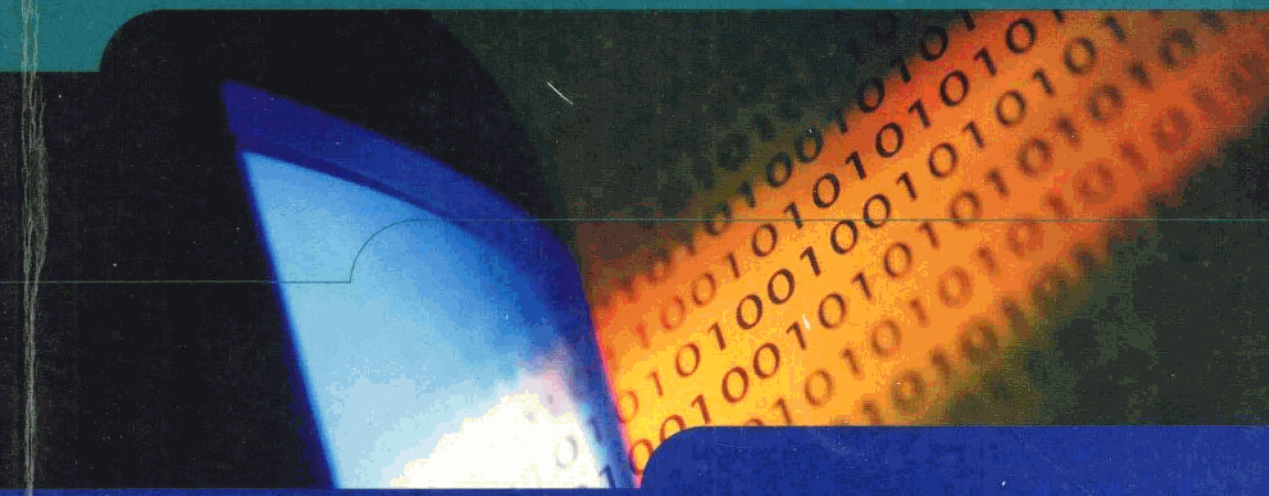


保密技术检查参考

BAOMI JISHU JIANCHA CANKAO

III

国家保密局 虞金龙 编著

金城出版社
GOLD WALL PRESS

说　明

本人于2000年开始从事计算机及网络的保密技术检查工作，参与了互联网上涉及国家秘密信息的检查工作和部分单位的计算机及网络的保密检查工作。在检查过程中，看到了不少违反保密规定的现象，查出了一些涉密网络存在的问题，发现了涉密网络在建设、使用、管理和扩展中存在的矛盾，了解了国内计算机及网络的应用现状，掌握了一些检查方法。为了加强交流，促进技术检查工作，本人利用业余时间把2000年以来，有关计算机及网络检查方面的讲课内容进行了整理，供大家参考。

书中介绍的检查工具和软件，因设计人员的思路和方法各不相同，所使用的名词和概念也不一致，对功能的描述欠清楚，直接影响检查工具和检查软件的使用。为此，本人在使用这些检查工具和软件时，有意识地对其功能进行了尝试，并构建环境进行了验证，通过长时间的反复使用，积累了一些经验，有了一些粗浅体会。书中将本人对这些检查工具和软件的认识介绍给大家，供检查人员在使用这些检查工具和软件时参考。另外，检查工具和软件在不断升级和更新，新的版本功能会更完善，使用会更方便。

要做好计算机及网络检查工作，除了能熟练使用已有的检查工具外，检查人员还应该能够根据检查对象和任务写出特定的检查软件，实现对某个特定操作系统或网络的检查。由于编写检查软件涉及编程语言和操作系统等方面的内容，在此不作介绍。

由于编者水平所限，书中有错误之处，请谅解和指正。

虞金龙

2006年6月26日

目　录

第一章

计算机及网络检查综述

1.1 当前计算机及网络存在的问题

随着通信技术迅猛发展，计算机芯片集成度不断提高，器件成本不断降低，应用软件更加人性化、智能化，推进了计算机的普及与应用，与通信和计算机技术相结合的网络已成为当今世界信息交流的主要和重要手段。我国计算机网络应用虽然起步较晚，但近几年发展很快。到目前为止，党政机关都相继建立了自己的内部办公网络和连接全国的系统纵向网，提高了办公自动化能力和工作效率。

