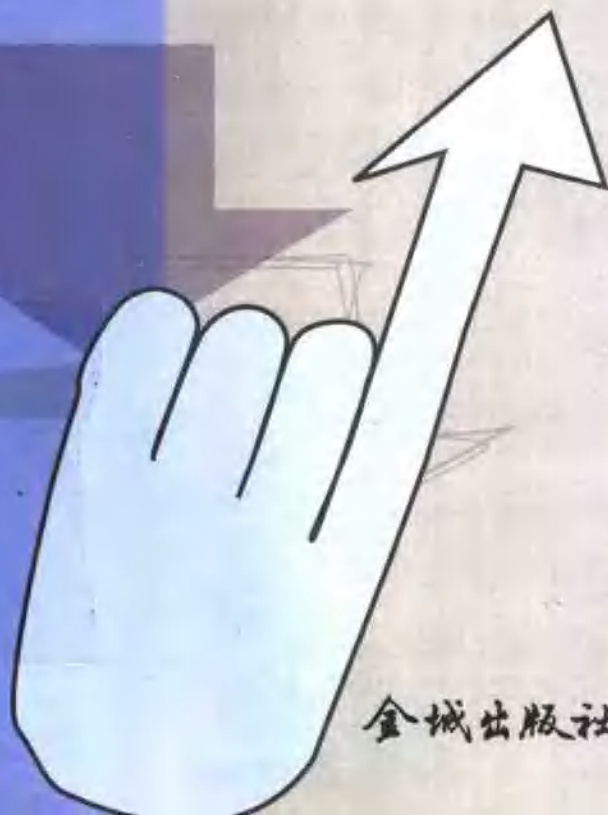


信息安全保密 重难点问题解答

南京军区保密委员会办公室 编



金城出版社

信息安全保密知识系列参考教材之一

信息安全保密 重难点问题解答

南京军区保密委员会办公室 编

江南社会学院图书馆藏书

金城出版社

图书在版编目 (CIP) 数据

信息安全保密重难点问题解答/南京军区保密委员会
办公室编. —北京: 金城出版社, 2001.9

ISBN 7-80084-390-4

I. 信… II. 南… III. ①电子计算机-安全技术-法
规-中国-问答 ②信息-保密-法规-中国-问答
IV. D922.145-44

中国版本图书馆 CIP 数据核字 (2001) 第 062126 号

金城出版社出版发行

(北京朝阳区和平街 11 区 37 号楼 100013)

河北省高碑店市鑫昊印刷有限责任公司印刷

850 × 1168 毫米 1/32 7.625 印张 180 千字

2001 年 9 月第 2 版 2002 年 5 月第 3 次印刷

印数: 8001—12000 册

ISBN 7-80084-390-4/T·13

定价: 12.00 元

前 言

江主席深刻指出：“新的科学技术尤其是电子信息技术迅速发展和广泛使用，大大提高了我们的工作效率，也使得政治、军事、经济、科技等领域中秘密信息的存储、处理、传递发生了很大变化。这种科技进步的新形势，要求我们转变过去以管好涉密文件为主的工作方式，努力探索加强保密工作的新路子。”江主席的指示精辟阐明了新时期信息安全保密工作的特点，指明了保密工作的正确方向。我们必须高度重视，切实转变保密观念，拓宽工作思路，不断适应新形势对保密工作的要求。

随着现代通信和计算机网络技术的广泛应用，高技术条件下窃密与反窃密的斗争愈演愈烈，做好信息安全保密工作，十分重要而又紧迫。针对当前信息安全保密意识淡化、知识贫乏的现状，南京军区保密委员会结合信息安全保密工作实际，编写了《信息安全保密重难点问题解答》一书。该书抓住工作中常见的疑难问题，介绍信息安全、计算机网络基础知识，力求帮助广大读者增强信息安全保密意识，掌握信息安全保密知识。同

时，为军队和地方信息安全保密知识培训提供一本重点突出、操作性强的参考教材。

全书分基础知识、防电磁辐射泄密与通信安全、病毒与防治、黑客与防范、计算机及网络安全技术、安全保密行政管理和附录七部分。编写中从提出“是什么”入手，然后说明“为什么”、“怎么防”的问题。一问一答，简明扼要。

