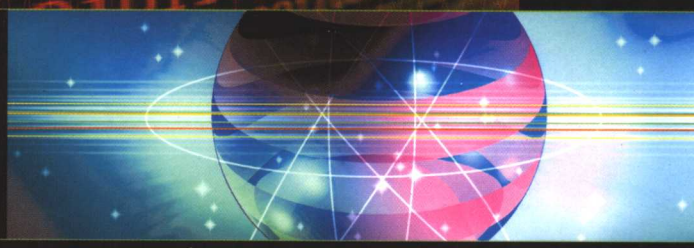
中等职业教育电子信息类专业
“双证课程”培养方案配套教材

国家信息化
计算机教育认证
CEAC
指定教材

CEAC

信息安全技术

主编　谭建伟
指导　中国职业技术教育学会
审定　CEAC信息化培训认证管理办公室



高等教育出版社
HIGHER EDUCATION PRESS

中等职业教育电子信息类专业“双证课程”培养方案配套教材

信息安全技术

主编　谭建伟

指导　中国职业技术教育学会

审定　CEAC 信息化培训认证管理办公室

高等教育出版社

内容简介

本书是高等教育出版社与CEAC信息化培训认证管理办公室联合推出的认证课程教材，与CEAC电子技术专业助理工程师认证课程配套。

本书从技术和管理的角度全面讲解了计算机网络的安全防护和安全应用知识，内容涉及信息系统实体安全防护、信息加解密技术、PKI技术、防范黑客入侵技术、防火墙技术、计算机病毒防治技术、备份技术信息安全管理技术以及相关的法律规范等。书中章节相互关联又自成体系，内容能满足读者全面、系统学习网络安全的需要。本书注重信息安全技术的科学性和实用性，力求做到内容简洁、通俗易懂，其中实例、习题和实际应用紧密关联，能有效提升信息安全技能水平。

本书可作为中等职业学校计算机网络专业网络安全课程和专业证书培训课程的教材，也可作为参加CEAC认证考试的人员复习考试用书，还可供计算机网络安全管理者参考使用。

图书在版编目（CIP）数据

信息安全技术/谭建伟主编. —北京：高等教育出版社，2006.7

ISBN 7-04-019823-1

Ⅰ. 信… Ⅱ. 谭… Ⅲ. 信息系统-安全技术-专业学校-教材 Ⅳ. TP309

中国版本图书馆CIP数据核字（2006）第069687号

策划编辑 李 波 **责任编辑** 俞丽莎 **封面设计** 于 涛 **责任绘图** 黄建英
版式设计 王艳红 **责任校对** 张 颖 **责任印制** 毛斯璐

出版发行 高等教育出版社
社 址 北京市西城区德外大街4号
邮政编码 100011
总 机 010－58581000

经 销 蓝色畅想图书发行有限公司
印 刷 北京市联华印刷厂

开 本 787×1092 1/16
印 张 13
字 数 310 000

购书热线 010－58581118
免费咨询 800－810－0598
网 址 http://www.hep.edu.cn
http://www.hep.com.cn
网上订购 http://www.landraco.com
http://www.landraco.com.cn
畅想教育 http://www.widedu.com

版 次 2006年7月第1版
印 次 2006年7月第1次印刷
定 价 19.30元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

物料号 19823－00

中等职业教育电子信息类专业“双证课程”培养方案配套教材

编 审 委 员 会

出 版 说 明

中等职业教育肩负着为社会主义建设培养数以亿计的高素质劳动者的历史任务。要完成这个历史重任，职业教育应增强服务于社会经济发展的意识，要从学科本位向就业与职业技能为本位转变。职业学校要坚持以服务为宗旨，以就业为导向，面向社会、面向市场办学，深化办学模式和人才培养模式改革，努力提高职业教育的质量和效益。

在职业教育中，国家提倡学历证书、培训证书或职业资格证书并举的双证书制度。双证书制度作为沟通职业教育与行业用人需求，联系职业教育与劳动就业制度的桥梁，起到越来越重要的作用，是促进职业学校学生就业的重要举措之一。

