重点大学信息安全专业规划系列教材

信息安全管理概论

胡勇 吴少华 编著

清华大学出版社

重点大学信息安全专业规划系列教材

信息安全管理概论

胡勇 吴少华 编著

清华大学出版社
北京

内 容 简 介

本书对信息安全管理理论与方法论做了全面的论述，也对信息安全管理的工程技术实践做了方法论的总结，包括识别信息系统及资源的方法和分类原则，识别信息系统资产的脆弱性、威胁、影响，风险分析过程描述，以及信息系统安全等级保护有关的可操作性技术方法；基于风险管理，从资源分析、风险分析与评估、安全需求分析，到安全保护策略和安全措施选择的工程实践方法和实务操作的详细描述。

本书是面向大专院校信息安全管理专业的基础教材，读者对象定位于大学计算机和通信类一级学科下的专业硕士、信息安全本科学生，以及从事信息系统管理和信息安全管理的工程技术人员。

图书在版编目(CIP)数据

信息安全管理概论/胡勇，吴少华编著. --北京：清华大学出版社，2015
重点大学信息安全专业规划系列教材
ISBN 978-7-302-39703-8

Ⅰ. ①信… Ⅱ. ①胡… ②吴… Ⅲ. ①信息系统－安全管理－高等学校－教材 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字(2015)第 061848 号

责任编辑：付弘宇　王冰飞
封面设计：常雪影
责任校对：李建庄
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
课 件 下 载：http://www.tup.com.cn，010-62795954
印 装 者：北京国马印刷厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：14　　**字　　数**：353 千字
版　　次：2015 年 11 月第 1 版　　**印　　次**：2015 年 11 月第1 次印刷
印　　数：1～2000
定　　价：29.00 元

产品编号：060273-01

INTRODUCTION

出版说明

由于网络应用越来越普及，信息化的社会已经呈现出越来越广阔的前景，可以肯定地说，在未来的社会中，电子支付、电子银行、电子政务以及多方面的网络信息服务将深入到人类生活的方方面面。同时，随之面临的信息安全问题也日益突出，非法访问、信息窃取，甚至信息犯罪等恶意行为导致信息的严重不安全。信息安全问题已由原来的军事国防领域扩展到整个社会，因此社会各界对信息安全人才有强烈的需求。

信息安全本科专业是2000年以来结合我国特色开设的新的本科专业，是计算机、通信、数学等领域的交叉学科，主要研究确保信息安全的科学和技术。自专业创办以来，各个高校在课程设置和教材研究上一直处于探索阶段。但各高校由于本身专业设置上来自于不同的学科，如计算机、通信和数学等，在课程设置上也没有统一的指导规范，在课程内容、深浅程度和课程衔接上，存在模糊不清、内容重叠、知识覆盖不全面等现象。因此，根据信息安全类专业知识体系所覆盖的知识点，系统地研究目前信息安全专业教学所涉及的核心技术的原理、实践及其应用，合理规划信息安全专业的核心课程，在此基础上提出适合我国信息安全专业教学和人才培养的核心课程的内容框架和知识体系，并在此基础上设计新的教学模式和教学方法，对进一步提高国内信息安全专业的教学水平和质量具有重要的意义。

为了进一步提高国内信息安全专业课程的教学水平和质量，培养适应社会经济发展需要的、兼具研究能力和工程能力的高质量专业技术人才。在教育部相关教学指导委员会专家的指导和建议下，清华大学出版社与国内多所重点大学共同对我国信息安全人才培养的课程框架和知识体系，以及实践教学内容进行了深入的研究，并在该基础上形成了“信息安全人才需求与专业知识体系、课程体系的研究”等研究报告。

本系列教材是在课程体系的研究基础上总结、完善而成，力求充分体现科学性、先进性、工程性，突出专业核心课程的教材，兼顾具有专业教学特点的相关基础课程教材，探索具有发展潜力的选修课程教材，满足高校多层次教学的需要。

本系列教材在规划过程中体现了如下一些基本组织原则和特点。

(1) 反映信息安全学科的发展和专业教育的改革，适应社会对信息安全人才的培养需求，教材内容坚持基本理论的扎实和清晰，反映基本理论和原理的综合应用，在其基础上强调工程实践环节，并及时反映教学体系的调整和教学内容的更新。

(2) 反映教学需要，促进教学发展。教材要适应多样化的教学需要，正确把握教学内容和课程体系的改革方向，在选择教材内容和编写体系时注意体现素质教育、创新能力与实践能力的培养，为学生知识、能力、素质协调发展创造条件。

(3) 实施精品战略，突出重点。规划教材建设把重点放在专业核心(基础)课程的教材建设上；特别注意选择并安排一部分原来基础比较好的优秀教材或讲义修订再版，逐步形成精品教材；提倡并鼓励编写体现工程型和应用型的专业教学内容和课程体系改革成果的教材。