本书编写工作是在张维平、孙建华、周争光、章新文、王国义、滕建明等领导同志的具体领导和关心下完成的，并得到了国家保密局、解放军保密办，特别是金城出版社的大力支持，舒权武同志对编写工作进行了认真筹划和精心安排，田宏林同志负责具体编写，赵小军、高峰、郭晓劲、王琦、黄一军、任园林也参与了部分编写工作，在此一并致谢。由于资料有限，对一些问题的学习研究不够，书中缺点和不足之处，敬请广大读者批评指正。

编 者

2001年8月20日

目 录

第一章 基础知识 (1)

- 1) 什么是信息? (1)
- 2) 什么是信息技术? (1)
- 3) 什么是信息战? (2)
- 4) 信息战与电子战是一样的吗? (3)
- 5) 什么是计算机网络? (4)
- 6) 什么是计算机信息系统? (4)
- 7) 什么是计算机信息系统安全保密? (5)
- 8) 计算机信息系统安全保护的内容有哪些? (5)
- 9) 各种逻辑结构的计算机网络其安全性如何? (7)
- 10) 什么是 TCP/IP 协议? (9)
- 11) 什么是 IP 地址 (互联网协议地址)? (11)
- 12) 什么是计算机安全? (11)
- 13) 计算机不安全性的来源有哪些? (13)
- 14) 计算机窃密和破坏手段有哪些? (13)
- 15) 计算机安全机制应包含哪些方面? (14)
- 16) 计算机安全的应急措施有哪些? (14)
- 17) 计算机信息系统安全分为哪几类? (14)
- 18) 为什么说计算机系统是脆弱的? (15)
- 19) 威胁计算机保密安全的主要因素是什么? (16)

- 20) 目前流行的操作系统安全吗? (17)
- 21) 现代信息安全与传统信息安全有什么不同? (18)
- 22) 我国信息安全的形势如何? (19)
- 23) 通常讲的计算机犯罪指哪些行为? (19)
- 24) 关于计算机安全有哪些条例和法规? (23)
- 25) 计算机信息安全的法律责任有哪些规定? (25)
- 26) 我国刑法涉及窃取国家秘密的条款有哪些? (27)

第二章 防电磁辐射泄密与通信安全 (29)

- 27) 在房间里操作计算机是否就绝对安全? (29)
- 28) 电磁信号泄漏的途径有几种? (31)
- 29) 如何防止计算机电磁辐射泄密? (31)
- 30) 计算机电磁干扰器有哪几种类型? (32)
- 31) 怎样正确连接防电磁辐射干扰器? (33)
- 32) 目前常用的窃听技术有哪些? (33)
- 33) 使用通信工具应当遵守哪些保密规定? (35)
- 34) 为什么不能在普通有线电话上谈论国家
秘密? (35)
- 35) 使用有线电话传递涉密信息应当采取
哪些措施? (36)
- 36) 为什么不能用普通传真机传输国家秘密? (37)
- 37) 使用传真机传递涉密信息应当采取哪些
措施? (37)
- 38) 为什么不能在普通移动电话上谈论国家
秘密? (37)
- 39) 使用移动电话传递涉密信息应当采取
哪些措施? (37)

第三章 病毒与防治 (39)

