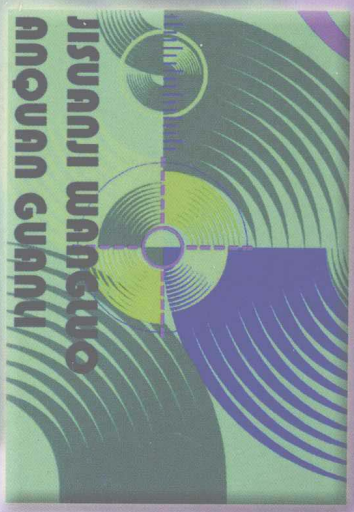
普通高等教育“十五”国家级规划教材

教育部高职高专规划教材

Jiaoyubu Gaozhi Gaozhuan Guihua Jiaocai

张佳南 主编

计算机网络安全管理



中国财政经济出版社

普通高等教育“十五”国家级规划教材
教育部高职高专规划教材

计算机网络安全管理

主编　张佳南
杨良耀

中国财政经济出版社

图书在版编目（CIP）数据

计算机网络安全管理/张佳南主编. —北京：中国财政经济出版社，2002.9

普通高等教育“十五”国家级规划教材. 教育部高职高专规划教材

ISBN 7-5005-5987-9

Ⅰ.计… Ⅱ.张… Ⅲ.计算机网络-安全技术-高等学校：技术学校-教材 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2002）第 060186 号

中国财政经济出版社出版

URL：http://www.cfeph.com.cn

E-mail：cfeph@drc.gov.cn

社址：北京海淀区阜成路甲 28 号 邮政编码：100036

发行电话：88190616 88190655（传真）

北京财经印刷厂印刷

850×1168 毫米 32 开 10.875 印张 254 000 字

2002 年 12 月第 1 版 2002 年 12 月北京第 1 次印刷

定价：16.00 元

ISBN 7-5005-5987-9/TP·0056

出 版 说 明

教材建设工作是整个高职高专教育教学工作的重要组成部分。改革开放以来，在各级教育行政部门、学校和有关出版社的共同努力下，各地已出版了一批高职高专教育教材。但从整体上看，具有高职高专教育特色的教材极其匮乏，不少院校尚在借用本科或中专教材，教材建设仍落后于高职高专教育的发展需要。为此，1999 年教育部组织制定了《高职高专教育基础课程教学基本要求》（以下简称《基本要求》）和《高职高专教育专业人才培养目标及规格》（以下简称《培养规格》），通过推荐、招标及遴选，组织了一批学术水平高、教学经验丰富、实践能力强的教师，成立了“教育部高职高专规划教材”编写队伍，并在有关出版社的积极配合下，推出一批“教育部高职高专规划教材”。

“教育部高职高专规划教材”计划出版 500 种，用 5 年左右时间完成。出版后的教材将覆盖高职高专教育的基础课程和专业主干课程。计划先用 2～3 年的时间，在继承原有高

职、高专和成人高等学校教材建设成果的基础上，充分汲取近几年来各类学校在探索培养技术应用型专门人才方面取得的成功经验，解决好新形势下高职高专教育教材的有无问题；然后再用2～3年的时间，在《新世纪高职高专教育人才培养模式和教学内容体系改革与建设项目计划》立项研究的基础上，通过研究、改革和建设，推出一大批教育部高职高专规划教材，从而形成优化配套的高职高专教育教材体系。

“教育部高职高专规划教材”是按照《基本要求》和《培养规格》的要求，充分汲取高职、高专和成人高等学校在探索培养技术应用性专门人才方面取得的成功经验和教学成果编写而成的，适合高等职业学校、高等专科学校、成人高校及本科院校举办的二级职业技术学院和民办高校使用。

教育部高等教育司

2000 年 12 月

前　言

当前，我们正处在由工业时代向信息时代过渡的时代，有人称之为“后工业时代”，也有人称之为“前信息时代”。这个时代的一个显著特征是信息化。信息化的涵义是信息技术和信息在广度（普及）和深度（提高）上的发展，其具体标志为：信息技术高度发展；信息系统普及使用；信息资源极大丰富；信息意识和信息利用水平空前提高。

信息技术是人类开发和利用信息的技术。信息系统是信息技术应用于信息过程的产物。现代信息技术和信息系统延伸了人的感官、大脑和语言系统，拓展了人的信息活动空间，是信息化的基础和动力。由于 Internet、Intranet 和 Extranet 综合运用了现代信息技术，承载了无数的信息系统，已成为人类最重要的信息环境，故也有人将信息化称为网络化，将信息时代称为网络时代。

