全国计算机技术与软件专业技术资格（水平）考试指定用书

信息安全工程师教程

张焕国 主编
杜瑞颖 傅建明 严飞 副主编
全国计算机专业技术资格考试办公室 组编

清华大学出版社

全国计算机技术与软件专业技术资格（水平）考试指定用书

信息安全工程师教程

张焕国 主编
杜瑞颖 傅建明 严飞 副主编
全国计算机专业技术资格考试办公室 组编

清华大学出版社

内 容 简 介

全国计算机技术与软件专业技术资格（水平）考试（以下简称“计算机软件考试”）是由人力资源和社会保障部、工业与信息化部领导下的专业技术资格考试，纳入全国专业技术人员职业资格证书制度统一规划。为适应“十三五”期间计算机软件行业发展需要，满足社会多方对信息安全技术人员的迫切需求，根据人力资源和社会保障部办公厅《关于2016年度专业技术人员资格考试计划及有关问题的通知》（人社厅发[2015]182号），在2016年下半年计算机技术与软件专业技术资格（水平）考试中将开考“信息安全工程师（中级）”。“信息安全工程师（中级）”岗位的人才评价工作的实施，将成为科学评价我国信息安全专业技术人员的重要手段，也将为我国培养和选拔信息安全专业技术人才，发挥重要作用。

本书根据信息安全工程师考试大纲的要求进行编写，内容主要包括信息安全基本概念、基本技术和基本应用等方面，讲授方法注重理论联系实际，突出实用技术。全书共分 8 章，具体内容包括：信息安全基础、密码学基础与应用、网络安全基础、信息系统安全基础、应用系统安全基础、网络安全技术与产品、信息系统安全工程、应用安全工程。

本书是计算机软件考试中“信息安全工程师”岗位的考试用书，也可作为信息安全相关专业学生和从业人员学习信息安全技术的教材，还可用做相关信息技术领域从业人员的技术参考书。

图书在版编目（CIP）数据

信息安全工程师教程/张焕国主编. —北京：清华大学出版社，2016
全国计算机技术与软件专业技术资格（水平）考试指定用书
ISBN 978-7-302-44081-9

Ⅰ. ①信… Ⅱ. ①张… Ⅲ. ①信息安全–安全技术–资格考试–教材 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字（2016）第 124724 号

责任编辑：杨如林　柴文强
封面设计：何凤霞
责任校对：胡伟民
责任印制：宋　林

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：清华大学印刷厂
装 订 者：三河市新茂装订有限公司
经　　销：全国新华书店
开　　本：185mm×230mm　印　张：54.5　防伪页：1　字　数：1410 千字
版　　次：2016 年 7 月第 1 版　　印　次：2016 年 7 月第1 次印刷
印　　数：1～4000
定　　价：128.00 元

产品编号：070135-01

序　言

由人力资源和社会保障部、工业和信息化部共同组织的“全国计算机技术与软件专业技术资格（水平）考试”（简称软考），肩负着科学评价选拔软件专业技术人才的光荣使命，肩负着正确引导软件行业专业技术人员潜心钻研、提高能力、加强创新的光荣使命，肩负着加强软件行业专业技术人才队伍建设的光荣使命。自 1991 年开考以来，软考坚持专业化、国际化、品牌化的发展方向，全国累计报名人数 330 万人，培养选拔软件行业专业技术人才 64 万人，部分考试标准与日本、韩国互认，为全国计算机和软件专业技术人员（包括香港、澳门和台湾地区来大陆就业的人员）提供了科学的评价体系和评价机制，为推动“两化”深度融合，提高工业信息化水平，走新型工业化道路提供了有力支撑。

党中央、国务院一直高度重视信息技术产业发展。以 2000 年的《国务院关于印发鼓励软件产业和集成电路产业发展的若干政策的通知》（国发【2000】18 号文件）和 2011 年的《国务院关于印发进一步鼓励软件产业和集成电路产业发展的若干政策的通知》（国发【2011】4 号文件）为重要标志的一系列政策措施，为软件产业和集成电路产业乃至整个信息技术产业发展提供了强劲动力。2011 年，我国软件产业实现业务收入超过 1.84 万亿元，产业规模是 2005 年的 4.7 倍，同比增长 32.4%，超过“十一五”期间平均增速 4.4 个百分点，实现了“十二五”的良好开局。软件产业占电子信息产业比重从 2000 年的 5.8%上升到 19.9%。软件企业数量超过 3 万家，从业人数超过 300 万人。2012 年上半年，我国软件产业实现软件业务收入 10988 亿元，同比增长 26.2%。软件和信息服务业的持续快速发展，国民经济和社会信息化建设的深入开展，使软件人才和信息技术人才供给不足的问题依旧突出。按照国发【2011】4 号文件提出的“努力培养国际化、复合型、实用性人才”的要求，工业和信息化部教育与考试中心组织一批理论水平高、实践经验丰富的专家学者和业界精英，结合考试大纲和软件产业技术发展趋势，对原有的“全国计算机技术与软件专业技术资格（水平）考试教材和辅导用书”进行了更新，为广大软件行业从业人员提高学习能力、实践能力、创新能力和职业道德水平提供了依据。