- 40) 什么是计算机病毒? (39)
- 41) 计算机病毒是怎样产生的? (41)
- 42) 计算机病毒由哪些基本模块构成? (42)
- 43) 计算机病毒怎样分类? (44)
- 44) 什么是计算机病毒的演化体? (45)
- 45) 计算机病毒有哪些危害? (47)
- 46) 计算机病毒进入目标系统的方法有哪几种? (47)
- 47) 如何预防计算机病毒? (49)
- 48) 为什么有时候不能及时发现计算机已感染
病毒? (49)
- 49) 发现计算机病毒后应如何处置? (51)
- 50) 什么是文件型病毒和系统引导型病毒? (51)
- 51) “良性”病毒是不是对计算机系统没有危害? (52)
- 52) 为什么保存硬盘分区记录和 DOS 引导分区记录
内容有利于清除系统引导型病毒? (53)
- 53) 为什么文件型病毒较难清除? (54)
- 54) 为什么计算机病毒有时需要重复几次运行杀毒
程序才能彻底消除? (56)
- 55) 什么是“米氏”病毒? (57)
- 56) “黑色星期五”病毒是怎样一种病毒? (58)
- 57) 为什么说“DIR-2”病毒是一种特殊的文件型
病毒? (60)
- 58) 为什么说“新世纪”病毒是一种混合型病毒? ... (62)
- 59) 宏病毒是一种怎样的病毒? (63)
- 60) 怎样识别和清除宏病毒? (65)

- 61) 为什么“CIH”病毒会破坏计算机的主板? (66)
- 62) 为什么使用光盘上的软件有时也会感染病毒? ... (68)
- 63) 对计算机病毒研究、制造、传播有哪些限制性
规定? (70)
- 64) 计算机病毒的杀除方法? (70)
- 65) 怎样用“KV300”系列杀毒软件查杀宏病毒? (71)
- 66) 用杀毒软件消除了病毒, 为什么有的软件
还是不能使用? (72)
- 67) 计算机网络病毒有哪些特点? (72)
- 68) 怎样防止计算机病毒对网络的攻击? (74)
- 69) 怎样对付网络病毒? (76)
- 70) 在网络环境下, 计算机病毒的主要来源有
哪些? (77)
- 71) 在网络服务器上安装了防病毒软件, 为什
么网络系统还可能感染病毒? (77)
- 72) 为什么无盘工作站也会感染病毒? (78)
- 73) “蠕虫事件”是怎么回事? (79)
- 74) 为什么防杀计算机病毒软件产品能清除计算机
病毒? (81)
- 75) 防杀计算机病毒产品主要有哪些类型? (82)
- 76) 怎样使用“VRV”杀毒软件清除病毒? (84)
- 77) 什么是计算机病毒防火墙? (87)
- 78) 怎样使用“VRV”病毒防火墙? (88)
- 79) 如何使用 HDGUARD 防病毒系统? (90)
- 80) 计算机上安装了防病毒卡是不是就可以防病
毒了? (92)
- 81) 微机 BIOS 中的防病毒功能有什么局限? (92)

82) 为什么说“计算机病毒”是未来战争中一种拥有巨大威力的武器?	(92)
83) 防范计算机病毒危害有哪几种办法?	(94)
第四章 黑客与防范	(97)
84) 什么是黑客?	(97)
85) 为什么要警惕“黑客”的入侵?	(97)
86) 网络黑客常用的攻击方法及对策有哪些?	(99)
87) 黑客攻击手段主要有哪几种?	(100)
88) 黑客远程攻击的一般步骤是什么?	(101)
89) 为什么“黑客”入侵有巨大的危害?	(102)
90) 怎样防御黑客入侵?	(107)
91) 如何防止黑客的袭击?	(108)
92) 什么是特洛伊木马和意大利香肠方式的计算机犯罪行为?	(110)
93) 怎样手工检查和清除“特洛伊木马”黑客程序?	(113)
94) 怎样防范“特洛伊木马”黑客程序?	(114)
95) 什么是计算机系统“后门”?	(115)
96) 安全漏洞是怎样划分的?	(116)
97) 什么是拒绝服务的攻击?	(116)
98) 谁制造了“蠕虫病毒”?	(118)
99) 电子邮件轰炸和电子邮件“滚雪球”是指什么?	(119)
100) “黑客战”主要有些什么手段?	(121)
101) 什么是“网络战”?	(122)
102) 网络战是怎样应用于实战的?	(124)

- 103) 网络安全保密的体系结构是什么? (124)
- 104) 美军是怎样在科索沃战争中试验网络战的? ... (125)

第五章 计算机及网络安全技术..... (127)

