第 1 章

信息技术与信息安全

本章导读：

今天的社会是信息化社会，我们在很多场合都在谈信息、信息化和信息安全。本章旨在通过对信息、信息技术、信息化和信息安全等基本概念的介绍，使大家对与我们的工作、学习及生活息息相关的这些信息概念有一个全面的了解。同时还对信息安全技术和计算机病毒防范作了较为详细的介绍，这对大多数信息技术应用人员来说是非常必要的，知道并利用这些知识有助于我们更好地、更流畅地使用信息技术。本章最后，我们还对信息法律制度与信息道德规范以及中小学教师信息素养与信息道德作了科学地概括和详尽地阐述，对中小学教师和今后未来要从事教育工作的师范生来说，具有很强的指导意义。

1.1 信息与信息化

1.1.1 信息的概念

广义的信息是指一切消息，即世界上一切事物的运动、状态和特征的反映。狭义的信息是指有使用价值的情报，即通过文字、数据、图像或信号等形式表现出来的，可以传递、处理、储存的对象。信息产生于人类的认识与思维过程中，信息有下列特殊属性。

（1）信息是客观存在的。有的信息是人可以感知的，如温度、语言的内容；有的信息是人不能直接感知的，如微电子信号。人凭借感官获取的信息是极少的，通过各种工具，例如测温仪、显微镜，则可以获得更多的信息。各种自动化仪器能代替人去测量信息、处理信息并自动发出指令。

（2）信息可以生成，可以被感知、存储、加工和传输。

（3）信息可以由一种存在形式转化为另一种存在形式。例如，光信号被转换为电信号，电信号被转换为磁信号，磁信号被转换为“开”或“关”的机械信号后，再被转换为数字信号（“0”、“1”两个数字的有规律组合）。信息存在形态的可转换性，是现代信息技术的物质基础。

信息具有能被有目的地使用并满足人类社会多方面需求的性质，被列为同能源、材料并列的三大重要资源之一。随着人们获取、整理、传播、使用信息的能力不断提高，信息给人类带来的福利日益增加，已成为国民经济和社会发展的重要资源。信息资源具有价值和使用价值，但不会因为使用而消失，它能够被重复使用。信息的使用价值因使用主体的能力或智力不同而异。信息的内容是可以通约相加的，不受存在形式的限制，人们对其进行检索、整理、综合、概括和利用，不会因时间、空间、语言、地域、行业差异而发生内容改变。信息的公用性是永恒的，信息的私有性是暂时的，信息产品是社会财富，没有终极所有权。信息产品可以是商品。

1.1.2 信息技术与信息化

1．信息技术

研究信息的产生、传递和处理的技术称为信息技术，包括信息的产生、收集、交换、存储、传输、

显示、识别、提取、控制、加工和利用等。在繁杂的现代信息技术中，最主要的是传感技术、通信技术和计算机技术。它们相当于人的感觉器官、神经系统和思维器官，是信息社会的感官、神经和大脑。高精确、高效率、高可靠地收集各种信息是传感技术的任务；通信技术则要解决高速度、高质量、及时准确、安全可靠地传递和交换信息的问题；而高速度、高智能、多功能、多品种地处理和加工各种形式的信息，就是计算机技术的目标。

信息技术的根本特征就是将传感技术、通信技术和计算机技术结合成具有信息功能、智能功能和综合功能的信息网及各种智能信息系统。信息技术极大地扩展了人类的信息能力，放大了人类的智力功能。电子技术、激光技术、生物技术、空间技术、海洋技术等都是信息技术的支撑技术。新材料技术、新能源技术则是信息技术及其支撑技术的基础。微电子技术的突破对于信息技术的发展具有重要的作用。微电子技术是集成电路及其应用技术和产品的总称。微电子技术是节约材料、能源、空间和劳动的技术，它的工艺新、产品换代快、品种产量多、应用面广，集中体现了现代技术的精华，推动着以电子计算机技术为代表的信息技术的突飞猛进。

信息技术的主要特点是高度的扩展性和渗透性，强大的纽带作用和催化作用，以及有效地节省资源和节约能源的功能。信息技术未来的发展趋势主要是研制超高速集成电路，研制超级计算机和第五代计算机（人工智能计算机）。此外，还要创造新的制造业技术，推进办公室自动化等。电子计算机的发明和全球卫星通信的实现，给人类社会带来了迄今为止最深刻而广泛的信息革命，带来了经济和社会的信息化。建立在现代科学基础之上的信息技术充分显示了它的强大威力。信息技术，它是新技术革命的核心与先导。它不仅是科学技术现代水平的测量器，也是新技术革命到来的主要标志。信息技术是当今技术发展中的带头技术，它既能改造传统技术，本身又能开拓出新方向和新用途。新材料技术、新能源技术、生物技术、海洋技术、空间技术等领域，都是以信息技术为基础。当代新技术革命中最活跃的领域，就是信息技术。在人类的历史上，信息技术的每次变革都把人类推向新的文明阶段。当前信息技术的发展，使人类的生产方式和生活方式都发生了革命性的变化，开创了人类智力解放的新纪元。毫无疑问，信息技术的革命性变化必将引起社会和文化的大变革。