当前，我国正处在全面建成小康社会的决定性阶段。坚持走中国特色新型工业化、信息化、城镇化、农业现代化道路，推动信息化和工业化深度融合、工业化和城镇化良性互动、城镇化和农业现代化相互协调，促进工业化、信息化、城镇化、农业现代化同步发展，是党中央的重要战略部署。造就规模宏大、素质优良的人才队伍，推动我国由人才大国迈向人才强国，既是构成这一重要战略部署的紧迫任务，也是实施这一重要战略部署的关键措施。从现在起至全面建成小康社会的这一历史时期，信息技术仍然是走

中国特色新型工业化、信息化、城镇化、农业现代化道路的先导性技术；全国计算机技术与软件专业技术资格（水平）考试也应该看做是落实党的十八大关于“推进各类人才队伍建设，实施重大人才工程，加大创新创业人才培养支持力度，重视实用人才培养”指示的重要组成部分。好雨知时节，当春乃发生——我相信，全国计算机技术与软件专业技术资格（水平）考试教材和辅导用书的及时更新必将为我国信息技术人才队伍发展壮大、为软件和信息服务产业做大做强、为服务经济转型升级做出更大的贡献；同时我们也要注意到，近年来，以云计算、物联网、移动互联网和大数据技术等为热点的新一代信息技术，正在对软件和信息服务产业带来一系列深刻变化，也对软件和信息技术在各个领域的应用产生重要影响，我希望，在保持这套教材和辅导用书在一个时期内相对稳定的同时，也要注意及时反映信息技术的新变化、新进展，以跟上软件和信息服务产业蓬勃发展的需要，跟上信息化以及新型工业化、城镇化和农业现代化建设蓬勃发展的需要。

前　言

人类社会在经历了机械化、电气化之后，进入了一个崭新的信息化时代。在信息时代，人们生活和工作在信息空间或网络空间中。所谓信息空间或网络空间就是人们赖以生存的信息环境，它是所有信息系统的集合。

在信息时代，信息成为一种重要的战略资源。信息技术改变着人们的生活和工作方式，信息产业成为世界第一大产业。信息的获取、存储、传输、处理和安全保障能力成为一个国家综合国力的重要组成部分。

我国非常重视信息技术人才队伍的建设。伴随着信息产业的发展，人力资源和社会保障部、工业与信息化部共同组织了“全国计算机技术与软件专业技术资格（水平）考试”，通过这项制度，已为我国培养选拔了几十万计算机与软件服务专业技术人才（包括香港、澳门和台湾地区来大陆就业的人员）。部分考试标准与日本、韩国互认。该考试由于其权威性和严肃性，得到了社会各界及用人单位的广泛认同，并为推动国家信息产业发展，特别是计算机和软件服务产业的发展，以及提高各类信息技术人才的素质和能力发挥了重要作用。

当前，信息技术与产业欣欣向荣，处于空前繁荣的阶段，但是另一方面，危害信息安全的事件不断发生，信息安全的形势非常严峻。敌对势力的破坏、黑客入侵、利用计算机实施犯罪、恶意软件侵扰、隐私泄露等，是我国信息网络空间面临的主要威胁和挑战。我国已经成为世界信息产业大国，但是还不是信息产业强国，在信息产业的基础性产品研制、生产方面还比较薄弱，例如，计算机操作系统等基础软件和 CPU 等关键性集成电路，我国现在还部分依赖国外的产品，这就使得我国的信息安全基础不够牢固。

随着计算机和网络在军事、政治、金融、工业、商业等部门的广泛应用，社会对计算机和网络的依赖越来越大，如果计算机和网络系统的安全受到破坏，不仅会带来巨大的经济损失，还会引起社会的混乱。因此，确保以计算机和网络为主要基础设施的信息系统的安全已成为世人关注的社会问题和信息科学技术领域的研究热点。当前，我国正处在全面建成小康社会的决定性阶段，实现我国社会信息化并确保信息安全是我国全面建成小康社会的必要条件之一。而要实现我国社会信息化并确保信息安全的关键是人才，这就需要我们培养造就规模宏大、素质优良的信息化和信息安全人才队伍。