- 105) 计算机硬件攻击技术有哪几种? (127)
- 106) 计算机硬件防御技术有哪几种? (128)
- 107) 计算机软件攻击技术有哪几种? (129)
- 108) 计算机软件防御技术有哪几种? (131)
- 109) 计算机网络攻击技术有哪几种? (133)
- 110) 计算机网络防御技术有哪几种? (134)
- 111) 为什么要在计算机信息系统中设置用户
口令? (136)
- 112) 为什么说“超级用户”的口令对计算机信息
系统是至关重要的? (136)
- 113) 计算机信息系统核对口令的过程是怎样的? ... (137)
- 114) 如何设置比较安全的口令? (139)
- 115) 怎样设置计算机的 CMOS 开机口令? (139)
- 116) 怎样设置 Windows 屏幕保护程序密码? (140)
- 117) 设置了硬件开机口令, 计算机就安全了吗? ... (140)
- 118) 哪些是计算机的物理安全? (141)
- 119) 怎样才能保证终端的安全? (144)
- 120) 怎样使屏幕保护程序自动运行? (146)
- 121) 怎样禁止光盘的自动运行功能? (147)
- 122) 怎样删除“开始”菜单中的有关命令和
项目? (147)
- 123) 怎样删除“网上邻居”等系统图标? (148)
- 124) 怎样在图形界面下隐藏某个驱动器图标? (149)

125) 怎样禁止使用 MS-DOS 方式?	(150)
126) 怎样禁止使用控制面板中的特殊功能?	(150)
127) 怎样删除“新建”子菜单中的命令?	(152)
128) 怎样清除“运行”等对话框中的历史记录? ...	(153)
129) 怎样禁止使用注册表编辑器?	(153)
130) 怎样提高你的计算机在网络上的安全性?	(154)
131) 计算机信息系统常用的安全保密防范技术 有哪些?	(154)
132) 计算机信息系统的安全保密措施有哪些?	(156)
133) 计算机信息系统技术安全保密管理的内容 是什么?	(157)
134) 计算机网络是怎样实现资源共享的?	(158)
135) 为什么要进行计算机网络的风险分析?	(161)
136) 保证计算机网络安全的主要技术措施是 什么?	(164)
137) 什么是计算机网络防火墙?	(165)
138) 如何建立防火墙规则集?	(167)
139) 什么是防火墙的安全策略?	(169)
140) 为什么防火墙对网络安全具有保护作用?	(170)
141) 为什么当前防火墙技术还不能完全解决 网络安全问题?	(171)
142) 什么是计算机信息系统的物理隔离?	(172)
143) 什么是单主板安全隔离计算机?	(173)
144) 什么是网络安全隔离卡?	(174)
145) 什么是网络监听?	(175)
146) 什么是计算机网络防御?	(178)
147) 什么叫入侵检测?	(179)
148) 什么叫漏洞检测?	(180)

- 149) 为什么要对计算机涉密信息的传输进行加密? (181)
- 150) 怎样保护 Windows NT 网络的口令? (182)
- 151) 具有军线拨号上网功能的网络安全吗? (182)
- 152) 计算机配上终端加密机后网络安全吗? (182)
- 153) 什么叫虚拟专用网络 (VPN)? (183)
- 154) Windows NT 的安全机制有哪些? (183)
- 155) 为什么要对计算机信息系统的用户实行授权控制? (185)
- 156) 怎样对 Windows95/98 操作系统非法用户的权限进行限制? (187)
- 157) 怎样分配管理权限? (188)
- 158) 怎样保护用户名和提高口令的安全性? (191)
- 159) 怎样隐藏系统管理员的用户账号? (194)
- 160) 确保网络设备物理安全的重要性是什么? (195)
- 161) 为什么 Windows NT 网络操作系统要不断安装最新的服务器补丁包? (195)
- 162) 计算机信息系统身份认证对口令的要求是什么? (196)
- 163) 计算机信息系统审计跟踪的要求是什么? (196)
- 164) 计算机日志、计算机审计和计算机安全这三者有哪些关系? (197)
- 165) 为什么要加强 WWW 服务器的安全措施? (199)
- 166) 为什么用 E-mail 电子邮件通信不安全? (201)
- 167) 数据库管理系统是怎样对它的用户进行安全管理的? (202)