信息是一种抽象的概念。它作用于人的认知过程，可以影响人的认识和行为；它作用于系统，可以影响系统的存在状态和运动方式。

信息是一种特殊的资源，具有异化性、存储性、传递性、可控性、共享性和非线性等性质。在信息时代，信息的作用越来越突出，被称为财富和力量的“倍增器”。有效地获取、处理、传递、控制和利用信息是信息化的直接目标。

网络空间（也称虚拟空间）是信息时代人类信息活动的主要空间。人类在实际空间中的各种矛盾和斗争势必会反映到虚拟空间中来。信息作为一种资源，围绕信息获取权、控制权和使用权的斗争势必会在虚拟空间展开。伴随信息时代的到来，信息化和信息战、信息网络和信息犯罪的矛盾将始终存在。进攻信息战和信息犯罪，两者既有共同之处，也有不同之处。共同之处在于：都要利用网络的脆弱性达到入侵和破坏网络的目的。不同之处在于：前者是国家或集团行为，后者是个人或团伙行为；前者的目标和影响是全局的，后者的目标和影响是局部的；前者作用的过程是持续的，后者作用的过程是短促的；前者所用资源是举国的，后者所用资源是有限的；前者通常与其他对抗方式紧密相关，后者通常与其他对抗方式无关。进攻信息战和信息犯罪是两类性质不同的网络威胁。为了应对这些网络威胁，必须高度重视网络安全。网络安全在军事领域被称之为防御信息战，在信息时代是事关全局的战略问题。

网络安全涉及诸多的领域，是一个复杂的系统工程问题。按照系统工程的观点，系统是由要素组成的；要素是相互关联的，即按某种结构组织在一起；要素和结构决定了系统的功能和性质。研究系统，不仅要关注其组成，更要关注其结构，尤其对于复杂的系统更应如此。本此精神，本书在讨论网络安全时，注重了其知识、技术和管理的体系结构。

网络安全的知识结构可以分为三个层次：计算机网络理论和广义信息理论是基本理论；可信计算机网络理论和密码学理论是

应用基础理论；网络防护、系统防护和应用防护是其具体应用。技术结构包括防护技术、检测技术、反应技术和恢复技术。管理结构包括有关人、财、物、信、时的管理。网络安全领域和其他领域一样，人的因素第一。需要网络工作者有良好的素质；需要有关人员树立正确的网络安全观，认识网络安全以下的基本性质：普遍性，即所有网络都存在安全问题，无一例外，过去存在，现在存在，将来也会存在；对抗性，即安全是针对威胁而言的，两者是相反相成的，只有充分认识威胁，才能有效保障安全；相对性，即没有“天衣无缝”的绝对安全，风险较小的“相对安全”才是我们的目标；系统性，即非一、二件安全产品所能解决问题的，而是要在分析网络资源及其分布、重要性、脆弱性、威胁性的基础上形成完整的安全解决方案；综合性，即从应用层到物理层，综合运用密码和非密码技术，采取防护、检测、反应和恢复多种措施，人、技术和制度方面有力支持；动态性，即网络安全技术是随信息技术、黑客技术和病毒技术发展而发展的；网络安全需求是随网络威胁环境变化而变化的，网络安全系统必须及时维护和更新。

本书共十五章，分为四个部分：

第一部分（第一章至第三章）主要阐述网络安全的重要性、必要性和针对性；

第二部分（第四章至第十三章）主要阐述网络安全的概念、理论和方法；

第三部分（第十四章）主要阐述网络安全管理的主要方面；

第四部分（第十五章）主要阐述网络安全技术的发展方向和我们的对策。

本书是计算机网络安全管理的基础知识，突出了概念和方法，力求通俗易懂，不追求系统性、完整性和理论性。读者在阅

读每章之后，可结合思考题，掌握所学的内容。实际应用中，可以本书的内容为线索，阅读有关书籍和文献，深入掌握所需要的知识。

本书由张佳南主编，郑小玲、汪佑民参编。张佳南撰写了纲目、前言、第十、十二、十四、十五章和思考题；郑小玲撰写了第一至第八章；汪佑民撰写了第九、十一、十三章。张佳南对全书进行审校和补充；郑小玲承担了全书的文字编辑工作。在本书编撰过程中，欧成君编辑进行了全程跟踪和指导，在此表示真挚地感谢！

