“九五”军队级重点教材

信息网络安全

张红旗摇等 编著

清 华 大 学 出 版 社

(京)新登字 员缘愿号

内 容 简 介

本书是中国人民解放军信息工程大学组织编写的“九五”军队级重点教材，全书由四个部分组成。第员~缘章为第一部分，从信息的价值特点入手，重点研究信息网络安全的基本内涵、安全需求与策略、基本技术、基础设施和安全服务体系问题。第远~愿章为第二部分，主要研究信息网络系统的安全理论与技术，包括安全协议、防火墙与 灾害技术、入侵检测技术等。怨~员远章为第三部分，研究信息网络的安全工程理论和建设，包括安全工程模型与系统建设、安全操作系统、信息网络安全管理与测评认证等。最后一部分第员愿章介绍了几种常用的安全工具软件。

本书可供国内各高校信息安全等专业的本科生、研究生使用，对从事信息安全研究工作的科技人员和关心信息安全领域的其他同志也可提供参考和帮助。

图书在版编目(悦孕)数据

信息网络安全 辕张红旗等编著 郾—北京 清华大学出版社，圆园园圆

陨杂月晕 苑原猿园圆原园缘猿缘远原愿

Ⅰ郾信…摇Ⅱ郾张…摇Ⅲ郾计算机网络—安全技术摇Ⅳ郾栽孕猿怨猿郾园愿

中国版本图书馆 悦陨孕数据核字(圆园园圆)第 园愿缘远远远号

出 版 者：清华大学出版社(北京清华大学学研大厦，邮编：员园园园愿源)
澡贼贼责:辕辕votw.tup.tsinghua.edu.cn
责任编辑：丁摇岭
印 刷 者：清华大学印刷厂
发 行 者：新华书店总店北京发行所
开摇摇本：苑愿苑伊员园怨圆摇员辕员远摇印张：员远摇字数：猿缘缘千字
版摇摇次：圆园园圆年 员员月第 员版摇圆园园圆年 员员月第 员次印刷
书摇摇号：陨杂月晕 苑原猿园圆原园缘猿缘远原愿辕栽孕·猿缘远远
印摇摇数：园园园员~源园园园
定摇摇价：圆愿郾园园元

序

随着全球信息化的飞速发展，我国建设的各种信息化系统已成为国家关键基础设施，人们在享受网络带来的巨大便利的同时，网络信息安全问题也越来越突出地摆在我们面前。信息安全保障能力是 圆员世纪综合国力、经济竞争实力和生存能力的重要组成部分，是世界各国奋力攀登的至高点。信息安全问题如果解决不好将全方位危急我国的政治、军事、经济、文化和社会生活的方方面面，使国家处于信息战和高度经济金融风险之中。

自主构建网络信息安全防御体系不仅需要先进的技术和设备，还需要严格的管理和完善的法律，特别是需要培养和造就一大批掌握先进理论和技术的高层次信息安全人才。值得高兴的是国内许多院校已意识到信息安全人才培养的重要性和紧迫性，在信息工程、计算机科学与技术等专业开设了有关网络安全的课程。然而却很难找到合适的教材，特别是公开出版的全面反映信息网络安全的专著几乎没有。本书就是在这一背景下，为了适应教学需要，结合长期从事信息安全方面的理论教学与科研工作，参考了国内外有关著作和文献编写而成的。

本书与其他信息安全的书籍不同，没有侧重密码理论与技术，尽管它是信息安全的核心技术，因为这方面的专著很多，而是把重点放在信息网络安全体系上。本书从信息的价值特点入手，研究了信息网络安全的基本内涵、安全需求、安全策略、基本技术、基础设施和安全服务体系问题；全面论述了网络安全协议、防火墙与 灾备技术、入侵检测技术等信息网络系统的安全理论与技术；结合实例介绍了信息网络的安全工程理论和建设的有关问题，包括安全工程模型与系统建设、安全操作系统、信息网络安全管理与测评认证等；最后，介绍了几个常用的安全工具软件。本书力求紧跟国内外网络安全技术前沿，全面、系统地反映信息网络安全的理论与实践。

