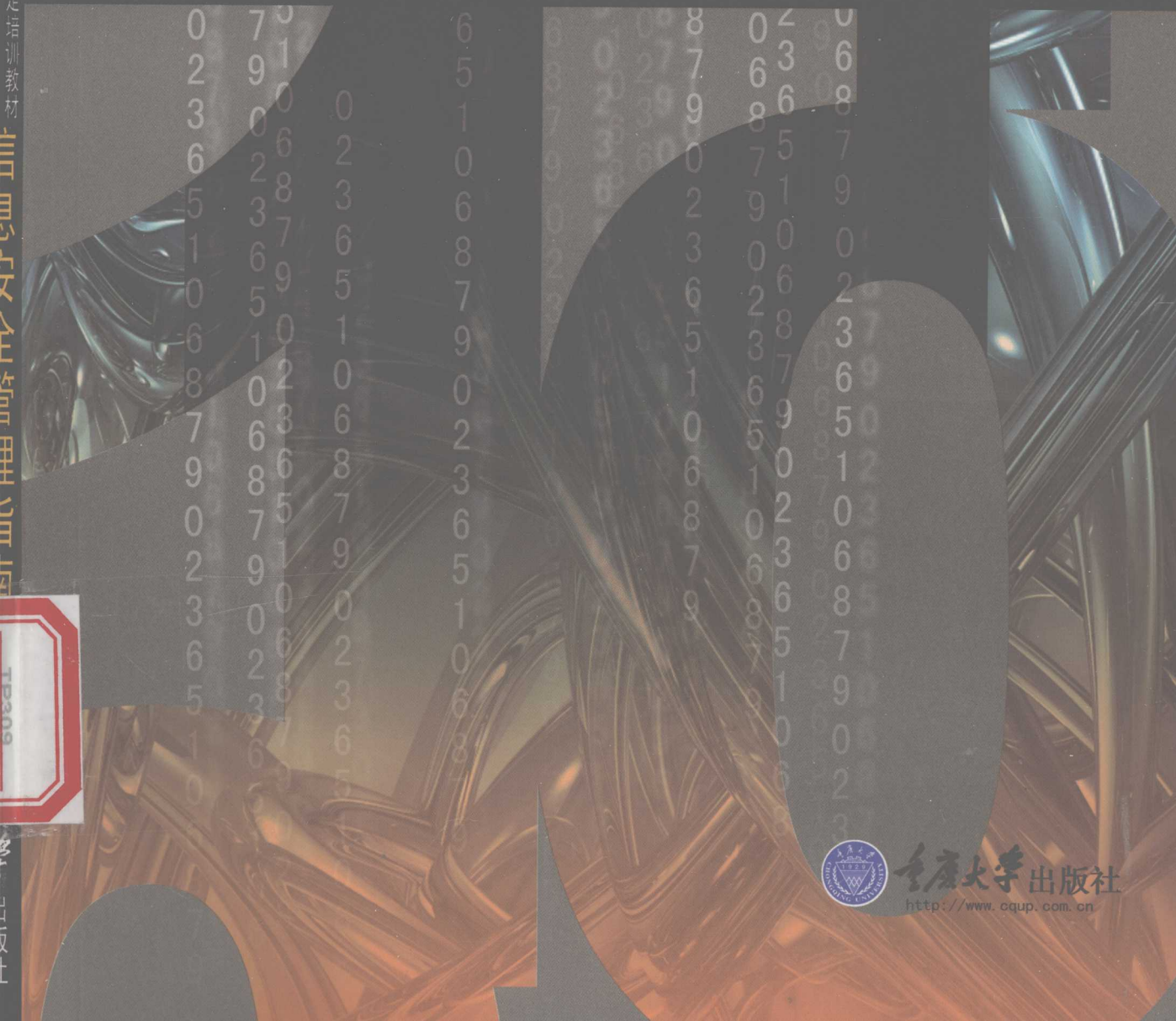
全国信息技术人才培养工程指定培训教材
信息安全理论与实用技术丛书

信息安全管理指南

信息产业部电子教育中心　组编
戴宗坤　主编

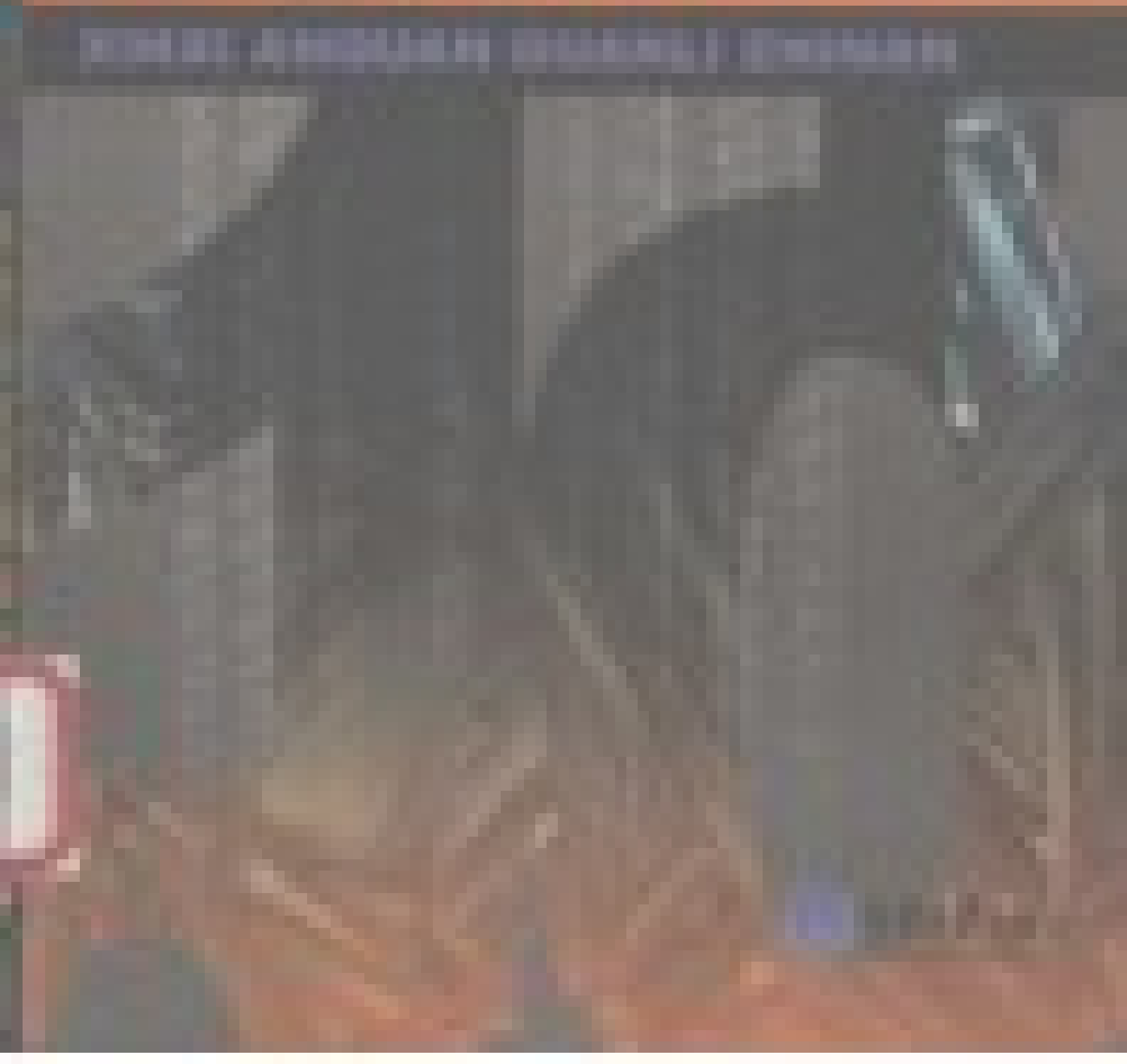
XINXI ANQUAN GUANLI ZHINAN



重庆大学出版社
http://www.cqup.com.cn

全国信息技术人才培养工程指定培训教材
信息安全管理指南

情報安全管理指南



全国信息技术人才培养工程指定培训教材

信息安全理论与实用技术丛书

信息安全管理指南

信息产业部电子教育中心 组 编
戴宗坤 主 编
罗万伯 胡 勇 吴少华 副主编

重庆大学出版社

内容简介

本书从信息安全有关的法律法规、行政、技术和工程管理等方面精辟地阐述了信息安全管理的理论、方法和工程实践，包括从信息安全角度识别信息系统及资源的方法和分类原则、识别并针对信息系统资源的脆弱性、威胁、影响等因素进行风险管理的过程、识别与对抗风险的理论与方法、以及从资源分析、风险分析与评估、安全需求分析到安全保护策略和措施选择的工程实践和实务操作等。