本书既可作为高职、高专和本科生的教科书，也可作为教师的教学参考书。因为时间仓促，肯定会有差错和不尽人意之处，敬请读者指正。

主　编

2002 年 3 月于北京

目　录

第一章　绪论……（1）
第一节　信息社会和信息化……（1）
第二节　信息化和 Internet ……（3）
第三节　信息化和信息战……（4）
第四节　网络威胁和网络安全……（6）
第五节　网络全系统、全过程安全防护……（8）
思考与练习……（8）
第二章　Internet 和 Intranet ……（9）
第一节　Internet / Intranet / Extranet ……（9）
第二节　TCP / IP 协议的安全问题 ……（14）
第三节　UNIX 系统的安全问题 ……（17）
第四节　Web 服务器和浏览器的安全问题……（25）
思考与练习……（29）
第三章　网络威胁分析……（30）

第一节 网络威胁的来源……（30）
第二节 网络威胁的特征……（35）
第三节 网络入侵的过程……（40）
第四节 网络攻击的手段……（44）
第五节 攻击影响的评估……（51）
思考与练习……（53）
第四章 可信计算机及其网络……（54）
第一节 计算机网络安全目标……（54）
第二节 计算机安全评估准则……（59）
第三节 计算机安全模型……（64）
第四节 网络安全模型……（69）
第五节 网络安全的分级……（75）
第六节 网络安全的范围……（78）
思考与练习……（80）
第五章 系统安全防护……（81）
第一节 识别与验证……（81）
第二节 访问控制……（89）
第三节 审计跟踪……（100）
第四节 安全操作系统……（103）
第五节 安全数据库管理系统……（108）
思考与练习……（115）
第六章 网络安全防护……（116）
第一节 防火墙……（116）
第二节 虚拟专用网……（131）
思考与练习……（144）
第七章 密码技术应用……（145）
第一节 密码学基础……（146）

第二节　传输信息加密……（157）
第三节　存储信息加密……（162）
第四节　数据完整性……（165）
第五节　数字签名……（169）
第六节　密钥管理……（172）
思考与练习……（187）
第八章　入侵检测……（188）
第一节　入侵检测概述……（188）
第二节　脆弱性扫描……（199）
第三节　系统级入侵检测……（203）
第四节　网络级入侵检测……（206）
思考与练习……（210）
第九章　病毒防治……（211）
第一节　计算机病毒的特征……（211）
第二节　计算机病毒的分类……（216）
第三节　计算机病毒的检测……（219）
第四节　计算机病毒的清除……（227）
第五节　计算机病毒预防……（231）
思考与练习……（239）
第十章　反应与恢复……（240）
第一节　入侵反应……（240）
第二节　受损系统和网络的恢复……（249）
思考与练习……（253）
第十一章　网络环境安全……（254）
第一节　机房安全……（254）
第二节　网络传输介质安全……（264）
第三节　设备安全……（268）

思考与练习…… (271)
第十二章 网络安全规划…… (272)
第一节 安全策略制定…… (272)
第二节 安全服务需求…… (281)
第三节 安全机制设定…… (282)
第四节 安全系统集成…… (284)
第五节 安全系统仿真…… (290)
思考与练习…… (294)
第十三章 网络安全系统…… (295)
第一节 电子商务安全系统…… (295)
第二节 电子邮件安全系统…… (305)
思考与练习…… (316)
第十四章 网络安全管理…… (317)
第一节 法规管理…… (317)
第二节 技术管理…… (319)
第三节 市场管理…… (321)
第四节 运行管理…… (323)
第五节 情报管理…… (326)
第六节 人员管理…… (329)
思考与练习…… (330)
第十五章 后 记…… (331)
第一节 网络安全技术的发展方向…… (331)
第二节 网络安全对策…… (333)
思考与练习…… (334)
主要参考文献…… (335)

第一章

绪　论

计算机网络对人类经济和生活的冲击是其它任何信息载体所无法比拟的，它的高速度发展和全方位渗透，推动了整个社会的信息化发展。由于计算机网络具有分布广域性、结构开放性、资源共享性和信道共用性等特点，所以增加了网络的实用性，同时也使计算机网络变得脆弱，使其面临严重的威胁。网络安全问题已成为计算机网络应用领域中最突出的问题。在我们具体探讨网络安全管理问题之前，先简单了解一下信息化进程、信息化与Internet、信息战、网络威胁与网络安全等问题。