(4) 支持一纲多本，合理配套。专业核心课和相关基础课的教材要配套，同一门课程可以有多本具有各自内容特点的教材。处理好教材统一性与多样化，基本教材与辅助教材、教学参考书，文字教材与软件教材的关系，实现教材系列资源的配套。

(5) 依靠专家，择优落实。在制定教材规划时，依靠各课程专家在调查研究本课程教材建设现状的基础上提出规划选题。在落实主编人选时，要引入竞争机制，通过申报、评审确定主编。书稿完成后认真实行审稿程序，确保出书质量。

繁荣教材出版事业，提高教材质量的关键是教师。建立一支高水平的、以老带新的教材编写队伍才能保证教材的编写质量，希望有志于教材建设的教师能够加入到我们的编写队伍中来。

重点大学信息安全专业规划系列教材

联系人：魏江江 weijj@tup.tsinghua.edu.cn

FOREWORD

前言

这是一本面向大专院校信息安全管理专业的基础教材，读者对象定位于大学计算机和通信类一级学科下的专业硕士、信息安全本科学生，以及从事信息系统管理和信息安全管理工作的工程技术人员。

本书的作者曾在2004年承担由国务院信息化工作办公室下达的“信息安全管理指南”研究项目，此后十年来作者与同事们在信息安全本科和专业硕士的教学中结合项目的研究成果致力于对信息安全管理理论和工程实践进行与时俱进的探索，获得了一些新的知识与研究成果，在此基础上编撰成本书，以此奉献给国内从事信息安全教学与信息安全管理的朋友们。虽然作者尽了最大努力，并力求在书稿中体现中国特色和国家对信息安全管理的方针政策，但由于信息安全问题随着信息化的发展不断出现新情况，有的情况符合预期，有的情况则需要继续审视，加之作者的视野和水平所限，书中仍存在需要探索和商榷，甚至错误的地方；更由于作者在信息安全管理理论和方法研究方面的视角可能与国内同行有所不同，因此本书中如有与他人观点和管理实践不一致的地方，则应该是可以在学术上争鸣的见仁见智的事情；但作者和同事们将尽最大努力，与国内同行们继续努力，虚心学习他们的研究经验和成果，以矫正、丰富和完善我们在这一领域的研究和实践。我们希望，现在呈现给读者朋友的这本书能对读者朋友们系统地认识信息安全管理中的问题有所帮助。

本书既对信息安全管理理论与方法论有较为全面的论述，也对信息安全管理的工程技术实践做了方法论的总结，其中涉及的内容有识别信息系统及资源的方法和分类原则，识别信息系统资产的脆弱性、威胁、影响，进行风险分析的过程描述，以及与信息系统安全等级保护有关的可操作性技术方法；从信息安全管理角度进行基于风险管理的从资源分析、风险分析与评估、安全需求分析到安全保护策略和安全措施选择的工程实践方法和实务操作的详细描述。

本书由胡勇、吴少华编写，其中胡勇负责设计全书的结构，并编写第1、3、6章，吴少华编写第2、4、5章以及附录。

本书的编撰得到了戴宗坤、罗万伯两位老师的热情鼓励和直接指导，在此表示衷心的感谢。

本书的配套课件可以从清华大学出版社网站 www.tup.com.cn 下载，关于本书及课件使用的任何问题请联系 fuhy@ tup.tsinghua.edu.cn。

编　者

2015 年 10 月

CONTENTS

目录

CHAPTER 1

第1章 引 言

1.1 背景

我国的信息化建设正处在蓬勃发展时期，各种基于互联网的信息化应用如雨后春笋不断涌现；各种组织或机构出于管理和业务流程的需要已经或正在建设自己的网络信息系统，这些信息系统或为组织业务提供自动化、数字化、网络化管理的技术支持和决策辅助，或为社会提供信息服务，或为个人、团体提供交流平台，等等，由此催生出一大批新兴产业。由于网络信息系统的高度互连互通性和其技术标准的开放性，对安全性的考虑不足，以及存在各种各样的威胁，使信息系统面临信息泄露、篡改，身份被假冒，网络活动被监控，甚至数据、组件、系统被损或被毁等风险，从而导致有形无形的资产损失或系统故障、瘫痪直至崩溃。这些问题就是信息安全问题，由此而伴生的另一个问题就是信息系统的安全保障问题。

信息系统安全保障是一个很广泛的概念，本书重点从管理角度就开放互连网络环境下的信息系统的安全保障问题进行系统论述，包括信息系统在设计、开发、实施、运行和维护直至报废的整个生命周期的安全保障问题，给出解决问题的管理原则和工程方法，目的在于确保信息系统在国家法律法规框架内的安全、有序和健康的运行。