本书是"全国信息技术人才培养工程教材"之一，适于用作与信息技术和信息安全相关专业本科生、研究生的教材，也是相关专业从业人员值得优选的参考书。

图书在版编目(CIP)数据

信息安全管理指南/臧宗坤主编. —重庆：重庆大学出版社，2008.3

(信息安全理论与实用技术丛书)

ISBN 978-7-5624-4348-3

Ⅰ.信… Ⅱ.臧… Ⅲ.信息系统—安全管理—指南

Ⅳ.TP309-62

中国版本图书馆CIP数据核字(2008)第002487号

全国信息技术人才培养工程指定培训教材

信息安全理论与实用技术丛书

信息安全管理指南

[illegible]

臧宗坤 主编

[illegible]

[illegible]

[illegible]

重庆大学出版社出版发行

[illegible]

[illegible]

印刷：重庆市国际印刷有限公司

开本：787×1092 1/16 印张：14.25 字数：287千

2008年3月第1版 2008年3月第1次印刷

印数：1—3 000

ISBN 978-7-5624-4348-3 定价：25.00元

全国信息技术人才培养工程教材
编委会

通讯地址：北京 4356 信箱教育中心
http://www.ceiaec.orgl/

“全国信息技术人才培养工程教材”丛书序

当今世界，随着信息技术在经济社会各领域不断深化的应用，信息技术对生产力以至于人类文明发展的巨大作用越来越明显。党的“十六大”提出要“坚持以信息化带动工业化，以工业化促进信息化”，“优先发展信息产业，在经济和社会领域广泛应用信息技术”，明确了我国经济发展的道路，赋予了信息产业新的历史使命。近年来，日新月异的信息技术呈现出新的发展趋势，各类信息技术加快了相互融合和渗透的步伐，信息技术与其他技术的结合更加紧密，信息技术应用的深度、广度和专业化程度不断提高。

我国的信息产业作为国民经济的支柱产业正处于有利的国际、国内形势中，电子信息产业的规模总量已进入世界大国行列。但是我们也清楚地认识到，与国际先进水平相比，我们在产业结构、核心技术、管理水平、综合效益、普及程度等方面，还存在较大差距，缺乏创新能力与核心竞争力，“大”而不强。国际国内形势的发展，要求信息产业不仅要做大，而且要做强，要从制造大国向制造强国转变，这是信息产业今后的重点工作。要实现这一转变，人才是基础。机遇难得，人才更难得，要抓住本世纪头二十年的重要战略机遇期，加快信息产业发展，关键在于培养和使用好人才资源。《中共中央、国务院关于进一步加强人才工作的决定》指出，人才问题是关系党和国家事业发展的关键问题，人才资源已成为最重要的战略资源，人才在综合国力竞争中越来越具有决定性意义。

为抓住机遇，迎接挑战，实施人才强业战略，信息产业部启动了“全国信息技术人才培养工程”。该项工程旨在通过政府政策引导，充分发挥全行业和全社会教育培训资源的作用，建立规范的信息技术教育培训体系、科学的培训课程体系、严谨的信息技术人才评测服务体系，培养造就大批行业急需的、知识技能结构合理的高素质信息技术应用型人才，以促进信息产业持续快速协调健康发展。

由各方专家依据信息产业对技术人才素质与能力的需求，在充分吸取国内外先进信息技术培训课程优点的基础上，信息产业部电子教育中心精心组织编写了信息技术系列培训教材。这些教材注重提升信息技术人才分析问题和解决问题的能力，对各层次信息技术人才的培养工作具有现实的指导意义。我谨向参与本系列教材规划、组织、编写的同志们致以诚挚的感谢，并希望该系列教材在全国信息技术人才培养工作中发挥有益的作用。