2．信息化

信息化表现为人类在信息采集、传播、处理和利用的能力在数量和手段上急速扩张，掌握了诸如遥感遥测、卫星通讯、微波通讯、光导纤维通讯、电子计算机、智能控制技术等现代信息技术，从而使人类掌握和交换的信息量以指数形式递增；信息的时间滞后缩短，还表现为信息的接收和利用面扩大，原来只能为少数人或机构使用的信息被越来越多的普通人广泛利用。同时，越来越多的信息物化到各种产品中，从而减少了产品的物质损耗，提高了产品价值中的智能和信息的比重，出现了新型的知识密集型产业。信息（尤其是其中的知识）成为了生产力、竞争力和经济成就的关键因素。现代计算机和现代通信系统相结合形成的信息处理系统正在代替人的部分脑力活动，在使生产过程自动化的同时，也在使办公室工作、服务行业和家庭生活走向自动化；信息产业或智力产业部门在社会生产中所占的比例不断上升，所有这些趋势都是社会信息化的表现。第二次世界大战以来，许多国家大大加快了信息化的进程。

信息和物质、能量同是生产力的要素。人类对信息认识、利用的水平和程度，反映了人类对外部世界（包括自然和社会本身）的认识和改造水平，标志着社会的发展程度。信息化社会的出现表明人类不仅能改造和利用自然力来扩张自己的体力，而且能够利用自然来扩展自己的智力。促使人类认识世界和认识自身的能力发展到一个新的阶段。加速社会信息化，使信息革命渗透到生产和社会生活的各个领域中，将使整个社会发生深刻变化。信息在整个生产和社会生活中的价值和作用将不断提高，智能化生产和通讯革命将改变大机器生产那种集中统一、大批量生产的特点，它使生产更加灵活多样，

也更加分散，更能满足人们的不同要求；它还将改变产业结构，改变人的工作方式；同时它将打开每个人的视野，改变人获取和发送信息的途径和能力，密切个人与社会、个人与世界的关系，从而使社会结构和社会组织及其工作方法发生变化，使世界各国更加紧密地联系在一起。

信息社会中，人类智力资源的开发至关重要。信息技术的发展和应用为开发人类智力资源提供了新的手段，为人类社会的发展开拓了光明的前景；同时它又要求人们调整生产结构、生活方式和生产组织，改变以往的思想观念、生活习惯和生活方式。

1.2 信 息 安 全

随着现代通信技术的迅速发展和普及，特别是随着互联网进入千家万户，计算机信息的应用与共享日益广泛和深入。各种信息系统已成为国家基础设施，支撑着金融、通信、交通和社会保障等方方面面，信息成为人类社会必需的资源。与此同时，计算机信息的安全问题也日益突出，情况越来越复杂。从大的方面来说，计算机信息安全问题已经威胁到国家的政治、经济、军事、文化和意识形态等领域；从小的方面来说，计算机信息安全问题也涉及人们能否保护个人隐私和私有财产安全等。因此，加强计算机信息安全研究，营造计算机信息安全氛围，既是时代发展的客观要求，也是保证国家安全和个人财产安全的必要途径。

1.2.1 信息安全的重要性

随着信息技术日新月异的发展，近些年来，企业在信息化应用和要求方面也在逐步提高，信息网络覆盖面也越来越大，网络的利用率稳步提高。利用计算机网络技术与各重要业务系统相结合，可以实现无纸化办公，有效地提高了工作效率，如外部门户网站系统、内部网站系统、办公自动化系统、营销管理系统、财务管理系统、生产管理系统等。然而，信息化技术给我们带来便利的同时，各种网络与信息系统安全问题也逐渐暴露出来。信息安全是企业信息系统运作的重要部分，是信息流和资金流流动过程中的重要保障，一旦出现安全问题，企业将付出极大的代价。

1.2.2 信息安全的概念

信息安全的静态定义采用国际标准化组织 ISO（International Standard Organization）对“计算机安全”的定义：“为数据处理系统建立和采用的技术上和管理上的安全保护，保护计算机硬件、软件数据不因偶然和恶意的原因而遭到破坏、更改和泄露。”这个定义没有考虑网络的因素，偏重于静态信息保护。信息安全的动态定义则增加了对信息系统能连续正常工作的要求。本书所述的信息系统是指计算机网络信息系统，在不会发生歧义时，常将计算机网络信息系统安全简称为信息安全。网络信息系统安全的目标是保护信息的保密性（Confidentiality）、完整性（Integrity）、可用性（Availability）、抗否认性（Non. Repudiation）和可控性（Controllability）。

