NCIE
规划职业人生

Broadview
www.broadview.com.cn

国家人事部
国家信息产业部
信息专业技术人才知识更新工程（“653工程”）指定参考教材

全国信息安全技术水平考试授权教材

THE NATIONAL
CERTIFICATION OF
INFORMATION SECURITY ENGINEER

全国信息安全技术水平考试

一级学员教材

全国信息安全技术水平考试教材编委会　编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

NCIE
规划职业人生

全国信息安全技术水平考试授权教材

国家人事部
国家信息产业部 信息专业技术人才知识更新工程（“653工程”）指定参考教材

全国信息安全技术水平考试
一级学员教材

全国信息安全技术水平考试教材编委会 编著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

本书由全国信息安全技术水平考试教材编委会组织编写，以全国信息安全技术水平考试一级大纲为依据，坚持零起点原则。所含 8 章内容着重分析描述信息安全的基础知识，以建立完备的信息安全观念，掌握主机安全的配置维护为指导，进行了全面、中立的叙述。

本书可作为全国信息安全技术水平考试（NCSE）一级考试用书，也可作为自学信息安全的读者的参考教材。

图书在版编目（CIP）数据

全国信息安全技术水平考试一级学员教材 / 《全国信息安全技术水平考试教材》编委会编著.
—北京：电子工业出版社，2006.6
全国信息安全技术水平考试授权教材
ISBN 7-121-02533-7

Ⅰ. 全… Ⅱ. 全… Ⅲ. 计算机网络－安全技术－水平考试－教材 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2006）第 040421 号

责任编辑：韩 明
印 刷：北京东光印刷厂
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
经 销：各地新华书店
开 本：787×1092 1/16 印张：20.75 字数：501 千字
印 次：2006 年 6 月第 1 次印刷
印 数：5000 册 定价：58.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

专家指导委员会

委员名单

高新民　中国信息协会副会长　国家信息中心原主任

邬贺铨　中国工程院副院长　中国工程院院士　信息产业部电信科学技术研究院副院长

王　越　中国科学院院士　中国工程院院士　北京理工大学名誉校长

潘云鹤　中国工程院院士　浙江大学校长

顾冠群　中国工程院院士　东南大学校长

卢锡城　中国工程院院士　中国人民解放军国防科学技术大学副校长

张乃通　中国工程院院士　哈尔滨工业大学通信技术研究所所长

李乐民　中国工程院院士　电子科技大学通信与信息工程学院　教授

沈昌祥　中国工程院院士　国家信息化专家咨询委员会委员

邓寿鹏　国务院发展研究中心技术经济研究部　研究员

张尧学　教育部高教司　司长

王渝次　国务院信息化工作办公室网络与信息安全组组长

魏　卓　人事部专业技术人员管理司　副司长

王耀光　信息产业部人事司　副司长

洪京一　信息产业部信息化推进司　副司长

方滨兴　信息产业部国家计算机网络与信息安全管理中心主任　教授

刘玉珍　信息产业部电子人才交流中心　主任

文宏武　电子工业出版社社长　总编辑

牛　晋　公安部信息通信局　副局长

阎保平　中国科学院计算机网络信息中心主任　研究员

李明树　中国科学院软件研究所所长　教授　博导

吴世忠　中国信息安全产品测评认证中心主任　研究员

王行刚　中国科学院计算技术研究所首席科学家　研究员　博导

冯登国　中国科学院信息安全国家重点实验室主任　博导

卿斯汉　中国科学院信息安全技术工程研究中心主任　研究员

贺也平　中国科学院软件技术研究所信息安全中心　副主任

袁振华　中共中央办公厅信息中心原副主任　研究员

祝世雄　中国电子科技集团公司第三十研究所副总工　研究员
屈延文　信息产业部太极计算机联合实验室　教授
王贵骁　中国信息安全产品测评认证中心副主任　高工
马建峰　西安电子科技大学信息安全教育部重点实验室主任　教授
王怀民　国防科技大学信息安全研究所所长　教授
杨义先　北京邮电大学信息安全中心教授　博导
戴宗坤　四川大学信息安全研究所副所长　教授
吴　江　兴唐通信科技股份有限公司　副总工
雷利民　中国电子科技集团公司第三十研究所高工　研究员
沙学军　哈尔滨工业大学通信技术研究所　教授
沈继业　中联绿盟信息技术（北京）有限公司　总经理
王东英　安氏互联网安全系统（中国）有限公司　副总裁
赵大平　冠群电脑（中国）有限公司　技术总监
刘　兵　北京中科网威信息技术有限公司　技术总监