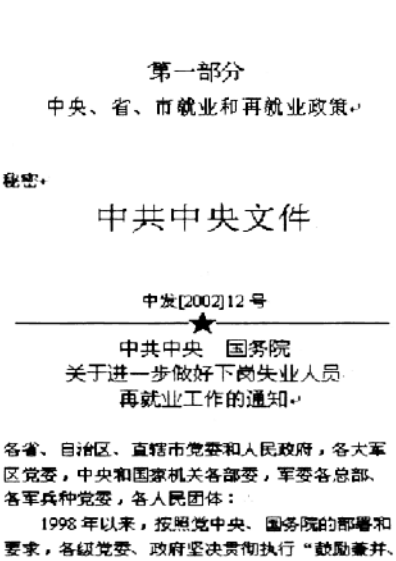
随着计算机网络应用的不断扩大，从简单的文字处理到网上办文，从信息查阅到信息上网，从网上发通知到网上传阅文件，已基本实现了网络办公模式。随着信息量的增加，网络上保存和处理信息也已从日常办公信息向部门敏感信息、涉及党和国家秘密的信息发展。这些保存和处理涉及国家秘密信息网络的安全保密性究竟如何，国家秘密信息是否能像传统的纸质文件一样使用和管理，网络中的国家秘密信息能否得到有效的控制和保护等信息保密问题，一直困扰着保密工作者。近几年，通过对国际互联网上的网页内容和全国党政机关，要害部门、部位，以及军工企业的计算机网络进行了抽查，发现在涉及国家秘密信息保密上存在以下一些问题。

1.1.1 在国际互联网上发现的泄密事件和隐患

1. 涉密信息上国际互联网

按照《计算机信息系统国际联网保密管理规定》(国保发［1999］10号）第八条规定“上网信息的保密管理坚持‘谁上网谁负责’的原则。凡向国际联网的站点提供或发布信息，必须经过保密审查批准。”可是在国际互联网信息检查中，发

现部分政府网站违反保密规定，直接将标有密级的文件在互联网上公开发布，造成国家秘密信息的广泛传播，泄露了国家秘密；一些咨询服务网站、法律顾问网站除了登载秘密文件资料外，还将涉密信息制作成光盘、书籍出售或提供下载服务，严重泄密；还有一些网站将大量涉密信息和不宜公开的信息违规上网。在2005年上半年对互联网站清理整顿工作中，就发现了200多个网页内容涉嫌国家秘密（有的标有密级）。例如：



第一部分

中央、省、市就业和再就业政策

秘密

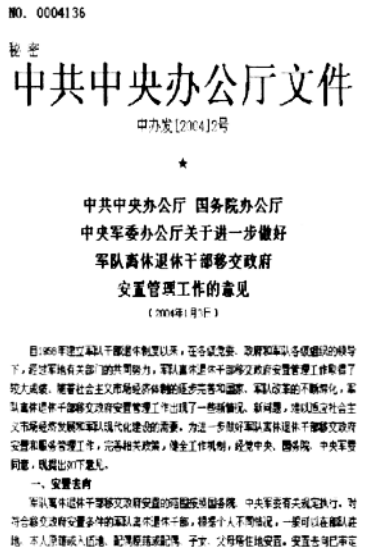
中共中央文件

中发[2002]12号

中共中央　国务院
关于进一步做好下岗失业人员
再就业工作的通知

各省、自治区、直辖市党委和人民政府，各大军区党委，中央和国家机关各部委，军委各总部、各军兵种党委，各人民团体：

1998年以来，按照党中央、国务院的部署和要求，各级党委、政府坚决贯彻执行“鼓励兼并、



NO. 0004136

秘密

中共中央办公厅文件

中办发[2004]2号

中共中央办公厅　国务院办公厅
中央军委办公厅关于进一步做好
军队离休退休干部移交政府
安置管理工作的意见

（2004年1月下）

目前，军队离休干部退休制度以来，在各级党委、政府和军队各级组织的领导下，经过军地有关部门的共同努力，军队离休干部移交政府安置管理工作取得了较大成绩。随着社会主义市场经济体制的逐步完善和国家、军队改革的不断深化，军队离休退休干部移交政府安置管理工作出现了一些新情况、新问题，难以适应社会主义市场经济发展和军队现代化建设的需要。为进一步做好军队离休退休干部移交政府安置和服务管理工作，完善相关政策，健全工作机制，经党中央、国务院、中央军委同意，现提出如下意见。

