DIANLI QIYE
XINXI XITONG ANQUAN DENGJI BAOHU PEIXUN JIAOCAI

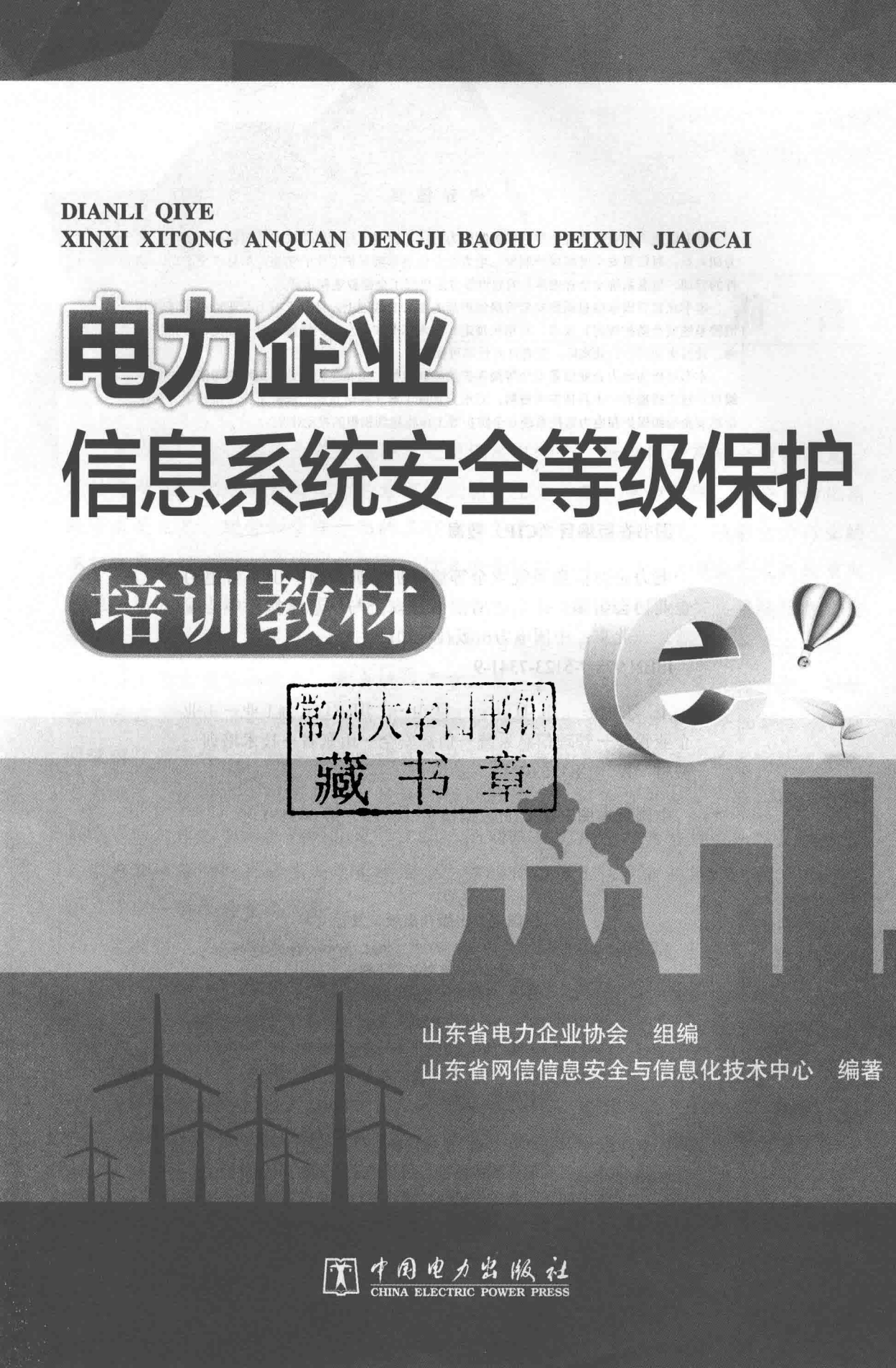
电力企业信息系统安全等级保护培训教材

山东省电力企业协会　组编
山东省网信信息安全与信息化技术中心　编著

中国电力出版社
CHINA ELECTRIC POWER PRESS

DIANLI QIYE
XINXI XITONG ANQUAN DENGJI BAOHU PEIXUN JIAOCAI

电力企业信息系统安全等级保护培训教材



山东省电力企业协会　组编
山东省网信信息安全与信息化技术中心　编著

中国电力出版社
CHINA ELECTRIC POWER PRESS

内 容 提 要

本书以电力行业信息安全等级保护制度为主线，以电力行业信息安全等级保护的各项工作为切入点，对信息安全等级保护制度、电力企业信息等级保护工作的实施、信息安全产品、事件的管理、信息系统安全管理体系的建设等方面进行了全面叙述和讲解。

本书在宣贯国家信息系统安全等级保护基本要求的基础上，结合了电力行业特点和《电力监控系统安全防护规定》要求，对相关规定、技术标准和安全防护措施予以了细化、补充和完善，使其更加符合行业实际，更有针对性和可操作性。

本书可作为电力企业信息安全等级保护的培训教材，也是电力企业实施网络与信息安全等级保护技术措施的一本具体参考资料，对电力企业了解掌握信息登记保护工作，做好电力企业信息安全等级保护和电力监控系统安全防护等工作将起到积极的推动作用。

