高等学校信息安全专业规划教材

信息安全标准与法律法规

主　编　陈忠文　副主编　麦永浩

WUHAN UNIVERSITY PRESS
武汉大学出版社

信息安全标准与法律法规

第二版

主　编　陈忠文　副主编　麦永浩

WUHAN UNIVERSITY PRESS
武汉大学出版社

图书在版编目(CIP)数据

信息安全标准与法律法规/陈忠文主编;麦永浩副主编. —2 版. —武汉:武汉大学出版社,2011. 10

高等学校信息安全专业规划教材

ISBN 978-7-307-09183-2

Ⅰ. 信… Ⅱ. ①陈… ②麦… 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—中国—高等学校—教材

Ⅳ. TP309-65 D922. 17

中国版本图书馆 CIP 数据核字(2011)第 189158 号

责任编辑:林 莉 责任校对:黄添生 版式设计:支 笛

出版发行:**武汉大学出版社** (430072 武昌 珞珈山)

(电子邮件:cbs22@ whu. edu. cn 网址:www. wdp. whu. edu. cn)

印刷:通山金地印务有限公司

开本:787 × 1092 1/16 印张:18. 25 字数:453 千字

版次:2009 年 1 月第 1 版 2011 年 10 月第 2 版

2011 年 10 月第 2 版第 1 次印刷

ISBN 978-7-307-09183-2/TP · 414 定价:33. 00 元

高等学校信息安全专业规划教材
编　委　会

内容提要

本书主要以高等学校信息安全、公安和计算机等专业学生为对象，在介绍信息安全和法律相关基础知识的基础上，结合典型案例，重点分三部分（信息系统安全保护相关法律法规、互联网络安全管理相关法律法规和其他有关信息安全的法律法规），系统讲述了我国信息安全的相关法律法规，同时详细介绍了国际国内与信息安全相关的主要标准。

本书除适合于高等学校信息安全及相关专业的教学外，对从事信息和网络安全方面的管理人员、技术人员和执法人员也有实际的参考价值。

序 言

二十一世纪是信息的时代，信息成为一种重要的战略资源。信息科学成为最活跃的学科领域之一，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。信息的安全保障能力成为一个国家综合国力的重要组成部分。

当前，以 Internet 为代表的计算机网络的迅速发展和“电子政务”、“电子商务”等信息系统的广泛应用，正引起社会和经济的深刻变革，为网络安全和信息安全开拓了新的服务空间。

世界主要工业化国家中每年因利用计算机犯罪所造成的经济损失远远超过普通经济犯罪。内外不法分子互相勾结侵害计算机系统，已成为危害计算机信息安全的普遍性、多发性事件。计算机病毒已对计算机系统的安全构成极大的威胁。社会的信息化导致新的军事革命，信息战、网络战成为新的作战形式。

总之，随着计算机在军事、政治、金融、商业等部门的广泛应用，社会对计算机的依赖越来越大，如果计算机系统的安全受到破坏将导致社会的混乱并造成巨大损失。因此，确保计算机系统的安全已成为世人关注的社会问题和计算机科学的热点研究课题。

信息安全事关国家安全，事关经济发展，必须采取措施确保我国的信息安全。

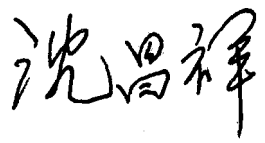
发展信息安全技术与产业，人才是关键。培养信息安全领域的专业人才，成为当务之急。2001 年经教育部批准，武汉大学创建了全国第一个信息安全本科专业。2003 年经国务院学位办批准武汉大学建立信息安全博士点。现在，全国设立信息安全本科专业的高等院校已增加到 70 多所，设立信息安全博士点的高等院校和科研院所也增加了很多。2007 年“教育部高等学校信息安全类专业教学指导委员会”正式成立，并在武汉大学成功地召开了“第一届中国信息安全学科建设与人才培养研讨会”。我国信息安全学科建设与人才培养进入蓬勃发展阶段。