（1）保密性。保密性针对信息被允许访问（Access）对象的多少而不同。所有人员都可以访问的信息为公开信息，需要限制访问的信息一般为敏感信息或秘密，秘密可以根据信息的重要性及保密要求分为不同的密级。例如，国家根据秘密泄露对国家经济、安全利益产生的影响（后果）不同，将国家秘密分为秘密级、机密级和绝密级三个等级，可根据其信息安全的实际情况，在符合《国家保密法》的前提下将信息划分为不同的密级。如广州市涉密计算机信息系统分为 A（国家绝密级）、B（国家机密级）、C（国家秘密级）、D（工作秘密级）四个级别。这里的保密性是指信息不泄露给非授权用户，不被非法利用，即使非授权用户得到信息也无法知晓信息的内容。保密性通常通过访问控制来阻止非授权用户获得机密信息的途径，通过加密技术来阻止非授权用户获知信息内容。

（2）完整性。信息完整性一方面是指信息在生成、传输、存储和使用过程中不被篡改、丢失、缺损等，另一方面是指信息处理方法的正确性。不正当的操作，如误删除文件，有可能造成重要文件的丢失。一般通过访问控制阻止篡改行为，通过消息摘要算法来检验信息是否被篡改。完整性是数据未经授权不能进行改变的特性，其目的是保证信息系统上的数据处于一种完整和未损的状态。

（3）可用性。可用性是指信息及相关的信息资源在授权人需要的时候可以随时获得。例如，通信线路中断故障会造成信息在一段时间内不可用，影响正常的商业运作，这是针对信息可用性的破坏。网络环境下的拒绝服务攻击（DoS）和分布式拒绝服务（DDoS）都属于对可用性的攻击。可用性是信息资源服务功能和性能可靠性的度量，是对信息系统总体可靠性的要求。要保证系统和网络能提供正常的服务，除了备份和冗余配置外，没有特别有效的方法。

（4）不可否认性。不可否认性是指保证用户无法在事后否认曾对信息进行的生成、签发、接收等行为，是针对通信各方信息真实同一性的安全要求。一般应用数字签名和公证机制来保证不可否认性。

（5）可控性。可控性是指可以控制授权范围内的信息流向及行为方式，对信息的传播及内容具有控制能力。为保证可控性，通常通过握手协议和认证对用户进行身份鉴别，通过访问控制列表等方法来控制用户的访问方式，通过日志记录用户的所有活动以便于查询和审计。

1.2.3 信息安全因素和安全措施

对计算机信息安全起主要影响的因素有以下几种。

（1）计算机信息系统的使用与管理人员。包括普通用户、数据库管理员、网络管理员、系统管理员，其中各级管理员对系统安全承担重大的责任。

（2）信息系统的硬件部分。包括服务器、网络通信设备、终端设备、通信线路和个人使用的计算机等。信息系统的硬件部分的安全性主要包括两个方面：物理损坏和泄密。物理损坏直接造成信息丢失且不可恢复，而通信线路、终端设备可能成为泄密最主要的通道。

（3）信息系统的软件部分。主要包括计算机操作系统、数据库系统和应用软件。软件设计不完善（如存在操作系统安全漏洞，软件后门接口等）以及各种危险的应用程序也是造成信息系统不安全的重要因素。例如，利用软件漏洞和后门避开信息系统的防范系统，网络黑客可以实施他们的犯罪行为。

针对计算机信息安全因素，一般采取的安全措施有：

（1）管理制度措施。一是国家层面上建立信息安全的相关法律法规，对使用者进行强制约束；二是各使用单位建立使用管理规范和细则，从源头上消除使用者的非安全行为。

（2）技术措施。采用技术手段，堵住信息安全漏洞，在信息流通的过程中将有害信息（软件）过滤清除，达到不对计算机系统和用户造成危害的目的。常见信息安全技术手段有：防火墙技术、防病毒技术、访问控制技术、数据加密技术等。

1.2.4 信息安全技术简介

1．访问控制技术

访问控制是网络安全防范和保护的主要策略，它的主要任务是保证网络资源不被非法使用，它是保证网络安全最重要的核心策略之一。

访问控制包括入网访问控制、网络权限控制、目录级控制以及属性控制等多种手段。

（1）入网访问控制。入网访问控制为网络访问提供了第一层访问控制。它控制哪些用户能够登录到服务器并获取网络资源，控制准许用户入网的时间和准许他们在哪台工作站入网。一般通过用户名和口令进行识别来达到控制的目的。

（2）权限控制。网络的权限控制是针对网络非法操作所提出的一种安全保护措施。用户和用户组被赋予一定的权限，包括可以访问哪些目录、子目录、文件和其他资源。

（3）目录级安全控制。网络应允许控制用户对目录、文件、设备的访问。用户在目录一级指定的权限对所有文件和子目录有效，用户还可进一步指定对目录下的子目录和文件的权限。对目录和文件的访问权限一般有 8 种：系统管理员权限、读权限、写权限、创建权限、删除权限、修改权限、文件查找权限、访问控制权限。这些权限的有效组合可以让用户有效地完成工作，同时又能控制用户对服务器资源的访问，从而加强了网络和服务器的安全性。

（4）属性安全控制。网络系统管理员应给文件、目录等指定访问属性。属性安全在权限控制的基础上提供更进一步的安全性。网络上的资源都应预先标出一组安全属性。用户对网络资源的访问权限对应一张访问控制表，描述用户对网络资源的访问能力。属性设置可以覆盖已经指定的任何受托者指派和有效权限。属性往往能控制以下几个方面的权限：向某个文件写数据、拷贝一个文件、删除目录或文件、查看目录和文件、执行文件、隐含文件、共享、系统属性等。