图书在版编目（CIP）数据

电力企业信息系统安全等级保护培训教材／山东省电力企业协会组编；山东省网信信息安全与信息化技术中心编著．—北京：中国电力出版社，2015.3

ISBN 978-7-5123-7341-9

Ⅰ．①电… Ⅱ．①山… ②山… Ⅲ．①电力工业－工业企业管理－管理信息系统－信息安全－山东省－技术培训－教材 Ⅳ．①F426.61

中国版本图书馆 CIP 数据核字（2015）第 043181 号

中国电力出版社出版、发行

（北京市东城区北京站西街 19 号 100005 http：//www.cepp.sgcc.com.cn）

航远印刷有限公司印刷

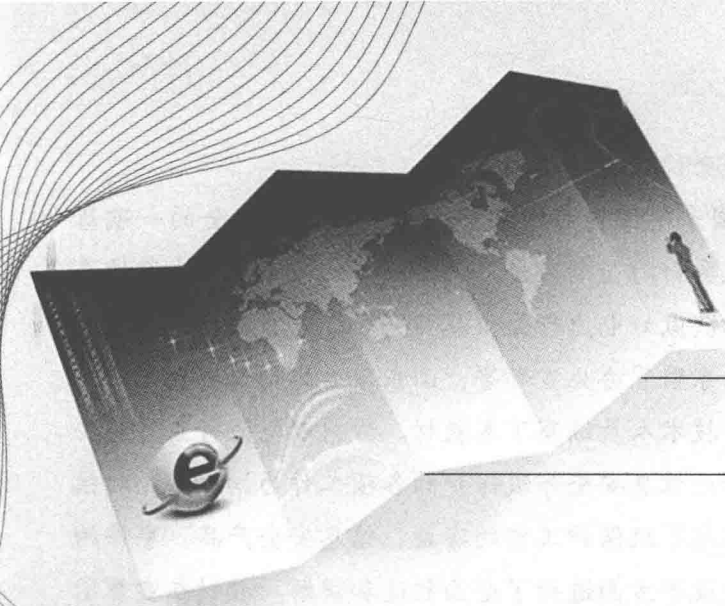
各地新华书店经售

*

2015 年 3 月第一版 2015 年 3 月北京第一次印刷

787 毫米×1092 毫米 16 开本 21.5 印张 551 千字

印数 0001—7000 册 定价 **70.00** 元



前　言

电力系统的信息安全是一项涉及电网调度自动化、继电保护及安全控制装置、厂站自动化、配电网自动化、电力市场交易、生产管理、电力营销、办公自动化系统等有关生产、经营和管理方面的多领域、复杂的大型系统工程。随着电力行业的不断发展和信息化水平的不断提高，信息安全问题已成为影响电力安全生产的重大问题。电力工业的特点决定了电力信息安全不仅具有一般计算机信息网络信息安全的特征，而且还具有电力实时运行控制系统信息安全的特征，任何一个安全漏洞，一旦遭受恶意破坏和攻击，都会造成严重后果，甚至威胁到整个系统的安全，导致电网瘫痪。2000 年以来，我国电力监控系统相继发生了“二滩电厂停机事件”、“时间逻辑炸弹事件”、“换流站感染病毒事件”等多起信息安全事件，造成事故或形成安全隐患，这些事例说明电力监控系统所面临的安全风险日益增大。如何确保电力系统不同企业之间及其内部在进行方便、高效信息交换和相互协作的同时，防止来自于内外域各种用户非法或无意的攻击、误操作，防止信息泄漏等，已成为电力安全工作中一项极为重要的任务。

为确保电力信息系统和基础信息网络安全，保障电力安全生产和系统稳定运行，2004 年以来，原国家电监会、国家能源局陆续发布了《电力二次系统安全防护规定》、《电力行业信息系统安全等级保护定级工作指导意见》、《电力行业网络与信息安全通报暂行办法》、《电力行业网络与信息安全应急预案》、《电力行业信息系统安全等级保护基本要求》、《电力行业网络与信息安全管理办法》等一系列规章、规定和文件，不断健全完善电力信息系统安全防护制度体系，引领电力行业信息安全等级保护、风险评估、信息通报、应急处置等工作逐渐走向规范化、法制化的道路。2014 年 9 月 1 日，国家发展改革委第 14 号令《电力监控系统安全防护规定》正式开始实施，对加强电力监控系统信息安全管理，防范黑客及恶意代码等对电力监控系

统的攻击及侵害，保障电力系统安全稳定运行意义重大。

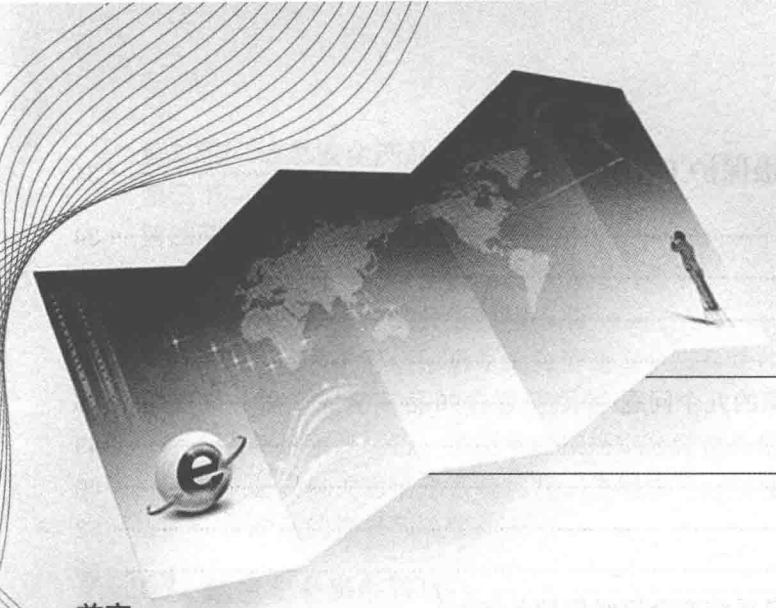
信息系统安全等级保护是在国家范围内推行的对于网络与信息安全的一项基本制度，电力监控系统安全防护主要针对与电力生产、供应密切相关的电力监控系统提出具体的安全防护措施。为切实做好电力行业信息安全等级保护相关规定的宣贯和培训工作，按照国家能源局山东监管办公室部署，山东省电力企业协会精心策划，邀请信息安全相关技术组织、技术人员编写了本教材。教材以电力行业信息安全等级保护制度为主线，以电力行业信息安全等级保护的各项工作为切入点，对信息安全等级保护制度、电力企业信息等级保护工作的实施、信息安全产品、事件的管理，信息系统安全管理体系的建设等方面进行了全面叙述和讲解。教材在宣贯国家信息系统安全等级保护基本要求的基础上，结合了电力行业特点和《电力监控系统安全防护规定》要求，对相关规定、技术标准和安全防护措施予以了细化、补充和完善，使其更加符合行业实际，更有针对性和可操作性。本教材除作为电力企业信息安全等级保护的培训教材之外，也是电力企业实施网络与信息安全等级保护技术措施的一本具体参考资料，对电力企业了解掌握信息登记保护工作，扎实做好电力企业信息安全等级保护和电力监控系统安全防护等工作将起到积极的推动作用。

