“攻克要塞”公众号

软考课程
5天通关

信息安全工程师

5天修炼

施 游 朱小平 编著

- 方法独特，提炼精辟，饱含著名一线培训讲师的**黄金经验**
- 全新的**思维导图**，精心梳理考纲、教程、考题所涉知识脉络
- 简化教程、突出重点，我们把厚书读薄，您把薄书读透
- 告别题海战术，助您轻松考过**信息安全工程师考试**

中国水利水电出版社
www.waterpub.com.cn

信息安全工程师5天修炼

施　游　朱小平　编著

中国水利水电出版社
www.waterpub.com.cn
·北京·

内 容 提 要

计算机软件考试作为国家级的专业技术人员资格水平考试，是目前行业内最具权威的资格水平考试。信息安全工程师（中级）作为其中一个岗位，通过该考试并获得证书的人员，表明已具备从事相应专业岗位工作的水平和能力。

本书结合作者培训经验，安排了5天的学习内容。本书利用“思维导图”来帮助考生梳理考纲、教程、考题所涉及的知识脉络；对于重点和难点进行标记并进行详细阐述和分析；对于一般性的知识点和通俗易懂的知识，简单分析。最终实现把书读薄，把书读透，花较少的精力亦能获得更好的成绩。最后，还给出了一套全真的模拟试题并给出了详细的分析。

本书可供广大有志于通过考试的考生考前复习使用，也可供各类高等院校（或培训班）的教师教学、培训使用。

图书在版编目（CIP）数据

信息安全工程师5天修炼 / 施游，朱小平编著. -- 北京 : 中国水利水电出版社，2017.3（2017.6重印）
ISBN 978-7-5170-5219-7

Ⅰ. ①信… Ⅱ. ①施… ②朱… Ⅲ. ①信息安全－安全技术－资格考试－自学参考资料 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2017)第040333号

责任编辑：周春元　　加工编辑：孙　丹　　封面设计：李　佳

书　名	信息安全工程师5天修炼 XINXI ANQUAN GONGCHENGSHI 5 TIAN XIULIAN
作　者	施　游　朱小平　编著
出版发行	中国水利水电出版社 （北京市海淀区玉渊潭南路1号D座　100038） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）68367658（营销中心）、82562819（万水）
经　售	全国各地新华书店和相关出版物销售网点
排　版	北京万水电子信息有限公司
印　刷	三河市铭浩彩色印装有限公司
规　格	184mm×240mm　16开本　17.75印张　422千字
版　次	2017年3月第1版　2017年6月第2次印刷
印　数	3001—6000册
定　价	58.00元

凡购买我社图书，如有缺页、倒页、脱页的，本社营销中心负责调换

编委会成员

I

前言

网络安全已成为信息时代国家安全的战略基石。随着互联网化、信息技术的飞速发展，政治、经济、军事等领域都面临着网络与信息安全等问题。一旦信息基础设施被破坏、信息泄露，将给国家、企业、个人带来巨大的损失和影响。维护网络与信息安全就成为了国家、社会、企业发展的前提。网络安全成为关乎全局的重大问题，信息化程度越高的行业，其安全工作越重要，对相关人才的需求也越迫切。

计算机软件考试作为国家级的专业技术人员资格水平考试，是目前行业内最具权威的资格水平考试。计算机软件考试纳入全国专业技术人员职业资格证书制度的统一规划，信息安全工程师（中级）作为其中一个岗位，通过该考试并获得证书的人员，表明已具备从事相应专业岗位工作的水平和能力，用人单位可根据工作需要从获得证书的人员中择优聘任相应专业技术职务（中级对应工程师）的人员。

我们在线上、线下进行的考前辅导中，与很多“准信息安全工程师”交流过，他们都反映出一个心声：“考试涉及面太广，教程 1000 多页不可能看完，密码学太难看不懂，工作太忙没有时间复习。”

为了帮助“准信息安全工程师”们，结合我们 10 多年的软考辅导心得，我们想就以历次培训经典的 5 天时间，共 30 多个学时作为学习时序，将本书命名为“信息安全工程师的 5 天修炼”，寄希望于考生能在 5 天的时间里有所飞跃。5 天的时间很短，但真正深入学习也很不容易。真诚地希望“准信息安全工程师”们能抛弃一切杂念，静下心来，将 5 天的学习当作一个修炼项目来做，相信一定会有意外的收获。

然而，信息安全工程师考试的范围十分广泛，如信息安全基础、安全法规和标准、计算机网络基础、密码学、网络安全、系统安全、应用配置等领域知识，这里每一门知识都可以扩展为一门或者多门课程。同时，大部分考生们是没有足够的时间反复阅读教程的，也没有时间和精力耗费在旷日持久的复习上。所以，我们坚持简化教程、突出重点，利用“思维导图”来帮助考生梳理考纲、教程、考题所涉及的知识脉络；对于重点和难点进行标记，并进行详细阐述和分析；对于一般性的知识点和通俗易懂的知识简单分析。最终实现把书读薄，把书读透，花较少的精力亦能获得很好的成绩。