2014 年，习近平主席在中央网络安全与信息化领导小组会议上指出：没有网络安全就没有国家安全，没有信息化就没有现代化。网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我国建成网络强国。

“十三五”时期，我国要积极推动网络强国建设。网络强国涉及技术、应用、文化、安全、立法、监管等诸多方面，不仅要突出抓好核心技术突破，还要提供更加安全可靠的软硬件支撑，加快建设高速、移动、安全、泛在的新一代信息基础设施，在不断推进新技术新业务应用，繁荣发展互联网经济的同时，要强化网络和信息安全，而培育高素质人才队伍是实施网络强国战略的重要措施。2015 年，国务院学位委员会和教育部增设“网络空间安全”一级学科。我国信息安全学科建设和人才培养，迎来了全面高速发展的新阶段。

与此同时，全国计算机技术与软件专业技术资格（水平）考试办公室决定开始开展“信息安全工程师”岗位的人才评价工作，以加快推动信息安全专业的人才队伍建设。我们相信，这一措施将成为科学评价我国信息安全专业技术人员的重要手段，也将为我国培养和选拔信息安全专业技术人才，发挥重要作用。

为了配合“信息安全工程师”考试工作的开展，给准备参加考试的技术人员提供一本适用的教材，我们编写了《信息安全工程师教程》一书。全书共分 8 章，主要内容如下：

第 1 章 信息安全基础，主要介绍：信息安全概念、信息安全法律法规、信息安全管理基础和信息安全标准化知识。本章的内容是基本的，但是对信息安全技术人员来说是重要的。

第 2 章 密码学基础与应用，主要讲解：密码学的基本概念、分组密码、序列密码、Hash 函数、公钥密码体制、数字签名、认证和密钥管理。本章的介绍强调基本概念、基本技术和基本应用技术，努力避免较复杂的数学理论。

第 3 章 网络安全基础，主要介绍：计算机网络基本知识、网络安全的基本概念、网络安全威胁、网络安全防御和无线网络安全。

第 4 章 信息系统安全基础，主要讨论：计算机设备安全、操作系统安全、数据库系统的安全、恶意代码、计算机取证和嵌入式系统安全。

第 5 章 应用系统安全基础，主要讲解：Web 安全、电子商务安全、信息隐藏、网络舆情和隐私保护。

第 6 章 网络安全工程，主要介绍：网络安全需求分析与基本设计、网络安全产品的配置与使用、网络安全风险评估实施和网络安全防护技术的应用。本章强调网络安全的基本技术与应用。

第 7 章 信息系统安全技术与产品，主要介绍：访问控制、信息系统安全的需求分析与设计准则、信息系统安全产品的配置与使用和信息系统安全测评。本章强调信息系统安全的基本技术与应用。

第 8 章 应用安全工程，主要介绍：Web 安全的需求分析与基本设计、电子商务安全的需求分析与基本设计、嵌入式系统的安全应用、数字水印在版权保护中的应用和位置隐私保护技术的应用。本章强调应用系统安全的基本技术与应用。

本书由张焕国主编，杜瑞颖、傅建明、严飞副主编。参加编写的还有：陈晶、罗敏、赵波、彭国军、王张宜、牛晓光、王丽娜、任延珍、张立强、赵磊、武小平、王张宜、王鹃、余发江、郑鹏、王志波、叶登攀、余荣威等各位老师。

本书的编写工作得到湖北省软件工程师考试办公室夏波的指导和帮助，特向她表示感谢。

尽管作者们作了很大努力，力图使本书理论联系实际、简明扼要、通俗易懂，但因作者水平和经验所限，书中难免会有不妥和错误之处。对此，作者恳请读者的理解和批评指正，并于此先致感谢之意。