（5）服务器安全控制。网络允许在服务器控制台上执行一系列操作。用户使用控制台可以装载和卸载模块，可以安装和删除软件等操作。网络服务器的安全控制包括：可以设置口令锁定服务器控制台，以防止非法用户修改、删除重要信息或破坏数据；可以设定服务器登录时间限制、非法访问者检测和关闭的时间间隔。

访问控制通常有三种策略：自主访问控制（DAC）、强制访问控制（MAC）、基于角色的访问控制（RBAC）。

2．数据加密技术

数据加密技术是数字签名等技术的基础。所谓数据加密技术是指将明文信息经过加密钥匙及加密函数转换，变成无意义的密文，而接收方则将此密文经过解密函数、解密钥匙还原成明文。加密技术是网络安全技术的基石。

（1）对称加密技术。对称加密采用了对称密码编码技术，它的特点是文件加密和解密使用相同的密钥，即加密密钥也可以用作解密密钥，这种方法在密码学中叫做对称加密算法，对称加密算法使用起来简单快捷，密钥较短，且破译困难；除了数据加密标准（DNS）以外，另一个对称密钥加密系统是国际数据加密算法（IDEA），它比 DNS 的加密性好，而且对计算机功能要求也没有那么高。

（2）非对称加密技术。1976 年由 Deffie 和 Hellman 两人提出了一种公开密钥密码技术，即非对称加密技术。非对称加密技术允许在不安全的媒体上交换信息，也称之为“公开密钥系统”。与对称加密算法不同，非对称加密算法需要两个密钥：公开密钥和私有密钥。公开密钥与私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。因为加密和解密使用的是两个不同的密钥，所以称这种算法是非对称加密算法。

数据通信前，信息接收者通过公开信道公布自己的加密密钥（公钥），任何向其发送信息者可使用这个公钥将信息加密后发送给他，他用自己未曾公开的私钥对接收到信息进行解密。因为只有他拥有解密私钥，所以所发送的信息即使被他人截获也不会泄密。这种技术被广泛应用于身份认证、数字签名等信息交换领域。

3．数字签名技术

所谓“数字签名”就是通过某种密码运算生成一系列符号及代码组成的电子密码进行签名，代替书写签名或印章，对于这种电子式的签名还可进行技术验证，其验证的准确度是一般手工签名和图章

验证而无法比拟的。“数字签名”是目前电子商务、电子政务中应用最普遍、最成熟、可操作性最强的一种电子签名方法。它采用了规范化的程序和科学化的方法，用于鉴定签名人的身份以及对一项电子数据内容的认可。它还能验证文件的原文在传输过程中有无变动，确保传输电子文件的完整性、真实性和不可抵赖性。

4．身份认证技术

身份认证是计算机系统的用户在进入系统或访问不同保护级别的系统资源时，系统确认该用户的身份是否真实、合法和惟一的过程。身份认证可以防止非法人员进入系统，防止非法人员通过违法操作获取不正当利益、访问受控信息、恶意破坏系统数据的完整性。身份认证可以归纳为三大类：

（1）根据你所知道的信息来证明你的身份，假设某些信息只有你本人知道，如暗号、密码等，通过询问这个信息就可以确认你的身份。

（2）根据你所拥有的东西来证明你的身份，假设某一件东西只有你本人拥有，如 IC 卡、 USB Key 、单位数字证书等，通过输入这些信息也可以确认你的身份。

（3）根据你独一无二的身体特征来证明你的身份，比如指纹、面貌等。

5．防火墙技术

防火墙是信息安全中最重要也是最常用的技术。防火墙（Firewall）是指在本地网络与外界网络之间的一道防御系统，是这一类防范措施总称。防火墙是在两个网络通信时执行的一种访问控制规划，它能允许“被同意”的人和数据进入本地网络，同时将“不被同意”的人和数据拒之门外，最大限度地阻止网络中的黑客来访问本地网络。防火墙是一种非常有效的网络安全模型，通过它可以使企业内部局域网与Internet之间或者与其他外部网络互相隔离、限制网络互访，从而达到保护内部网络的目的。

（1）防火墙是网络安全的屏障。防火墙（作为阻塞点、控制点）能极大地提高内部网络的安全性，并通过过滤不安全的服务而降低风险。由于只有经过精心选择的应用协议才能通过防火墙，所以网络环境变得更安全。

（2）防火墙可以强化网络安全策略。通过以防火墙为中心的安全方案配置，能将所有安全软件（如口令、加密、身份认证、审计等）配置在防火墙上。与将网络安全问题分散到各个主机上相比，防火墙的集中安全管理更经济。

（3）对网络存取和访问进行监控审计。如果所有的访问都经过防火墙，那么防火墙就能记录下这些访问，并进行日志记录，同时也能提供网络使用情况的统计数据。当发生可疑动作时，防火墙能进行适当的报警，并提供网络是否受到监测和攻击的详细信息。

