 计算机的广泛应用推动了社会的发展和进步，但也带来了一系列的社会问题。现在，西方发达国家把他们的社会由于广泛使用计算机称为“ 脆弱的社会 ”。计算机的脆弱性一般表现在计算机犯罪、敌对国家的破坏、意外事故和自然灾害、电磁波干扰、工作人员的失误以及计算机本身的缺陷等许多方面，突出表现是容易泄密和被窃密。 （一）计算机泄密的主要途径 1、计算机电磁波辐射泄密 计算机辐射主要有四个部分：显示器的辐射；通信线路（连接线）的辐射、主机的辐射；输出设备（打印机）的辐射。计算机是靠高频脉冲电路工作的，由于电磁场的变化，必然要向外辐射电磁波。这些电磁波会把计算机中的信息带出去，犯罪分子只要具有相应的接收设备，就可以将电磁波接收，从中窃得秘密信息。据国外试验，在1000米以外能接收和还原计算机显示终端的信息，而且看得很清晰。微机工作时，在开阔地带距其100米外，用监听设备就能收到辐射信号。计算机电磁辐射大致分为两类：第一类是从计算机的运算控制和外部设备等部分辐射，频率一般在10兆赫到1000兆赫范围内，这种电磁波可以用相应频段的接收机接收，但其所截信息解读起来比较复杂。第二类是由计算机终端显示器的阴极射线管辐射出的视频电磁波，其频率一般在6．5兆赫以下。对这种电磁波，在有效距离内，可用普通电视机或相同型号的计算机直接接收。接收或解读计算机辐射的电磁波，现在已成为国外情报部门的一项常用窃

密技术，并已达到很高水平。 2、计算机联网泄密 计算机网络化是计算机发展史上的重要阶段，它使计算机只能在机房里对不同信息的单项数据的分类、加工和整理，发展成为使信息的收集、加工、贮存、传输融为一体，扩大了计算机的应用范围，使计算机的应用深入到社会各个方面。计算机网络横跨大陆和海洋，可将世界范围内的计算机联接起来，每个用户都可通过自己的终端，充分利用各个计算机存贮的大量文字、数据和图像资料。计算机网络化带来的信息交流、知识融汇，使人们能充分利用全人类创造的全部知识财富，由此产生的深远影响将难以估量。然而，由于计算机网络结构中的数据是共享的，主机与用户之间、用户与用户之间通过线路联络，就存在许多泄密漏洞。 首先，“ 数据共享 ”时计算机系统实行用户识别口令，由于计算机系统在分辨用户时认“ 码 ”不认“ 人 ”，这样，那些未经授权的非法用户或窃密分子就可能通过冒名顶替、长期试探或其它办法掌握用户口令，然后打入联网的信息系统进行窃密。 其次，计算机联网后，传输线路大多由载波线路和微波线路组成，这就使计算机泄密的渠道和范围大大增加。再者，网络越大，线路通道分支就越多，输送信息的区域也越广，截取所送信号的条件就越便利，窃密者只要在网络中任意一条分支信道上或某一个节点、终端进行截取。就可以获得整个网络输送的信息。 3、计算机媒体泄密 计算机具有惊人的存贮功能。它可以对湖水般涌来的各种信息进行传递、加工和存贮，可以将大量秘密文件和资料由纸张介质变为磁性介质和光学介质。一个汉字至少要占55平方毫米，同样面积的集成电路存贮器可存贮50万个汉字。为了自动地、高效地加工和利用各种信

息，越来越多的秘密数据和档案资料被存贮在计算机里。 计算机的存贮器分为内存贮器和外存贮器两种，内存贮器要求存取速度快，外存贮器要求存贮容量大。如前所述，存贮在内存贮器的秘密信息可通过电磁辐射或联网交换被泄露或被窃取，而大量使同磁盘、磁带、光盘、U盘的外存贮器很容易被非法篡改或复制。由于磁盘经消磁十余次后，仍有办法恢复原来记录的信息，存有秘密信息的磁盘被重新使用时，很可能被非法利用磁盘剩磁提取原记录的信息。计算机出故障时，存有秘密信息的硬盘不经处理或无人监督就带出修理，就会造成泄密。秘密信息和非秘密信息放在同一媒体上，明密不分，容易造成泄密。存有秘密信息的磁盘等媒体被盗或携带出国，就会造成大量的国家秘密外泄，其危害程度将是难以估量的。百考试题收集 4、计算机工作人员泄密 （1）无知泄密。如由于不知道计算机的电磁波辐射会泄露秘密信息，计算机工作时未采取任何措施，因而给他人提供窃密的机会。又如由于不知道计算机软盘上剩磁可以提取还原，将曾经存贮过秘密信息的软盘交流出去，因而造成泄密。 （2）违反规章制度泄密。如将一台发生故障的计算机送修前既不做消磁处理，又不安排专人监修，造成秘密数据被窃。又如由于计算机媒体存贮的内容缺乏可观性，因而思想麻痹，疏于管理，容易造成媒体的丢失。 （3）故意泄密。外国情报机关常常采用金钱收买、色情引诱和策反别国的计算机工作人员。窃取信息系统的秘密。这比利用电子监听、攻击网络等办法有用得多。如程序员被策反，就可以得知计算机系统软件保密措施，获得使用计算机的口令或密钥，从而打入计算机网络，窃取信息系统、数据库内的重要秘密；操作