感谢学员在教学过程中给予的反馈！

感谢合作培训机构给予的支持！

感谢中国水利水电出版社在此套丛书上的尽心尽力！

感谢湖南师范大学信息化办公室陈宇主任、张智勇主任和全体同事们的大力支持，他们为本书提了不少宝贵意见，甚至参与了部分编写工作！

我们自知本书并非完美，我们的教师团队也必然会持续完善本书。读者在阅读过程中有任何想法和意见，欢迎关注“攻克要塞”公众号（扫描以下二维码），与我们交流。

编 者

2017 年 1 月

II

目 录

冲关前的准备

不管基础如何、学历如何，拿到这本书的就算是有缘人。5 天的关键学习并不需要准备太多的东西，不过还是在此罗列出来，以做一些必要的简单准备。

（1）本书。如果看不到本书那真是太遗憾了。

（2）至少 20 张草稿纸。

（3）1 支笔。

（4）处理好自己的工作和生活，以使这 5 天能静下心来学习。

◎考试形式解读

信息安全工程师考试有两场，分为上午考试和下午考试，两场考试均在同一天。而且两场考试中都要合格，方可拿到信息安全工程师证书。

上午考试的内容是**信息安全基础知识**，考试时长为 150 分钟，考题均为单项选择题（其中含 5 分的英文题）。上午考试共计 75 道题，每题 1 分，满分 75 分，通常 45 分过关。

下午考试的内容是**信息安全应用技术**，考试时长为 150 分钟，笔试，问答题。一般为 5 道大题，每题 10~20 分，每道大题含若干个小问，满分 75 分，通常 45 分过关。

◎答题注意事项

上午考试答题时要注意以下事项：

（1）记得带 2B 以上的铅笔和橡皮。上午考试答题采用填涂答题卡的形式，阅卷是由机器阅卷的，所以需要使用 2B 以上的铅笔；带好一点的橡皮是为了修改选项时擦得比较干净。

（2）注意把握考试时间，上午考试时间有 150 分钟，但题量较大，一共 75 道题，每道题答题时间不到 2 分钟，最后还要留出 10 分钟填涂答题卡以及核对选项。

（3）做题先易后难。上午考试中一般前面的试题会容易一点，大多是知识点性质的题目，以及少量计算题，个别题会有一定难度，难题常出现在 60 ~ 70 题之间。考试时建议先将容易做的和自己会的做完，其他的先跳过去，在后续的时间中再集中精力做难题。

下午考试答题采用的是专用答题纸，题型可以是选择题、填空题、简答题、计算题等。下午考

试答题时要注意以下事项：

（1）先易后难。先大致浏览一下 5 道考题，考试往往既会有知识点问答题，也会有计算题，同样先将自己最为熟悉和最有把握的题先完成，再重点攻关难题。

（2）问答题最好以要点形式回答。阅卷时多以要点给分，不一定要求和参考答案一模一样，常以关键词语或语句意思表达相同或接近为判断是否给分或给多少分的标准。因此答题时要点要多写一些，以涵盖到参考答案中的要点。比如，如果题目中某问题给的是 5 分，则极可能是 5 个要点，一个要点 1 分，回答时最好能写出 7 个左右的要点。

◎制定复习计划

5 天的集中学习对每位考生来说都是一个挑战，这么多的知识点要在短短的 5 天时间内看完是很不容易的，也是非常紧张的，但也是值得的。学习完这 5 天，相信你会感到非常充实，通过考试胜券在握。先看看这 5 天的内容是如何安排的吧（如表 1-1 所示）。

表 1-1　5 天修炼学习计划表

时间		学习内容
第 1 天　学习基础，熟悉法律	第 1～4 学时	信息安全基础知识
	第 5～8 学时	安全法规和标准
第 2 天　夯实基础，学习密码学	第 1 学时	密码学基本概念
	第 2 学时	分组密码
	第 3 学时	序列密码
	第 4 学时	Hash 函数
	第 5 学时	公钥密码体制
	第 6～8 学时	数字签名、认证、密钥管理
第 3 天　学习网络和网络安全	第 1～4 学时	计算机网络基础
	第 5～8 学时	网络安全
第 4 天　再接再厉，深入实践	第 1～2 学时	系统安全
	第 3～4 学时	应用安全
	第 5～6 学时	信息系统安全
	第 7～8 学时	安全配置
第 5 天　模拟测试，反复操练	第 1～2 学时	模拟测试 1（上午试题）
	第 3～4 学时	模拟测试 1（下午试题）
	第 5～6 学时	模拟测试 1（上午试题点评）
	第 7～8 学时	模拟测试 1（下午试题点评）