（5）防止内部信息的外泄。通过利用防火墙对内部网络的划分，可实现内部重点网段的隔离，从而限制了局部重点或敏感网络安全问题对全局网络造成的影响。另外，隐私是内部网络非常关心的问题，一个内部网络中不引人注意的细节可能包含了有关安全的线索而引起外部攻击者的兴趣，甚至因此而暴露了内部网络的某些安全漏洞。使用防火墙就可以隐蔽那些透漏内部细节的服务，如 Finger 服务器，DNS 等。

目前防火墙已经在Internet上得到了广泛的应用。但是，防火墙并不能解决所有的网络安全问题，而只是网络安全政策和策略中的一个组成部分，了解防火墙技术并学会在实际操作中应用防火墙技术，对于维护网络安全具有非常重要的意义。

1.3 计算机病毒和防病毒知识

1.3.1 计算机病毒的定义

编制者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码被称为计算机病毒（Computer Virus），其具有非授权可执行性、隐蔽性、破坏性、传染性、可触发性。

1.3.2 计算机病毒的特点

计算机病毒具有以下几个特点。

（1）寄生性。计算机病毒寄生在其他程序之中，当执行这个程序时，病毒就起破坏作用，而在未启动这个程序之前，它不易被人发觉的。

（2）传染性。计算机病毒不但本身具有破坏性，更有害的是具有传染性，一旦病毒被复制或产生变种，其速度之快令人难以预防。

（3）潜伏性。有些病毒像定时炸弹一样，可预先设计发作时间。比如黑色星期五病毒，等到条件具备的时候病毒程序自启动，对系统进行破坏。

（4）隐蔽性。计算机病毒具有很强的隐蔽性，有的可以通过防病毒软件检查出来，有的根本就查不出来，有的时隐时现、变化无常，这类病毒处理起来通常很困难。

1.3.3 计算机病毒的类型

1．按照病毒的破坏情况分类

（1）良性病毒。良性病毒是指其不包含立即对计算机系统产生直接破坏作用的代码。这类病毒为了表现其存在，只是不停地进行扩散，从一台计算机传染到另一台，并不破坏计算机内的数据。

（2）恶性计算机病毒。恶性病毒是指在其代码中包含有损伤和破坏计算机系统的程序，在其传播或发作时会对系统产生直接的破坏作用。

2．按照计算机病毒攻击的系统分类

（1）攻击DOS系统的病毒。这类病毒出现最早。

（2）攻击 Windows 系统的病毒。由于 Windows 的图形用户界面（GUI）和多任务操作系统深受用户的欢迎，因此是病毒最多的一种。

（3）攻击 UNIX 系统的病毒。当前，UNIX 系统应用非常广泛，并且许多大型的企业均采用 UNIX 作为其服务器主要的操作系统，所以 UNIX 病毒的出现，对人类的信息处理也是一个严重的威胁。

（4）攻击 OS/2 系统的病毒。

3．按照病毒的攻击机型分类

（1）攻击微型计算机的病毒。这是世界上传染最为广泛的一种病毒。

（2）攻击小型机的计算机病毒。

（3）攻击工作站的计算机病毒。

4．按照计算机病毒的链接方式分类

由于计算机病毒本身必须有一个攻击对象以实现对计算机系统的攻击，计算机病毒所攻击的主要对象是计算机系统的可执行程序。

（1）源码型病毒。这种病毒攻击高级语言编写的程序，该病毒在高级语言所编写的程序编译前插入到源程序中，经编译后成为可执行程序的一部分。

（2）嵌入型病毒。这种病毒是将自身嵌入到现有程序中，把计算机病毒的主体程序与其攻击的对象以插入的方式链接。这种计算机病毒是难以编写的，一旦侵入程序体后也比较难消除。如果同时采用多态性病毒技术，超级病毒技术和隐蔽性病毒技术，将给当前的反病毒技术带来严峻的挑战。

（3）外壳型病毒。外壳型病毒将其自身包围在主程序的四周，对原来的程序不作修改。这种病毒最为常见，易于编写，也易于发现，只要测试原文件的大小即可发现。

（4）操作系统型病毒。这种病毒用它自己的程序加入或取代操作系统的部分模块进行工作。它们在运行时，用自己的处理逻辑取代操作系统的部分原程序模块，当被取代的操作系统模块被调用时，病毒程序得以运行。操作系统型病毒具有很强的破坏力，可以导致整个系统的瘫痪。

5．按照计算机病毒的寄生部位或传染对象分类

根据寄生部位或传染对象分类，可以分为以下几种。

（1）磁盘引导区传染的计算机病毒。磁盘引导区传染的病毒主要是用病毒的全部或部分逻辑取代正常的引导记录，而将正常的引导记录隐藏在磁盘的其他地方。由于引导区是磁盘能正常使用的先决条件，因此，这种病毒在运行的一开始（如系统启动）就能获得控制权，其传染性较大。

