特色专业

普通高等教育信息安全类国家级特色专业系列规划教材

信息安全标准与法律法规

周世杰　蓝 天　傅 翀　赵 洋　编著

科学出版社

普通高等教育信息安全类国家级特色专业系列规划教材

信息安全标准与法律法规

周世杰　蓝　天　傅　翀　赵　洋　编著

科学出版社

北　京

内 容 简 介

本书主要介绍了国内外信息安全标准和法律法规的背景知识、发展状况，并对较有影响力的标准和法律法规进行了详细说明。通过对本书的学习，读者可对标准的概念、国内外信息安全标准及法律法规有一个较为全面的了解。全书共分为三个部分，由 12 章组成，内容包括标准概述，立法、司法和执法概述，信息安全国际标准概况，我国信息安全标准概况，信息安全主要应用标准介绍，信息安全管理相关国际标准，我国计算机信息系统安全等级保护标准，信息安全法律法规概况，信息安全国家法律，信息安全行政法规，信息安全部门规章和规范性文件。

本书可作为高等院校信息安全专业高年级本科生与研究生的教材，也可作为信息安全专业人员培训班的培训教材，以及供从事相关工作的技术人员和对信息安全感兴趣的读者阅读参考。

图书在版编目(CIP)数据

信息安全标准与法律法规 / 周世杰等编著. —北京：科学出版社，2012

（普通高等教育信息安全类国家级特色专业系列规划教材）

ISBN 978-7-03-034434-2

Ⅰ. ①信… Ⅱ. ①周… Ⅲ. ①信息系统-安全技术-标准-高等学校-教材 ②信息系统-安全技术-法规-世界-高等学校-教材 Ⅳ. ①TP309-65 ②D912.1

中国版本图书馆 CIP 数据核字(2012)第 105741 号

丛书策划：匡 敏 潘斯斯

责任编辑：潘斯斯 张丽花 / 责任校对：包志虹

责任印制：阎 磊 / 封面设计：迷底书装

科 学 出 版 社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

保定市中画美凯印刷有限公司印刷

科学出版社发行 各地新华书店经销

*

2012 年 12 月第 一 版 开本：787×1092 1/16

2012 年 12 月第一次印刷 印张：16 1/4

字数：426 000

定价：35.00 元

（如有印装质量问题，我社负责调换）

《普通高等教育信息安全类国家级特色专业系列规划教材》

编 委 会

丛 书 序

当今社会，信息已经成为最具活力的生产要素和重要战略资源。信息技术改变着人们的生活和工作方式。信息产业已成为世界第一大产业。信息的获取、处理和安全保障能力成为综合国力的重要组成部分，信息安全已成为影响国家安全、社会稳定和经济发展的决定性因素之一。

目前关于信息安全的定义和内涵，尚未形成一个统一的说法。不同的学者给出了不同的诠释。尽管这些诠释不尽相同，但是其主要内容却是相同的。我们应当从信息系统角度来全面诠释信息安全的内涵。

信息安全学科是综合计算机、电子、通信、数学、物理、生物、管理、法律、教育等学科演绎而成的交叉学科，它与这些学科既有紧密的联系和渊源，又具有本质的不同，从而构成一门独立的学科。

随着学科的交叉发展和产业的整合，各专业方向已彼此渗透交融。如何拓宽专业方向，如何体现专业特色，是当前我国高等学校信息安全类专业在办学方面所迫切需要探讨的问题。教育部高等学校信息安全类专业教学指导委员会起草的《普通高等学校信息安全本科指导性专业规范》，按照“统一与特色相结合，宽口径，最小集合，最低标准，分类指导”的原则，对本专业的核心知识领域和知识单元的覆盖范围作了规定，旨在培养德、智、体等全面发展，掌握自然科学、人文科学基础和信息科学基础知识，系统掌握信息安全学的基本理论、技术和应用知识，并具备科学研究和实际工作能力的信息安全高级专门人才。