《中华人民共和国职业教育法》中明确规定了“在我国实行学历证书、培训证书和职业资格证书制度”。“证书标准”有助于推动职业学校人才培养模式的转变，起到促进就业作用，职业教育工作者、行业企业专家、相关政府部门或行业组织需要共同努力，科学、理智地选择各类职业认证及培训教学资源。

全国哲学社会科学“十五”规划重点课题“职业教育与就业准入制度互动关系研究”课题组在中国职业技术教育学会、信息产业部信息化培训认证管理办公室的指导下，在教育行政部门、劳动和社会保障行政部门有关领导和学者的支持下，研发成功了中等职业教育电子信息类专业“双证课程”培养方案，该方案于2005年通过中国职业技术教育学会、信息产业部信息化培训认证管理办公室组织的专家鉴定。根据该方案，我们共同组织编写了中等职业教育电子信息类专业“双证课程”唯一配套教材，并列入劳动和社会保障部全国职业培训与技能鉴定教材。

本套教材贯彻了课题改革的成果，突出行业需求、符合教学管理要求，力图体现当前中等职业教育教学改革与创新思想。主要特点有:

（1）依据行业企业需求开发。配套教材根据信息产业发展对复合型高技能人才需求的特点，结合信息产业部最新推出的“CEAC——院校IT职业认证证书”标准要求，通过认证表明了持证人具备了相应认证的技术水平和应用能力，可以作为相关岗位选聘人员、技术水平鉴定的参考依据。将其引入学历教育，可以使中职学生在不延长学制的情况下，同时获得职业证书，提高就业的竞争力。

（2）依据最新专业目录开发。配套教材以教育部最新制定的《中等职业教育专业目录》中的电子信息大类专业设置情况为依据，进行专业课程建设。根据行业的职业认证的要求，每个专业的培养方案中，有3～5门课程与相应的职业认证要求直接对应。

通过对电子信息行业的职业分析，我们重点开发了一系列职业专项能力教材。因为职业专项能力采用循序渐进的方式进行培养，反映了某项职业专门技术从易到难的训练过程，也是理论学习从简到难的过程，故又称为“链式课程”（Chain Curriculum）教材。同时将努力配套立体化教学资源，以保证这些课程的授课质量。

本套教材包括“计算机及应用专业（办公自动化方向）”、“计算机及应用专业（计算机及

外设维修方向）”、“计算机软件技术专业（可视化程序设计方向）”、“计算机软件技术专业（模块级代码开发方向）”、“计算机网络技术专业（网络工程与维护方向）”、“计算机网络技术专业（网络管理与应用方向）”、“信息管理专业（企业信息化方向）”、“计算机信息管理专业（数据库管理与维护方向）”等专业方向的22门认证课程教材。

教材根据教育部“技能型紧缺人才培养方案”和中等职业教育电子信息类“企业技能型人才培养方案”编写，运用以就业为导向的职业能力系统化的开发方法开发而成。教材注重对学生职业技能的培养，使认证考试和中等职业学校日常教学紧密结合。教材出版的同时，将为教师提供可供教学使用的电子演示方稿和考证复习题，以帮助学生顺利取得“CEAC——院校IT职业认证证书”。

由于时间仓促，本套教材还不可避免地存在这样那样的不足，甚至由于学识水平所限，虽竭智尽力，仍难免谬误，希望专家、同行、学者给予批评指正。

高等教育出版社

CEAC信息化培训认证管理办公室

2006年4月

序

我很高兴看到，根据全国哲学社会科学“十五”规划重点课题“职业教育与就业准入制度互动关系研究”成果之一的“中等职业教育‘双证课程’培养方案”，编制出了“中等职业教育电子信息类专业‘双证课程’培养方案”。该培养方案的系列配套教材，将由高等教育出版社出版。