第六章 安全保密行政管理 (205)

- 168) 为什么说加强计算机信息系统安全保密工作具有重要的意义? (205)
- 169) 计算机信息系统安全保密行政管理主要有哪几项内容? (205)
- 170) 当前计算机信息系统安全保密存在的主要问题是什么? (206)
- 171) 目前计算机网络信息系统面临的主要安全问题是什么? (206)
- 172) 计算机网络信息系统安全保密工作具有什么特点? (207)
- 173) 计算机网络信息系统安全保密管理具有什么样的特征? (207)
- 174) 计算机网络信息系统安全保密工作应当坚持的原则是什么? (208)
- 175) 抓计算机网络信息系统安全保密工作的关键环节是什么? (209)
- 176) 计算机信息系统、共享型数据库、多用户计算机的管理有哪些要求? (212)
- 177) 计算机信息系统是怎样划分安全等级的? (212)
- 178) 怎样开展对计算机安全问题的教育和培训? ... (214)
- 179) 计算机网络信息系统安全保密建设需要什么样的人才? (217)
- 180) 计算机网络信息系统安全保密的目标是什么? (217)
- 181) 什么是计算机网络信息系统的五层防护

- 体系? (217)
- 182) 什么是三层密码保密体系? (218)
- 183) 怎样对计算机网络信息系统的安全保密性能
进行审查? (218)
- 184) 如何确定计算机信息系统工作人员(系统
操作人员、管理人员和安全保密人员)的
涉密范围和访问权限? (218)
- 185) 如何划定存储涉密信息的硬盘、软盘、光盘、
磁带等介质的密级? (219)
- 186) 为什么要对计算机存储介质实行严格
管理? (219)
- 187) 计算机信息存储介质应有哪些安全
措施? (219)
- 188) 计算机信息系统的涉密信息和数据存取有哪些
规定? (220)
- 189) 保管处理过涉密信息或者重要数据的
存储介质有什么保密措施? (220)
- 190) 怎样防止境外驻华机构、人员窃取计算机
信息系统秘密? (220)
- 191) 为什么涉密计算机系统在设备维修后要进行
技术安全检查? (220)
- 192) 计算机房应建立哪些制度? (221)
- 193) 当发现恶意攻击、黑客侵袭、计算机病毒
危害、网上窃密及破坏、电磁攻击以及其他
重大破坏活动或者征候时应采取什么
措施? (221)
- 194) 经批准上国际互联网的计算机应当怎样进行
管理? (221)

附 录	(222)
一、部分常用术语英汉对照	(222)
二、部分术语注释	(226)

第一章 基础知识

1) 什么是信息?

关于信息的定义，目前学术上尚无定论。如果从科学、严密、广泛应用的角度来考虑，则下述定义比较明确：所谓信息，就是客观世界中各种事物的变化和特征的最新反映，是客观事物之间联系的表征，也是客观事物状态经过传递后的再现。这一定义包括三点内容：(1) 差异。信息的意义就在于反映差异，没有差异也就不称其为信息，信息存在形式不仅标志着客观事物的存在，而且以物质的属性或运动状态为内容，是以物质某方面的性质或与其他物质间的差异为基础的。(2) 特征。信息要反映客观事物在时间、空间上的不同状态，不同事物总要呈现出不同状态，以区别这一事物和那一事物；同一事物在不同时间和空间也有不同的状态，以区别出发展的变化，这就是特征。(3) 传递。信息是可传递的，只有经过传递才能在传受者之间沟通、传播，使不知者得知，成为有用的知识和情报，体现其价值。

2) 什么是信息技术?

信息技术，是扩展人的获取、传递和利用信息功能的技术。它主要包括三项基本技术，即传感技术、通信技术和计算机技术。

传感技术是延长和增强人的感官功能的技术，主要解决信息的大量获取问题。通信技术是神经传递功能扩展的技术，主要解