王耀先

二〇〇四年四月十二日

前 言

本书是作者在2004年承担由国务院信息化工作办公室下达的“信息安全管理指南”研究项目的基础上，结合与同事们十多年来在信息安全管理方面的理论研究成果和工程实践经验，并经过多次修改最后形成。虽然作者尽了极大努力，并力求在书稿中体现中国特色和国家对信息安全管理的方针政策，但由于水平所限，书中仍可能存在需要精雕细刻甚至需要刀劈斧砍的地方；更由于信息安全管理理论和方法研究在国内还处于探索阶段，因此本书中如有与他人观点和管理实践不一致的地方，那应该是可以在学术上争鸣的见仁见智的事情了；再则，作者和同事们虽然尽了极大努力，但毕竟是迄今为止所做的事情，这种努力还会继续下去。总之，现在呈现给读者朋友的这本书，是我们多年辛勤劳动的结果，希望对读者朋友有所帮助。

作者和同事们在信息安全理论与方法研究方面已经投入了大量的资源和精力，出于职业良心和教学、科研的需要，我们先后将研究成果和经验心得以译著、专著和工具书的形式向社会毫无保留地奉献了。其中，于2000年4月由机械工业出版社出版了《防火墙与因特网安全》(译)；于2000年9月由金城出版社出版了《信息系统安全》、《信息系统安全工程学》和《VPN与网络安全》；于2003年3月由电子工业出版社出版了《英汉网络信息安全辞典》，同时出版了《信息系统安全》、《信息系统安全工程学》和《VPN与网络安全》的修订版；于2005年5月由重庆大学出版社出版了《信息安全应用基础》、《信息安全实用技术》和《信息安全法律法规与管理》，本书正好与这三本书构成一个完整体系，这也是作者与重庆大学出版社友好合作的完美体现。

本书涉及与信息安全有关的法律法规，行政、技术和工程管理的方方面面，既有信息安全管理理论与方法论的介绍；也有从信息安全管理角度识别信息系统及资源的方法和分类原则，以及识别信息系统资产的脆弱性、威胁、影响进而进行风险管理的过程描述；还有从信息安全管理角度识别风险、对抗风险的理论和方法的论述，以及进行基于风险管理的从资源分析、风险分析与评估、安全需求分析，到安全保护策略和措施选择的工程实践方法和实务操作的详细描述。从事信息系统的安全规划、设计、建设和保护，以及从事技术开发、信息安全咨询服务和产品生产的人们，都可以从本书中找到他们在其他地方找不到的东西；同时本书也可作为与信息技术和信息安全专业有关的研究生、本科生或培养高级专业技术人才时的教材或参考书。

参加本书编写的有戴宗坤、罗万伯、胡勇和吴少华等人。其中，戴宗坤负责全书的内容规划和设计，并主写第1、2章；罗万伯负责全书结构设计并主写第3、4章；胡勇起草“本书涉及的术语和定义”以及主写第5、6章；吴少华主写第7章以及附录。全书由戴宗坤和罗万伯审校，参加本书资料收集和整理的还有陈超、朱爱华等。

本书的编撰得到国务院信息化工作办公室王渝次司长和赵泽良副司长的热情鼓励和直接指导，在此表示衷心感谢。

戴宗坤

2007年夏

本书涉及的基本术语和定义

信息技术(Information Technology,IT)　获取、加工、存储、变换、显示和传输文字、数值、图像与视频、音频和言语信息,以及提供这些服务的方法与设备的总称。这一术语有时与自动电子处理设备的含义很难严格区分。

信息技术安全,IT 安全(IT Security)　与定义、获得以及维持信息技术系统及其组件机密性、完整性、可用性、可确认性、抗抵赖性和可靠性等有关的所有技术方面。

信息技术安全策略,IT 安全策略(IT Security Policy)　对一个组织的信息系统包括敏感信息在内的所有资产实施管理、保护以及分配控制措施的规则和指令(集)。