中等职业教育肩负着为社会主义建设培养数以亿计的高素质劳动者的历史任务。全面建设小康社会，走新型工业化道路，提高产业竞争力，推进城镇化，解决“三农”问题，促进就业和再就业，对提高劳动者素质、加快技能型人才培养提出了迫切要求。

为适应经济社会迅速变革的需要，职业教育应坚持以学生为中心、以能力为本位的原则，增强服务经济社会发展和人的发展的能力。以服务为宗旨，以就业为导向，面向社会和市场办学，深化办学模式和人才培养模式改革，提高教育教学质量，是职业教育一项长期的任务。中等职业教育要根据行业企业需求，设置专业、开发课程，推进精品课程和精品教材建设。紧跟当今世界行业企业生产和技术进步的要求，不断更新教材和教学内容，增强职业教育的适应性和针对性。实行产教结合，加强校企合作，积极开展“订单式”培养。优化课堂教学和实训环节，强化就业技能和综合职业能力培养，大力推行学历证书和职业证书教育。

“中等职业教育电子信息类专业‘双证课程’培养方案”及其系列配套教材，是国家信息化培训认证管理办公室和中国职业技术教育学会合作的结果，是进行电子信息类专业建设和课程改革的有益探索。这种由电子信息领域教育专家和信息产业行业部门合作，在对信息产业人才需求进行分析基础上，有针对性地设计出符合产业发展需求的技能型人才培养方案，编写出配套教材并由行业部门颁发相应的职业证书，将有利于提高学生的职业能力，有利于职业学校人才培养“供需对路”，有利于教育更好地为行业企业服务。在国内还少有成套方案、成熟经验的情况下，能在较短的时间内编写出系列教材及相应的数字化教学资源，实属难能可贵。

希望这套教材的出版，对中等职业教育电子信息类专业建设有所裨益和推动，并再接再厉，在不断借鉴国内外经验的基础上，在教育教学中不断改革和实践，以期该套教材日臻完善。

刘来泉

2006年4月10日

刘来泉：中国职业技术教育学会常务副会长

序

党的十六大、十六届五中全会和《2006—2020年国家信息化发展战略》对推进信息化建设提出了更新、更高的要求。要完成好信息化推进的各项任务，人才是关键。培养大批既有专业技术，又能熟练运用电子信息技术的人才，已成为加快经济社会发展的迫切任务之一。

马叔平同志牵头研究的全国哲学社会科学“十五”规划重点课题“职业教育与就业准入制度互动关系研究”取得了一系列成果，其中之一“中等职业教育电子信息类专业‘双证课程’培养方案”已通过评审。本课题以信息产业和信息化的需求为导向，研究如何培养急需的信息化人才和信息产业一线技术工人，我感到非常及时。

我非常欣慰地看到，该课题在研究中很好地体现了“坚持以就业为导向，增强职业教育主动服务经济社会发展的能力”的原则。在对信息产业行业的人才需求进行调查分析的基础上，结合国家有关的职业标准、行业认证标准，制定符合信息产业发展和信息化建设需要的“人才培养”方案，既有利于培养符合需求、供需对路的人才，促进信息产业和信息化的发展，同时也有利于教育部门深化教育改革，提高办学质量和效益，实在是值得肯定的。

信息化推进司作为信息产业部负责推进信息化工作的职能部门，肩负着推动信息化人才培养的职责。该方案符合推进信息化建设、促进信息化人才培训的工作目标。期待该方案在推动信息产业人才培养方面能够发挥积极作用，为我国信息化建设做出应有的贡献。

陈伟

2006年4月6日

陈伟：信息产业部信息化推进司司长

前　言

如今，计算机网络这一人类伟大的发明已经广泛深入到社会生活的各个角落，人们利用计算机网络传输数据、遨游网络世界，充分享受着计算机网络带来的快乐。在计算机帮助我们工作、学习、生活的同时，也带来了新的安全威胁，诸如财务系统感染病毒、信息全部丢失、黑客的侵入使军事情报泄密、盗发 E-mail 侵犯个人隐私等现象，使人们不得不关注计算机网络的安全应用问题。许多重大黑客事件表明，计算机网络存在许多漏洞，而中国计算机网络的安全防护能力相对薄弱，据报道中国 95%以上的与 Internet 相连的主机曾遭受过黑客攻击。作为计算机网络的应用者，如果不了解安全防护知识，没有安全应用防护技能，就很难有效、可靠地使用计算机，所以普及计算机网络安全教育是大势所趋。