教材在编写过程中得到了国家能源局山东监管办有关领导和同志们的指导帮助，在此一并表示衷心感谢。教材编写过程中参考了部分国家标准、有关书籍和资料，在此，谨向作者及编辑表示衷心的感谢。

由于编者水平有限，教材中还存在许多不足和纰漏，敬请读者批评指正，以便日臻完善，使之成为服务电力事业的一本好书。

编　者

2014年11月29日



目 录

前言

第一章 信息安全等级保护制度简介 1

第一节 开展信息安全等级保护工作的重要性和紧迫性 1
一、我国当前面临的信息安全形势 1
二、我国互联网近年信息安全事件回顾 3
三、我国信息安全等级保护制度发展历程 4
四、电力行业开展信息安全等级保护工作的重要性和紧迫性 6
五、电力行业信息安全等级保护工作开展情况 7
第二节 信息安全等级保护基本概念 8
一、信息安全等级保护基本内容 8
二、信息等级保护工作的地位和作用 13
三、信息安全等级保护工作的五个主要环节 13
四、信息安全等级保护工作中的责任分工 15
五、信息安全等级保护主要法律法规体系 17
六、信息安全等级保护主要技术标准体系 19
第三节 电力行业开展等级保护工作的法律法规依据和技术标准介绍 22
第四节 违反国家信息安全等级保护制度的法律责任 22
一、《信息安全等级保护管理办法》的有关规定 22
二、《信息安全等级保护备案实施细则》的有关规定 23
三、《公安机关信息安全等级保护检查工作规范》的有关规定 23
四、《计算机信息网络国际联网安全保护管理办法》（公安部令第 33 号）、
《互联网安全保护技术措施规定》（公安部令第 82 号）有关规定 23
五、《电力行业网络与信息安全管理办法》的有关规定 25
六、《电力行业信息安全等级保护管理办法》的有关规定 26
七、《电力监控系统安全防护规定》的有关规定
（国家发改委令 2014 年第 14 号） 31

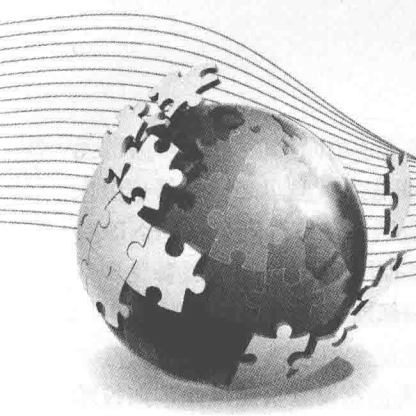
第二章 电力信息系统安全等级保护工作的实施 34
第一节 定级工作 34
一、工作组织 34
二、定级原理 35
三、定级方法 36
四、定级过程中需要注意的九个问题 45
五、定级报告模版 49
六、定级报告案例 50
第二节 备案工作 52
一、召开专家评审会 53
二、按照要求填写《信息系统安全等级保护备案表》 53
三、听取上级主管部门意见 61
四、准备备案所需要的所有文件材料 61
五、到管辖的公安机关备案 62
第三节 安全建设整改 62
一、安全建设整改的主要工作内容 63
二、安全建设整改工作流程 64
三、安全建设整改标准应用 64
四、安全保护能力目标 66
五、安全管理制度建设整改 66
六、安全技术措施建设整改 67
七、信息系统安全建设工作 67
八、信息系统安全整改工作实施 79
第四节 等级测评 86
一、等级测评原则 87
二、等级测评的内容 87
三、等级测评的方法和强度 88
四、等级测评的对象 88
五、等级测评指标 90
六、等级测评质量保障 91
七、等级测评管理 92
八、等级测评工作实施 93
第五节 安全自查和监督检查 97
一、定期信息安全自查 97
二、公安机关监督检查 97
第三章 信息安全产品管理 101
第一节 信息安全产品的概念 101