为叙述方便，本书对信息系统安全和信息安全的概念不做特别区分，同理对信息系统安全保障和信息安全保障也不做特别区分。但是信息安全保障和信息系统安全保障是有区别的，前者是一个更大范围的概念，后者被包含在前者中。

信息系统安全保障涉及保护信息与系统和对抗敌对威胁这两方面的高技术综合应用。在这一应用过程中又要求将技术措施和法律性的行政管控手段结合起来。《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27号文)明确规定，国家对信息安全保障工作的基本原则是“立足国情，以我为主，坚持管理与技术并重；正确处理安全与发展的关系，统

筹规划，突出重点，强化基础性工作；明确国家、企业、个人的责任和义务；充分发挥各方面的积极性，共同构筑国家信息安全保障体系。”科学的信息安全管理方法与实践对于信息安全保障的贡献在于两个方面，一是通过管理将信息安全技术转化为信息安全保障能力，二是以管理优势弥补技术的不足和缺失，全面优化和提升信息安全保障能力。

1.2 目的和范围

本书针对计算机网络信息系统在开放互连网络环境下的安全管理问题给出指导性的原则和工程方法，包括从管理角度对规划、设计、开发、实施、运行和维护信息系统的安全问题的识别到确保信息系统的运行始终处于安全、健康、有序和可控的状态所涉及的技术和非技术的方法和原则，以供各类信息系统在规划、设计、开发、施工和运行维护过程中参考。

1.3 适用性

本书关于信息安全管理的技术和非技术的工程方法和原则主要适用于开放系统互连网络环境下的各类信息系统，包括计算机网络信息系统和公用通信网络系统等，以及与信息技术有关的网络基础设施。

1.4 本书结构

本书共 6 章，第 1 章是引言；第 2 章为本书直接引用的基本术语和定义（依其在本书中首次出现的顺序排列）以中文形式给出，同时给出相应的英文单词或词组；第 3 章是信息安全管理概述；第 4 章为信息安全管理和组织结构；第 5 章是信息管理方法与过程；第 6 章为信息安全管理的实施。附录部分给出了与本书内容有关的名词和术语（以英文字母升序排列，同时给出相应的中文单词与词组）的词条性释义，以及英文缩略语的全称和对应的中文名词或术语。

1.5 习题与思考题

1. 查找并阅读中办发[2003]27 号文件，深入理解其中关于安全与发展的关系、统筹规划和突出重点的论述。

2. 说明信息安全管理与信息安全技术之间的关系。

3. 信息安全管理在信息系统安全保障体系中的地位和作用。

CHAPTER 2

本书直接引用的术语和定义 第2章

2.1 术语

信息技术(Information Technology,IT)

信息技术指获取、存储、加工、变换、显示和传输文字、数值、图像与视频、音频和语言信息的技术,以及提供这些技术的方法与设备的总称。这一术语有时与自动电子处理设备的含义很难严格区分。

从对信息的开发和使用角度看,信息技术可分为3个层次:第一层是硬件,主要指数据的获取、存储、处理、显示和传输的计算机和网络通信设备或组件技术;第二层是信息加工与通信软件,包括数据的获取、存储、加工、显示和传输的逻辑运算和网络通信有关的各种软件系统或模块技术,这部分技术只对开发人员可见;第三层是应用软件,指面向终端用户进行检索、查询、完成业务流程、统计分析、辅助决策等软件系统或模块技术。

信息技术安全,IT安全(IT security)

信息技术安全指获得并维持信息技术系统及其组件机密性、完整性、可用性和可控性等有关的所有方面。

信息技术安全策略,IT安全策略(IT security Policy)

信息技术安全策略指对一个组织的信息系统的所有资产(包括敏感信息在内)实施管理、保护以及分配控制措施的规则和指令。

信息安全(information security)

信息安全指保证信息和信息系统的机密性、完整性、可用性和可控性,从而使信息和信息系统免遭未授权的访问、占用、泄露、干扰、修改、重放和破坏,并保证使用和操作信息和信息系统的任何实体的身份不被假冒或欺骗、实体的来源与行为可被唯一跟踪和不可抵赖的总的特性。其中,机密性指对信息(也包括任何形式的个人隐私和专用权信息)和信息系统的访问或泄露只限于被授权者的特性;完整性指信息和信息系统不受到任何形式的未授权修改和重放的特性,还包括信息和信息系统的来源的真实性;可用性指信息

和信息系统能及时地和可靠地为授权者提供访问和使用，以及能在面对各种攻击或出现差错和故障的情况下继续提供实质性服务，并且能够及时地恢复正常服务的特性；可控性指对信息系统中出现的可预见和未预见的事件具有应对措施或应急处理预案，可控制事态的发展。

国家(信息)安全系统(National Security System)