一、安置去向

军队离休退休干部移交政府安置的问题按照国务院、中央军委有关规定执行，对与合移交政府安置多年的军队离休干部，确需个人下周恤金，一般可以在原驻地、本人原籍或入伍地、配偶原籍或配偶、子女、父母现住地安置。安置去向已审定

造成以上问题的原因，主要是有部分政府网站没有保密管理，将网站委托其他单位代管；有的网站是几家单位合办，上网信息无人审查和管理；有些军事网站、论坛对网民发表个人信息、观点放任自流，没有检查和限制措施，涉及国家秘密的资料和技术参数在论坛上随意发表，造成许多涉及军队和国防建设等敏感信息外泄；有的网站管理不规范，保密责任不落实，上网信息没有经过严格的保密审查；更为严重的情况是有的人将标有密级的文件，通过复印时遮盖密级的方法去掉密级标志，然后发布到国际互联网上。

2. 境外敌对分子将我涉密文件在国际互联网上公布

美国等西方国家控制着国际互联网的顶级域名服务器和IP地址的分配权，把国际互联网视为“封不住、禁不止、打不断”的重型武器。他们还运用加密和代理技术，设立了专门对付我国有害信息过滤的“动态网”，作为访问其他有害网站的跳板。他们还设立中文网站，将通过各种渠道搜集到的我国家秘密发布在这些中文网站上，制造矛盾，挑拨离间，破坏我国家的社会稳定。

另外，我内部少数知密人员视党纪国法不顾，违反保密规定，向境外提供国

家秘密的情况也时有发生。


密码电报

机密

长治市公安局

转发省厅《关于进一步开展打击取缔邪教维护社会稳定的通知》的通知

长公政字[2002]第26号

各县（市）区公安（分）局国保大队、直属分局国保科：

为进一步开展打击取缔邪教组织，维护我市社会政治稳定，认真贯彻落实省委领导的重要批示，根据省厅的通知要求，现将省厅《关于进一步开展打击取缔邪教维护社会稳定的通知》转发你们，请结合当地实际认真贯彻执行。邪教活动较为突出的县（市）区，要行细分析研究邪教活动的特点、规律，进一步完善工作方案，要加大打击力度，确保“十六大”召开期间的社会政治稳定。

3. 处理涉密信息的计算机上国际互联网

法国《情报世界》引述法国国防部“战略事务专责小组”撰写的报告指出，在比尔·盖茨领导的新产品开发小组中有美国国家安全局安插的人员，美国国家安全局的特工曾协助微软在其视窗软件中安装秘密程序，以便当局窃取使用该软件用户的资料。该报告披露了美国微软公司与美国情报机构之间的种种可疑之处，认为微软公司推出的许多产品肯定含有“间谍程序”，其中“后门程序”能够解读所截获的信息。另外，美国国家安全局每天要对传真和电子邮件进行监测，用世界上功能最强的计算机对其进行处理，从中收集有价值的情报。

德国《明镜》周刊报道，德国今后在敏感部门使用的计算机不再使用微软产品，他们认为美国专门从事间谍工作的情报部门——美国国家安全局掌握全部微软软件产品的源代码，还能够破解通过这些软件传送的文件，即使这些文件是加密的也不安全。

通过对国际互联网扫描，查出不少用于涉密工作的计算机上国际互联网，其硬盘上存有大量的涉密信息，有标有秘密、机密和绝密的文件，还有领导准备讲的发言稿和涉密数据统计表等等。

4. 违反保密规定在国际互联网上处理涉密信息

《计算机信息系统保密管理暂行规定》（国保发［1998］1号）第十一条规定：“国家秘密信息不得在与国际网络联网的计算机信息系统中存储、处理、传递。”《计算机信息系统国际联网保密管理规定》（国保发［1999］10号）第七条规定“涉及国家秘密的信息，包括在对外交往与合作中经审查、批准与境外特定对象合法

