军队“2110工程”建设项目 信息安全技术

信息安全保密技术

XINXI ANQUAN BAOMI JISHU

王宇 阎慧 编著

国防工业出版社
National Defense Industry Press

军队“2110 工程”建设项目　信息安全技术

信息安全保密技术

王 宇　阎 慧　编著

国防工业出版社
·北京·

内 容 简 介

本书诠释了信息安全保密的概念，构建了信息安全保密体系，从物理、平台、数据、通信、网络等层面全面、系统地介绍了信息安全保密的各项技术，给出了开展信息安全保密检查、保密工程和安全风险管理的规范和方法，以及典型的信息安全保密实施方案，具有较强的针对性和可操作性。

本书可作为高等院校信息安全及相关专业研究生和高年级本科生的教材，也可作为从事信息安全保密工作管理和技术人员的参考书。

图书在版编目(CIP)数据

信息安全保密技术／王宇，阎慧编著. —北京：国防工业出版社，2012.11 重印

军队“2110 工程”建设项目. 信息安全技术

ISBN 978-7-118-06777-4

Ⅰ. ①信… Ⅱ. ①王… ②阎… Ⅲ. ①信息系统－安全技术 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字(2010)第 036330 号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路 23 号 邮政编码 100048)

北京嘉恒彩色印刷有限责任公司

新华书店经售

*

开本 710×960 1/16 **印张** 13 **字数** 223 千字

2012 年 11 月第 1 版第 2 次印刷 **印数** 3001—6000 册 **定价** 28.00 元

(本书如有印装错误，我社负责调换)

国防书店：(010)88540777 发行邮购：(010)88540776

发行传真：(010)88540755 发行业务：(010)88540717

装备指挥技术学院“2110 工程”教材(著作)

编审委员会

装备指挥技术学院信息安全技术教材(著作)

编 委 会

序

计算机技术、通信技术、网络技术的发展，给军队指挥自动化系统、综合电子信息系统的建设与发展带来了深刻的影响。未来以电子战、网络战和作战保密等为主要作战样式的信息化战争，离不开信息技术的支撑。武器装备的信息化、网络化加快了信息技术在装备的研制、试验、采购、指挥、管理、保障和使用全过程中的渗透与应用。因此，在军队深入开展军事信息技术学科的建设，加强军事人才信息化素质与能力的培养，是继往开来的一件大事，也是对军事装备学、作战指挥学等学科建设的有力支持。

为了总结梳理装备指挥技术学院军事信息技术学科的建设成果，提升学科建设水平和装备人才培养质量，在军队“2110 工程”专项经费支持下，在装备指挥技术学院“2110 工程”教材（著作）编审委员会统一组织指导下，军事信息技术学科领域的专家学者编著了一批适应装备人才培养需求，对我军装备信息化和装备信息安全工作具有主要指导作用的系列丛书。

编辑这套丛书是我院军事信息技术学科建设的重要内容，也是体现军事信息技术学科建设水平的重要标志。通过系统、全面地梳理，将军队开展信息化建设的实践经验进一步理论化、科学化，形成具有军事装备特色的军事信息技术知识体系。

本套丛书定位准确、内容创新、结构合理、针对性强，一方面总结了我院军事信息技术学科建设和装备信息化人才培养的理论研究与实践探索的重要成果和宝贵经验；另一方面紧紧围绕我军武器装备信息化建设的需要，以装备全寿命管理的信息化和装备信息保障为主要内容，着重基本概念、原理的论述和技术方法的应用，其编著出版对于推进军事信息技术学科的建设，提高装备人才的培养质量，加快装备信息化建设和军事斗争准备具有十分重要的现实意义和深远的历史意义。

装备指挥技术学院
信息安全技术教材（著作）编委会
2009 年 12 月

前　言

当代信息技术具有以下突出特点

(1) 融合性。人与社会的融合(渗透),即当代信息技术把数据、文字、声音、图像等多种形式的信息从产生、传递、处理到使用都融合起来,把人和社会组织的各种行为、关系、过程融合起来,以实现信息的网络化、数字化进程,同时也是网络信息技术全面社会化的进程。网络已经深入社会各个角落。

(2) 开放性。信息技术的网络化、数字化发展,把人和社会组织的行为领域、工具领域和时空领域极其广泛地联系起来,并扩展开来,形成了一种独特的时空效应,任何一台信息终端或个人,既存在于一个特定的时间和空间,同时又关联着和表现出与全球任何一个时空点的关系。信息无处不在,开放已成必然。

(3) 结构性和工程化。信息技术不是以离散的个别工具形态的方式存在着,而是以结构化和工程化的方式存在着,并在过程中发挥全面作用。社会信息化标志着信息技术已经深入到社会各项工程中。因此,要从体系的角度认识信息技术。

