置	271
9.2.5 信息系统安全等级保护实施方案	272
9.2.6 实施信息安全等级保护管理经验	275
9.3 网络信息安全等级保护应用案例	276
9.3.1 统一电力信息安全综合工作平台	276
9.3.2 两级信息安全技术督查体系	278
9.3.3 统一分层信息运维综合监管系统	280
9.3.4 一体化信息外网安全监测系统	283
9.3.5 智能型移动存储介质管理系统	285
9.3.6 统一管理信息系统调运体系	287
第10章 网络空间信息安全战略及应用分析	289
10.1 网络空间安全发展趋势及战略	289
10.1.1 网络空间安全基本概念	289
10.1.2 中国网络空间安全理论与治理战略	290
10.1.3 美国网络空间安全“三步曲”发展战略	293
10.1.4 美国网络空间安全立法对我国的启示	295
10.1.5 世界各国信息安全保障的现状和发展趋势	296
10.2 网络空间安全与治理基础知识	298
10.2.1 互联网、因特网、万维网及三者的关系	299
10.2.2 国际互联网名称与数字地址分配机构	300
10.2.3 国际电信联盟及其国际标准	302
10.2.4 网络空间域名解析体系风险分析	304
10.2.5 现代信息化体系网络作战的攻击方法	305
10.3 网络空间安全与治理应用分析	307

10.3.1	网络信息安全与现代信息社会的关系.....	307
10.3.2	国家网络信息空间安全与发展战略文化.....	308
10.3.3	网络主权是国家主权在网络环境下的自然延伸.....	309
10.3.4	基于国家顶级域名联盟的自治根域名解析体系.....	311
10.3.5	产学研用管五位一体保障网络信息安全.....	313
10.3.6	自主可控是保障网络信息安全的内在需要.....	315
参考文献.....		317

第1章 绪 论

信息技术的发展,以其拓展人类感知、处理、存储、传递的能力,为人类开拓出崭新的生存空间。网络已经成为继陆、海、空、天之外的国家第5大主权空间。习近平主席关于“没有网络安全,就没有国家安全”,“没有信息化,就没有现代化”的科学论断,揭示了网络安全及信息化在国家战略中的重要地位和作用。

1.1 背景及意义

互联网是20世纪最伟大的发明之一,自从1994年我国首次全功能接入互联网,中国互联网已经过二十多年的发展,网民规模迅速扩大。截至2015年6月,中国网民已达6.68亿人,超过整个欧盟的总人口数量。随着现代信息和网络技术的不断发展和广泛应用,国际信息化浪潮更加深刻地影响和改变着人们的生产方式、生活方式、工作方式,不断推出的各种网络接入更加便捷,应用更加多样,内容极大丰富,网络已经变得“无处不在、无时不在、无所不包”,极大地促进了国家经济、政治、文化、社会等各个方面的发展。信息已经成为人类社会发展的关键战略资源。对中国而言,网络空间最大限度地激发了信息化高速发展的活力,蕴含着新一轮技术革命的丰厚能量,网络技术的迭代式发展和互联网公司的创新应用,让互联网经济成为拉动消费需求的重要力量。网络空间为维护、延长中国的战略机遇期赢得了新的发展机会,又为中国开拓新的发展空间创造了历史条件。但与此同时,网络和业务发展过程中也出现了许多新情况、新问题、新挑战,世界各国对信息安全的重视程度不断提高,国际信息安全领域动作频繁,各国政府、军队、相关企业成为该领域的主角。美国著名未来学家托夫勒所预言:“计算机网络的建立与普及将彻底地改变人类生存及生活的模式,而控制与掌握网络的人就是主宰。谁掌握了信息,控制了网络,谁就将拥有整个世界”。网络信息安全已经成为国家战略重点。云计算、云安全、大数据、物联网、智慧地球、智能化安全产品、网络战等新概念、新技术和新产品层出不穷,国际信息安全领域的发展呈现出一些新特点和新趋势。发展信息安全工程技术已成为世界各国信息化建设的重要任务,信息安全已成为维护国家安全和社会稳定的重要基石。

2000年初,国家启动了“十五”重大科技攻关项目“国家信息安全应用示范工程”,国家电力公司承担电力系统信息安全示范工程项目。辽宁省电力有限公司成为电力系统信息安全示范工程试点单位,全面组织“辽宁电力系统信息安全应用示范工程”。2002年启动了国家“863”项目“国家电网调度中心安全防护体系研究及示范工程”,提出了我国电力系统信息安全防护总体策略:“安全分区、网络专用、横向隔离、纵向认证”,由此形成

了以边界防护为要点、多道防线构成的纵深防护体系。2006 年,国家电网公司实施了信息化 SG186 工程,全面建设一体化企业级信息集成平台,人、财、物等 8 大类业务应用,技术、标准、安全防护等 6 个保障体系,大力推进集团企业的信息化建设,推动信息化向集中统一和优化整合方向发展。2011 年,国家电网公司在 SG186 工程的基础上,全面启动了“覆盖面更广、集成度更深、智能化更高、安全性更强、互动性更好、可视化更优”的信息化 SG-ERP 工程建设,根据电网信息安全防护特点,建设电网信息安全三道防线以实现网络纵深防御,进一步提升了信息系统的安全保障能力,我国电力信息安全达到国际一流水平。