员被收买，就可以把计算机保密系统的文件、资料向外提供.维修人员被威胁，就可对用进入计算机或接近计算机终端的机会，更改程序，装置窃听器等。（二）计算机的保密防范措施 计算机的保密防范主要从技术、行政和法律三个方面着手：1、技术防范（1）使用低辐射计算机设备。这是防止计算机辐射泄密的根本措施，这些设备在设计和生产时，已对可能产生信息辐射的元器件、集成电路、连接线和CRT等采取了防辐射措施，把设备的信息辐射抑制到最低限度。（2）屏蔽。根据辐射量的大小和客观环境，对计算机机房或主机内部部件加以屏蔽，检测合格后，再开机工作。将计算机和辅助设备用金周屏蔽笼（法拉第笼）封闭起来，并将全局屏蔽笼接地，能有效地防止计算机和辅助设备的电磁波辐射。不具备上述条件的，可将计算机辐射信号的区域控制起来，不允许外部人员接近。（3）干扰。根据电子对抗原理，采用一定的技术措施，利用干扰器产生噪声与计算机设备产生的信息辐射一起向外辐射。对计算机的辐射信号进行干扰，增加接收还原解读的难度，保护计算机辐射的秘密信息。不具备上述条件的，也可将处理重要信息的计算机放在中间，四周置放处理一般信息的计算机。这种方法可降低辐射信息被接收还原的可能性。（4）对联网泄密的技术防范措施：一是身份鉴别。计算机对用户的识别，主要是核查用户输入的口令，网内合法用户使用资源信息也有使用权限问题，因此对口令的使用要严格管理。当然，对用户的识别还有其它方法，如使用磁性卡片、指纹、声音、视网膜图像等对用户进行鉴别。二是监视报警。对网络内合法用户工作情况作详细记录，对非法用户，计算机将其闯入网络的尝试次数、

时间、电话号码等记录下来，并发出报警，依此追寻非法用户的下落。三是加密。将信息加密后存贮在计算机里，并注上特殊调用口令。这样，窃密者突破一般口令进入计算机后，也无法将信息调出。在信息传输过程中，对信息进行加密（一次或二次伪装），窃密者即使截收到信号也一无所知。四是数字签名。（5）对媒体泄密技术防范措施：一是防拷贝。防拷贝技术实际上是给媒体做特殊的标记，如在磁盘上产生激光点、穿孔、指纹技术等特殊标记，这个特殊标记可由被加密程序加以识别，但不能轻易地被复制。二是加密。对媒体中的文件进行加密，使其以常规的办法不能调出。由于密文加密在理论上还没有形成完善的体系，所以其加密方法繁多，没有一定的规律可循，通常可以分为代替密码、换位密码和条积密码方法。三是消磁。百考试题整理 2、行政管理 （1）建立严格的机房管理制度，禁止无关人员随便进出机房，网络系统的中心控制室更应该有严格的出入制度。同时，机房选址要安全可靠，重要部门的机房要有必要的保安措施。（2）规定分级使用权限。首先，对计算机中心和计算机数据划分密级，采取不同的管理措施，秘密信息不能在公开的计算机中心处理，密级高的数据不能在密级低的计算机中心处理；其次，根据使用者的不同情况，规定不同使用级别，低级别的机房不能进行高级别的操作；在系统开发中，系统分析员、程序员和操作员应职责分离，使知悉全局的人员尽可能少一些。（3）加强对媒体的管理。录有秘密文件的媒体，应按照同等密级文件进行管理，对其复制、打印、借阅、存放、销毁等均应遵守有关规定。同一片软盘中不要混录秘密文件和公开文件，如果同时录有不同密级的文

件，应按密级最高的管理。同时，还应对操作过程中临时存放过秘密文件的磁盘以及调试运行中打印的废纸作好妥善处理。（4）加强对工作人员的管理。因为设备由人操纵，制度由人制定并遵守。人员的问题，首先要牢固树立保密观念，使其认识到新时期保密问题的重要性、紧迫性，从而增强保守国家秘密的意识。保密教育要经常抓，常抓不懈；要抓好人员的选配和日常的考察，做到不合格的坚决不用，现有工作人员中发现问题要及时处理，坚决调离，以保证队伍的纯洁精干和效能；要搞好智力投资，不断提高使用和管理人员的科学技术水平，使其真正了解所有设备的性能，掌握防止泄密的知识和防范措施；利用和创造机会扩展他们的知识面，增强主动性，减少盲目性，以防因无知而泄密；还要建立奖惩制度，定期考核，奖优罚劣，完善激励机制。 3、法律监督 计算机保密防范必须以法律法规为依据。目前我国已有《保密法》、《计算机信息系统安全保护条例》和《计算机信息网络国际联网管理暂行规定》。按照规定和要求，做好计算机的保密防范工作，不得利用计算机从事危害国家安全、泄露国家秘密的违法犯罪活动。F8F8" 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com