闲话不多说了，开始第 1 天的学习吧。

1

学习基础，熟悉法律

第 1 天学习的知识点包括信息安全基础知识、安全法规和标准。

第 1 章　信息安全基础知识

本章考点知识结构图如图 1-0-1 所示。

图 1-0-1　考点知识结构图

1.1 信息安全研究方向

目前信息安全的研究包含密码学、网络安全、信息系统安全、信息内容安全、信息对抗等方向。

网络空间是所有信息系统的集合，网络空间安全的核心是信息安全。网络空间安全学科是研究信息的获取、存储、传输、处理等领域中信息安全保障问题的一门学科。

1.2 信息安全理论基础

信息安全理论基础包含的学科如下：

（1）通用理论基础。

- 数学：包含代数、数论、概率统计、组合数学、逻辑学等知识。
- 信息理论：包含信息论、控制论、系统论。
- 计算理论：包含可计算性理论、计算复杂性理论。

（2）特有理论基础。

- 访问控制理论：包含各种访问控制模型、授权理论。
- 博弈论：一些个人、团队、组织面对一定的环境条件，在一定的规则约束下，依靠掌握的信息，同时或先后，一次或多次，从各自允许选择的行为或策略进行选择并实施，并各自取得相应结果或收益的过程。
- 密码学：研究编制密码和破译密码的技术科学。

1.3 信息安全方法论

网络安全方法论是研究解决安全问题的方法，具体内容有**理论分析、逆向分析、实验验证、技术实现**。

1.4 信息系统安全层次

信息系统安全可以划分为四个层次，具体如表 1-4-1 所示。

表 1-4-1 信息系统安全层次

层次	属性	说明
设备安全	设备稳定性	设备一定时间内不出故障的概率
	设备可靠性	设备一定时间内正常运行的概率
	设备可用性	设备随时可以正常使用的概率

续表

层次	属性	说明
数据安全	数据秘密性	数据不被未授权方使用的属性
	数据完整性	数据保持真实与完整，不被篡改的属性
	数据可用性	数据随时可以正常使用的概率
内容安全	政治健康	略
	合法合规	
	符合道德规范	
行为安全	行为秘密性	行为的过程和结果是秘密的，不影响数据的秘密性
	行为完整性	行为的过程和结果可预期，不影响数据的完整性
	行为的可控性	可及时发现、纠正、控制偏离预期的行为

1.5 信息安全管理

信息安全管理是维护信息安全的体制，是对信息安全保障进行指导、规范的一系列活动和过程。**信息安全管理体系**是组织在整体或特定范围内建立的信息安全方针和目标，以及所采用的方法和手段所构成的体系。该体系包含**密码管理、网络管理、设备管理、人员管理**。

1.5.1 密码管理

密码技术是保护信息安全的最有效手段，也是保护信息安全的最关键技术。各国政府相应出台了各种密码管理政策用于控制密码技术、监控密码市场等。目前我国密码管理相关的机构是国家密码管理局，全称国家商用密码管理办公室。

国家出台密码相关的主要政策有《商用密码管理条例》（中华人民共和国国务院第 273 号令，1999 年 10 月 7 日发布）、《电子认证服务密码管理办法》《证书认证系统密码及其相关安全技术规范》《商用密码科研管理规定》《商用密码产品生产管理规定》和《商用密码产品销售管理规定》《可信计算密码支撑平台功能与接口规范》《IPSec VPN 技术规范》。

《商用密码管理条例》相关的重要规定如下：

第二条 本条例所称商用密码，是指对不涉及国家秘密内容的信息进行加密保护或者安全认证所使用的密码技术和密码产品。

第三条 商用密码技术属于国家秘密。国家对商用密码产品的科研、生产、销售和使用实行专控管理。

第四条 国家密码管理委员会及其办公室（以下简称国家密码管理机构）主管全国的商用密码管理工作。

1.5.2 网络管理

网络管理是对网络进行有效而安全的监控、检查。网络管理的任务就是检测和控制。OSI 定义的网络管理功能有性能管理、配置管理、故障管理、安全管理、计费管理。

注意：详细的网络管理知识参见本书的 SNMP 部分。

1.5.3 设备管理

设备安全管理包含设备的选型、安装、调试、安装与维护、登记与使用、存储管理等。设备管理相关标准有：《电子计算机机房设计规范》（GB50173-9）、《计算站场地技术条件》（GB2887-89）、《计算站场地安全要求》（GB9361-88）。

1.5.4 人员管理

人员管理应该全面提升管理人员的业务素质、职业道德、思想素质。网络安全管理人员首先应该通过安全意识、法律意识、管理技能等多方面的审查；之后要对所有相关人员进行适合的安全教育培训。