张焕国
于武汉大学
2016 年 3 月

目　录

第 1 章　信息安全基础

本章的内容是信息安全的基础之一，主要介绍信息安全概念、信息安全法律法规、信息安全管理基础和信息安全标准化知识。

本章的内容是最基本的，对于从事信息安全领域工作的读者来说，具有重要指导意义。

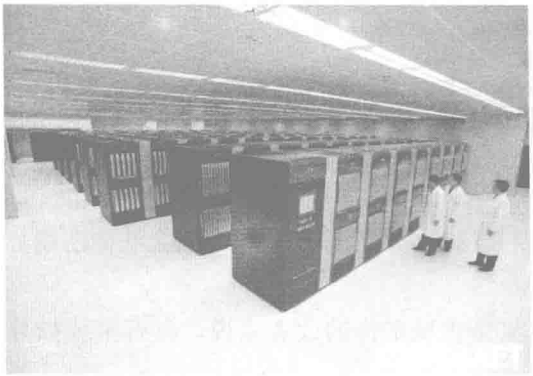
1.1　信息安全概念

本节介绍信息安全的基本概念，主要介绍信息安全的时代需求、网络空间安全学科的内涵、研究内容、理论基础、方法论基础等方面的内容。

1.1.1　信息安全是信息时代永恒的需求

人类社会在经历了机械化、电气化之后，进入了一个崭新的信息化时代。在 20 世纪中叶，出现了一批重要的理论：信息论、控制论、系统论、图灵机理论、冯·诺伊曼理论、计算理论等等，它们共同构成了信息科学技术的理论基础。在这些理论的支撑和指导下，信息科学技术得到突飞猛进的发展，取得了辉煌的成就，造就了信息技术与产业几十年的繁荣。信息产业超过钢铁、机械、石油、汽车、电力等传统产业，成为世界第一大产业。信息和信息技术改变着人们的生活和工作方式。离开计算机、网络、电视和手机等电子信息设备，人们将无法正常生活和工作。信息就像水、电、石油一样，与所有行业、所有人都相关，成为一种基础资源。因此，信息成为当今最具活力的生产要素和最重要的战略资源，以计算机网络为核心的信息系统成为国家的重要基础设施。

经过 30 多年的改革开放，我国已经成为信息产业大国。大多数中低档电子信息产品的产量和拥有量，我国都居世界第一。例如，个人计算机、手机、电话机、电视机等电子信息产品的产量和拥有量，我国都居世界第一。2009 年 1 月 8 日，我国国防科技大学研制出天河-1 号超级计算机，运算速度 2.57 千万亿次/秒，排名世界第一。2013 年 5 月国防科技大学又研制出天河-II 号超级计算机（见图 1-1），运算速度 33.86 千万亿次/秒，排名世界第一，而且比排在第二位的美国 “泰坦” 计算机快一倍。但是，我国还不是信息产业强国。我国在诸如 CPU 芯片、计算机操作系统等核心芯片和基础软件方面仍然依赖国外产品。



（1）天河-I 型超级计算机

（2）天河-II 型超级计算机

图 1-1 天河超级计算机

当前，除了电子信息科学技术继续高速发展之外，量子和生物等新型信息科学技术正在建立和发展。量子信息科学技术的研究和发展催生了量子计算机、量子通信和量子密码。早在 2001 年美国 IBM 公司就研制出 7 个量子位的示例型量子计算机，向世界宣告了量子计算机原理的正确性和可行性。2011 年 9 月 2 日，美国加州大学圣芭芭拉分校的科学家宣布，研制出具有冯·诺依曼计算机结构的量子计算机，并成功地进行了小合数的因子分解实验（参见图 1-2）。2012 年 3 月 1 日 IBM 公司又宣布找到了一种可以大规模提升量子计算机量子位数的关键技术。2014 年 4 月，奥地利科学家实现了 103 量子位的量子纠缠态，大大超过以前的 11 量子位。同时期，美国密歇根大学制造出世界上第一块可升级且可大规模生产的量子计算机芯片。由此可以看出，量子计算技术正在迅速发展。

除了美国之外，加拿大的量子计算机技术也取得了长足的发展。2007 年 2 月加拿大 D-Wave System 公司宣布研制出世界上第一台商用 16 量子位的量子计算机(参见图 1-3)。2008 年 5 月提高到 48 量子位。2011 年 5 月 30 日又提高到 128 量子位，并开始公开出售，1000 万美元一台。美国著名军火制造商洛克希德马丁公司购买了这种量子计算机，用于新式武器的研制。2013 年初又大幅度地提高到 512 量子位，价格也上升为 1500 万美元一台。著名信息服务商谷歌公司购买了这种量子计算机，用于提高信息搜索效率和研究量子人工智能。

2014 年 9 月 3 日谷歌公司宣布投资 50 亿美元与 UCSB 的研究团队联合研制量子计算机。2015 年 12 月 19 日中国阿里巴巴公司与中科院宣布联合研究量子计算和量子通信。这是我国首次由企业参与的量子信息科学技术的研究，具有重要的意义。