教育部为推进“质量工程”，自 2007 年 10 月开始，先后三批遴选了国家级特色专业建设点。目前，有十余所高校被批准为信息安全国家级特色专业建设点。在教材建设方面，2008 年 10 月，教育部高教司在《关于加强“质量工程”本科特色专业建设的指导性意见》中指出：“教材建设要反映教学内容改革的成果，积极推进教材、教学参考资料和教学课件三位一体的立体化教材建设，选用高质量教材，编写新教材。”为了适应新形势下对信息安全领域人才培养的需求，本届信息安全类专业教学指导委员会经过广泛深入调研，主要依托信息安全专业国家级特色专业建设点，与科学出版社共同组织出版本套《普通高等教育信息安全类国家级特色专业系列规划教材》，旨在贯彻专业规范和教学基本要求，总结和推广各特色专业建设点的教学经验和教学成果，提高我国信息安全专业本科教学的整体水平。

本套丛书在组织编写中，重点突出了以下几方面的特色。

1. 体现专业特色，贯彻专业规范和教学基本要求。依托“国家级特色专业建设点”，汇总优秀教学成果，将特色专业教育的内容、国内外科研教学的成果、信息安全专业规范与教学基本要求结合起来，内容安排围绕专业规范，体现核心知识单元与知识点。

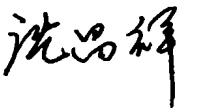
2. 按照分类指导原则，满足多层面的需求。针对同一类课程，根据不同的教学层次（普通院校、重点院校或研究型大学、应用型大学）和学时要求（多学时、少学时），涵盖不同范围的拓展知识单元，编写适合不同层面需求的教材。注重与先修课程、后续课程的有机衔接，每本书在重视系统性和完整性的基础上，尽量减少内容重复。

3. 拓宽专业基础，面向工程应用，加强实践环节。注重反映本学科领域的最新成果和发展方向，适当拓宽专业基础知识的范围，以增强所培养人才的适应性；面向工程应用，突出工科特色，反映新技术、新工艺；注重实践环节的设置，以促进学生的实际动手能力和创新能力的培养，真正使教材能够达到培养“厚基础、宽口径、会设计、可操作、能发展”人才的目的。

4. 注重立体化建设。本套丛书除了主教材外，还将逐步配套学习辅导书、教师参考书和多媒体课件等，为任课教师提供丰富的配套教学资源，方便教师教学，同时帮助学生复习与自学，使本套丛书更加易教易学。

本套丛书的编写汇聚了全国高校的优势资源，突出了多层次与适应性、综合性与多样性、前沿性与先进性、理论与实践的结合。在教材的组织和出版过程中得到了相关高校教务处及学院的帮助，在此表示衷心的感谢。

根据信息安全发展战略的要求，我们将对本套丛书不断更新，以保持教材的先进性和适用性。热忱欢迎全国同行以及关注信息安全领域教育及发展前景的广大有识之士对我们的工作提出宝贵意见和建议！



教育部高等学校信息安全类专业教学指导委员会主任委员

中国工程院院士

2011 年 4 月

前　言

随着信息技术的不断发展和我国社会信息化进程的不断深入，信息系统本身的脆弱性和复杂性也日益呈现出来。信息安全事件和问题不断暴露，受到了政府和社会的广泛关注。各国纷纷研制和颁布信息安全相关标准与法律法规，我国也对信息安全的标准和法律法规建设相当重视，已经建成一套基本上满足我国经济和社会发展需要的标准和法律体系，为促进国民经济和社会发展发挥了积极作用。掌握相关标准和法律法规，使得信息安全从业人员能够有据可依、有法可循；了解相关标准和法律法规，对于规范信息系统使用者的行为也是有必要的。

本书主要介绍了国内外信息安全标准和法律法规的背景知识、发展状况，并对较有影响力的标准和法律法规进行了详细说明。通过对本书的学习，读者可对标准的概念、国内外信息安全标准及法律法规有一个较为全面的了解。全书共分为三个部分，由 12 章组成，内容包括标准和法律法规基本概念、信息安全国际国内标准概况、信息安全主要应用和管理标准、我国计算机信息系统安全等级保护标准、信息安全国际国内法律法规概况、信息安全国家法律、行政法规、部门规章、规范性文件和地方法规等。