安全教育对象不仅仅包含网络管理员，还应该包含用户、管理者、工程实施人员、研发人员、运维人员等。

安全教育培训内容包含法规教育、安全技术教育（包含加密技术、防火墙技术、入侵检测技术、漏洞扫描技术、备份技术、计算机病毒防御技术和反垃圾邮件技术、风险防范措施和技术等）和安全意识教育（包含了解组织安全目标、安全规定与规则、安全相关法律法规等）。

1.6 ISO 安全体系结构

ISO 制定了国际标准 ISO7498-2-1989《信息处理系统开放系统互连基本参考模型 第 2 部分安全体系结构》。该标准描述了开放系统互连（OSI）的基本参考模型，为协调开发现有的与未来系统互连标准建立起了一个框架。其任务是提供安全服务与有关机制的一般描述，确定在参考模型内部提供服务与机制的位置。图 1-6-1 给出了开放系统互连安全体系结构示意图。

ISO 的开放系统互连安全体系结构包含了安全机制、安全服务、OSI 参考模型，并明确了三者之间的逻辑关系。

- 安全机制：保护系统免受攻击、侦听、破坏及恢复系统的机制。
- 安全服务：加强数据处理系统和信息传输的安全性服务，利用一种或多种安全机制阻止安全攻击。
- OSI 参考模型：开放系统互连参考模型，即常见的七层协议体系结构。

网络安全体系结构借鉴了开放系统互连安全体系结构，具体如图 1-6-2 所示。

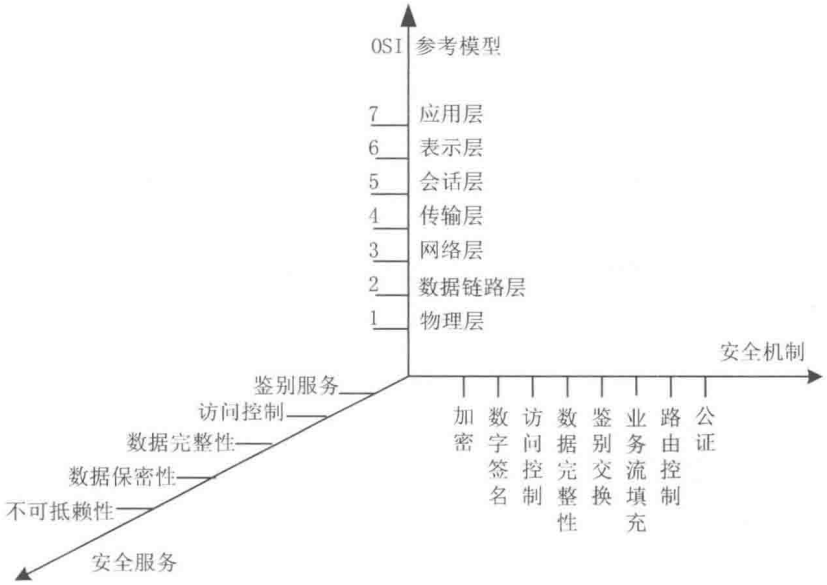

图 1-6-1 开放系统互连安全体系结构示意图

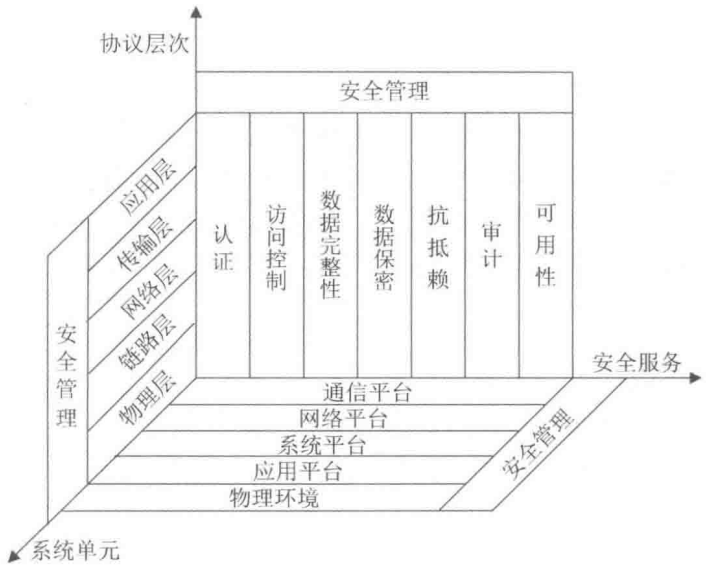

图 1-6-2 网络安全体系结构图

网络安全体系结构包含三部分内容：协议层次、系统单元、安全服务。

- 协议层次：TCP/IP 协议。
- 系统单元：该安全单元能解决哪些系统环境的安全问题。
- 安全服务：该安全单元能解决哪些安全威胁。