全国信息网络安全专业技术人员继续教育培训教材

QUANGUO XINXI WANGLUO ANQUAN ZHUANYE JISHURENYUAN JIXUJIAOYU PEIXUN JIAOCAI

◎ 主　编　庞　南
◎ 副主编　刘　旸　方　明

XINXI ANQUAN GUANLI JIAOCHENG

信息安全管理教程

中国人民公安大学出版社

全国信息网络安全专业技术人员继续教育培训教材

信息安全管理教程
信息安全技术教程
互联网信息内容安全管理教程
互联网上网服务营业场所安全管理教程

ISBN 978-7-81109-535-7
9 787811 095357 >

责任编辑／王宏勇　王景红
封面设计／金色天平

定价：35.00元

全国信息网络安全专业技术人员继续教育培训教材

信息安全管理教程

主　编　庞　南

副主编　刘　旸　方　明

中国人民公安大学出版社

·北　京·

图书在版编目（CIP）数据

信息安全管理教程/庞南主编. —北京：中国人民公安大学出版社，2007.1

全国信息网络安全专业技术人员继续教育培训教材

ISBN 978-7-81109-535-7

Ⅰ.信… Ⅱ.庞… Ⅲ.信息系统-安全管理-教材 Ⅳ.TP309

中国版本图书馆 CIP 数据核字（2006）第 137594 号

信 息 安 全 管 理 教 程

XINXI ANQUAN GUANLI JIAOCHENG

主　编　庞　南

副主编　刘　旸　方　明

出版发行：中国人民公安大学出版社
地　　址：北京市西城区木樨地南里
邮政编码：100038
经　　销：新华书店
印　　刷：河北省昌黎县第一印刷厂

版　　次：2007 年 1 月第 1 版
印　　次：2007 年 1 月第 1 次
印　　张：14.25
开　　本：787 毫米×1092 毫米　1/16
字　　数：328 千字

ISBN 978-7-81109-535-7/D·505
定　　价：35.00 元

E-mail:cpep@public.bta.net.cn
www.phcppsu.com.cn　　www.jgclub.com.cn
本书咨询电话：(010)63485228　63453145

《全国信息网络安全专业技术人员继续教育培训教材》编辑委员会

编者的话

党的十六届五中全会提出，我国在国民经济和社会发展第十一个五年规划中将全面落实“以信息化带动工业化、大力发展信息产业”的重要战略。目前，我国国民经济和社会信息化进程全面加快，信息技术得到广泛应用，网络与信息系统的基础性、全局性作用进一步增强，成为国家的关键基础设施。随着信息化的发展，信息安全问题日益增加、日渐突出。网络攻击、病毒传播、垃圾邮件等迅速增长，利用网络进行盗窃、诈骗、敲诈勒索、窃密等案件逐年上升，严重影响了网络的正常秩序，严重损害了人民群众的利益；网上色情、暴力等不良和有害信息的传播，严重危害了青少年的身心健康；针对网络和信息系统的破坏活动，以及网络与系统自身的安全问题严重影响着通信、金融、能源、交通等关键基础设施正常运转和安全；境内外敌对势力利用网络与信息技术手段所进行的捣乱、破坏活动，对社会政治稳定造成威胁。信息安全已经上升为事关国家经济安全、社会稳定的全局性战略问题，是国家安全的重要组成部分。必须从促进经济发展、维护社会稳定、保障国家安全、加强精神文明建设的高度，充分认识信息安全保障工作的重要性，增强做好这项工作的紧迫感、责任感和自觉性。

加强信息安全保障工作，必须立足国情，以我为主，坚持管理与技术并重。当前，进一步加强信息网络安全专业技术人员队伍建设，提高信息网络管理和使用单位信息安全管理和技术防范水平，是做好信息网络安全保障工作，维护信息网络安全的一项重要措施。根据公安部、人事部关于在全国开展信息网络安全专业技术人员继续教育工作的统一部署，结合信息网络安全管理和技术人