本书是一本以网络安全基本原理为基础，以网络安全基本技术为落脚点，以贴近网络安全应用的实际内容为对象的计算机网络安全技术基础教材。书中不涉及过多、过深的计算机安全专业理论以及空洞的专业名词和生涩的专业术语，对可操作内容列出了完整的操作步骤，期望对提高职业学校学生的安全防护技能有所帮助。计算机网络安全技术的特殊性使得每章内容相对独立，每章都争取有针对性地解决一些实际应用中的安全问题。同时，也注意兼顾计算机网络安全理论体系的完整性，做到章节内容渐进、衔接、呼应。

作为 CEAC 培训认证的专门教材，本书按照 CEAC 认证考试大纲的要求，全面详细讲解考纲内容，并力争重点突出，难点弱化。书中理论知识习题以认证考试的标准化题型为基准，同时兼顾实际应用和理论复习的需求。

全书共分 10 章。第 1 章全面介绍信息网络安全的基本概念，帮助读者建立网络安全防护理论的整体框架。第 2 章讲解信息系统实体安全防护技术，只有从最基本的应用环境入手，才能有效保证应用中的安全。第 3 章介绍信息加密和应用管理，帮助用户了解信息加密的概念、掌握实用的加/解密技术，保护信息和系统的安全。第 4 章讲解 PKI 技术，目的是让读者了解日益走近我们的 PKI，自如应对网络事务。第 5 章介绍防范黑客的技术，旨在帮助大家认识黑客的危害，了解黑客入侵的手段，学会防范黑客入侵的方法，掌握木马清除技术。第 6 章学习防火墙技术，它是防范黑客入侵技术的延伸，也是防范黑客入侵最基本的手段，学会使用个人防火墙对保护自己的计算机安全有极大的帮助作用。第 7 章介绍防治计算机病毒的基本方法，教会用户高效率地使用防病毒软件查找、清除计算机病毒。第 8 章讲解数据备份，帮助用户了解为什么要备份和怎么备份数据。第 9 章讲述安全管理、监察和安全评估，让读者了解安全管理涉及的基本内容和方法，建立安全管理的基本思想，学会最基本的安全管理技术。第 10 章讲述信息领域应该遵守的法律规范和可能承担的法律责任，强化法制意识，做遵纪守法的计算机应用者。

本书由谭建伟任主编，第 1、5 章以及附录由谭建伟编写，第 2 章由李晓峰编写，第 3、7 章由王建民编写，第 4 章由苗静芝编写，第 6 章由刘会霞编写，第 8 章由李燕山编写，第 9 章

由韩忠编写，第10章由张志强编写。全书由谭建伟统稿。王强对书稿进行了认真审阅，提出了许多修改意见，全体作者深表感谢。

由于编者水平有限，编写时间仓促，加之对计算机安全问题认识、理解的局限性，使书中难免存在错误和不当之处，敬请读者批评指正。

编　者

2006．4

郑重声明

目　录

第1章

信息安全概述

本章学习以下内容：

- 发生危害信息安全事件的原因
- 信息安全的概念
- 信息安全包含的内容
- 信息安全产品应用现状

计算机科学和计算机产业的迅猛发展，促进了人类社会的进步和繁荣，计算机的普及应用也为人类社会创造了巨大财富。目前，计算机已经深入到人类社会的方方面面，大到国家的政治、经济、军事领域，小到居家生活，人与计算机的联系越来越密切。人们过度依赖计算机必然导致大量的数据被集中存储于计算机中，并通过网络在计算机设备之间传送。计算机中的信息资源有别于其他资源，它可以同时被很多人共享使用，如果在信息传输和使用的过程中，没有安全保护措施，就可能出现信息被截收、删除、修改等危害事件，使信息泄露或被非法篡改，这说明计算机网络系统具有脆弱性和危险性。