(4) 非直观性。信息技术的核心本质是“比特”,是数字化数据,是看不见、摸不着的“存在”。最典型的例证就是网络犯罪取证,任何芯片、硬盘和软盘上的数据,从技术和法理上很难与某个“犯罪主体”的“犯罪事实”直接建立“证据”关系,因此信息技术难以把握与评价。为了适应信息技术的特点,要以创新的精神和跨越方式解决信息安全保密问题。

传统的信息安全模式有两层含义:

(1) 基于工具和工具可信的含义。即解决信息安全保密,主要依靠可信的具体工具(如安全的计算机、网络或系统)。事实上,信息技术的特点决定了不存在完全可信的计算机和完全可信的网络,而来自

于人、计算机等信息系统的弱点始终存在着。任何单独的安全保密工具，如果不是用于支撑和构建一个完整的信息安全保密平台，其安全功能就与实际的保密需求“无关”。因此，要从体系上搭建信息安全保密的管理和技术平台。

(2) 静止的含义。信息安全保密本身和解决信息安全保密问题都是一个过程。这个过程既包括了安全利益关系和目标的变动不定，也包括了安全威胁与保护的技术手段的此消彼涨，还包括“技术工程平台”的结构变化，以及人和社会组织关于安全保密的行为规则的不断调整。这是一个复杂系统的控制论过程，也是一个不断反馈从而不断优化安全保密能力的过程。

无论从社会还是从技术上，无论从目的还是从手段上，都没有一成不变的安全、一劳永逸的安全和一蹴而就的安全。必须对信息安全保密实施风险管理，同时运用控制论的思想来加强安全控制。

解决信息安全保密的问题，无论是核心秘密还是非核心秘密的保密，无论是宏观决策还是微观管理，都必须基于信息技术的特点，实施“工程化”的可靠管理和“过程”的反馈控制。具体表现在：①建立信息安全保密体系框架；②对信息安全保密实施风险管理；③增强对信息系统的安全控制。

本书从体系的角度探讨了信息安全保密的各项技术，介绍了如何实施信息安全保密工程，开展信息安全风险管理，全面、系统地归纳总结当代信息技术条件下加强保密管理的理论和技术方法。本书共分11章，第1章、第2章、第10章、第11章由王宇编写，第3章、第4章由江健编写，第5章由韩伟杰编写，第6章由吴忠望编写，第7章由阎慧编写，第8章由咎彧弘、李宇明编写，第9章由姚宏林编写。王宇、阎慧负责全书审定。书中参考借鉴了大量的资料和最新研究成果，在此对原作者表示衷心的感谢。书中存在错误和不当之处，望广大读者批评指正，以便进一步修订完善。

编　者

目 录

第1章　信息安全保密概述

随着高科技的迅猛发展，国际互联网的广泛应用，人们已进入信息时代，无意识泄密、间接泄密、计算机网络泄密等现象时有发生。信息安全保密属于国家和军队保密工作的重要内容。在现代化的军队中，信息安全保密是提升军队威慑和实战能力的重要保证。在信息战时代，信息安全保密能力就是战斗力。

信息安全是历史上“保密”与“破译”的扩展，一直存在于信息技术的发展历程之中。通信的“保密”与“破译”已有几千年的历史了，但直至1949年Shannon发表《保密系统的信息理论》才把其纳入科学轨道。随着信息技术的发展与应用，信息安全的内涵在不断地延伸。从最初的信息保密性发展到信息的完整性、可用性、可控性和不可否认性，进而又发展为“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等涉及多方面的基础理论和实施技术。信息安全主要包括物理安全、网络安全、数据安全、信息内容安全、信息基础设施安全与公共、国家信息安全，是一个多层次、多因素、多目标的复合系统。重视信息安全已成为各国政府和社会普遍关注的焦点而研究信息安全面临的安全政策、安全技术、安全管理、安全产业、信息安全基础设施和信息安全的有效评估等问题，则是摆在我们面前的重要任务。

1.1　基本概念

信息是事物运动的状态和状态变化的方式，是与能量、物质一起构成物质世界的三大组成要素。

信息安全（INFOSEC），指保护信息及信息系统在信息存储、处理、传输过程中不被非法访问或修改，而且对合法用户不发生拒绝服务的相关理论、技术和规范。

信息安全的概念涵盖了信息、信息载体、信息环境和接触信息的人四个方面的安全。信息指信息自身，信息载体指信息的承载体，包括物理平台、系统平台、通信平台、网络平台和应用平台等。信息环境指信息及信息载体所处的环境，包括硬环境和软环境。接触信息的人包括信息、信息载体和信息环境的管理人员和使用人员。信息、信息载体、信息环境和接触信息的人是信息安全的四大保护对象，其相互关系如图1.1所示。