第二节　信息安全产品分等级管理 …… 101
第三节　信息安全产品的分类 …… 102
第四节　信息安全产品的分级使用 …… 102
一、国家对信息安全产品的分级使用要求 …… 103
二、信息安全产品分级检测标准 …… 103
三、不同保护等级信息系统对信息安全产品功能和可信性保证的要求 …… 103
第五节　信息安全产品的分级使用管理 …… 105
一、信息系统运营、使用单位按规定分级使用信息安全产品 …… 105
二、公安机关对信息系统运营、使用单位分级使用信息安全产品的指导和监督检查 …… 105
第四章　信息安全事件管理 …… 106
第一节　信息安全事件定义 …… 106
第二节　信息安全事件分类 …… 106
一、有害程序事件（MI） …… 106
二、网络攻击事件（NAI） …… 107
三、信息破坏事件（IDI） …… 107
四、信息内容安全事件（ICSI） …… 107
五、设备设施故障（FF） …… 107
六、灾害性事件（DI） …… 107
七、其他事件（OI） …… 107
第三节　信息安全事件的分级 …… 108
一、特别重大事件（Ⅰ级） …… 108
二、重大事件（Ⅱ级） …… 108
三、较大事件（Ⅲ级） …… 108
四、一般事件（Ⅳ级） …… 108
第四节　信息安全事件的管理流程 …… 109
一、规划和准备 …… 109
二、使用 …… 109
三、评审 …… 110
四、改进 …… 110
第五节　信息安全事件管理的关键过程 …… 110
第六节　信息安全事态的发现与报告 …… 111
第七节　信息安全事态/事件的评估与决策 …… 111
第八节　信息安全事件的响应 …… 112
一、立即响应 …… 112
二、判断事件是否在控制之下 …… 113
三、后续响应 …… 113
四、危急求助 …… 114

五、法律取证分析 …… 114
六、通报 …… 115
七、上报 …… 115
八、活动日志和变更控制 …… 115
第九节 信息安全事件的分级处置 …… 116
第五章 信息系统安全管理体系建设 …… 118
第一节 信息系统安全管理的原则 …… 118
第二节 管理制度建设 …… 119
一、总体安全管理策略 …… 119
二、安全管理策略的制定 …… 120
三、安全管理策略的发布 …… 120
四、安全管理规章制度内容 …… 120
五、安全管理规章制度的制定 …… 121
六、策略与制度文档的评审和修订 …… 121
七、策略与制度文档的保管 …… 122
第三节 管理机构设置 …… 122
一、建立安全管理机构 …… 122
二、信息安全领导小组职责 …… 123
三、信息安全职能部门职责 …… 123
四、集中管理机构的设置 …… 123
五、集中管理机构职能 …… 123
第四节 人员安全管理 …… 124
一、安全管理人员配备 …… 124
二、关键岗位人员管理 …… 124
三、人员录用管理 …… 125
四、人员离岗管理 …… 125
五、人员考核与审查 …… 125
六、第三方人员管理 …… 125
七、信息安全教育 …… 126
八、信息安全专家 …… 126
第五节 安全建设管理 …… 126
第六节 运行和维护管理 …… 132
一、运行与维护管理基本要求 …… 132
二、运行和维护管理其他要求 …… 141
第六章 信息安全技术体系建设 …… 147
第一节 物理安全通用技术要求 …… 147
一、环境安全 …… 148
二、设备安全 …… 150

三、记录介质安全 …… 151
第二节 运行安全通用技术要求 …… 151
一、风险分析 …… 152
二、信息系统安全性检测分析 …… 152
三、信息系统安全监控 …… 152
四、安全审计 …… 153
五、信息系统边界安全防护 …… 155
六、备份与故障恢复 …… 155
七、恶意代码防护 …… 156
八、信息系统的应急处理 …… 156
九、可信计算机技术和可信连接技术 …… 156
第三节 数据安全通用技术要求 …… 156
一、身份鉴别 …… 157
二、抗抵赖 …… 158
三、自主访问控制 …… 159
四、标记 …… 159
五、强制访问控制 …… 160
六、用户数据完整性保护 …… 162
七、用户数据保密性保护 …… 162
八、数据流控制 …… 163
九、可信路径 …… 163
十、密码支持 …… 163
第四节 不同安全防护级别信息系统保护基本技术要求 …… 163
一、第一级基本技术要求 …… 163
二、第二级基本技术要求 …… 165
三、第三级基本技术要求 …… 168
四、第四级基本技术要求 …… 173
第五节 不同安全保护级别信息系统的基本配置 …… 179
一、局域计算环境安全及其分等级安全机制配置 …… 179
二、局域计算环境边界防护及其分等级安全机制配置 …… 183
三、用户环境安全和边界防护及其分等级安全机制配置 …… 185
四、网络系统安全及其分等级安全机制配置 …… 186
五、安全域之间互操作的安全机制配置 …… 190
六、密码安全机制分等级配置 …… 190
七、安全管理总体要求及其分等级配置 …… 191
八、安全管理中心及其分等级安全机制配置 …… 192
第七章 《信息系统安全等级保护基本要求》解读 …… 193
第一节 《信息系统安全等级保护基本要求》主要作用 …… 193
第二节 《信息系统安全等级保护基本要求》主要特点 …… 193

第三节 《信息系统安全等级保护基本要求》与其他标准的关系……194
第四节 《信息系统安全等级保护基本要求》的框架结构……194
第五节 《信息系统安全等级保护基本要求》描述模型……195
第六节 《信息系统安全等级保护基本要求》安全要求……196
第七节 《信息系统安全等级保护基本要求》逐级增强的特点……196
第八节 《信息系统安全等级保护基本要求》技术类要求……200
一、物理安全要求……200
二、网络安全要求……205
三、主机安全要求……210
四、应用安全要求……215
五、数据安全及备份要求……221
第九节 《信息系统安全等级保护基本要求》管理类要求……223
一、安全管理制度要求……223
二、安全管理机构要求……225
三、人员安全管理要求……228
四、系统安全建设管理要求……231
五、系统运维管理要求……237
第十节 《电力行业信息系统安全等级保护基本要求》简介……243
一、编制背景……243
二、主要内容与框架……244
三、与国标基本要求的差异……244
四、行业基本要求安全层面简介……245
第十一节 电力行业管理信息系统类要求（摘录）……250
第十二节 电力行业生产控制信息系统类要求（摘录）……281
附录A 电力监控系统安全防护规定……330
附录B 电力行业网络与信息安全管理办法……333