全国信息安全技术水平考试授权教材

编　　委　　会

主　任：刘玉珍　文宏武
副主任：郭建兵　王希征

主　编：吴剑锋
副主编：李　宁　李建伟
编　委：罗晓凡　张　欣　秦　凯　徐　锋

关于信息专业技术人才知识更新工程（“653工程”）

目标任务

根据我国信息技术发展和信息专业技术人才队伍建设的实际需要，从2006年至2010年，在我国信息技术领域将开展大规模的专业技术人员继续教育活动，每年开展专业技术人才知识更新培训12万人次左右，6年内共培训信息技术领域各类中高级创新型、复合型、实用型人才60~70万人次。通过专项继续教育活动，使各类信息专业技术人才更新专业知识，提高创新能力，进一步健全和完善信息技术领域的继续教育工作体系、服务体系和制度体系，为全面提升我国信息专业技术人员的整体素质提供良好的继续教育和培训服务。

实施原则

（一）坚持以提高自主创新能力为核心，着力提高信息专业技术人才的科技水平和专业素质，不断加快我国信息专业技术人才知识更新的步伐。

（二）紧密结合信息专业技术岗位的实际需求，紧跟世界信息技术发展步伐，统筹规划，分类实施，增强信息专业技术人才培养的针对性和实效性。

（三）以中高级专业技术人才为重点，优先培训急需紧缺行业和专业的技术业务骨干，带动整个信息技术领域知识更新培训工作的开展。

（四）按照政府推动、单位支持、个人自愿的原则，积极整合各类社会资源，充分发挥各方积极性，不断推进“653工程”实施的社会化和市场化。

主要内容

（一）根据我国经济社会发展和科技创新的需要，紧跟世界信息技术发展的步伐。以信息技术领域中高级专业技术人才为重点，在软件与集成电路、通信工程、信息安全、电子商务、电子政务等重点领域，每年举办一定数量的专业技术人才高级研修班和学术技术交流论坛，培养信息技术中高级复合型、骨干型人才。对参加“653工程”范围内高级研修班的专业技术人才统一颁发《人事部专业技术人员高级研修班结业证书》。

（二）依托国家在信息技术领域建设的重要项目、重点工程和重大课题，有针对性地开展各类继续教育活动，有目的、有计划地培训相关行业领域的专业技术骨干，推进项目、资金、人才培养的一体化建设。

（三）建立广泛合作机制，与各相关行业、协会合作开展高层次人才培养工作。根据相关行业、协会的人才需求特点，在企业信息化与资源规划（ERP）、医疗卫生信息化、

安全生产信息化等多个领域，与科技部、卫生部、国家安全生产监督管理总局等众多行业主管部委建立紧密合作，积极引入用友软件、恩爱普软件（SAP）、华为、中兴等国内外著名科技企业参与行业信息化人才培养，不断优化培养机制，联合各行业配套培养中高级信息技术人才。

（四）以社会发展客观需求为指导，把握信息技术领域的最新趋势和主流，以软件、网络、信息安全、数据库、动漫、游戏等当前紧缺人才领域为突破口，确立10个重点实施专业领域，不断丰富和完善课程体系与教材课件，逐步建立一套适合我国国情、与国际标准接轨的信息专业技术人才职业能力培养与测评体系，培养中高级专业技术人才。

（五）推动“产、学、研”技术合作，积极结合高等院校和职业院校的教育资源优势，面对政府部门信息中心和广大院校、科研机构，集中开展电子政务、信息化办公等应用型信息技术人才知识更新培训。

（六）鼓励各地区、各企事业单位结合信息化发展的需求，开展专项技术培训和岗位培训，具备条件的地区和大型企事业单位可将培训计划报“653 工程”办公室，经评估纳入到“653 工程”的统一规划。

（七）选择上海、深圳、大连、无锡、成都、西安等信息产业比较发达的城市作为实施“653 工程”的重点，人事部、信息产业部予以积极的政策支持，地方政府配套加大资金投入，通过典型城市的示范作用，促进全国信息技术领域“653 工程”的实施。

（八）建立包括卫星、因特网等多种有效实施途径和手段在内的远程教育培训网络，面向全国特别是中西部地区的信息专业技术人才，实施信息技术远程继续教育。采取多种优惠方式，开展普及性知识更新培训，努力普及推广各类先进适用的信息技术知识，缩小“数字鸿沟”。