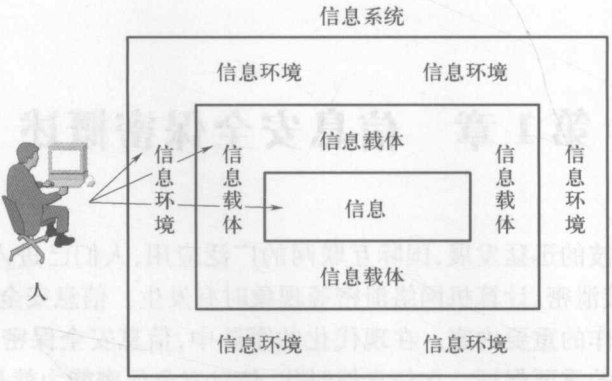

图 1.1　信息安全的保护对象及其定位关系

随着 RFID 等识别技术、传感技术和短距离无线等技术的发展和普及，配备无线通信功能的传感器和控制芯片将附着在任何物体乃至动物、植物上。人们可以在任意时间、任意地点使用任意工具，与任何客户端（包括人、手机、电脑、电视、冰箱、电子音响及任何设备或物品）实现无线连接并交换信息，人类将迈进网络和应用无所不在的“泛网时代”。信息安全保护对象的主要内容如表 1.1 所列。

表 1.1　信息安全保护对象的分类和示例

大类	子 类	示　例
信息		文字、图形、图片、音频、视频、动画、装备外形等形式
信息载体	物理平台	计算芯片（CPU、控制芯片、专用处理芯片等）、存储介质（磁盘、光盘、U 盘、移动存储设备、磁带等）、通信介质（双绞线、光纤、微波、电缆、红外线、卫星、交换设备等）、人机界面（终端、打印机、复印机、扫描仪、数字摄像机等）等硬件
	系统平台	操作系统、数据库系统等系统软件
	通信平台	通信协议及软件
	网络平台	网络协议及软件
	应用平台	应用协议及软件
信息环境	硬环境	机房、电力、照明、温控、湿控、防盗、防火、防震、防水、防雷、防电磁辐射、防电磁干扰等设施
	软环境	国家及军队法律、行政法规、部门规章、经济政治、社会文化、思想意识、教育培训、人员素质、组织机构、监督管理、安全认证等方面
接触信息的人		信息系统管理人员、信息使用及维护人员

信息安全保密是指为防止信息泄密、窃密和破坏，对涉密载体、涉密信息系统及其所存储的信息和数据、相关的环境与场所，以及安全保密产品的安全保护，以抵御技术窃密与破坏，保护秘密信息与信息系统的安全。

因此，加强信息安全保密，必须把握信息的本质，做好信息安全。

1.2 内涵诠释

1.2.1 信息的基本性质

信息的基本性质如下：

(1) 信息来源于物质，又不是物质本身，信息不等于物质。

(2) 信息来源于精神世界。

(3) 由于信息可以脱离源物质而载荷于媒体物质，可以被无限制地复制和传播，因此信息可为众多用户共享。

(4) 信息可被观察者感知、检测、提取、存储、传递、识别、显示、分析、处理、应用和共享，它是决策的依据、控制的基础和管理的保证。

(5) 在开放的系统中，信息的价值并不恒定。

(6) 获取的信息量越多，人们对客观事物的认识的不确定程度、未知程度、怀疑程度和模糊程度就会减少。

针对第(1)、(2)点，说明涉密信息不一定是实物，如文件、图片、声音、视频等，也有可能是对事物的主观认识产物，即位于人的脑海中，或直接来源于人的构思及想象。

针对第(3)点，说明信息具有流动性、可复制性、任意传播性。因此，对涉密信息及其接触涉密信息的人进行保密管理，就显得十分困难和复杂，以往的纸质涉密载体的保密管理方法是否还能满足对涉密信息的跟踪管理值得我们重新审视。

针对第(4)点，说明对信息的保密必须贯彻到信息的整个生命周期中，即从信息刚刚产生开始，就要采取有效的技术或管理措施加以保护，控制知悉范围，加强审计跟踪。

针对第(5)、(6)点，说明信息是具有价值的。信息的价值差体现在窃密与保密双方对关键信息的掌握程度。从某种角度上看，现代信息化战争打的就是信息保密战，如何保住己方的核心秘密，如何获取敌方的核心秘密，就是决定战争胜负的关键。因此，信息保密十分重要。

所以，信息具有不确定性、流动性。由于信息本身的特性，特别是信息及网