第一章 信息安全等级保护制度简介

随着我国国民经济和社会信息化进程的全面加快，信息系统的基础性、全局性作用日益增强，信息资源已成为国家经济建设和社会发展的重要资源之一。保障信息安全、维护国家安全、公共利益和社会稳定，成为信息化发展中迫切要解决的重大问题。而我国的信息安全保障工作尚处于起步阶段，存在着信息安全滞后于信息化发展、信息安全缺乏统一的政策指导、信息系统安全建设和管理缺乏标准规范、信息安全防范能力不足等问题。为了从整体上解决我国信息安全存在的突出问题，党中央高度重视，各有关方面协调配合、共同努力，逐步建立了我国信息安全等级保护制度。信息安全等级保护是国家信息安全保障工作的基本制度，开展信息安全等级保护工作是实现国家对重要信息系统重点保护的重大措施，也是一项事关国家安全、社会稳定、公共利益的基础性工作。通过开展信息安全等级保护工作，可以有效解决我国信息安全面临的威胁和存在的主要问题，充分体现“适度安全、保护重点”的目的，将有限的财力、物力、人力投入到重要信息系统安全保护中，按标准建设安全保护措施，建立安全保护制度，落实安全责任，有效保护基础信息网络和关系国家安全、经济命脉、社会稳定的重要信息系统的安全，有效提高我国信息安全保障工作的整体水平。

第一节 开展信息安全等级保护工作的重要性和紧迫性

一、我国当前面临的信息安全形势

近年来，国际信息安全环境日趋复杂。西方各国不断加强网络战备，并通过安全壁垒打压我国高新技术企业。同时，我国基础网络、重要信息系统、工业控制系统的安全风险日益突出，网络犯罪和新兴技术的安全威胁持续加大。国内外因素交织，我国信息安全发展形势严峻而复杂。

1. 世界各国纷纷加强网络战备，网络空间剑拔弩张

当前，网络空间已经上升为与海、陆、空、太空并列的第五空间，世界各国都高度重视并加强网络战的攻防实力，发展各自的“网络威慑”能力。首先，世界各国都在加快组建网络部队，已经有美国、俄罗斯、以色列、伊朗、韩国等 40 多个国家成立了网络部队，并逐步扩大网络部队的规模。例如，美国网络部队总人数已经达到 7 万人以上；俄罗斯网络战部队规模达 7000 人；以色列国防军网络部队“C4I”编制约 3000 人；韩国于 2011 年将网络司令部人员增加到 1000 人，并将其提升为独立部队；日本防卫省于 2014 年 3 月成立了一支由 90 名自卫队队员组成，负责 24h 监视防卫省及自卫队的网络战部队；印度政府于 2012 年 10 月开始计划和私营部门联手实施培训 50 万“网络战士”。其次，世界各国不断增加网络武器、网络安全人才等方面的投入。例如，美国国防部 2012 年在网络安全和网络技术方面的预算达到 34 亿美元，主要用于新

一代网络武器研发方面；北约C3局（NC3A）于2012年3月份签署了合同价值约5800万欧元的网络防御投资计划；韩国于2012年投入19亿韩元启动“白色黑客”计划以培养网络安全人员。最后，各国不断加强网络演习，以提高网络对抗实战能力。欧盟网络与信息安全局（ENISA）发布的报告显示，近两年来网络演习的频率大幅提高。纵观当今各国在网络空间的战备竞赛，可以预见，未来的几年网络空间的局势将更加复杂，难免会出现局部网络冲突。

2. 西方启动贸易保护安全壁垒，相关企业将受重大冲击

随着中国经济的快速发展，西方各国频繁使用各种手段为中国企业设置贸易壁垒，如技术壁垒和绿色壁垒等，近来一些国家又启动了安全壁垒这种新的贸易保护主义工具。2012年3月，澳大利亚政府以担心来自中国的网络攻击为由，禁止华为技术有限公司对数十亿澳元的全国宽带网设备项目进行投标。美国国会于2012年10月8日发布华为、中兴“可能对美国带来安全威胁”的调查结果报告，认为华为和中兴为中国情报部门提供了干预美国通信网络的机会，并建议相关美国公司尽量避免同华为和中兴合作。华为和中兴遭遇安全壁垒的根本原因在于他们国际竞争力的大幅提升，自身已经掌握该行业的核心技术和专利资源，技术壁垒等手段在他们身上已经无法产生效果。在美国调查报告发布之后，已经出现一些国家跟风的苗头，考虑到当前国际经济持续下行的趋势，2014年后以国家安全为由的贸易保护主义行为将更加盛行，相关企业的国际化步伐将会长期受到影响，我国高新技术产业的全球布局也将面临新的阻力。

3. 关键信息基础设施安全状况堪忧，国家安全面临挑战

当前，我国基础网络、重要信息系统和工业控制系统等关键信息基础设施多使用国外的技术和产品。据统计，我国芯片、操作系统等软硬件产品，以及通用协议和标准90%以上依赖进口，这些技术和产品的漏洞不可控，使得网络和系统更易受到攻击，同时也面临着敏感信息泄露、系统停运等重大安全事件的安全风险。以基础网络为例，由中国电信和中国联通运营的互联网骨干网络承担着中国互联网80%以上的流量，然而这些骨干网络70%～80%的网络设备都来自于思科，几乎所有的超级核心节点、国际交换节点、国际汇聚节点和互联互通节点都由思科掌握。与此同时，国际上针对关键信息基础设施的网络攻击持续增多，甚至出现了政府和恐怖分子支持的高级可持续性威胁APT。APT是针对特定组织的、复杂的、多方位的网络攻击，这类攻击目标性强，持续时间长，一旦攻击成功则可能导致基础网络、重要信息系统和工业控制系统等大面积瘫痪。我国关键信息基础设施核心技术受制于人的局面在短期内难以改变，这在未来几年中将成为我国国家安全的严峻挑战。