为了增进信息安全领域的学术交流、为信息安全专业的大学生提供一套适用的教材，2003 年武汉大学组织编写了一套《信息安全技术与教材系列丛书》。这套丛书涵盖了信息安全的主要专业领域，既可用做本科生的教材，又可作为工程技术人员的技术参考书。这套丛书出版后得到了广泛的应用，深受广大读者的厚爱，为传播信息安全知识发挥了重要作用。现在，为了能够反映信息安全技术的新进展、更加适合信息安全教学的使用和符合信息安全类专业指导性专业规范的要求，武汉大学对原有丛书进行了升版。

我觉得升版后的这套新教材的特点是内容全面、技术新颖、理论联系实际，努力反映信息安全领域的新成果和新技术，符合信息安全类专业指导性专业规范的要求，适合教学使用。在我国信息安全专业人才培养蓬勃发展的今天，这套新教材的出版是非常及时的和十分有益的。

我代表编委会对图书的作者和广大读者表示感谢。欢迎广大读者提出宝贵意见，以便能够进一步修改完善。

中国工程院院士，武汉大学兼职教授



2008年8月28日

前 言

随着现代信息技术的发展，计算机和计算机网络作为信息收集、存储、加工、检索和传输的工具，得到了日益广泛的应用。但是，当我们在充分享受现代技术给我们的生产、工作、学习和生活带来的方便、快捷、高效的同时，也越来越深切地感受到网络有害信息、计算机病毒以及黑客攻击等带来的无尽烦恼和巨大损失。信息安全问题已日益引起个人、组织、政府乃至国际社会的高度重视。我国政府一方面注重开发各种先进的信息安全技术，另一方面努力加强信息安全立法工作，加大执法力度，同时积极稳步地推进与国际接轨的信息安全标准体系的建立，从而多方面指导人们正确使用计算机信息系统，保障信息的安全。

作为计算机信息系统现在或将来的建设者、使用者或管理者，除了开发和运用先进的信息安全技术外，还应认真学习和充分利用相关法律知识来保护信息的安全，学会依照信息安全标准来建立、实施和改进组织的信息安全管理。编写本书的目的就是要让读者充分了解我国的信息安全法律法规以及国际国内的信息安全标准，以便为未来的信息安全实践更好地服务。

本书包括三个部分共 9 章内容：

第一部分（第 1~3 章）：在介绍信息安全和法律相关基础知识的基础上，通过实例分析了信息安全涉及的法律问题，并介绍了国内外现行的法律体系和信息系统安全的法律规范。

第二部分（第 4~7 章）：分三大块比较全面地介绍了信息系统安全保护相关法律法规、互联网络安全管理相关法律法规和其他有关信息安全的法律法规。

第三部分（第 8~9 章）：比较详细地介绍了我国有关信息安全的标准和著名的信息安全管理国际标准 ISO/IEC 27002。

本书尽量结合现实中发生的具体案例对相关法律法规和标准进行介绍分析，以帮助读者对条文更好地深入理解。本书适合于高等学校相关专业（如信息安全专业、公安类专业和计算机专业等）的教学、培训使用。此外，本书对从事信息和网络安全方面的管理人员、技术人员和执法人员也有实际的参考价值。

为帮助读者更方便地学习，作者建立了本书的教学博客 http：//blog.sina.com.cn/u/1463006444，书中涉及的相关法律法规和标准均可在博客中找到。

由于编者水平有限，书中错漏之处在所难免，敬请读者批评指正。

作 者

2011 年 8 月

目 录

第一部分 总 论

第二部分 信息安全法律法规

第三部分 信息安全标准

第一部分 总 论

第1章 绪 论

1.1 信息安全概述

1.1.1 什么是信息?

ISO/IEC 的 IT 安全管理指南（GMITS，即 ISO/IEC TR 13335）对信息（Information）的解释是：信息是通过在数据上施加某些约定而赋予这些数据的特殊含义。一般意义上的信息概念是指事物运动的状态和方式，是事物的一种属性，在引入必要的约束条件后可以形成特定的概念体系。通常情况下，我们可以把信息理解为消息、信号、数据、情报和知识。

信息本身是无形的，借助于信息媒体以多种形式存在或传播，它可以存储在计算机、磁带、纸张等介质中，也可以记忆在人的大脑里，还可以通过网络、打印机、传真机等方式进行传播。

对于现代企业来说，信息是一种资产，包括计算机和网络中的数据，还包括专利、标准、商业机密、文件、图纸、管理规章等，就像其他重要的商业资产那样，信息资产具有重要的价值，因而需要进行妥善保护。

信息是有生命周期的，从其创建或诞生，到被使用或操作，到存储，再到被传递，直至其生命期结束而被销毁或丢弃，各个环节各个阶段都应该被考虑到，安全保护应该兼顾信息存在的各种状态，不能够有所遗漏。

1.1.2 什么是信息安全?