第 1 章为绪论。本章主要介绍了信息和信息安全的基本概念以及信息安全涉及的法律问题。

第 2 章为标准概述。本章主要介绍了标准和标准化的概念，标准化的意义、发展过程和原理。

第 3 章为立法、司法和执法概述。本章从立法、司法和执法三个方面对国内外主要的法律体制、制度和组织进行了介绍。

第 4 章为信息安全国际标准概况。本章对主要的信息安全国际标准体系进行了介绍，包括 ISO/IEC、ITU、美国标准体系、英国标准体系、IETF 和 RFC。

第 5 章为我国信息安全标准概况。本章首先对我国信息安全标准化情况、标准概况和标准化未来发展趋势进行了简介，然后从安全技术、物理安全、系统与网络、应用与工程、管理五方面介绍了我国的信息安全标准体系的组成。

第 6 章为信息安全主要应用标准介绍。本章主要介绍了应用相关的信息安全标准，包括密码学相关、计算机网络相关、电子商务相关以及数据库相关的安全标准。

第 7 章为信息安全管理相关国际标准。本章首先简要介绍了管理相关的信息安全国际标准 BS 7799、ISO/IEC 17799 和 ISO/IEC 27000 族，然后围绕 ISO/IEC 27002 及 ISO/IEC 27001 对信息安全管理相关的国际标准进行了阐述。

第 8 章为我国计算机信息系统安全等级保护标准。本章单独介绍我国的信息安全重要标准——计算机信息系统安全等级保护标准，首先是对安全保护等级划分的概述，然后分别对信息系统安全保护等级划分准则、安全管理要求和通用安全技术要求进行了详细的说明。

第 9 章为信息安全法律法规概况。本章主要对国内外信息安全法律法规的现状进行了介绍，包括美国、欧洲、亚洲和我国的信息安全法律法规概况。

第 10 章为信息安全国家法律。本章对我国已有的主要信息安全国家法律进行了详细解读，包括保守国家秘密法、国家安全法、反不正当竞争法、电子签名法、关于维护互联网安全的决定和刑法修正案(七)关于信息安全的修订与解读等。

第 11 章为信息安全行政法规。本章对我国已有的主要信息安全行政法规进行了详细解读，包括计算机信息系统安全保护条例、计算机信息网络国际联网管理暂行规定实施办法、商用密码管理条例、互联网信息服务管理办法、电信条例、计算机软件保护条例、认证认可条例和信息网络传播权保护条例等。

第 12 章为信息安全部门规章和规范性文件。本章对我国目前主要的信息安全部门规章和规范性文件进行了详细解读，包括保密局、科委、公安部、密码管理局和其他部门发布的部门规章和规范性文件等。

赵洋参与第 1～4 章以及其他部分章节的编写工作；傅翀参与第 5～8 章以及其他部分章节的编写工作；蓝天参与第 9～12 章以及其他部分章节的编写工作；周世杰负责全书统稿工作。在本书完稿之际，作者要衷心感谢所有对本书出版作出贡献的人，感谢电子科技大学信息安全系的所有教师，特别是程红蓉博士、聂旭云博士、陈伟博士和曹晟博士对本书的审阅，他们为本书的顺利出版做了大量有益的工作。

由于时间仓促和水平有限，内容难免有所疏漏，恳请读者批评指正，使本书得以进一步改进和完善。本书中的规范性文件仅供参考，若要使用，请与发文原件进行核对。

编　者

2012 年于蓉城

目　录

第 3 部分 信息安全法律法规

第1部分　总　论

第1章 绪 论

1.1 信息安全概述

信息安全本身包括的范围很大。大到国家军事政治等机密的安全，小到如防范商业企业机密泄露、青少年对不良信息的浏览、个人信息的泄露等。网络环境下的信息安全体系是保证信息安全的关键，包括计算机安全操作系统、各种安全协议、安全机制(数字签名、信息认证、数据加密等)，直至安全系统，其中任何一个安全漏洞便可以威胁全局安全。信息安全服务至少应该包括支持信息网络安全服务的基本理论，以及基于新一代信息网络体系结构的网络安全服务体系结构。

1.1.1 信息的定义

中文“信息”一词有着很悠久的历史，早在两千多年前的西汉，即有“信”字的出现，常可作消息来理解。一千多年前，唐代诗人杜牧在《寄远》诗中写到：“塞外音书无信息，道傍车马起尘埃”。李中的《暮春怀故人》中也有“梦断美人沉信息，目穿长路倚楼台”的佳句。宋代的李清照则发出“不乞隋珠与和璧，只乞乡关新信息”的感叹，在她心目中，来自家乡的信息比珍贵的“隋珠”与“和璧”的价值更高。