交换的国家秘密信息，不得在国际联网的计算机信息系统中存储、处理、传递。”明确规定了上国际互联网的计算机不准处理涉及国家秘密的信息。但是在检查中，见到不少单位用于处理涉密信息的计算机都比上国际互联网的计算机差，硬件配置低、机型旧、速度慢、应用软件少、使用不方便。有的工作人员因缺乏信息安全保密意识，为图方便，存在侥幸心理，在上国际互联网的计算机上处理国家秘密信息。在某单位检查上国际互联网的计算机时，查出硬盘中保存有本单位业务工作信息或涉密信息的计算机占63%，超过半数。有的人错误地认为，只要上国际互联网的计算机在不连接国际互联网的情况下处理涉密信息不会出问题，结果有意或无意地将处理过程中的涉密信息保存在计算机的硬盘上，又没有及时检查和清除，造成大量的业务信息和涉密信息积存在硬盘上。2004年，在对某单位保密检查中，检查了70多台连接国际互联网的计算机，查出了30多台用于处理业务信息，内容涉及大量内部信息和与某些重要任务相关的国家秘密，严重违反了计算机保密管理的有关规定。用上国际互联网的计算机处理涉及国家秘密信息就相当于把国家秘密放到国际互联网上，是一种泄密行为。

在检查中，还发现有的单位的网络取名不规范、不统一，造成已有的规章不能发挥作用。有不少单位建有与国际互联网相连接的网络，其名称有“政务外网”、“××信息港”、“外网”和“某市政务网”等，造成有一部分人员用连接该网的计算机直接处理和保存涉密信息。在指出其错误时，他们感到很惊讶，不知道自己使用的网络是国际互联网，有的人还争辩，计算机从配发到现在没有上过国际互联网（浏览国际互联网），不承认自己使用的是国际互联网，认为只有通过拨号或电信部门安装的宽带才是国际互联网，在单位用的网络是办公网，不是国际互联网。反之，有的单位将国际互联网上的网页下载到内网服务器上，供内网用户浏览，造成有个别用户误解自己使用的计算机网络是国际互联网。

1.1.2 涉密计算机网络存在的问题

1. 在网络建设中重应用，轻信息安全保密

按照《中华人民共和国保守国家秘密法》的规定，“国家秘密被不应知悉者知悉的”就是泄密。在检查中发现有不少单位为了加快本系统的信息化发展速度，只讲效率不讲隐患，只求速度不求安全，在计算机网络的互联互通上下了很大功夫，投入大量资金，实现了资源共享。其中有不少的网络，对国家秘密信息的使用完全没有控制，网络中的所有用户不分权限都可以浏览服务器中的信息，是一个信息完全开放的网络。

按照保密规定，处理国家秘密信息的网络属于涉密网，涉密网必须按相关要求来建设，网络使用前要进行审批，达不到保密要求的网络不能处理国家秘密信

息。但是现有的涉密网络多数没有按保密要求建设，有的单位在原有的网络上增加了几个信息保密产品或采取了简单的信息保护措施就处理国家秘密信息，存在很大的隐患，用这种网络处理国家秘密信息极易造成泄密。例如，有一个省为了加快本地信息化建设，构建了一个以省委和省政府为核心，横向连接全省各厅（局）的计算机和局域网，纵向连接各地（市）的计算机网络，覆盖全省各党政机关的政府办公网。虽然实现了基层上报信息及时，主管部门下达信息迅速，政务信息公开，提高了办事效率，但在整个网络的建设中，却采取了省网络管理部门出政策，各地、各部门自行负责规划和建设的办法。出现了条件好、领导重视的单位或地区在接入大网时采取了防火墙和入侵检测等信息保护措施；领导不重视、条件差的单位或贫困地区就没有采取任何信息保护措施，将本地网络直接接入大网的现象。这种网络末端节点延伸到乡镇，覆盖面宽，给信息安全保密带来了很多问题。经检查，发现网络中处理的信息有的内容涉及到部门业务工作中的敏感问题，还有的内容涉及国家秘密。

在网络建设，特别是涉密网络的建设中，这种重应用，轻信息安全保密的做法是非常危险的，不把党和国家的利益放在首要位置，国家秘密信息一旦被不该知悉者知悉，造成泄密，其后果无法挽回。

2. 涉密计算机网络没有进行审批

按照《涉及国家秘密的通信、办公自动化和计算机信息系统审批暂行办法》（中保办发［1998］6号）第十二条规定："保密部门对具备投入运行条件的涉密系统应当批准使用。对不完全具备投入运行条件的应指出存在的问题和漏洞，由其主管部门（单位）改进后另行报批；对不采取改进措施继续使用的，应当责令其主管部门（单位）停止使用。"

当前，在政府部门存在很多讲不清楚，涉密性质界定不清的内部网络。有的内部网络，管理部门按照非涉密网建设，而使用人员却把它当作涉密网使用，所有的业务工作信息都在网上处理，极易出现网络信息安全保密无人过问，发生问题也无人知晓的现象。