信息安全是一个广泛而抽象的概念，不同领域不同方面对其概念的阐述都会有所不同。建立在网络基础之上的现代信息系统，其安全定义较为明确，那就是：保护信息系统的硬件、软件及相关数据，使之不因为偶然或者恶意侵犯而遭受破坏、更改及泄露，保证信息系统能够连续、可靠、正常地运行。在商业和经济领域，信息安全主要强调的是削减并控制风险，保持业务操作的连续性，并将风险造成的损失和影响降低到最低程度。

信息作为一种资产，是企业或组织进行正常商务运作和管理不可或缺的资源。从最高层次来讲，信息安全关系到国家的安全；对组织机构来说，信息安全关系到正常运作和持续发展；就个人而言，信息安全是保护个人隐私和财产的必然要求。无论是个人、组织还是国家，保持关键信息资产的安全性都是非常重要的。

信息安全的任务，就是要采取措施（技术手段及有效管理）让这些信息资产免遭威胁，或者将威胁带来的后果降到最低程度，以此维护组织的正常运作。

1.1.3 信息安全的基本属性

不管信息入侵者怀有什么样的企图，采用什么手段，他们都要通过攻击信息的以下几种安全属性来达到目的。所谓“信息安全”，在技术层面上的含义就是保证在客观上杜绝对信息安全属性的安全威胁从而使得信息的主人在主观上对信息的本源性放心。信息安全的基本属性有以下五个。

1. 完整性（integrity）

完整性是指信息在存储或传输过程中保持不被修改、不被破坏、不被插入、不延迟、不乱序和不丢失的特性。对于军用信息来讲，完整性被破坏可能就意味着延误战机、自相残杀或闲置战斗力。破坏信息的完整性是对信息安全发动攻击的最终目的。

2. 可用性（avaliability）

可用性是指信息可被合法用户访问并能按要求顺序使用的特性，即在需要时就可以取用所需的信息。对可用性的攻击就是阻断信息的可用性，例如破坏网络和有关系统的正常运行就属于这种类型的攻击。

3. 保密性（confidentiality）

保密性是指信息不泄露给非授权的个人和实体，或供其使用的特性。军用信息的安全尤其注重信息的保密性（相比较而言，商用信息则更注重于信息的完整性）。

4. 可控性（controllability）

可控性是指授权机构可以随时控制信息的机密性。美国政府所提倡的“密钥托管”、“密钥恢复”等措施就是实现信息安全可控性的例子。

5. 可靠性（reliability）

可靠性是指信息以用户认可的质量连续服务于用户的特性（包括信息的迅速、准确和连续地转移等）。

“信息安全”的内在含义就是指采取一切可能的方法和手段，来千方百计保住信息的上述“五性”的安全。

1.1.4 保障信息安全的三大支柱

保障信息安全无论对一个国家而言还是对一个组织而言都是一个复杂的系统工程，需要多管齐下，综合治理。目前普遍认为，信息安全技术、法律法规和信息安全标准是保障信息安全的三大支柱。

1. 信息安全技术

各种信息安全技术的应用主要在技术层面上为信息安全提供具体的保障。目前主要采用的信息安全技术有：数据加密技术、防火墙技术、网络入侵检测技术、网络安全扫描技术、黑客诱骗技术、病毒诊断与防治技术等。值得一提的是，尽管信息安全技术的应用在一定程度上对信息的安全起了很好的保护作用，但它并不是万能的，由于疏于管理等原因而引起的安全事故仍然不断发生。

2. 信息安全法律法规

国家、地方以及相关部门针对信息安全的需求，制定与信息安全相关的法律法规，从法律层面上来规范人们的行为，使信息安全工作有法可依，使相关违法犯罪能得到处罚，促使