在《红楼梦》第十六回里，讲到贾政突然奉旨入朝，贾府上下不知是祸是福，都惶惶不安。后来，随从贾政入朝的赖大等三四个管家气喘吁吁地跑回府来，贾母便唤进赖大来细问端的。赖大禀道：“小的们只在临敬门外伺候，里头的信息一概不能得知。后来还是夏太监出来道喜，说咱们家大小姐晋封为凤藻宫尚书，加封贤德妃。……”《红楼梦》是一部现实主义的伟大古典著作，作者曹雪芹在这部作品中为我们留下了他那个时代的极为丰富的活语言材料。在上面那段引文中，“信息”一词十分自然地出于赖大之口，说明它在当时民间口语中已使用得很平常了。

在古人的文章里，信息的意思多指消息。因为“信息”能够带来家人的问候与平安的消息，所以，在通讯并不发达的古代，古人对“信息”充满了期盼。一个词能历经时代的变迁而保持生命的活力是一回事，使用它的人对它的内涵作何理解则是另一回事。从李中到曹雪芹，“信息”这个词基本上是作为“音信”、“消息”的同义词来使用的。在现代汉语中，在这样的意义上使用“信息”一词，在很长一个时期反倒少了。

“信息”一词来源于拉丁文“informatio”，意思是指解释、陈述。在英语中，表达这个概念的词是 information。早些时候出版的英汉词典中，information 的汉语释义是“消息、见闻、情报、知识、通知、报道”等等。就是说，英语中的 information 与汉语中的“信息”，本来的涵义是大体相当的。后来，information 在收入专业英汉词典时，只用“信息”作为它的汉语释义，这时，它已经作为现代科学技术的一个基本概念而崭露头角了。information(信息)被改造和发展成新的科学概念，是在通信理论的研究中发生的。通信，即使在狭义上理解，在人类社会也有悠久的历史沿革；information(信息)的本来涵义，即音信、消息、情报等等，也是与人类的通信行为或通信过程密不可分的。

人类社会的进步和科学技术的进步，就包含着通信手段和通信技术的不断进步。不过，通信在严格意义上成为科学研究的对象，还只是20世纪才发生的事。随着社会的进步、科学技术的发展，人们对信息的认识也越来越深入，信息概念的含义也在不断地改变和发展。现在，人们所说的“信息”已成为一个包含内容很丰富、意义很深刻的概念，以至人们很难给它下一个确切的定义。作为一个严谨的科学术语，信息的定义却不存在一个统一的观点，这是由它的极端复杂性决定的。信息的表现形式数不胜数：声音、图片、温度、体积、颜色……信息的分类也不计其数：电子信息、财经信息、天气信息、生物信息……要对信息作一个严密而又具有普适性的定义，就必须从本质上来把握信息。现在学术界主要有以下几种观点：

美国数学家、信息论的奠基人克劳德·艾尔伍德·香农(Claude Elwood Shannon)在他的著名论文《通信的数学理论》(1948)中提出计算信息量的公式，即若一个信息由 n 个符号所构成，符号 k 出现的几率为 p_k，则有

$$H = \sum_{k=1}^{n} p_k \log_2 p_k$$

这个公式和热力学的熵的计算方式一样，故也称为信息熵。从公式可知，当各个符号出现的几率相等，即“不确定性”最高时，信息熵最大。故信息可以视为“不确定性”或“选择的自由度”的度量。

美国数学家、控制论的奠基人诺伯特·维纳在他的《控制论——动物和机器中的通讯与控制问题》中认为，信息是“我们在适应外部世界，控制外部世界的过程中同外部世界交换的内容的名称”。英国学者阿希贝认为，信息的本性在于事物本身具有变异度。意大利学者朗高在《信息论：新的趋势与未决问题》中认为，信息是反映事物的形成、关系和差别的东西，它包含于事物的差异之中，而不在事物本身。