4. 新兴技术应用范围日益拓展，安全威胁将持续加大

随着移动互联网、下一代互联网和大数据等新兴技术的广泛应用，伴随这些技术而来的信息安全威胁将对我国信息安全带来新的挑战。在移动互联网领域，用户和应用的数量快速增长，相关数据显示，截止到2014年6月，中国移动互联网网民达到6.86亿，2014年底全球互联网用户已有近30亿。与此同时，移动终端恶意软件数量暴增，据相关统计数据显示，2014年一季度共监测到Android平台恶意、高危软件总数突破200万，隐私窃取类软件比例持续上升。手机病毒黑色产业链进一步强化，病毒攻击技术与攻击方式也得到广泛提升，针对网银、支付、汇款等敏感财产信息进行收集窃取等新的特征显露，安全威胁持续加大。在下一代互联网领域，IPv6即将逐步取代IPv4成为支撑互联网运转的核心协议，但仍然存在一些难以解决的安全隐患，如难以应对拒绝服务攻击等，而且在从IPv4向IPv6进行迁移的过程中，还会出现一些新的安全风险。大数据分析技术的广泛应用将使我国一些关键数据面临安全威胁。2012年3月，美国总统奥巴马宣布启动“大数据研究与开发计划”，旨在提高从庞大而复杂的科学数据中提取知识的能

力。我国目前有大量地理数据、经济运行数据被外企所掌握，如谷歌、沃尔玛等企业。大数据分析技术能够窃取这些数据中所隐含的一些关键信息，这将对我国国家安全产生重大的影响。随着这些新兴技术应用的日益深入，带来的安全风险将进一步加剧。

5. 网络犯罪技术方式不断革新，安全防范面临严峻挑战

随着网络技术的快速发展，网络犯罪的技术手段也不断革新，网络技术产品的功能越来越丰富，也带来了新的技术漏洞和安全隐患，这都增加了信息安全防范的压力。一方面，网络犯罪技术不断革新，呈现智能化趋势。2012 年 7 月，迈克菲和卫报研究人员发布的一份报告揭露，一种高度复杂的全球性金融服务欺诈活动在欧洲、南美和美国蔓延，该攻击基于成熟的 SpyEye 和 Zeus 恶意软件，犯罪分子增加了绕过物理身份验证、自动化数据库搜索等新特性，通过基于云服务器的自动化攻击手段在全球范围内进行诈骗，目前主要针对高额企业账户。另一方面，近场通信（NFC）和 WIFI 等技术手段成为网络犯罪分子关注的热点。在 Black Hat2012 大会上，研究人员展示了如何使用近场通信技术的漏洞入侵 Android 系统，并指出其他智能手机也存在类似的问题。研究人员于 2012 年 2 月确认公共场合的免费 WIFI 存在泄露用户隐私的安全隐患。在 Defense2012 大会上，一些黑客展示了针对 WIFI 的 MS-CHAPv2 身份验证协议的攻击手段。

6. 网络安全损失日趋严重，影响程度将进一步加剧

当前，因网络安全问题产生的经济损失大幅提高，造成的危害也明显增大。2012 年诺顿网络安全报告显示，在过去的一年中，网络犯罪致使全球个人用户蒙受的直接损失高达 1100 亿美元，每秒就有 18 位网民遭受网络犯罪的侵害，平均每位受害者蒙受的直接经济损失总额为 197 美元。对于中国而言，则有 84%的中国网民曾遭受过网络犯罪侵害，估计有超过 2.57 亿人成为网络犯罪受害者，所蒙受的直接经济损失达人民币 2890 亿元。惠普研究部门发现，典型的美国公司 2012 年因为网络犯罪而发生的成本为 890 万美元，较 2011 年增长 6%，较 2010 年增长 38%。从目前的发展趋势来看，网络犯罪等安全问题的影响范围和影响程度将进一步加大。

信息安全新形势要求我国必须加强信息安全保障工作，尤其是要确保关键基础设施的安全。

二、我国互联网近年信息安全事件回顾

中国互联网网络安全报告显示，去年国家互联网应急中心（CNCERT）共接收境内网络安全事件报告 30684 起，较 2012 年增长 71.2%。从数据不难看出，随着互联网的飞速发展，我国网络信息安全正面临严峻的挑战。以下是我国近年来关注度较高的网络信息安全事件：

2014 年 8 月 2 日，名为“××神器”的手机病毒开始通过网络大面积传播。电信运营商及时发现并采取应急措施，阻拦威胁短信千万余条，尽管如此，仍有上百万部手机在半天内受到感染。病毒会向受感染用户手机的通讯录自动群发短信，诱骗其他用户点击，该病毒会将短信记录转发至某固定手机号码，获取个人隐私和网银短信验证码等，受害用户个人信息安全受到极大威胁。

2014 年 1 月 21 日，国际互联网节点出现故障致使我国 2/3 的 DNS 服务器瘫痪，所有通用顶级域根出现异常，导致大量网站域名解析不正常，国内网络大面积瘫痪。包括百度在内的多家知名网站都未能幸免。

2013 年 8 月 25 日 00:06 起，中国互联网络信息中心管理运行的国家．CN 顶级域名服务器遭受大规模拒绝服务攻击，严重影响用户正常访问 CN 网站。调查发现，此次攻击系黑客利用僵尸网络向 CN 顶级域名系统持续发起大量查询请求，造成 CN 系统的互联网出口带宽