第一节
信息社会和信息化

信息化是指在经济和社会活动中，通过普遍地采用信息技术和电子信息设备，有效地开发和利用信息资源，促进经济发展和社会进步。

在人类历史上，物质、能源和信息一直是人类社会发展的三大基本资源，工业革命使人类在生产利用物质和能源两种资源上取得了巨大成功，高效率、专业化的大生产创造了一个个经济奇迹，人类社会进入工业化阶段。第二次世界大战以后，以微电子技术、计算机技术、通信技术、网络技术为代表的现代信息技术，使人类对信息资源的开发利用摆脱了迟缓、分散的传统方式，代之以高效率、专业化、多样化的现代方式。信息成为生产力的重要因素和社会发展的战略资源，信息技术成为当今世界最先进的生产力。

广泛利用信息技术，建设国家信息网络，发展信息产业，充分开发利用信息资源，提高经济效益，加速推进信息化进程，成为当今世界经济竞争的焦点。进入 90 年代以来，信息化已成为世界各国经济和社会发展的战略选择，成为衡量一个国家现代化水平和综合国力的重要标志。一些国家相继制定并实施了“信息高速公路”计划。我国政府也高度重视国家信息化建设，我国的通信业务以世界最快的速度发展，“金”字工程推动了国民经济各个领域的信息基础设施建设，Internet 也成为我国信息化应用的热点，华夏大地涌动着信息革命的浪潮。

在全球信息化浪潮推动下，人类社会正由工业社会迈向信息社会。信息社会的基本特征是信息化。在信息社会里，信息技术高速发展，信息资源空前丰富，人们对信息的需求越来越迫切，计算机网络对整个社会的的影响越来越大，社会对计算机网络的依赖也越来越强，尤其是计算机技术和通信技术相结合所形成的信息基础设施建设已经成为反映信息社会特征最重要的基础设施建设。人们建立了各种各样的信息系统，使得人类社会的一些机密和财富高度集中于计算机中。但是这些信息系统都是依靠计算机网络对信息进行传输、存储和处理的，因此，以网络方式获得

信息和交流信息已成为信息社会的一个重要特征。

网络正在逐步改变人们的工作方式和生活方式，成为当今社会发展的一个主题。随着网络的开放性、共享性和互联程度扩大，特别是 Internet 的普遍使用，网络的重要性和对社会的影响也越来越显著。人类在感受网络对社会文明的巨大贡献的同时，也认识到网络信息安全问题已成为影响国家、企业大局和长远利益而亟待解决的重大关键问题。

第二节
信息化和 Internet

信息技术的发展推动了信息化发展的进程，数字化、网络化成为它的技术特点。所以有人说，信息化就是数字化和网络化。以 Internet 为代表的信息网络向人们展示了信息化的网络化特点，它将全球 180 多个国家和地区、100 多万个各类网络、1 亿多台主机连接起来，为 5 亿多用户提供了多样化的信息服务，把巨大的地球变成了信息瞬间可达、方便交换的“地球村”。

网络化、数字化的特点使信息空间跨越国境，有别于传统方式的信息获取、存储、处理、传输和使用，从而也给现代社会的正常发展带来了一系列的前所未有的风险和威胁。信息安全成为数字化安全的基础和信息化成功的关键。特别是面对某些妄图以信息能力称霸的超级大国的信息战威胁，我们必须高度重视维护国家的主权独立和安全，高度重视在信息化基础上发展我国的经济实力。

第三节
信息化和信息战

信息化是信息应用的一场革命，它推动了社会的进步与发展。但同时也应该看到，信息系统中的错误和漏洞必然成为攻击者攻击的目标。因此，在信息化进程中不可避免地伴随着信息战。

一、信息战的概念

目前，我们所面临的问题是信息化问题，我们所面临的战争是信息化战争。那么什么是信息化战争呢？信息化战争归结起来，就是将作战中的各个环节都予以信息化，再加上一个完善的信息指挥控制系统对各种信息化了的资源予以优化，以取得最优的效能。在信息化战争中除了以信息技术武装传统作战中的各个环节之外，又开辟了一个新的作战领域，即在信息及信息系统方面的对抗，人们把这方面的对抗称为信息战。

信息战是一种以获得信息权力为目标的没有硝烟的战争，信息战可以说是一种国家行为的恶意攻击。信息战的攻击目标包括各种军事指挥、通信系统、能源、运输和金融等与国家的政治、经济、文化密切相关的系统。信息战所采用的信息攻击手段主要为电子干扰、电子压制、各种类型的电脑病毒等。在和平时期，信息战处于相对隐蔽状态，但是一旦战争爆发，信息战将出其不易地发挥出巨大的破坏力。