2014 年 2 月 27 日,中央网络安全与信息化领导小组成立,由中共中央总书记、国家主席习近平担任组长,李克强总理担任第一副组长,统筹协调各个领域的网络安全和信息化重大问题,制定实施国家网络安全和信息化发展战略、宏观规划和重大政策,不断增强安全保障能力。习近平主席关于“没有网络安全,就没有国家安全”,“没有信息化,就没有现代化”的科学论断,将网络安全及信息化国家战略提高到前所未有的高度,预示着中国在打一场网络安全和信息化的翻身仗方面,也将迎来新的历史突破。强化网络信息安全,并与国家信息化整体战略双轮驱动,对中华民族伟大复兴,实现两个一百年奋斗目标具有重大战略意义。

1.2 国内外网络信息安全发展简述

1.2.1 国际网络信息安全工程技术发展历程

第一个时期是通信安全时期,以 1949 年香农发表的《保密通信的信息理论》为里程碑,主要研究对称密码算法和分析。在这个时期通信技术还不发达,计算机只是零散地位于不同的地点,信息系统的安全仅限于保证计算机的物理安全以及通过密码(主要是序列密码)解决通信安全的保密问题。把计算机安置在相对安全的地点,不容许非授权用户接近,就基本可以保证数据的安全性了。这个时期的安全性是指信息的保密性,对安全理论和技术的研究也仅限于密码学。这一阶段的信息安全可以简称为通信安全,它侧重于保证数据在从一地传送到另一地时的安全性。

第二个时期为计算机安全时期,在 20 世纪 60 年代后,半导体和集成电路技术的飞速发展推动了计算机软硬件的发展,计算机和网络技术的应用进入了实用化和规模化阶段,数据的传输已经可以通过计算机网络来完成。这时候的信息已经分成静态信息和动态信息。1969 年,美国兰德公司给美国国防部的报告中指出“计算机太脆弱了,有安全问题”——这是首次公开提到计算机安全。在当时和其后的相当一段时间,“计算机安全”的内涵主要是指实体安全,即物理安全。

1976 年,现代密码学时代,以提出非对称(公钥)密码思想为标志,非对称密码体制及相关技术迅速发展。1977 年美国国家标准局(NBS)公布的国家数据加密标准(DES)

和 1983 年美国国防部公布的可信计算机系统评价准则 (TCSEC-Trusted Computer System Evaluation Criteria, 俗称橘皮书, 1985 年再版) 标志着解决计算机信息系统保密性问题的研究和应用迈上了历史的新台阶。到了 20 世纪 80 年代后期, “网络安全” 和 “信息安全” 才开始逐步被广泛采用。

第三个时期是在 20 世纪 90 年代兴起的网络时代。从 20 世纪 90 年代开始, 由于互联网技术的飞速发展, 信息无论是企业内部还是外部都得到了极大的开放, 而由此产生的信息安全问题跨越了时间和空间, 信息安全的焦点已经从传统的保密性、完整性和可用性三个原则衍生为诸如可控性、抗抵赖性、真实性等其他的原则和目标。

第四个时期是进入 21 世纪的信息安全保障时代, 其主要标志是《信息保障技术框架》(IATF)。如果说对信息的保护, 主要还是处于从传统安全理念到信息化安全理念的转变过程中, 那么面向业务的安全保障, 就完全是从信息化的角度来考虑信息的安全了。体系性的安全保障理念, 不仅是关注系统的漏洞, 而且是从业务的生命周期着手, 对业务流程进行分析, 找出流程中的关键控制点, 从安全事件出现的前、中、后三个阶段进行安全保障。面向业务的安全保障不是只建立防护屏障, 而是建立一个 “深度防御体系”, 通过更多的技术手段把安全管理与技术防护联系起来, 不再是被动地保护自己, 而是主动地防御攻击。也就是说, 面向业务的安全防护已经从被动走向主动, 安全保障理念从风险承受模式走向安全保障模式。信息安全阶段也转化为从整体角度考虑其体系建设的信息安全保障时代。

1.2.2 我国网络信息安全发展历程及趋势

我国网络信息安全工程技术发展经历了以下 5 个阶段。

第一阶段: 20 世纪 80 年代末之前。1986 年, 中国计算机学会计算机安全专业委员会正式开始活动, 以及 1987 年国家信息中心成立第一个专门安全机构, 从一个侧面反映了中国计算机安全事业的起步。这个阶段的典型特征是国家尚没有相关的法律法规, 没有较完整意义的专门针对计算机安全方面的规章, 安全标准也少, 谈不上国家的统一管理, 只是在物理安全及保密通信等个别环节上有些规定, 广大应用部门也基本上没有意识到计算机安全的重要性, 只有个别部门和少数有计算机安全意识的人们开始在实际工作中进行摸索。在此阶段, 计算机安全的主要内容就是实体安全, 20 世纪 80 年代后期开始了防计算机病毒及计算机犯罪的工作, 但都没有形成规模。

第二阶段: 20 世纪 80 年代末至 20 世纪 90 年代末。20 世纪 80 年代末, 随着我国计算机应用的迅速拓展, 各个行业、企业的安全需求也开始显现。除了此前已经出现的病毒问题, 内部信息泄漏和系统宕机等成为企业不可忽视的问题。此外, 20 世纪 90 年代初, 世界信息技术革命使许多国家把信息化作为国策, 美国 “信息高速公路” 等政策也让中国意识到了信息化的重要性, 在此背景下我国信息化开始进入较快发展期, 中国的计算机安全事业也开始起步。

在这个阶段, 一个典型的标志就是关于计算机安全的法律法规开始出现——1994 年, 公安部颁布了 “中华人民共和国计算机信息系统安全保护条例”, 这是我国第一个计算机安