危害信息安全的因素很多，造成的安全问题也不尽相同，有信息系统自身的不可靠、工作环境存在的异常干扰、自然灾害等原因引起的安全问题，也有工作人员操作不当造成的安全问题，更有人为恶意破坏导致的安全问题。近几年大规模的计算机病毒侵袭事件接连不断，黑客入侵遍布全球，种种原因导致危害信息安全事件的数量急剧上升，信息安全也因此成为信息网络应用中的关键问题，成为世界各国关注的焦点。

1.1 危害信息安全的因素

信息领域的“危害”有两层含义，一是各种因素对信息造成的危害，二是利用信息产生危害。与其他危害相比，信息领域的危害具有较强的技术性，是一种新的危害形式，由此造成的后果也更为严重。

1.1.1 危害信息安全的形式

危害信息安全的表现形式多种多样，危害后果和抑制手段也不尽相同，这里归类列出常见的几种，旨在帮助大家认识危害的严重性，提高信息安全防护意识。

1．自然灾害

自然灾害对信息系统造成危害的事件在世界各国时有发生。如果建造机房、安装设备时没有考虑防水、防火、防静电、抗震、避雷等问题，那么信息系统工作环境抵御自然灾害的能力就会下降，发生灾害后有可能给信息系统造成很大的损失。例如，辽宁某铁路局控制机房因缺乏雷电防护设施曾3次遭受雷击，致使控制系统和一些终端设备损坏，严重影响了正常编组运输。日本东京电信局在电缆维护时，工人操作不慎造成火灾，由于缺乏有效的火灾控制手段，大火持续16小时，烧毁了大量的通信设备，导致数家银行和邮局的计算机通信系统中断，银行分布在各地的自动提款机被迫停机，邮局的一些业务只能暂停。

2．系统漏洞

系统本身存在的致命漏洞是威胁信息安全的重要因素。信息系统的大型化使得控制程序的复杂程度不断增加，隐藏其中的漏洞也越来越多，它们有可能引起系统崩溃，也有可能成为渗透系统的工具或通道。例如，微软公司曾在IE浏览器安全建议书中证实，IE浏览器存在安全漏洞，可能引起零位指针失效或内存失效等错误。思科公司曾承认它的Internetwork操作系统存在处理IPv6包的漏洞，若向受影响的思科设备发送特制的IPv6包，则有可能使设备遭受DoS攻击。

3．操作失误

工作人员缺乏责任心或因专业知识滞后造成操作失误，也会导致意想不到的灾难事件。例如，由于美国防空司令部指挥中心计算机操作员输入数据错误，引起防空警报，最高指挥部随即命令1 000枚核导弹进入待发状态，核战争一触即发。香港联合交易所工作人员在停电后按停警钟时，意外地按下后备电源的“紧急停止掣”，截断了大堂及自动对盘系统主机的电源，停电使系统停止工作4分58秒，结果导致收市延误，在延误收市的4分58秒期间，额外交易1 099宗，成交额约1亿多元。

4．病毒侵袭

计算机病毒的全球性蔓延对信息安全构成了严重威胁，且已经造成了巨大的损失，计算机病毒的危害之大，不亚于瘟疫。中国台湾大学生陈盈豪制造的“CIH”病毒，首次发作就使全球约6 000万台计算机受害。美国的莫里斯在互联网上传播“蠕虫”病毒，导致美国6 000多个系统瘫痪，直接损失9 600万美元。“爱虫”病毒的发作，使全球损失约100亿美元。我国某省财政厅财务管理系统感染病毒，破坏了3年的财务数据，造成无法挽回的巨大损失。