信息安全(Information Security)　提供信息和信息系统的机密性、完整性、可用性、可确认性和抗抵赖性,从而使信息和信息系统免遭未授权的访问、使用、泄露、干预、修改、重放和破坏,并保证使用和操作信息以及信息系统的任何实体的身份不被假冒或欺骗,实体的来源与行为可被唯一跟踪和不可抵赖。其中,机密性指对信息和信息系统的访问和泄露只限于被授权者的特性,包括任何形式的个人隐秘和专用权信息;完整性指信息和信息系统不受到任何形式的未授权修改和重放的特性,并且还包括信息和信息系统的来源真实性;可用性指信息和信息系统能及时、可靠地为授权者提供访问和使用,以及能在面对各种攻击或出现差错和故障的情况下继续提供实质性服务,并且能够及时地恢复正常服务的特性;可确认性指实体的行为被唯一跟踪到该实体的特性;抗抵赖性指对信息和信息系统进行使用和操作的行为及其内容不能在事后予以否认的特性。

国家(信息)安全系统(National Security System)　由某一(国家)机构,或机构的合约方,或机构所信任的其他组织所使用或运行的(包括任何通信系统在内

的)信息系统。这些信息系统或者涉及(国家)情(谍)报活动、国计民生和社会稳定;或者涉及与国家安全有关的密码活动、军事力量的指挥与控制或者作为武器与武器系统组成部分的装备,以及直接实现军事或情(谍)报业务的关键信息等的功能、操作和使用;或者在国家法律、法规和政策限制下已被授权保护其中的信息。

资产(Asset) 信息系统中对一个组织具有价值的任何东西和事物(包括硬件的或软件的、有形的或无形的、货币化的或非货币化的,等等)。

机密性(Confidentiality) 对信息和信息系统的访问和泄露只限于被授权者的特性,包括任何形式的个人隐秘和专用权信息。

数据完整性(Data Integrity) 信息(数据)不受到任何形式的未授权修改和重放的特性,并且还包括保证信息来源的真实性。

完整性(Integrity) 对数据完整性概念的合理延伸,指信息和信息系统不受到任何形式的未授权修改和重放的特性,并且还包括保证信息和信息系统来源的真实性。

可用性(Availability) 信息和信息系统能及时、可靠地为授权者提供访问和使用的服务能力,以及能在面对各种攻击或出现差错和故障的情况下继续提供实质性服务,并且能够及时地恢复正常服务的特性。

可确认性(Accountability) 又称可审查性,或可追查性,一种保证某一实体的行为可被唯一跟踪到该实体的特性。

真实性(Authenticity) 保证一个实体或资源的身份及来源就是所声称的那个实体或资源的身份和来源的特性。真实性往往通过对用户、进程、系统和信息的鉴别来实现。

抗抵赖性(Non-repudiation) 对否认和抵赖曾经使用和操作过信息或信息系统的行为或内容进行对抗的特性。

脆弱性(Vulnerability) 一个或一组信息和系统资产的弱点或缺陷,这些弱点或缺陷可能导致在系统安全规程、系统设计、系统实现、内部控制和运行等方面被威胁者开发利用或直接遭到破坏。

威胁(Threat) 旨在限制、阻止、破坏信息系统业务,或降低服务能力,或降低系统或设备能力有效性,或泄漏和窃取信息和系统资产等的潜在力量、能力和战略目标的总和,主要包括对信息和系统的机密性、完整性、可用性、可确认性和抗抵赖性等造成危害的可能性和危害程度的所有因素。

影响(Impact) 不期望的事件所引起的后果,包括有形的和无形的,货币化的和非货币化的。

风险(Risk) 给定的威胁利用某一或某组(信息系统)资产的脆弱性对一个组织造成损失的可能性(概率),以及损失后的后果的总和。

风险分析(Risk Analysis) 识别风险的时间和空间分布及其强度(或等级)的过程。

风险管理(Risk Management) 识别、确定、控制、降低、消除或转移影响系统资产安全性的不定因素的总过程,包括风险分析、绩效分析、安全保护措施的选择、实现与测试、安全评估,以及所有的与安全有关的监管活动。

残留风险(Residual Risk) 信息系统在采取保护措施后仍未消除的风险。

安全措施(Safeguard) 安全措施也称安全保护措施,是控制、降低、消除或转移风险的实践、程序和机制。

基线控制(Baseline Control) 一个(行业)系统或组织的信息系统从安全保障工程角度所建立的安全保护措施的最小集。

组织(Organization) 一个机构管理下的具有共同利益和共同安全属性的业务单位或部门的总称。例如,一个企业,一个机关,或一个法人单位,在本书中都是组织,有时也称为团体或共同体。

目 录