3. 涉密计算机网络与其他非涉密网逻辑隔离，没有真正实现物理隔离

《计算机信息系统国际联网保密管理规定》第六条要求"涉及国家秘密的计算机信息系统，不得直接或间接地与国际互联网或其它公共信息网络相联接，必须实行物理隔离。"按照《涉及国家秘密的通信、办公自动化和计算机信息系统审批暂行办法》（中保办发［1998］6号）第十六条规定："涉密系统不得直接或间接国际联网，必须实行物理隔离。"

在检查中，发现有的单位涉密计算机网络与国际互联网连接的现象仍然存在。有的虽然在两网间采用了防火墙隔离措施，但没有实现物理隔离。这种情况在前

几年较为普遍。随着信息安全和保密知识的不断普及，查处力度的增加，以及各级领导的重视和关注，涉密计算机网络与国际互联网直接和间接连接的情况不断减少，但仍时有发现。

当前，部委涉密网向下延伸中问题较多。据了解，各部委的涉密网在建设时都不同程度地采取了一些安全保密措施，但为了发挥网络的作用，有很多部委要求各省业务对口部门与自己的网络相连，成为部委纵向网。有一些部委的涉密网络，从省到部委的连接要求很严，而从地市到省的连接在安全保密要求上明显放松，发现有的地市将连接纵向涉密网的网络间接与国际互联网连接，虽然有些采取了防火墙措施，但没有实现物理隔离，存在泄密隐患。出现纵向涉密网络安全保密要求不落实现象，存在上严下松的情况，给整个涉密网络的安全保密带来严重的威胁。

在检查中还发现，有的内部网通过不同的方式与多个上级部门的专用网络相连，出现了几个相互独立的网络变成一个物理上相互联接的网络的情况，按照“木桶”原理，整个网络的安全保密性能将降到其中最差网络的等级，这对信息保密来讲是非常危险的，尤其是密级高的网络将会受到严重威胁。

4. 涉密计算机网络用户登录服务器的口令简单或长期不更换

《涉及国家秘密的通信、办公自动化和计算机信息系统审批暂行办法》(中保办发［1998］6号）第十七条规定：“处理秘密级信息的系统口令长度不得少于6个字符，口令更换周期不得长于一个月；处理机密级信息的系统口令长度不得少于8个字符,口令更换周期不得长于一周；处理绝密级信息的系统，应当采用一次性口令或生理特征等强认证措施。”可是，在实际使用中很少有人能按规定及时更换口令。

在检查中，发现网络中的计算机登录服务器，有的无账号和密码要求；有的登录账号采用每人的名字拼音，密码又按某一规律来组成；有的将账号和密码写成纸条贴在显示器上。据了解，大多数用户的口令长时间使用，不按要求定时更换。现在有很多猜密码的软件，这些弱密码很容易在短时间内被猜中，有了账号和密码，登录系统就很方便，这是涉密计算机网络使用中的一个大漏洞。

5. 涉密计算机网络对用户无权限控制

涉密计算机网络主要处理涉密信息，凡是带密级的信息都应受密级的限制，只能是一部分人员知悉，因此涉密电子文档在网络中必须有所控制，不能大家都能浏览。在检查中，发现有不少涉密网络没有对用户进行身份识别，有的虽然设了账号和密码，但对用户的权限没有控制到涉密文档，只要进入系统就能浏览全部信息；有的权限只控制到目录，只要有某个账号就能浏览特定的目录，不能控制每个涉密文档的知悉范围。

要确保涉密信息在有限制的范围内浏览，必须要有身份识别和权限控制。

6. 涉密计算机网络 IP 地址动态分配、IP 地址与网卡没有绑定

在检查中，发现有的网管人员，为了方便新增加的网络用户，减少网管人员的工作量，在涉密网中采用了 IP 地址自动分配模式。新用户只要在计算机的 TCP/IP 协议中选中“自动获得 IP 地址”选项，并把计算机接入网络，就可以自动获得一个合法的 IP 地址，不需要通过网管人员就能成为一个合法用户。还有的涉密网采用分网段方式分配 IP 地址，只要用户的计算机 IP 地址设置在该网段内便可以接入该网络，成为合法用户。对于这些网络，网络管理人员不能及时发现网络中用户的增加和减少情况，特别是一些非法用户的接入，网络管理人员就更无法及时发现，并采取措施阻断。