员工作实际，我们组织编写了《全国信息网络安全专业技术人员继续教育培训教材》。

本教材以邓小平理论和“三个代表”重要思想为指导，紧密结合国家信息安全保障工作相关法律法规和政策文件精神，以提升信息网络安全专业技术人员专业能力和更新专业知识，加快信息网络管理和使用单位信息安全人员队伍建设为目标，从工作实际出发，分为《信息安全管理教程》、《信息安全技术教程》、《互联网信息内容安全管理教程》和《互联网上网服务营业场所安全管理教程》四个分册，并将根据技术的发展和应用领域的新进展，不断修改完善和编制新教材，供从事不同岗位的信息网络安全专业技术人员使用，旨在通过培训学习，使信息网络安全专业技术人员全面掌握本岗位相关的信息网络安全法律法规、政策要求和基本的专业理论知识，掌握相关信息安全制度措施要求和基本技术技能，更好地开展信息安全保障工作。

由于编者水平有限，不足和疏漏之处在所难免，欢迎批评指正。

《全国信息网络安全专业技术人员继续教育培训教材》编写组

2006 年 11 月

目　录

第一章　信息安全概述

第一节　信息与信息安全

20世纪中叶，计算机的出现从根本上改变了人类加工信息的手段，突破了人类大脑及感觉器官加工利用信息的能力。应用电子计算机、通讯卫星、光导纤维组成的现代信息技术革命的成果，使人类进入了飞速发展的信息社会时代，成为人类历史上最重要的一次信息技术革命。目前，一场信息技术革命正在横扫整个社会，无论是产业还是家庭，人类生活的各个领域无不受其影响，它改变了我们的生活方式和商业形态，使各领域相辅相成、互惠互利。

一、信息与信息资产

什么是信息？近代控制论的创始人维纳有一句名言："信息就是信息，不是物质，也不是能量。"这句话听起来有点抽象，但指明了信息与物质和能量具有不同的属性。信息、物质和能量，是人类社会赖以生存和发展的三大要素。

（一）信息的定义

信息的定义，有广义的和狭义的两个层次。从广义上讲，信息是任何一个事物的运动状态以及运动状态形式的变化，它是一种客观存在。例如，日出、月落，花谢、鸟啼以及气温的高低变化、股市的涨跌等，都是信息。它是一种"纯客观"的概念，与人们主观上是否感觉到它的存在没有关系。而狭义的信息的含义却与此不同。狭义的信息，是指信息接受主体所感觉到并能被理解的东西。中国古代有"周幽王烽火戏诸侯"和"梁红玉击鼓战金山"的典故，这里的"烽火"和"击鼓"都代表了能为特定接收者所理解的军情，因而可称为"信息"；相反，至今仍未能破译的一些刻在石崖上的文字和符号，尽管它们是客观存在的，但由于人们（接受者）不能理解，因而从狭义上讲仍算不上是"信息"。同样道理，从这个意义上讲，鸟语是鸟类的信息，而对人类来说却算不上是"信息"。可见，狭义的信息是一个与接受主体有关的概念。

ISO 13335《信息技术安全管理指南》是一部重要的国际标准，其中对信息给出了明确的定义：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。信息是无形的，借助于信息媒体以多种形式存在和传播；同时，信息也是一种重要资产，具有价值，需要保护。

通常的信息资产分类

分　类	示　例
数　据	存在电子媒介的各种数据资料，包括源代码、数据库数据，各种数据资料、系统文档、运行管理规程、计划、报告、用户手册等
软　件	应用软件、系统软件、开发工具和资源库等
硬　件	计算机硬件、路由器、交换机、硬件防火墙、程控交换机、布线、备份存储设备等
服　务	操作系统、WWW、SMTP、POP3、FTP、MRPII、DNS、呼叫中心、内部文件服务、网络连接、网络隔离保护、网络管理、网络安全保障、入侵监控及各种业务生产应用等
文　档	纸质的各种文件、传真、电报、财务报告、发展计划等
设　备	电源、空调、保险柜、文件柜、门禁、消防设施等
人　员	各级雇员和雇主、合同方雇员等
其　他	企业形象、客户关系等