（2）操作系统传染的计算机病毒。操作系统是一个计算机系统得以运行的支持环境，它包括.com、.exe 等许多可执行程序及程序模块。操作系统传染的计算机病毒就是利用操作系统中所提供的一些程序及程序模块寄生并传染的。通常，这类病毒作为操作系统的一部分，只要计算机开始工作，病毒就处在随时被触发的状态。而操作系统的开放性和不绝对完善性给这类病毒出现的可能性与传染性提供了方便。操作系统传染的病毒目前广泛存在，“黑色星期五”即为此类病毒。

（3）可执行程序传染的计算机病毒。可执行程序传染的病毒通常寄生在可执行程序中，一旦程序被执行，病毒也就被激活，病毒程序首先被执行，并将自身驻留内存，然后设置触发条件，进行传染。

6．按照传播媒介分类

按照计算机病毒的传播媒介来分类，可分为单机病毒和网络病毒。

（1）单机病毒。单机病毒的载体是磁盘，常见的是病毒从软盘或 U 盘传入硬盘，感染系统，然后再传染给其他软盘或 U 盘，再传染其他系统。

（2）网络病毒。网络病毒的传播媒介不再是移动式载体，而是网络通道，这种病毒的传染能力更强，破坏力更大。

1.3.4　计算机病毒的表现形式

计算机受到病毒感染后，会表现出不同的症状，下面把一些常见的现象列出来，供用户参考。

（1）计算机不能正常启动。加电后计算机不能启动，或者可以启动，但所需要的时间比原来的启动时间变长了。有时也会突然出现黑屏现象。

（2）系统运行速度降低。如果发现在运行某个程序时，读取数据的时间比原来长，存取文件的时间都增加了，那就可能是由于病毒造成的。

（3）内存空间迅速变小。由于病毒程序要进驻内存，而且又能“繁殖”，因此使内存空间变小甚至变为“0”，导致内存溢出错误。

（4）文件内容和长度有所改变。一个文件存入磁盘后，本来它的长度和其内容都不会改变，可是由于病毒的干扰，文件长度可能改变，文件内容也可能出现乱码。有时文件内容无法显示或显示后又消失了。

（5）经常出现宕机现象。正常的操作是不会造成宕机的，如果计算机经常宕机，那可能是由于系统被病毒感染了。

（6）外部设备工作异常。因为外部设备受系统的控制，如果计算机中有病毒，那么外部设备在工作时可能会出现一些异常情况。

以上仅列出一些比较常见的病毒表现形式，肯定还会遇到一些其他的特殊现象，这就需要由用户自己判断了。

1.3.5 计算机病毒的传播

计算机病毒的传播方式主要包括以下几种。

（1）存储介质。包括软盘、硬盘、移动 U 盘和光盘等。在这些存储设备中，尤其以软盘和移动 U 盘是使用最广泛的移动设备，也是病毒传染的主要途径之一。

（2）网络。随着 Internet 技术的迅猛发展，Internet 在给人们的工作和生活带来极大方便的同时，也成为病毒滋生与传播的温床，当人们从 Internet 下载或浏览各种资料的同时，病毒可能也就伴随这些有用的资料侵入用户的计算机系统。

（3）电子邮件。当电子邮件（Email）成为人们日常生活和工作的重要工具后，电子邮件病毒无疑是病毒传播的最佳方式，近几年出现的危害性比较大的病毒几乎全是通过电子邮件方式传播。

1.3.6 计算机病毒的检测与防治

1．病毒防治策略

要采用“预防为主，管理为主，清杀为辅”的防治策略。

（1）不使用来历不明的移动存储设备（如软盘、光盘、U 盘等），不浏览非法网站、不阅读来历不明的邮件。

（2）系统备份。要经常备份系统，以便被病毒侵害后能够进行快捷恢复。

（3）安装防病毒软件，经常查毒、杀毒。

2．杀毒软件

杀毒软件一般由查毒、杀毒及病毒防火墙三部分组成。

（1）查毒过程。毒软件对计算机中的所有存储介质进行扫描，若遇到文件中某一部分代码与杀毒软件中的某个病毒特征值相同，就向用户报告发现了某病毒。

由于新的病毒不断出现，为保证防病毒程序能不断认识这些新的病毒程序，防病毒软件供应商会及时收集世界上出现的各种病毒，并建立新的病毒特征库向用户发布，用户要及时下载这种病毒特征库才有可能抵御网络上层出不穷的病毒的侵袭。

（2）杀毒过程。在设计杀毒软件时，按病毒感染文件的相反顺序写一个程序，以清除感染病毒，恢复文件原样。

（3）病毒防火墙。当外部进程企图访问防火墙所保护的计算机时，防火墙将直接阻止这样的操作，或者询问用户并等待用户命令。

当然，杀毒软件具有被动性，一般需要先有病毒及其样本才能研制查杀该病毒的程序，不能查杀未知病毒，有些软件虽声称可以查杀新的病毒，其实也只能查杀一些已知病毒的变种，而不能查杀一种全新的病毒。