上面两种 IP 地址的分配方式，直接影响到整个网络的信息安全保密。在检查中，检查人员用自带的笔记本电脑，很方便地接入了以上两种分配 IP 地址的网络，通过一些工具软件找出了网络中有漏洞的涉密计算机，轻而易举地下载了这些计算机硬盘中的部分文件。所有这些操作都是在用户毫无察觉的情况下完成的，网络管理人员也没有发现。

7. 涉密计算机网络客户端操作系统存在漏洞及管理员账号为空口令、弱口令等，造成网络内部不设防

在检查中，发现有不少单位在涉密网络建设中，只注重防范外部入侵，而忽视内部访问控制。有的涉密计算机网络，只是简单地将本单位的计算机连接在一起，虽然与国际互联网实现了物理隔离，但涉密计算机未按规定设置本机安全策略、未取消默认共享、未按规定设置启用系统口令和屏幕保护口令。通过扫描涉密网络中计算机操作系统存在的漏洞，发现有不少客户端的计算机操作系统存在严重漏洞，检查人员利用漏洞下载了这些涉密计算机硬盘上的文件。对这样不设防的网络，内部任何人员都可通过简单的操作获取网络中有漏洞计算机硬盘中的文件。

在一次检查中，对 6 个网络进行漏洞扫描，发现有 3 个网络存在严重的漏洞，占总量的 50%。检查人员利用共享漏洞下载了部分涉密计算机硬盘上的文件，有“××市委常委会议纪要”、“×办发××号”、“×府发××号”、“工作通报”、“××省长讲话”、“××省值班信息”、“省政府领导周安排”、“值班要情”等。

在检查某个地市机关办公网时，发现该网是一个部委的纵向网，通过该网中的计算机，使用专用软件工具，看到了省级机关部分有漏洞的计算机硬盘中的内容。在省级机关的计算机上，利用漏洞工具，通过网络还可以看到北京总部网络中的部分操作系统有漏洞的计算机硬盘上的文件。

在保密大检查中，对某省一涉密网络进行漏洞扫描，不到一小时，发现有 5 台计算机没有口令，有一台计算机口令为 1111，利用漏洞工具分别查看到这些计算机硬盘中保存的一些敏感文件。

在对某单位机密级内网进行检查时，通过对内网中在线的1300余台计算机进行扫描，发现有336台终端机存在高风险漏洞。对某研究所的机密级内网进行检查，通过对内网中在线的573台计算机进行扫描，发现有309台终端机存在高风险漏洞，如Microsoft Task Scheduler远程任意代码执行漏洞，微软DCOM接口缓冲区溢出漏洞，Messenger服务中缓冲区溢出漏洞等。还发现绝大多数内网终端机没有关闭默认共享、远程管理和远程IPC$，极少数的终端机提供了不必要的服务，开放了高风险端口。这将意味着局域网内的其他终端用户可以利用相关工具在该计算机中执行任意命令，包括植入木马程序，散布病毒，甚至可以不受限制地访问该计算机的所有文件，任意查阅和删除文件。

设置密码是给用户提供的一道保护防线，如果使用得当，可以起到保护作用，如果使用得不好，则形同虚设。

这些问题给计算机的信息安全带来极大的危险，尤其是涉及国家秘密的信息，被网内用户非法窃取，造成泄密也不易察觉。

8. 涉密计算机网络中涉密文件夹设置共享

2005年保密大检查时，对某市三个单位的涉密网络进行检查，发现每个网络都有共享文件。他们通过共享文件夹来交换各职能部门的信息，有的文件夹没有设置密码，网上用户都能阅读和修改；有的用户在设置共享文件时，虽然设置了密码，但安全性很差。现在国际互联网上有很多免费破译共享文件夹密码的软件，象破译WIN98操作系统设置的共享文件夹密码软件，破译1位只需几秒钟，N位长度的共享密码也只需N个几秒钟。利用设置共享文件夹来交换涉密信息是一种不安全的方法。

9. 涉密计算机网络没有审计功能

《涉及国家秘密的通信、办公自动化和计算机信息系统审批暂行办法》(中保办发［1998］6号）第二十条规定："涉密系统的审计跟踪应当符合以下要求：(一）涉密系统应当有详细的系统日志，记录每个用户的每次活动（访问时间、地址、数据、程序、设备等）以及系统出错和配置修改等信息。"在检查中，发现大多数涉密计算机网络没有审计功能，出现非法操作或信息被非法使用也无法发现和追查的情况。