信息技术领域“653 工程”由人事部和信息产业部共同组织实施，信息产业部具体负责。全国信息专业技术人才知识更新工程办公室负责“653 工程”的各项日常工作，办公室设立在信息产业部电子人才交流中心，由其承担具体工作。

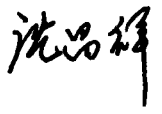
序

随着我国信息化不断深化发展，网络与信息系统的基础性、全局性作用日益增强，信息安全问题的重要性日趋显现，信息安全已经成为国家安全的重要组成部分。但我国开展电子政务、电子商务起步相对较晚，与国外先进国家相比，无论在网络安全意识还是网络安全防护技术等诸多方面都还存在不小差距，各级单位的信息网络安全处在一个相当薄弱的环节。为加强信息安全保障工作，必须有一批高素质的信息安全管理和技术人才。

高素质的信息安全人才队伍是保障国家重点基础网络和重要系统安全的基石，是制定信息安全发展战略规划与政策并建设国家信息安全保障体系的骨干力量，是发展我国信息安全产业这一战略性核心产业的排头兵。为此，国家信息化领导小组第三次会议要求加快人才培养，造就一支高素质的人才队伍，并作为国家信息化建设的一项战略性举措。

信息产业部国家信息化工程师认证考试管理中心面向信息安全各领域，适时推出了全国信息安全技术水平考试（NCSE），对于维护公共信息网络安全、提高我国整体信息安全水平、促进信息安全人才的规范培养、增进信息安全学术研究气氛将起到积极的作用。由中国科学院、西安电子科技大学等单位从事信息安全工作与研究人员编写、审校的国家信息安全技术水平考试系列教材，全面阐释了信息安全的基本理论和基础知识，内容涵盖了信息安全诸多学术领域的知识，对提高全社会的信息安全意识和提高实际应用能力具有切实的指导意义。

在此，谨向全国信息安全技术水平考试的顺利启动表示祝贺，相信该项考试将对完善我国信息安全人才培养体系起到积极的推动作用。



中国工程院院士

前　言

随着网络技术及其应用的普及和深入，电子商务、电子政务的开展、实施和应用，信息安全已经不再仅仅是科学研究人员和少数黑客的专利，日益庞大的网络用户群同样需要掌握信息安全知识。只有这样，才有可能构筑属于全社会的信息安全体系。

与早期网络技术的普及一样，对于数量庞大的普通用户群，信息安全问题始终是一个神秘而高深的话题。全国信息安全技术水平考试（NCSE）一级教学内容的策划与开发，都是围绕着“从无到有”的过程实现的。从零到一的变迁不同于普通的量变，我们希望所有的普通用户能够在学习 NCSE 一级的过程中实现质变，从信息安全的懵懂而又渴望的状态中获得解放，自信、自立地实现个人节点的安全。

那么，如何通过易于接受、易于理解的方式将基本的信息安全问题准确地传递给这些用户，如何通过简单、直接的实践使之快速获得信息安全知识并掌握信息安全技能，这些问题不仅仅意味着挑战，对于渴望创建国家信息安全认证标准的任何人、任何团队而言，它也意味着巨大的动力和登顶的诱惑，意味着思维细胞的快意创新和新旧开发理念的激烈碰撞，更意味着崭新的设计开发思想和研究成果的最终确立，并形成如下结论：必须坚持将认证体系及教育资源的策划、开发作为一项科学、一门艺术、一种享受来加以对待。

正是源于这样的基点，在 NCSE 教育资源的分析、策划、研发过程中，我们组织人力物力进行攻关，克服了众多技术、教育培训领域的难题，创造性地应用了大量教育资源开发领域的最新方法和技术，经过整个团队努力而辛勤的工作，NCSE 学员教材、教学指导书、实验指导书终于见诸于世。

本套丛书是在全国信息化工程师认证考试工作指导委员会的指导下，由全国信息安全技术水平考试教材编委会组织编写的。由于时间匆忙，兼之信息安全领域所包含的内容量极为庞大，因此难免存在挂一漏万之处，希望读者能够批评指正，可以发 E-mail 至 jsj@phei.com.cn。

如果您对全国信息安全技术水平考试的相关内容感兴趣，可以访问考试官方网站 http://www.ncie.gov.cn。

全国信息安全技术水平考试教材编委会

2006 年 5 月

目　录

第 1 章　信息安全基础

在信息时代里，信息主权是一个国家继政治主权和经济主权之后的新主权。在人类社会的三个进程中，物质在工业化前的社会中起关键作用，能量在工业化社会中起核心作用，信息则在当今的信息化社会中叱咤风云。发达国家信息工业在整个国民经济中所占的比例为 40%~60%，新兴工业国家占 25%~40%，发展中国家则占 25%以下。信息工业在一个国家的国民经济中所占的比例反映了这个国家的经济水平和工业发展水平。对信息安全的认识和掌控程度不仅影响一个国家的根本利益，而且影响企业和个人的利益，同时也反映了一个国家的现代化程度。本章主要描述以下要点：