（二）信息的特点

我们更为关注的是狭义信息。就狭义信息而论，它们具有如下共同特征：

（1）信息与接受对象以及要达到的目的有关。例如，一份尘封已久的重要历史文献，在还没有被人发现的时候，它只不过是混迹在废纸堆里的单纯印刷品，而当人们阅读并理解它的价值时，它才成为信息。又如，公元前巴比伦和阿亚利亚等地广泛使用的楔形文字，很长时间里人们都读不懂它，那时候，还不能说它是“信息”。后来，经过许多语言学家的努力，它能被人们理解了，于是，它也就成了信息。

（2）信息的价值与接受信息的对象有关。例如，有关移动电话辐射对人体的影响问题的讨论，对城市居民特别是手机使用者来说是重要信息，而对于生活在偏远农村或从不使用手机的人来说，就可能是没有多大价值的信息。

（3）信息有多种多样的传递手段。例如，人与人之间的信息传递可以用符号、语言、文字或图像等为媒体来进行；而生物体内部的信息可以通过电化学变化，经过神经系统来传递；等等。

（4）信息在使用中不仅不会被消耗掉，还可以加以复制，这就为信息资源的共享创造了条件。

二、信息安全

（一）信息安全的发展

信息安全的发展历经了三个主要阶段：

1. 通信保密阶段

在第一次和第二次世界大战期间，参战军方为了实现作战指令的安全通信，将密码学引入实际应用，各类密码算法和密码机被广泛使用，如 Enigma 密码机，在这个阶段中，关注的是通信内容的保密性属性，保密等同于信息安全。

2. 信息安全阶段

计算机的出现以及网络通信技术的发展，使人类对于信息的认识逐渐深化，对于信息安全的理解也在扩展，人们发现，在原来所关注的保密性属性之外，还有其他方面的属性也应当是信息安全所关注的，这其中最主要的是完整性和可用性属性，由此构成了支撑信息安全体系的三要素。

3. 安全保障阶段

信息安全的保密性、完整性、可用性三个主要属性，大多集中于安全事件的事先预防，属于保护（Protection）的范畴。但人们逐渐认识到安全风险的本质，认识到不存在绝对的安全，事先预防措施不足以保证不会发生安全事件，一旦发生安全事件，那么事发时的处理以及事后的处理，都应当是信息安全要考虑的内容，安全保障的概念随之产生。所谓安全保障，就是在统一安全策略的指导下，安全事件的事先预防（保护），事发处理（检测 Detection 和响应 Reaction），事后恢复（恢复 Restoration）四个主要环节相互配合，构成一个完整的保障体系。

（二）信息安全的定义

ISO 国际标准化组织对于信息安全给出了精确的定义，这个定义的描述是：信息安全是为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露。

ISO 的信息安全定义清楚地回答了我们所关心的信息安全主要问题，它包括三方面含义：

1. 信息安全的保护对象

信息安全的保护对象是信息资产，典型的信息资产包括了计算机硬件、软件和数据。

2. 信息安全的目标

信息安全的目标就是保证信息资产的三个基本安全属性。信息资产被泄露意味着保密性受到影响，被更改意味着完整性受到影响，被破坏意味着可用性受到影响，而保密性、完整性和可用性三个基本属性是信息安全的最终目标。

3. 实现信息安全目标的途径

实现信息安全目标的途径要借助两方面的控制措施，即技术措施和管理措施。从这里就能看出技术和管理并重的基本思想，重技术轻管理，或者重管理轻技术，都是不科学，并且是有局限性的错误观点。

（三）信息安全的基本属性

信息安全包括了保密性、完整性和可用性三个基本属性：

（1）保密性——Confidentiality，确保信息在存储、使用、传输过程中不会泄露给非授权的用户或者实体。

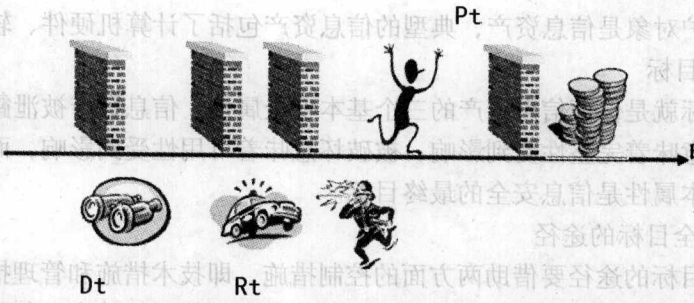
（2）完整性——Integrity，确保信息在存储、使用、传输过程中不被非授权用户篡改；防止授权用户对信息进行不恰当的篡改；保证信息的内外一致性。