本书被列为“九五”军队级重点教材，由解放军信息工程大学电子技术学院组织编写，张红旗担任主编。第 员 圆 猿 源章由张红旗编写，第 缘 远 苑 愿章由王昌胜编写，第 怨 员园 员员章由王鲁编写，张红旗负责统稿。在本书的策划和编写过程中，国内著名的信息安全专家、中国工程院院士沈昌祥同志给予了热情鼓励和指导，并担任本书的主审，电子技术学院副院长王亚弟教授、信息安全系陈性元博士、训练部赵春明副教授给予了具体的帮助，刘育楠、车天伟、丁浩、李晓飞、王娜、杨杨等同志为本书的出版做了大量的工作，在此一并表示衷心的感谢。

由于水平和时间有限，本书一定存在不少不足之处，希望得到读者的批评指正，以便进一步完善和提高。

编 者

圆园园员年 远月

于郑州解放军信息工程大学

目摇摇录

摇摇员苑园园摇员苑园园摇员苑园园摇

第 员章摇信息网络安全概述

员援员摇信息与信息网安全

员援员援员摇信息的价值特点与信息安全

世上没有无缘无故的爱，也没有无缘无故的恨，这句至理名言能够表达社会化的人与数字化的信息之间的关系。一切信息的“争”与“战”皆缘于人们对信息的“爱”与“恨”。

随着全球信息化的飞速发展，各种信息化系统已成为国家基础设施，它们支持着电子政务、电子商务、电子金融、电力、能源、通信、交通、科学研究、网络教育、网络医疗保健和社会保障等方方面面。信息成为人类个体或群体必须的重要资源。这种争战的目标，借用军事术语，可以概括为“制信息权”，而不只是简单地获得信息本身。

摇摇员援员援员摇信息特性与“制信息权”

信息作为一种人类社会的资源，其价值的特性不同于物质、资金和能源等资源。它具有自身的特殊性。信息价值不仅取决于信息的本身或内容，通常还取决于：

信息可靠性，即信息的来源可靠或可以信赖，排除混乱或伪造的；

信息时间性，即信息仍然是有效或有意义的，排除失效或过时的；

信息准确性，即信息内容是准确无误的，排除错误的或被篡改的；

信息传播性，即知道信息的人员范围，排除泄漏或失盗。

信息之所以是“信息”，根本在于它具有传播性的需求。没有信息的传播便没有信息存在的意义。同时，传播性导致信息的价值保值的特殊性。信息传播性对信息价值的影响存在三种状况，一种是传播范围越广越好，一种是越少越好、还有第三种是不多不少正好。

如果将获得信息本身定义为信息的可用性或可获得性，那么，制信息权就是能够获得信息，并能保障信息的可靠性、时间性、准确性和传播性要求。当一种信息会导致不同人类群体的利益冲突时，就会引起对信息的争战。这时的“制信息权”就是能够在第一时间获得可靠的、准确的信息，并能持续保障该信息的准确性与传播性。

摇摇员援员援圆摇制信息权与信息战

战争通常是民族或国家之间的对抗。从这种意义上，当国家或民族间发生制信息权的对抗时，就是信息战。它与参战的人力物力等规模因素关系不大。参战方都力图保护和扩大自己的制信息权，攻击和剥夺对方的制信息权。一个国家或民族面临信息战的威胁与该国的信息化程度密切相关。当一个国家建立了信息化的政治、经济和军事基础设施时，就步入了信息化社会。信息战就会直接导致信息化国家的政治、经济或军事上的损失，甚至

崩溃。

信息战是争夺信息的激烈形式，具有防御和进攻的双重性。只要有对抗存在，维护和扩大自己的制信息权就决非易事。拥有制信息权就必须能够在对抗环境中及时甚至第一时间获得信息、能够甄别信息的真伪、确保信息的准确无误传播并能够严格控制传播范围。

摇摇獲信息安全

对于信息的制权人，他必须能够持续地维护所控制的信息，保障信息的可用性、可靠性、准确性、时效性和传播性，防止信息受到无意的或人为的泄漏和破坏。这种对已控制信息的维护就是信息的安全管理。安全通常是相对受到威胁而言的。信息安全就是受控制的信息仍然是可靠的而非伪造的，准确的而非遭破坏或篡改的，有效的和可用的而非延误的或难以提取的，有传播范围限制时是被严格控制的或保密的，而非已经泄漏或失盗的。所以概括起来，人们将信息安全定义为：