10. 涉密计算机网络提供远程拨号上网

在检查中发现有的涉密计算机网络提供拨号服务，解决远郊区和移动用户上涉密网络的问题。这实际上是给涉密网络开了一个入侵通道，直接影响网络的安全。一旦电话号码、账号和密码泄露，网络就会遭到非法入侵者的入侵或攻击。入侵者可在世界任何地方通过拨号进入服务器，利用操作系统漏洞，查看、删除或修改服务器中的文件，修改安全设置，植入木马程序等，实施远程控制。据了

解，有的涉密网络提供的电话号码、账号和密码是长期不更换的，其中账号和密码是按照某一规律产生，知道其中一个账号和密码就可以推断出其他账号和密码。

11. 涉密计算机网络使用传真、复印、打印多功能一体机，并连接电话网

《关于加强政府上网信息保密管理的通知》（国保发［1999］4号）第三条规定："涉密信息网络必须与公共信息网络实行物理隔离。在与公共信息网相连接的信息设备上，不得存储、处理和传递国家秘密信息。"

按照保密规定，涉密计算机网络必须实行物理隔离，防止涉密计算机网络内的信息传递到其他网络中，造成泄密。当前比较流行的多功能一体打印机很受政府部门欢迎，既能接收传真，又能打印文件。这种打印机能同时接入电话网和计算机，把计算机输出打印的涉密信息输入到一体机的内部存储器，发送传真的信息通过扫描也进入一体机的内部存储器，两者共用一个内部存储器，输出由软件控制。当打印时，一体机将内部存储器中的信息复制到纸上；当发传真时，一体机将内部存储器中的信息传送到电话线上。如果对一体机的软件稍作修改，就可以将所有打印数据除了打印外，同时通过电话线路转发到某个指定的服务器或传真机。所以涉密计算机及涉密网使用一体机时，不能与电话网物理连接，否则将存在泄密隐患。

12. 涉密计算机网络中的客户机使用无线键盘

《计算机信息系统保密管理暂行规定》（国保发［1998］1号）第十九条规定："计算机信息系统应采取相应的防电磁信息泄漏的保密措施。"

在检查中，发现有的涉密计算机使用无线键盘。因为涉密计算机的键盘是涉密信息的主要入口，当使用无线键盘时，输入的内容是通过无线电波传给主机，虽然其信号的发射功率不大，但只要有相应的接收设备就可以接收和解调输入的内容。特别是在一些办公环境比较差的场所，存在输入的涉密信息被他人接收还原的可能，存在泄密的危险。

13. 涉密计算机网络中的终端计算机接入有线电视网

《关于加强政府上网信息保密管理的通知》（国保发［1999］4号）第三条规定："涉密信息网络必须与公共信息网络实行物理隔离。在与公共信息网相连接的信息设备上，不得存储、处理和传递国家秘密信息。"

在检查中，发现有的部委涉密计算机网中的终端计算机，安装有有线电视接收盒（也称"机顶盒"）。这种设备不但不影响计算机正常工作，还可以利用计算机的显示器观看有线电视节目，但是观看电视节目时必须打开计算机主机。这种终端计算机实际是将涉密计算机网络与有线电视网进行物理连接，存在涉密计算机网络中的涉密信息通过线路传递到有线电视网络上和涉密计算机网络中的电磁信号通过有线电视网向外发射的可能。

14. 涉密计算机电磁辐射没有防护措施

《计算机信息系统保密管理暂行规定》(国保发[1998]1号)第十九条规定:"计算机信息系统应采取相应的防电磁信息泄漏的保密措施。"

在检查中,发现有的单位办公室离马路很近,有的办公楼离涉外建筑物不远,处理绝密级信息的计算机和打印涉密文件的打字室没有任何防电磁辐射的措施。自1985年荷兰工程师范艾克发现计算机存在电磁辐射和用电视机接收还原了计算机显示屏上的信号后,引起了计算机安全界的极大关注,出现了不少公司对接收还原计算机视频辐射信号的研究,并研制出用于接收计算机视频信号的设备。早期的286低档计算机可用普通电视机稍加改装就可接收还原计算机屏幕上显示的内容,而现在的计算机已不能用这种电视机来接收还原,需要用宽带接收机和相应的数字处理技术才能接收还原计算机辐射的视频信号。

从已发现的窃密案件中可以看到,西方情报机构在80年代末已有接收电磁辐射的设备和还原技术,并应用到情报窃取中。因此,我们不能忽视计算机的电磁辐射问题,处理涉密信息的计算机应防止电磁辐射造成泄密。