狭义上，信息就是符号的排列顺序。但作为一个概念，信息有着多种多样的含义。一般来说，与信息这一概念密切相关的概念包括约束(constraint)、沟通(communication)、控制、数据、形式、指令、知识、含义、精神刺激、模式、感知以及表达。信息是人们在适应外部世界并使这种适应反作用于外部世界过程中，同外部世界进行互相交换的内容和名称。

尽管从不同的角度出发对信息存在不同的定义，但是就信息的一些基本性质还是达成以下一些了共识。

• 普遍性：只要有事物的地方，就必然存在信息。信息在自然界和人类社会活动中广泛存在。

• 客观性：信息是客观现实的反映，不随人的主观意志而改变。如果人为地篡改信息，那么信息就会失去它的价值，甚至不能称之为“信息”了。

• 动态性：事物是在不断变化发展的，信息也必然随之运动发展，其内容、形式、容量都会随时间而改变。

• 时效性：由于信息的动态性，那么一个固定的信息的使用价值必然会随着时间的流逝而衰减。

• 可识别性：人类可以通过感觉器官和科学仪器等方式来获取、整理、认知信息。这是人类利用信息的前提。

• 可传递性：信息可以通过各种媒介在人－人，人－物，物－物等之间传递。

• 可共享性：信息与物质、能量显著不同的是，信息在传递过程中并不是“此消彼长”，同一信息可以在同一时间被多个主体共有，而且还能够无限的复制、传递。

1.1.2 信息安全的定义

“安全”作为现代汉语的一个基本语词，在各种现代汉语辞书中有着基本相同的解释。《现代汉语词典》对“安全”的解释是“没有危险；不受威胁；不出事故”。当汉语的“安全”一词用来译指英文时，可以与其对应的主要有 safety 和 security 两个单词，虽然这两个单词的含义及用法有所不同，但都可在不同意义上与中文“安全”相对应。在这里，与信息安全相联系的“安全”一词，是 security。按照英文词典解释，security 也有多种含义，其中经常被提到的含义有两方面，一方面是指安全的状态，即免于危险，没有恐惧；另一方面是指对安全的维护，指安全措施和安全机构。没有危险是安全的特有属性，也是本质属性。单是没有外在威胁，并不是安全的特有属性；单是没有内在的疾患，也不是安全的特有属性。但是，包括了没有威胁和没有疾患这样内外两个方面的“没有危险”，则是安全的特有属性了。

那么，信息安全(information security)就是指信息处于“没有危险”的状态，是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。

自从世界上出现了文字之后，各国元首和军队指挥官就逐渐明白，非常有必要使用一些技巧来保证通信的机密性以及获知其是否被篡改。恺撒在公元前 50 年发明了恺撒密码，它被用来防止秘密的消息落入错误的人手中时被读取。第二次世界大战使得信息安全的研究取得了许多进展，并且标志着它开始成为一门专业的学问。20 世纪末以及 21 世纪初，通信、计算机软硬件以及数据加密领域得到巨大发展，小巧、功能强大、价格低廉的计算设备使得小公司和家庭用户能够负担和掌握对电子数据的加工处理，这些计算机进而很快被因特网连接起来。在因特网上快速增长的电子数据处理和电子商务应用，以及不断出现的国际恐怖主义事件，大大增加了对保护计算机及其存储、加工和传输的信息的需求。计算机安全、信息安全以及信息保障等学科，是和许多专业的组织一起出现的。它们都持有共同的目标，即确保信息系统的安全和可靠。

信息安全，简称信安，意为保护信息及信息系统免受未经授权的进入、使用、披露、破坏、修改、检视、记录及销毁。政府、军队、公司、金融机构、医院、私人企业积累了大量的有关它们的雇员、顾客、产品、研究、金融数据的机密信息。绝大多数此类信息现在被收集、产生、存储在电子计算机内，并通过网络传送到别的计算机。万一一家企业的顾客、财政状况、新产品线的机密信息落入了其竞争对手的手中，这种安全性的丧失可能会导致经济上的损失、法律诉讼甚至该企业的破产。保护机密的信息是商业上的需求，并且在许多情况中也是道德和法律上的需求。对于个人来说，信息安全对于其个人隐私具有重大的影响，但这在不同的文化中的看法差异相当大。信息安全的领域在最近这些年经历了巨大的成长和进化，有很多方式进入这一领域，并将之发展为一项事业。它提供了许多专门的研究领域，包括安全的网络和公共基础设施、安全的应用软件和数据库、安全测试、信息系统评估、企业安全规划以及数字取证技术等。