5．违法、违纪

人为恶意的攻击、破坏是威胁信息安全的重要原因，也是最难控制和防范的因素。此种危害的表现形式很多，有的对计算机进行物理破坏，有的放置逻辑炸弹，有的格式化磁盘，有的篡改信息、盗窃数据，也有的侵入重要、机密信息系统，造成严重危害国家安全的重大事件。

1.1.2 发生危害信息安全事件的诱因

危害信息安全事件的发生数量居高不下，且逐年增加，这说明危害信息安全有较为特殊的诱发原因，值得深究，它有助于我们认清发生危害信息安全事件的实质，有的放矢地开展防范工作。

1．信息系统本身的缺陷是诱发危害事件发生的主要原因

（1）信息系统的脆弱性

计算机信息系统本身的脆弱性是诱发危害信息安全事件最根本的原因。计算机以高速度、高精度地处理信息见长，它有许多其他设备不能比拟的优点，如信息存储密度高、易修改、能共享、网络传递方便等，正是这些优点使计算机备受人们青睐，也正是这些特点使计算机具有先天的脆弱性。高存储密度使处理大量信息成为可能，而在计算机存储的大量信息中隐藏少量非法信息不易察觉；信息易修改的特性给正常工作带来很多方便，修改后不留痕迹又使犯罪分子有机可乘，使追查犯罪困难重重；网络传递、共享能使人们快速、充分地利用信息资源，但信息传递过程中的窃听以及接收信息对象的难以甄别等问题，又使信息的泄露成为可能。

计算机信息系统的脆弱性和计算机技术的开放性，使针对信息系统的危害易于发生，而防护环节的薄弱又给了危害行为人以可乘之机，所以计算机信息系统的脆弱性不可避免地导致了危害信息安全事件的发生。

（2）信息系统管理的复杂性

计算机信息系统的功能日益强大，计算机软、硬件的复杂程度随之成倍增长，计算机信息系统的管理也日趋复杂化。正是因为网络和计算机信息系统具有管理复杂性，工作中稍有不慎或管理策略不当，都会使信息系统出现安全隐患。这些不易察觉的安全漏洞，对拥有高技术、法制观念不强、时刻想获取不法利益者是很大的诱惑；对刻意显示自己才能的人来说也是不可多得的机会。

信息系统管理的复杂性，使得管理难度增大，同时，维护信息安全的难度也增大。这必然导致信息的安全性相对下降，使更多的人有机会、有可能使用计算机或利用计算机从事非法活动。因此，危害信息安全事件的数量居高不下和信息系统管理复杂性有直接关系。

2．信息的重要性使之成为攻击目标

计算机应用环境逐渐增多，使存储其中的信息量和信息重要程度相应增加，信息和财富直接关联。有些计算机中存储的数据和信息的价值远远超过计算机系统本身，因此，大量安全事件的目标是计算机中的信息。通过窃取计算机系统中心机密信息，能够获取巨额财富，这对掌握计算机技术又想一夜暴富的人来说是很大的诱惑，也促使一些人甘冒风险以身试法，所以信息、机密和财富密不可分是导致危害信息安全事件发生的主要原因。

3．低风险的诱惑

从犯罪心理的角度看，犯罪行为人在实施犯罪前，会关心刑罚的轻重，更会关心受到惩罚的可能性。刑罚很重，但受到惩罚的可能性微乎其微，这样会降低刑罚的威慑作用，犯罪人就可能在趋利避害的侥幸投机心理支配下实施犯罪。危害信息安全的活动的技术含量较高，隐蔽性较强，被发现和查获的可能性小，高回报低风险，是许多人冒险从事危害信息安全活动的普遍心理。

4．道德理念的差异

人类长期形成的道德观念与计算机技术不协调，这也是诱发危害信息安全的一个原因。在计算机应用普及过程中，高技术人才一直是人们崇拜的偶像，他们所做的越轨行为往往被当成“天才”杰作。计算机应用环境固有的思维定式淡化了犯罪概念。私拆别人信件的人一定会有罪恶感，因为大多数人知道这是违法行为，但是不经允许点击、浏览别人的 E-mail 却往往被理解