持续地维护信息的保密性、完整性和可用性。

完整性包括了信息的可靠性和准确性，可用性包括了信息的可获得性和时间性，而保密性是对信息传播范围的控制。

如果说信息战是制信息权的对抗，必须具备防御和进攻的双重战略部署，那么，信息安全就是信息战的防御部署的核心。它保障已经获得的制信息权的运用和巩固。

员园园摇信息系统与信息安全

摇摇员信息系统

信息总是依托信息系统存在，表现为信息系统所存储、处理和交换的数据单元。完整的信息系统包括：

- 摇信息采集系统
- 摇信息存储系统
- 摇信息交换系统
- 摇信息处理系统
- 摇信息应用系统

信息采集系统对信息可靠性和准确性负直接的责任，对信息传播性负最初的责任。信息存储系统、信息交换系统、信息处理系统和信息应用系统对信息数据正确性和传播性负有责任。这里的信息数据正确性就是对信息的可靠性和准确性负责。信息时间性却不是信息系统本身能独立决定的。对信息系统来说，能做的就是及时地提供应用所需的信息数据，即保障信息可获得性。因而，信息安全问题成为信息系统的“信息数据”的安全。在信息系统中，信息安全就是保障系统中数据的完整性、保密性和可用性。

摇摇圆信息系统中安全的对抗性

信息系统是信息存在的空间，自然就是信息争战的场所。不同利益的人们在此展开对系统中信息数据控制权的较量，形成信息系统的控制方和系统的攻击方。从信息系统控制方的角度，进行的是保卫战，维护所控制信息的安全。从系统攻击方看，进行的是攻坚

战，力图夺得系统中信息、控制系统中信息，必要时，破坏系统中信息和系统，甚至使系统倒戈。从这种对抗性可以得出，信息系统中信息安全就是系统控制方总是能够抵御对系统的攻击。因而真正做到安全就必须知己知彼。图 员援员简明地表达了信息系统中信息安全的对抗性。

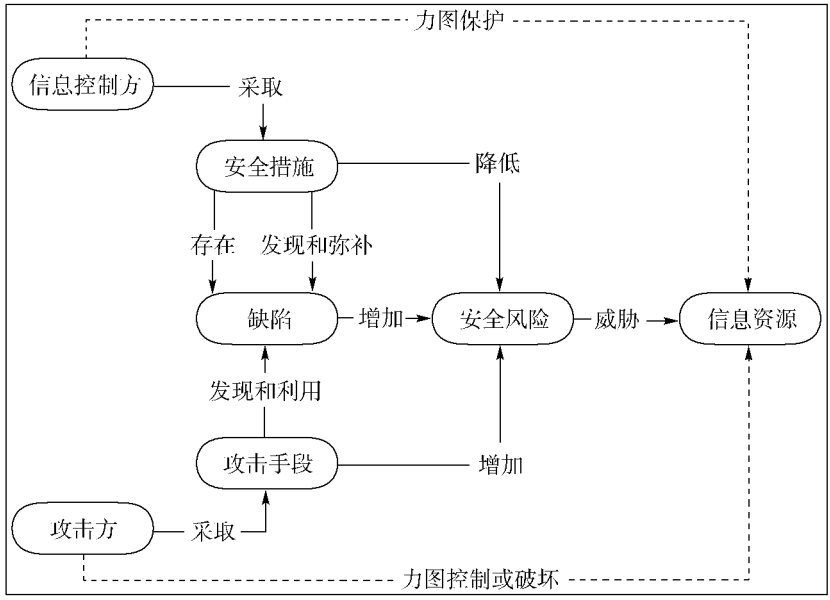

图 员援员摇信息对抗性模型

信息攻击的惟一着手点就是信息系统。攻击方可以利用信息系统的一切可以利用的资源和缺陷发动攻击，形成对信息系统的威胁。信息系统控制方在系统中采取安全措施，阻止攻击，保护信息，即建立信息系统的抗攻击和破坏的体系。安全的复杂性在于，攻击方的攻击手段是不断变化或发展的，而系统的安全措施难以做到绝对可靠或牢不可破。