- 信息安全的概念；
- 主机网络安全；
- 信息安全的标准化；
- 信息安全风险的管理；
- 信息与网络安全组件；
- 安全策略的制定与实施。

1.1　信息安全的概念

随着以 Internet 为代表的全球性信息化趋势日渐鲜明，信息网络技术的应用日渐普及，应用领域从传统的小型业务系统逐渐向大型的关键业务系统扩展，例如党政部门信息系统、金融业务系统、企业商务系统等。伴随着网络的普及，信息安全日益成为影响网络效能的重要因素。而 Internet 所具有的开放性、国际性和自由性在增加了应用自由度的同时，对安全性提出了更高的要求，主要表现在以下几个方面。

1．开放性的网络导致网络的技术是全开放的，任何一个人或团体都可能获得，因而网络所面临的破坏和攻击是多方面的，例如，可以对物理传输线路实施攻击，也可以对网络通信协议和实现实施攻击；可以对软件实施攻击，也可以对硬件实施攻击。国际性的网络还意味着网络的攻击不仅可以来自本地网络的用户，也可以来自 Internet 上的任何用户。也就是说，网络安全所面临的是国际化的挑战。

2．自由意味着网络对用户的使用并没有提供任何的技术约束，用户可以自由地访问网络，自由地使用和发布各种类型的信息。用户只对自己的行为负责，而没有任何的法律限制。

开放、自由、全球化的 Internet 的发展给政府机构和企事业单位带来了革命性的变化，使得他们能够利用 Internet 提高办事效率和市场反应能力，更具竞争力；同时他们又要面对网络开放带来的数据安全的新挑战。如何保护企业的机密信息不受黑客和工业间谍的入侵，已成为政府机构、企事业单位信息化健康发展所要考虑的重要问题之一。

1.1.1 信息安全的概念

信息安全包括 5 个基本要素：机密性、完整性、可用性、可控性与可审查性。机密性指确保信息不暴露给未授权的实体或进程。完整性意味着只有得到允许的人才能修改数据，并且能够判别出数据是否已被窜改。可用性说明得到授权的实体在需要时可访问数据，即攻击者不能占用所有的资源而阻碍授权者的工作。可控性表示可以控制授权范围内的信息流向及行为方式。可审查性指对出现的网络安全问题提供调查的依据和手段。

1.1.2 信息和网络安全现状

现在全球普遍存在信息安全意识欠缺的状况。人们在组建信息系统和网络的时候，并没有像买门时会想到买锁那样自然地想到信息安全和网络安全，这导致大多数的信息系统和网络存在着先天性的安全漏洞和安全威胁。

国际上也存在着信息安全管理不规范和标准不统一的问题。美国是西方国家中对信息安全比较重视的国家之一，同样存在着规范和标准跟不上技术进步发展的问题。西欧国家另有一套信息安全标准，尽管在原理和机构上同美国有相似甚至相同的部分，但是不同的部分也相当多。

在信息安全的发展过程中，企业和政府的要求有一致的地方，也有不一致的地方。企业更注重于信息和网络安全的可靠性，政府更注重信息和网络安全的可管性和可控性。美国政府组织的 KRS 系统，由于不受企业的欢迎而无法推广。在发展中国家，信息安全的投入量满足不了信息安全的需求，而且投入也常常被移用或错用。

信息和网络安全的技术仍然在发展过程中，“绝对的安全是不可能的”和“木桶原理”也让一些使用者踌躇不前，市场上“叫好不叫卖”的现象仍然存在。

同样在国内，信息安全产品的“假、大、空”现象在一定程度上仍存在，防火墙变成了所谓的“铜墙铁壁”。之所以产生这种情况，原因是多方面的，如监督不力，信息安全知识的普及程度不够等。

1.1.3 网络中存在的威胁

一般认为，目前网络中存在的威胁主要表现在以下几个方面。

- 非授权访问

没有预先经过同意，使用网络或计算机资源的行为称作非授权访问。例如，有意避开系统访问控制机制、对网络设备及资源进行非正常使用，或擅自扩大权限、越权访问信息。