1.1.3 笔记本电脑使用中存在的问题

1. 笔记本电脑使用管理缺少监督机制

有不少单位在笔记本电脑的使用过程中,没有严格按保密规定进行管理。在检查中发现,专人使用的笔记本电脑,多数存有大量的涉密文件。有的使用者从配发笔记本电脑开始,起草的所有文件全部保存在硬盘上,从没做过文件清理工作,硬盘上存有上千个业务文件,而且所有信息没有任何保护措施。有的使用者出差时还带这样的笔记本电脑,虽然使用很方便,但一旦被盗或被人非法拷贝,其损失将无法弥补。公用笔记本电脑的使用管理仍然停留在固定资产的层面,没有对处理和保存的信息进行管理。

在一个单位检查时,抽查放在办公桌上的部分笔记本电脑,发现有80%的笔记本电脑存在一机两用的情况,即既处理日常业务工作的文件并保存在硬盘中,同时又上国际互联网。

笔记本电脑的使用和管理非常混乱,没有监督检查机制,一机两用现象普遍,特别容易造成泄密。

2. 涉密笔记本电脑没有开机口令保护或口令设置简单

检查中发现,大多数机关使用的笔记本电脑既没有设置BIOS口令,也没有设置操作系统口令,打开电源就能进入计算机。有的虽然设置了操作系统口令,但口令设置较简单,不能有效保护笔记本电脑中的数据。

3. 笔记本电脑中保存的涉密信息没有保护措施

《计算机信息系统保密管理暂行规定》(国保发［1998］1 号)第六条规定："计算机信息系统应当采取有效的保密措施，配置合格的保密专用设备，防泄密、防窃密。所采取的保密措施应与所处理信息的密级要求相一致。"

检查中，发现多数处理涉密信息的笔记本电脑没有任何信息防护措施，所有的涉密信息都以明文形式保存在硬盘中，这样的笔记本电脑一旦被他人接触，涉密信息很容易被阅读或复制，造成泄密也不易发现。

4. 公用笔记本电脑处理涉密信息后，没有清除硬盘中保存的涉密信息或删除不净

检查中，在对公用笔记本电脑进行硬盘数据恢复时，发现有 50%以上的笔记本电脑硬盘上曾保存过涉密文件和上国际互联网的痕迹。经了解，公用笔记本电脑外借时，有些人用于起草文件，有些人用于上国际互联网或收发电子邮件。由于是公用笔记本电脑，借用者在归还时只把自己需要的文件拷贝到其它介质保存，而往往忽视清除保存在硬盘上的信息，从而造成了一台笔记本电脑一段时间处理涉密信息，一段时间上国际互联网，交替使用，谁也说不清是何时何人保存的文件，有的甚至借用人都已调走。另外，笔记本电脑管理人员只负责设备的借出、收回和保存，不过问硬盘上保存的信息，也不对硬盘文件进行清理。这种将大量的涉密文件保存在硬盘中，不及时清除的现象，是造成泄密的一大隐患。

5. 涉密笔记本电脑借给其他人使用，留下泄密隐患

《国家秘密设备、产品的保密规定》(国保［1992］53 号）第十五条："……无关人员不得接触、使用密品。"在检查中发现，有的人将自己使用的涉密笔记本电脑拿回家，供子女用来上国际互联网；有的人将自己的涉密笔记本电脑借给同事、朋友出差用；有的领导将自己处理保存涉密信息的笔记本电脑交给身边工作人员保管或使用，结果工作人员用涉密笔记本电脑上国际互联网，造成涉密计算机上国际互联网。涉密笔记本电脑保管不当，借给他人使用，将严重威胁国家秘密信息的安全。

6. 涉密笔记本电脑带有无线网卡

《计算机信息系统保密管理暂行规定》(国保发［1998］1 号）第十九条规定："计算机信息系统应采取相应的防电磁信息泄漏的保密措施。"

现在有不少单位使用带无线网卡的笔记本电脑处理涉密信息。为此，用 IBM-X40 笔记本电脑做了一个试验，当打开笔记本电脑电源后，发现 IBM-X40 笔记本电脑不断发信号，搜索网络，一旦外部有无线网络信号时，笔记本电脑就自动进行连接，成功后就接入外部网络。

当前，国际上通用的无线网卡采用 IEEE802.11a/b/g 标准，主要用来解决办公