因而总体上看，信息系统的安全是相对的，不是绝对的。这种相对性就是安全措施、攻击手段和安全缺陷的作用力对比。这种对比的结果就是信息系统中信息的安全风险。如果信息系统能够将信息的安全风险降到信息控制者可以接受的程度，该信息在这个系统中就是安全的，即信息的完整性、保密性和可用性维护失败的风险是信息制权人可以接受的。

员援圆摇信息网络与信息安全

现代信息系统是以计算机为信息管理主要设施、计算机网络为主要体系结构。信息战就是以计算机网络为战场，计算机技术为核心武器。保护自己计算机网络中的信息安全就是维护自己的制信息权。

员援圆援员摇信息网络

信息网络是现代信息系统主要的和重要的组成部分。本书所说的信息网络就是信息系

统中计算机网络部分。它也可能是一个信息系统的全部。信息网络就是提供网络化信息服务，其功能按照信息生命阶段划分，可以分为：

- 摇信息存储
- 摇信息交换
- 摇信息处理
- 摇存储与处理之间的调度
- 摇处理与交换之间的调度

这里的两种调度就是信息存取控制和信息交换控制。对应的网络设施就是：

- 摇信息交换系统
- 摇信息处理系统
- 摇存取控制系统
- 摇交换控制系统

信息网络的功能是通过网络组织实现的。从逻辑上，这些组织构成网络结构体系，即，网络为实现信息服务所采取的系统结构。现代网络体系结构基本上遵循了层次性原则，大体上可以分为图 员猿圆所示的层次：

网络应用系统
网络服务系统
网络通信系统
网络主机系统

图 员猿圆摇信息网络逻辑体系

摇摇在网络逻辑体系中，信息在不同层次上呈现不同的实体，或者说不同层次系统所识别和接受的信息单元不同。

- 摇应用信息单元
- 摇服务信息单元
- 摇通信信息单元
- 摇主机信息单元

摇摇圆摇信息网络中的信息安全

信息网络存在的意义在于它所承载的信息。信息的安全就是信息网络安全的全部意义。可以说，信息网络安全就是保障网络中信息的完整性、保密性和可用性。

(员) 网络中信息的完整性保障

信息完整性包括信息可靠性和准确性。信息网络作为用户信息的大载体，就现代网络技术而言，它并不能对接收的信息提供可靠性担保。这种可靠性担保只能由用户提供。网络能做到的是：把接收的信息与提供该信息的用户联系起来。所以，信息网络中信息的可靠性保障就转为信息与信息源的对应关系的保证或证明。

信息网络中信息的准确性保障主要取决于网络系统的软硬件的可靠性和抗攻击能力。从一般的安全概念出发，信息的准确性保障首先是防止人为地对信息数据的损坏或篡改。

当不能阻止对网络信息的篡改或损坏时，应该能够识别出被损坏或篡改的信息数据，并能恢复数据的原貌。

(圆) 网络中信息可用性保障

信息的可用性包括信息的可获得性和获得的时间性。无论是网络用户信息的可获得性，还是信息的时间性，都涉及信息网络系统的信息提取和传输的效率和可靠性。信息网络系统必须做到信息在用户或信息本身要求的时间内递交到应用系统或用户。这种保障首先由网络系统的配置能力和管理能力提供。从安全角度，这种保障就是维护或强化网络系统配置，保障网络服务的能力不受人为的破坏，阻止对网络资源的滥用。

(猿) 网络中信息的保密性保障

信息的保密性是信息传播性的重要方面。信息网络的服务本质是提供信息共享。信息的传播性对网络提出的要求可以是两方面的，一是保密方面的，一是共享方面的。共享要求网络系统的信息传播能力，是对网络中信息共享的功能和质量的要求，不是安全所关心的问题。保密则是要求网络系统控制对信息的直接或间接的提取。直接的提取就是通过访问信息载体获得信息内容，间接就是采用其他方式获得信息，如通过相关信息推测出不能直接获得的信息。

摇摇猿摇信息网络安全

信息网络中的信息安全是信息网络安全的核心。信息网络运转的目标就是提供信息服务。维护网络服务的安全性就是持续地、全程地维护网络中的信息安全。网络服务的安全需求就是信息网络的安全需求。网络信息服务的安全需求可以概括为：可靠性、保密性、完整性、抗抵赖性等，如图 员-猿所示。