严重拥塞。

2012 年 11 月，包括 EMS 在内 10 余家主流快递企业的快递单号信息被大面积泄露，并衍生出多个专门从事快递单号信息交易的网站。在“淘单 114”和“单号吧”两家网站上，展示快递单号的信息均被明码标价，售价从 0.4～2 元不等。

2012 年 2 月 9 日，国内主流电商淘宝网、当当网、1 号店等 B2C 网站用户个人信息泄露。同年 7 月，京东商城、当当网、1 号店等多家电商网站再次“集体”被曝账户信息泄露。

此外，2011 年底，CSDN 中文 IT 社区、天涯等众多互联网公司的账户密码信息被公开下载。国家互联网应急中心通过公开渠道获得疑似泄露的数据库有 26 个，涉及账号、密码 2.78 亿条，这些信息均为黑客攻击商业网站后窃取并泄露。2014 年 4 月 8 日，微软公司在向 2 亿多用户发布通牒 100 天后，停止了对 Windows XP 系统提供技术支持。微软表示，Windows XP 的运行环境存在很大的漏洞，微软发布的补丁不能有效抑制病毒的攻击，因此不断在其官网上告知用户可能承受一些风险。2 亿多 Windows XP 用户在失去了保护伞后，陷入“裸奔”状态，电脑安全隐患增加。工业和信息化部总工程师张峰表示，Windows XP 停止服务直接关系到广大用户的信息安全和利益，XP 用户将面临安全威胁。中国工程院院士倪光南也表示，Windows XP 停止服务是一个“重大的信息安全事件”。就在 Windows XP 系统停止服务的当天，全球互联网通行的安全协议 OpenSSL 曝出本年度最严重的漏洞。据悉，利用该漏洞，黑客坐在自家的电脑前，就可以实时获取到很多 https 开头网址的用户登录账号密码。

三、我国信息安全等级保护制度发展历程

美国国防部早在 20 世纪 80 年代就针对国防部门的计算机安全保密开展了一系列有影响的工作，并于 1987 年出版了一系列有关可信计算机数据库、可信计算机网络的指南等（又称彩虹系列），根据所采用的安全策略、系统所具备的安全功能将系统分为四类七个安全级别，将计算机系统的可信程度划分为 D、C1、C2、B1、B2、B3 和 A1 七个层次。20 世纪 90 年代，西欧四国（英、法、荷、德）联合提出了信息技术安全评估标准（ITSEC），ITSEC（又称欧洲白皮书）除了吸收 TCSEC（美国可信计算机系统评价标准）的成功经验外，首次提出了信息安全的保密性、完整性、可用性的概念，把可信计算机的概念提高到可信信息技术的高度上来认识。1991 年 1 月，美国联合其他国家共同宣布了制定通用安全评估准则（CC）的计划。1996 年 1 月出版了 1.0 版，它的基础是欧洲的 ITSEC、美国的包括 TCSEC 在内的新的联邦评估标准、加拿大的 CTCPEC，以及国际标准化组织 ISO：SC27WG3 的安全评估标准。CC 标准吸收了各先进国家对现代信息系统信息安全的经验与知识，对信息安全的研究与应用带来重大影响。

我国于 20 世纪 80 年代末开始研究信息系统安全防护问题，1994 年国务院颁布《中华人民共和国计算机信息系统安全保护条例》，规定计算机信息系统实行安全等级保护。这一重大决定，明确了关于实行信息安全等级保护制度的有关规定，提出从整体上、根本上解决国家信息安全问题的办法。

1999 年，国家标准 GB 17859—1999《计算机信息系统安全保护等级划分准则》颁布，提出从整体上、根本上、基础上来解决等级保护问题，对计算机信息系统安全保护能力划分为五个等级，即用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级，计算机信息系统安全保护能力随着等级的增高逐渐增强。

1999 年底，公安部与信息产业部、国家安全部、国家保密局、国家密码管理委员会等相关部门起草了《计算机信息系统安全保护等级制度建设纲要》，初步确立了安全保护等级制度的主

要适用范围、建设目标、建设原则、建设任务、实施步骤及措施等主要问题。

2000 年 11 月 10 日，国家发展计划委员会正式向公安部印发批复，同意将计算机信息系统安全保护等级评估认证体系建设项目列入 2000 年国家高技术产业发展项目计划。建设内容包括在北京和上海分别建立信息产品安全保护等级检测中心和计算机信息系统安全保护等级评估中心等。目标是初步建立我国计算机信息系统安全等级保护监督管理系统，为实施《计算机信息系统安全保护等级划分准则》提供基本条件。

2003 年，中共中央办公厅、国务院办公厅转发了《国务院信息化领导小组关于加强信息安全保障的意见》（中办发〔2003〕27 号），再次强调对信息安全进行等级保护，提出“要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南”。

2004 年公安部联合国家保密局、国家密码管理局、国家保密委员会和国务院信息化工作办公室发布《关于信息安全等级保护工作的实施意见》（公通字〔2004〕66 号），对信息安全等级保护的基本制度框架进行了规划。

2005 年底，公安部和国务院信息化工作办公室联合印发了《关于开展信息系统安全等级保护基础调查工作的通知》（公信安〔2005〕1431 号）。2006 年上半年，公安部会同国信办在全国范围内开展了信息系统安全等级保护基础调查。通过基础调查，基本摸清和掌握了全国信息系统特别是重要信息系统的基本情况，为制定信息安全等级保护政策奠定了坚实的基础。