3．网络病毒的防治

（1）基于工作站的防治技术。工作站就像是计算机网络的大门，只有把好这道大门，才能有效防止病毒的侵入。工作站防治病毒的方法有 3 种：一是软件防治，即定期或不定期地用反病毒软件检测工作站的病毒感染情况，软件防治可以不断提高防治能力；二是在工作站中安装防病毒卡，防病毒卡可以达到实时检测的目的；三是在网络接口卡上安装防病毒芯片，它将工作站存取控制与病毒防护合二为一，可以更加实时有效地保护工作站及通向服务器的桥梁。实际应用中，应根据网络的规模、数据传输负荷等具体情况确定使用哪一种方法。

（2）基于服务器的防治技术。网络服务器是计算机网络的中心，是网络的支柱。网络瘫痪的一个重要标志就是网络服务器瘫痪。目前基于服务器的防治病毒的方法大都采用防病毒可装载模块，以提供实时扫描病毒的能力。有时也结合在服务器上安装防毒卡的技术，目的在于保护服务器不受病毒的攻击，从而切断病毒进一步传播的途径。

（3）加强计算机网络的管理。计算机网络病毒的防治，单纯依靠技术手段是不可能十分有效地杜绝和防止其蔓延的，只有把技术手段和管理机制紧密结合起来，提高人们的防范意识，才有可能从根本上保护网络系统的安全运行。首先应从硬件设备及软件系统的使用、维护、管理、服务等各个环节制定出严格的规章制度，对网络系统的管理员及用户加强法制教育和职业道德教育，规范工作程序和操作规程，严惩从事非法活动的集体和个人。其次，应有专人负责具体事务，及时检查系统中出现病毒的症状，在网络工作站上经常做好病毒检测的工作。

网络病毒防治最重要的是：应制定严格的管理制度和网络使用制度，提高自身的防毒意识；跟踪网络病毒防治技术的发展，尽可能采用行之有效的新技术、新手段，建立“防杀结合、以防为主、以杀为辅、软硬互补、标本兼治”的最佳网络防病毒安全模式。

1.4　信息法律制度与信息道德规范

在信息化高度发展的今天，人们被现代信息技术所包围，人们的生活、学习越来越多地依赖信息技术所构建的网络虚拟世界。各种不同文化背景、不同价值和行为取向的人在这个虚拟世界里发生碰撞，如果没有完善的信息管理机制和技术防范手段，它就不会有序运转，会产生各种问题并对人们的现实生活产生不良影响。基于此，世界各国政府及组织纷纷提出了总体原则一致、细则各有不同的信息道德原则，制定了网络信息安全政策法规，目的旨在制约人们遵守信息社会法律制度，规范人们的信息道德行为。

1.4.1　信息法律制度

信息法律是指在调整信息活动中产生的社会关系的法律规范的总称，是对人们信息活动进行调控的法律措施，主要针对开发信息系统、处理信息的组织和对信息负有责任的个人。

一个国家的信息法律，主要包括知识产权法、信息安全法、信息公开法、电信法、电子商务法（电子签名与数字认证法等）、网络新闻信息传播法，还有专门针对有关计算机犯罪的法律等，涉及到信息的采集、加工、传播和利用等方方面面。

我国在信息技术活动的发展过程中，国家非常重视相应的法制建设，近年来颁布了一系列关于信

息技术发展与管理的法律法规，例如，我们国家就制定有《信息网络传播权保护条例》、《互联网信息服务管理办法》等，基本构筑了我国关于信息活动的法律法规体系。

1.4.2 信息道德规范

在信息传播交流活动中，只有信息法律法规是不够的，还需要建立起信息行为道德规范，作为信息法律制度的补充，对人们信息活动进行约束，以适应社会发展，满足社会道德规范。

信息道德是指在信息领域中用以规范人们相互关系的思想观念与行为准则，是在信息的采集、加工、存储、传播和利用等信息活动各个环节中，人们的道德意识、道德规范和道德行为的表现。信息道德受社会整体道德水平的影响，是社会道德水平的反映。

信息道德是约束人们信息行为的一种手段，它通过社会舆论、传统习俗等，使人们形成一定的观念和习惯，潜意识的存在于人们的头脑中，在信息活动中会促使人们自觉地通过自己的判断规范自己的信息行为。

信息道德与信息法律、法规、政策有密切的关系，它们是从不同的角度实现对信息及信息行为的规范和管理。信息道德以其巨大的约束力在潜移默化中规范人们的信息行为，是人们在外界的约束下自我形成的，各人水平不一。对不自觉、缺乏道德约束的人或道德约束无法涉及的信息领域，就必须制定相应的信息法律法规，以法制手段调节、约束人们的信息活动。所以信息法律是强制规范人们信息行为的法律制度，如不遵守则要承担法律后果。信息政策即信息法规属于准法律，它弥补了信息法律滞后的不足，其形式较为灵活，有较强的适应性和实时性，它在不违反现行法律的条件下由国家行政机关颁布，具有一定的强制性。一般而言，信息法律多由信息政策、信息道德上升而来。信息道德、信息政策和信息法律三者相互补充、相辅相成，信息道德是信息政策和信息法律建立和发挥作用的基础，信息政策和信息法律的制定和实施必须考虑现实社会的道德水平，信息法律是信息道德和信息政策的强化，它们在不同层面共同规范、促进人们的信息活动。