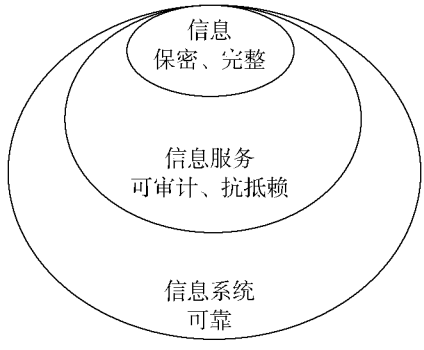

图 员-猿摇信息网络安全内涵

(员) 服务系统可靠性

网络服务可靠性是网络信息系统能够在规定条件下和规定的时间内完成规定的信息服务，从而实现信息的可用性。服务可靠性是信息网络安全的最基本要求之一，它要求网络系统具备抗攻击能力和系统恢复能力。网络服务的可靠性是建立在网络硬件、软件、人员、环境等可靠性的基础上的。

(圆) 可审计性和抗抵赖性

可审计性就是建立网络服务过程的记录，明确网络安全事件责任。

抗抵赖性也称作不可否认性，它是网络服务中特殊的安全需求。信息网络必须能够确认和保留服务信息的“源”和“宿”的证据。在必要时，可以通过它证明信息服务涉及的各方的身份和服务的过程。

(猿) 信息保密和完整性

首先，信息网络必须能够控制信息服务的对象和信息源，保障信息的保密性和完整性。

其次，信息网络必须在网络服务的全程维护信息的保密性和完整性。

员圆遥 网络安全系统

信息网络安全就是发生在信息网络上的信息保护战。在这样一个争夺战中，没有高瞻远瞩的战略和严密有效的战术就没有胜利的前提。

员圆遥员 安全战略思想

员圆遥员员 信息安全特点

信息网络安全的战略部署就是信息网络的安全泛策略。这种泛策略就是普遍适用的网络安全对策。它是建立在对信息网络安全特性的认识上的。既然信息安全是一场防御战，其战略部署就是以信息网络的安全防御为原则。基于 员圆遥员节信息安全的对抗性概念，信息安全必须建立持续的、发展的战略部署，即信息网络安全的防御体系必须建立在持续有效、适应发展的原则上。将网络安全建立在固定的防御体系上，无异于将安全建立在“马其诺防线”上。

员圆遥员圆 基于信息对抗性的安全战略

信息是否安全取决于信息系统的安全措施与攻击手段的力量对比。信息网络必须能够建立全面的安全风险判断和对策体系，在知己知彼的基础上建立严密的防御体系，并配备完善的对敌侦察和监视体系、对防御系统的加固和紧急恢复的快速反应体系。这就是所谓的基于信息安全对抗性的安全泛策略。简要地说，这种信息网络安全的战略思想就是要建立信息网络的安全策略、防御体系、监察体系和反应体系。这种安全泛策略通常表述为 孕阅陨模型，见图 员圆遥员

孕阅陨是这种模型 源个要素的英文缩写，即 孕燥造蚤糟赠(策略)、孕则燥贼藻糟贼(防御)、阅藻贼藻糟贼(监察) 和 砸藻泽责燥灶泽藻(反应)。防护、监察和反应组成了一个完整的、动态的安全循环，在安全策略的指导下保证信息网络的安全风险降到最低。

安全策略就是对具体信息系统安全性的定义。如在一个系统中，信息保密性的具体定义、信息完整性定义、信息服务安全定义、系统可靠性定义等等。通常这些定义形成文本，成为系统安全规范文件。当一个系统满足了安全策略，或者说实现了安全策略，这个系统就是安全的系统；反之，则系统不安全。

安全防御就是保护系统安全的防御性措施，即通过这些措施可以避免系统安全性的损

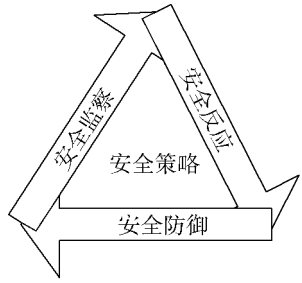

图 员员摇 动态安全模型

失。如系统的信息保密措施、完整性控制措施、数据可用性保障措施等等。

安全监察是对系统安全保护对象和保护措施的监管、对系统可能存在的安全缺陷的查找与分析、对可能受到的攻击的探测与分析。通过这些措施做到对系统安全状况知己知彼，同时可以威慑敌人。