2006 年 6 月，公安部、国家保密局、国家密码管理局、国务院信息化工作办公室联合下发了《关于开展信息安全等级保护试点工作的通知》（公信安〔2006〕573 号）。在 13 个省区市和 3 个部委联合开展了信息安全等级保护试点工作。通过试点，完善了开展等级保护工作的模式和思路，检验和完善了开展等级保护工作的方法、思路、规范标准，探索了开展等级保护工作领导、组织、协调的模式和办法，为全面开展等级保护工作奠定了坚实的基础。

2007 年 6 月，公安部、国家保密局、国家密码管理局和国务院信息化工作办公室联合下发了《信息安全等级保护管理办法》（公通字〔2007〕43 号），对信息安全等级的划分与保护、等级保护的实施与管理、法律责任等进行了规定；7 月，又下发了《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安〔2007〕861 号），对重要信息系统安全等级保护定级工作提出要求，并召开了“全国重要信息系统定级电视电话会议”，部署在全国范围内开展重要信息系统安全等级保护定级工作。之后，公安部制定的四个标准《信息系统安全等级保护定级指南》、《信息系统安全等级保护基本要求》、《信息系统安全等级保护实施指南》、《信息系统安全等级保护测评要求》报批稿开始在试点工作中使用。

2007 年 10 月，公安部发布《信息安全等级保护备案实施细则》，规范了备案受理、审核和管理等工作。

2009 年 10 月，公安部出台了《关于开展信息安全等级保护建设整改工作的指导意见》（公信安〔2009〕1429 号），并对中央和国家机关九十多个部委和直属机构等进行了等级保护建设整改工作培训。同年，公安部下发了《信息系统安全等级保护测评报告模板（试行）》。

2010 年 4 月，公安部出台了《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安〔2010〕303 号），对等级测评体系建设和信息系统的等级测评和建设整改工作提出了时间要求。

2010 年 12 月，公安部和国务院国有资产监督管理委员会联合出台了《关于进一步推进中央企业信息安全等级保护工作的通知》（公通字〔2010〕70 号），要求中央企业贯彻落实信息安全

等级保护制度。

四、电力行业开展信息安全等级保护工作的重要性和紧迫性

电力是关系国计民生的重要基础产业，也是千家万户的公共事业。电力的安全可靠供应事关经济发展、人民生活和社会稳定，保障电力系统安全是国家安全的重要组成部分。现代电力工业具有高度网络化、系统化、自动化的特征，以网络、数据库及计算机自动控制技术为代表的信息处理技术已成为支撑电力生产控制和生产经营管理不可或缺的基础要素，保障电力网络与信息系统安全已经成为电力系统安全稳定运行的重要前提。

同时，世界各国尤其是大国之间，在网络空间的控制与反控制、渗透与反渗透的斗争更加激烈，维护网络空间安全、保障国家重要基础设施安全已经成为国家战略的制高点。近年来发生的“震网”和“棱镜门”事件表明，某些西方大国为维持其全球霸权，一直在利用信息技术的原发优势，不断加强对其他国家网络空间的渗透、控制和破坏，对这些国家的政治、经济和军事安全构成了严重威胁。我国在网络空间方面，由于核心技术尚未完全掌握、关键设备大多从国外进口、国产水平较低、信息安全基础薄弱，维护网络空间安全，保障电力等国家关键基础设施和信息系统的安全，实现信息安全“能控、在控、可控”的任务非常艰巨。

我国电力系统的信息化从 20 世纪 60 年代就已经开始起步，早期主要集中在发电厂和变电站自动监测、控制等电力生产过程自动化，20 世纪 80～90 年代开始进入电力系统专项业务应用，涉及电网调度自动化、电力负荷控制、计算机辅助设计、计算机仿真系统等的使用。20 世纪末，电力信息技术进一步发展到综合应用，各级电力企业开始建立治理信息系统，实现治理信息化，电力信息化逐渐从生产操作层走向治理层，并向更深层次拓展。

相对于传统行业，我国电力行业的信息化建设发展较早，已经有了一定的规模。到目前为止，电力企业的网络普遍建立，电力专用通信网已日趋完善，形成了微波、卫星、光纤、无线移动通信等多种类通信手段，通信范围覆盖全国。在此基础上，基本建成从国家电网公司→区域电网中心→省电力公司→地市电力公司→变电所（局）的四级计算机网络和电力生产调度网络，成为生产控制、电力调度以及信息传输和交换的重要基础设施。

随着电力市场化以及电网建设的进一步发展，传统的电力系统业务正在发生变化，这主要体现在电力交易系统、电能量计量系统的建设；会议电视、变电站视频监控（无人值守）、输变电线路监控及电厂视频监控等视频业务的出现；传统单一主机的调度自动化体系架构向客户机/服务器体系架构的转变；监视全网运行状况，提供故障记录和分析的故障录波系统的建设；雷电定位系统、气象信息系统的建设；多媒体业务的出现等。因此，基于 Internet/Intranet 的体现信息化综合业务应用的治理信息系统将成为电力企业信息化的发展重点。

电力工业的特点决定了电力信息安全不仅具有一般计算机信息网络信息安全的特征，还具有电力实时运行控制系统信息安全的特征。电力系统的信息安全是一项涉及电网调度自动化、继电保护及安全控制装置、厂站自动化、配电网自动化、电力市场交易、生产管理、电力营销、办公自动化系统等有关生产、经营和管理方面的多领域、复杂的大型系统工程。其中，电网调度自动化、继电保护及安全控制装置、厂站自动化、配电网自动化、电力市场交易等系统属于监控系统，生产管理、电力营销、办公自动化等系统属于管理信息系统。监控系统主要负责电力系统的生产控制业务，它又分为实时生产系统和准实生产系统；管理信息系统主要负责电力系统的信息化管理。监控系统的安全等级高于管理信息系统，实时生产系统的安全等级最高。系统的安全等级不同，安全防护措施也不一样，实时生产系统是电力系统安全防护的重点和核