（3）可用性——Availability，确保授权用户或者实体对于信息及资源的正常使用不会被异常拒绝，允许其可靠而且及时地访问信息及资源。

（四）信息安全模型

人们一直致力于用确定、简洁的安全模型来描述信息安全，在信息安全领域中有多种安全模型，如 PDR 模型、PPDRR 模型等。

1. PDR 模型



PDR 模型之所以著名，是因为它是第一个从时间关系描述一个信息系统是否安全的模型。PDR 模型中的 P 代表保护、D 代表检测、R 代表响应，该模型中使用了三个时间参数：

（1）Pt，有效保护时间，是指信息系统的安全控制措施所能有效发挥保护作用的时间。

（2）Dt，检测时间，是指安全检测机制能够有效发现攻击、破坏行为所需的时间。

（3）Rt，响应时间，是指安全响应机制作出反应和处理所需的时间。

PDR 模型用下列时间关系表达式来说明信息系统是否安全：

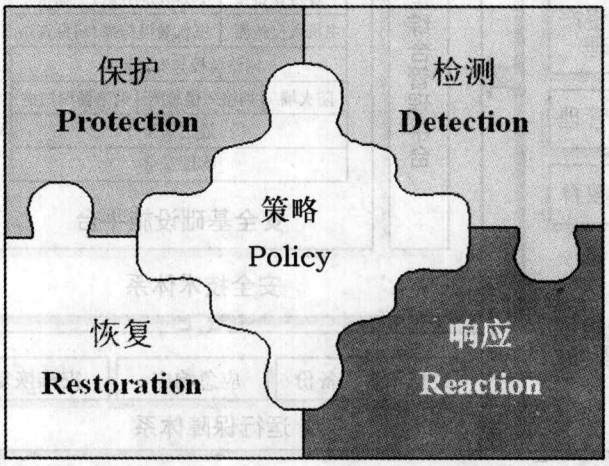
（1）Pt > Dt + Rt，系统安全，即在安全机制针对攻击、破坏行为作出了成功的检测和响应时，安全控制措施依然在发挥有效的保护作用，攻击和破坏行为未给信息系统造成损失。

（2）Pt < Dt + Rt，系统不安全，即信息系统的安全控制措施的有效保护作用，在正确的

检测和响应作出之前就已经失效，破坏和攻击行为已经给信息系统造成了实质性破坏和影响。

2. PPDRR 模型

正如信息安全保障所描述的，一个完整的信息安全保障体系，应当包括安全策略（Policy）、保护（Protection）、检测（Detection）、响应（Reaction）、恢复（Restoration）五个主要环节，这就是 PPDRR 模型的内容。



保护、检测、响应和恢复四个环节要在策略的统一指导下构成相互作用的有机整体。PPDRR 模型从体系结构上给出了信息安全的基本模型。

（五）信息安全保障体系

要想真正为信息系统提供有效的安全保护，必须系统地进行安全保障体系的建设，避免孤立、零散地建立一些控制措施，而是要使之构成一个有机的整体。在这个体系中，包括了安全技术、安全管理、人员组织、教育培训、资金投入等关键因素。信息安全建设的内容多、规模大，必须进行全面的统筹规划，明确信息安全建设的工作内容、技术标准、组织机构、管理规范、人员岗位配备、实施步骤、资金投入，才能够保证信息安全建设有序可控地进行，才能够使信息安全体系发挥最优的保障效果。

信息安全保障体系由一组相互关联、相互作用、相互弥补、相互推动、相互依赖、不可分割的信息安全保障要素组成。一个系统的、完整的、有机的信息安全保障体系的作用力远远大于各个信息安全保障要素的保障能力之和。在此框架中，以安全策略为指导，融汇了安全技术、安全组织与管理和运行保障三个层次的安全体系，达到系统可用性、可控性、抗攻击性、完整性、保密性的安全目标。信息安全保障体系的总体结构如下图所示：