安全反应是对安全监察到的安全事件的处理。它通常包括应急处理和后续处理。应急处理是紧急维护系统安全设施，恢复系统安全状态，保护所威胁的信息等资源。后续处理是分析安全事件状况，强化或更新系统安全防御措施，追究安全责任等。

安全防御、监察和反应都是以系统的安全策略为目标，通过系统组织结构方式，形成信息系统中有机的安全控制体系，即安全控制系统。

员员摇 安全控制系统

安全控制系统就是信息系统中既定的安全策略的贯彻体系，如图 员员所示。这里所说的“既定”是表明系统中任何一次具体的安全控制行为都是以一定安全策略为依据，而不是说系统中的策略必须是预先设定的或一成不变的。

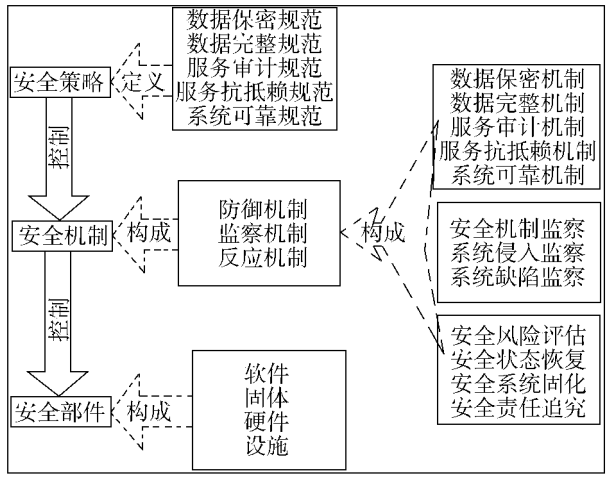

图 员员摇 安全控制系统

摇摇员郾安全机制

安全机制是实现某种安全策略的技术方案。通常实现某种策略的方案不止一项，可以视系统环境做出选择，如图 员郾缘所示。

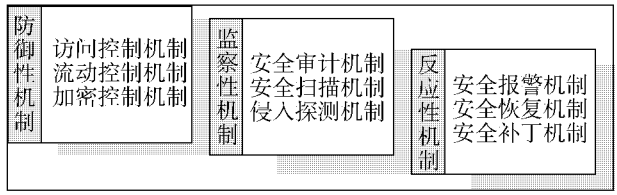

图 员郾缘摇安全机制

摇摇圆郾安全部件

安全部件是实现某种安全机制的系统部件，可以是软件、硬件、固件或设施等。通常，安全部件可以根据不同组合实现功能或性能不同的安全机制，关键在于安全部件的调度或配置管理。

员郾猿摇安全系统

信息系统通过它的安全控制系统执行安全战略思想，满足信息安全需求。根据安全战略思想，安全控制系统的组织内容必须适应系统安全形势的变化。这种变化的适应方式就是设立安全控制管理系统，满足信息系统对安全功能和性能需求的发展。对于安全控制系统组织的每一次改动，都是一个复杂的工程。安全控制系统本身必须可靠。这种可靠性保障的方式就是认证，即设立安全控制认证系统。通过安全控制系统、安全控制管理系统和安全控制认证系统，就可以提供可靠的安全系统，满足信息服务的可靠性要求。这种安全系统对整个信息系统来说，就是信息安全服务系统。通过安全服务管理，建立安全系统与信息系统其他部分之间的安全服务关系，如图 员郾苑所示。

摇摇员郾安全控制管理

安全控制管理的核心任务是保障安全控制系统正确配置，维护安全控制系统的可靠运转，使安全系统提供的服务能够满足信息服务安全需求。它包括：安全控制策略管理、安全机制管理、安全机制组件管理以及安全机制调度管理和安全组件调度管理。

摇摇圆郾安全控制认证

安全控制认证的核心任务是对安全控制系统的可靠性进行逻辑认证和动态分析，及时发现安全控制问题，提供安全控制的紧急处置和恢复。它包括：安全策略认证、安全机制认证、安全组件认证、安全机制对策略的保障认证以及安全组件对安全机制保障的认证。

摇摇猿郾安全系统服务

安全系统的安全功能对外就表现为安全系统的服务。通过安全服务，接受信息系统安