1.1.3 信息安全的基本属性

信息安全具有以下基本属性。

(1)保密性(Confindentialy)：保证未授权者无法享用信息，信息不会被非法泄漏而扩散；

(2)完整性(Integrity)：保证信息的来源、去向、内容真实无误；

(3)可用性(Availability)：保证网络和信息系统随时可用；

(4)可控性(Controllability)：保证信息管理者能对传播的信息及内容实施必要的控制及

管理；

(5)不可否认性(Non-Repudiation)：又称不可抵赖性，保证每个信息参与者对各自的信息行为负责。

其中，前三者又称为信息安全的目标——CIA。对信息安全的认识经历了数据保安阶段(强调保密通信)、网络信息安全时代(强调网络环境)和目前的信息保障时代(强调不能只是被动地保护，需要有保护——检测——反应——恢复四个环节)。

除了上述的信息安全五性外，还有信息安全的可审计性(Audiability)、可鉴别性(Authenticity)等。信息安全的可审计性是指信息系统的行为人不能否认自己的信息处理行为，与具有不可否认性的信息交换过程中行为可认定性相比，可审计性的含义更宽泛一些。信息安全的可鉴别性是指信息的接收者能对信息的发送者的身份进行判定，它也是一个与不可否认性相关的概念。

1.1.4 信息保障

保障信息安全有三个支柱，一个是技术，一个是管理，一个是法律法规。而我们日常提及信息安全时，多是在技术相关的领域，例如入侵检测技术、防火墙技术、防病毒技术、加密技术、认证技术等等，这是因为技术提供商在培育市场。而世界各国信息安全领域的研究，已经从早期的通信保密到信息安全发展到目前的信息保障。

1998 年 5 月 22 日，美国政府颁发了《保护美国关键基础设施》总统令(PDD-63)。围绕“信息保障”成立了多个组织，其中包括全国信息保障委员会、全国信息保障同盟、关键基础设施保障办公室、首席信息官委员会、联邦计算机事件响应能动组等 10 多个全国性机构。1998 年美国国家安全局(NSA)制定了《信息保障技术框架》(IATF)，提出了“深度防御策略”，确定了包括网络与基础设施防御、区域边界防御、计算环境防御和支撑性基础设施的深度防御目标。2000 年 1 月，美国发布了《保卫美国的计算机空间——保护信息系统的国家计划》。该计划分析了美国关键基础设施所面临的威胁，确定了计划的目标和范围，制定出联邦政府关键基础设施保护计划(其中包括民用机构的基础设施保护方案和国防部基础设施保护计划)以及私营部门、州和地方政府的关键基础设施保障框架。

1995 年，俄罗斯颁布了《联邦信息、信息化和信息保护法》，为提供高效益、高质量的信息保障创造条件，明确界定了信息资源开放和保密的范畴，提出了保护信息的法律责任。1997 年，俄罗斯出台的《俄罗斯国家安全构想》明确提出“保障国家安全应把保障经济安全放在第一位”，而“信息安全又是经济安全的重中之重”。2000 年，普京总统批准了《国家信息安全学说》，明确了联邦信息安全建设的目的、任务、原则和主要内容。第一次明确指出了俄罗斯在信息领域的利益是什么，受到的威胁是什么以及为确保信息安全首先要采取的措施等。

党的十五届五中全会提出了大力推进国民经济和社会信息化的战略举措——“以信息化带动工业化，发挥后发优势，实现社会生产力的跨越式发展”。同时，要求强化信息网络安全保障体系。

目前我国信息与网络安全的防护能力处于发展的初级阶段，许多应用系统处于不设防状态。国防科技大学的一项研究表明，目前我国与互联网相连的网络管理中心有 95%都遭到过境内外黑客的攻击或侵入，其中银行和证券机构是攻击重点。

当前我国的信息与网络安全研究，处于忙于封堵现有信息系统的安全漏洞阶段。要彻底解决这些迫在眉睫的问题，归根结底取决于信息安全保障体系的建设。目前，我们迫切需要根据国