国家(信息)安全系统指由某一(国家或政府)机构，或机构的合约方，或机构所信任的其他组织所运行或使用(包括通信基础设施在内)的信息系统。这些信息系统涉及(国家)情(谍)报活动，国计民生和社会稳定，与国家安全有关的密码活动，军事力量的指挥与控制，作为武器与武器系统组成部分的装备。

资产(asset)

资产指信息系统中对于一个组织具有价值的任何东西和事物(包括硬件的或软件的，有形的或无形的，货币化的或非货币化的，等等)。对资产的估价可采用定量、定性或定量与定性结合的计算方法。

机密性(confidentiality)

机密性指对信息和信息系统的访问和泄露只限于被授权者的特性，包括任何形式的个人隐私和专用权信息，也可理解为是信息和信息系统对未授权访问者不知其存在、不可访问(或不可接近)和不可理解的特性。

数据完整性(data integrity)

数据完整性指数据不受到任何形式的未授权修改和重放的特性，并且包括保证信息(数据)来源的真实性，其中的修改包括对数据的增加、减少、插入、生成和删除等操作行为。

完整性(integrity)

完整性是对数据完整性概念的合理延伸，指信息体和信息系统(包括软/硬件子系统和组(器)件)不受到任何形式的未授权修改和重放的特性，并且包括保证信息体和信息系统来源的真实性。完整性还适用于对连接的描述，即连接完整性。

可用性(availability)

可用性指信息和信息系统能适时地和可靠地为授权者提供访问和使用的服务能力，以及能在面对各种攻击或出现差错和故障的情况下继续提供实质性服务，并且能够及时地恢复正常服务的特性。

可确认性(accountability，又称可审查性或可追查性)

可确认性是一种保证某一实体的行为可被唯一跟踪到该实体的特性。

真实性(authenticity)

真实性是保证一个实体或资源的身份及来源就是其所声称的那个实体或资源的身份和来源的特性。真实性往往通过对用户、进程、协议层(例如网络层、传输层等)、系统和信息等实体的鉴别来实现。

抗抵赖性(non-repudiation)

抗抵赖性指对否认或抵赖曾经使用和操作过信息或信息系统的行为以及操作的内容进行对抗性证实的特性。

脆弱性(vulnerability)

脆弱性指一个或一组信息系统资源的弱点或缺陷。这些弱点或缺陷可能导致在规程(协议、格式等)、系统设计、系统实现、内部控制和运行等方面被敌对实体(威胁)开发和利用。

威胁(threat)

威胁指自然或人为(有意或无意)地限制、阻止、破坏信息系统正常运营,或降低服务(处理)能力,或降低系统或设备能力的有效性,或泄漏和窃取信息和系统资产等的潜在力量、能力和战略目标的总和。威胁包括对信息和系统的机密性、完整性、可用性、可确认性和抗抵赖性等特性造成危害的所有因素。

影响(impact)

影响指不期望的事件所引起的后果,包括有形的和无形的,货币化的和非货币化的损失。

风险(risk)

风险指给定的威胁利用某一或某组(信息系统)资源的脆弱性对一个组织造成损失的可能性(概率)以及损失(影响/后果)的总和。

风险分析(risk analysis)

风险分析指识别风险的时间和空间分布及强度(或等级),以此导出防范风险的安全需求的过程。

风险管理(risk management)

风险管理指通过适当的技术和管理措施实现阻止、降低、消除、转移或接受影响信息系统资产安全性的不定因素的总过程,包括风险分析、安全需求分析、安全保护措施的选择、实现与测试、安全评估以及所有与安全有关的管理活动。

残留风险(residual risk)

残留风险指信息系统在采取安全保护措施后仍未消除的风险,对残留风险必须评估其是否可接受。

安全措施(safeguard)

安全措施也称安全保护措施,是阻止、降低、消除或转移风险的实践、程序和机制。

积极防御(Active defence)

积极防御也称主动防御,其含义是坚持用发展的思路辩证地认识和解决信息安全保护问题,主动地应对安全风险。在对信息安全风险进行充分分析和评估的基础上构造安全防护与安全监管结合的保护体系,加强预警、应急处理和灾难备份。

基线控制(baseline control)

基线控制指一个(行业)系统或组织的信息系统从安全保障工程角度建立的安全保护措施的最小集。

组织(Organization)

组织指一个机构管理下的具有共同利益和共同安全属性的业务单位或部门的总称。例如,一个企业、一个机关或一个法人单位在本书中都以组织代称,有时也称为团体或共同体。

2.2 习题与思考题

1. 理解机密性、完整性和可用性的含义。
2. 信息系统资源和资产有什么区别与关系？
3. 脆弱性和威胁有什么关系？
4. 风险管理包括哪些过程？其中涉及哪些活动内容？
5. 残留风险的含义是什么？为什么说不宜也不能完全消除残留风险？