1.4.3 知识产权与软件版权保护

在国家制定的一系列信息法律法规中，尤其值得一提的是有关知识产权保护法，在信息技术高度发展的今天，需要我们特别引起重视。

知识产权（intellectual property right，可简称 IP），也称为“知识财产权”，是指“权利人对其所创作的智力劳动成果所享有的财产权利”，一般只在有限时期内有效。各种智力创造，比如发明、软件作品、文学和艺术作品，以及在商业中使用的标志、名称、图像以及外观设计，都可被认为是某一个人或组织所拥有的知识产权。知识产权是一种无形财产，具有专有性、时效性、地域性、认证性的特点。

知识产权是关于人类在社会生产实践中创造的智力劳动成果的专有权利。随着科学技术的发展，智力劳动成果在社会生产力的提高上所起的作用越来越大，为了保护成果创造人的利益，知识产权制度便应运而生，至今天，已日臻完善。目前，我国关于知识产权保护的法律法规主要有：《中华人民共和国知识产权保护法》、《中华人民共和国专利法》、《中华人民共和国商标法》、《中华人民共和国著作权法》，还有《计算机软件保护条例》、《信息网络传播权保护条例》等。这些法律法规的制定，为知识产权人的权益提供了法律保障，极大地调动了人们从事科学研究、技术创新和文艺创作的积极性，推动了社会生产力的提高，促进了人类文明进步和经济发展。

知识产权一般可分为两类，其划分有两种方式。第一种是按智力创造活动和有形标识物划分的，保护人在文化、产业各方面的智力创作活动为内容的归为一类，包括著作权和发明权；另一类则是以保护产业活动中的识别标志为内容的，包括商标权、商号权等。第二种划分方式则是按精神创作活动

和物质产业活动的成果来划分的，以保护和促进精神文化为主的归为著作权一类；以保护和促进物质产业活动为内容的则是归为工业产权一类，如专利权等。

由于科学技术的进步，人类智能产物的表现形式也日益增多，如版面设计、计算机软件、专有技术、集成电路等等，它们也受到产权保护，所以知识产权的范围也在不断扩大。

需要我们注意的是，在网络技术高度发展的今天，出现了大量网络侵权行为。网络侵权主要是网站侵权和网民侵权。网站侵权主要表现在，网站转载别的网站或他人的作品，如软件、文章、图片、音乐、动画等，既不注明出处和作者，也不向相关的网站和作者支付报酬，无论网站是否以赢利为目的，都构成了侵权。因为既使不以赢利为目的，但把属于别人的作品放在自己网站上供用户免费浏览、下载，间接造成了著作权人的损失。网民的侵权多为无意识的被动性侵权，例如，在论坛、博客、微信公众圈等言论公开的虚拟社区领域，大多数网民并不知道自己使用别人的作品如不注明出处和作者或向作者支付报酬，是一种侵权行为，虽然大多数网民主观上没有恶意。当然，如果是复制别人的作品以自己的名义发表那就是抄袭，属于主动的和恶意的侵权。不过，在自己的作品中引用（注明作品的出处和作者）是个例外，但权利人明确声明未经同意不得使用（转载、复制）的，须事先征得权利人的同意，否则一样构成侵权。

1.4.4 中小学教师信息素养与信息道德

要知道什么是信息素养，先得弄清楚什么是信息素质，这两个概念常常混淆混用。

信息素质（Information Quality），是人的素质的一部分，是人在社会信息知识、信息意识、接受教育、内外环境等因素影响下形成的一种稳定的、基本的、内在的个性心理品质。主要包含四个方面：信息意识、信息能力、信息道德、终身学习能力。其中信息能力是核心，即人们明确信息需求、选择信息、检索信息、分析信息、综合信息、评估信息、利用信息的能力。信息素质的形成既受后天环境因素的影响，也有先天个性因素的品质。

信息素养（Information Literacy）最早的标准定义由美国图书馆协会于 1989 年提出，是指个体能够认识到需要信息，并且能够对信息进行检索、评估和有效利用的能力。随着信息技术应用范围的迅猛发展，人们信息素养的概念也在不断深化。现在普遍认为信息素养是一个含义广泛的综合性概念，信息素养是人们对信息文化适应和创新的能力。首先，信息素养是一种基本能力，是一种对信息社会的适应能力，它涉及信息的意识、信息的能力和信息的应用。然后，信息素养是一种综合能力，涉及各方面的知识，是一个特殊的、涵盖面很宽的能力，它包含人文的、技术的、经济的、法律的诸多因素，和许多学科有着紧密的联系。它不仅包括利用信息资源和信息工具的能力，还包括获取识别信息、加工处理信息、传递创造信息的能力，更重要的是要在信息活动中具有独立自主的学习态度和方法、批判精神、强烈的社会责任感和参与意识、信息法律意识以及创新精神，不仅要适应信息文化，还要创新信息文化。掌握信息技术有助于信息素养的提高，但不是全部，信息素养是全方位的信息能力，信息技术只是它的一种工具。

信息素养的概念内涵由最初的“利用信息解决问题的技术、技能”逐渐发展最后成为包括信息意识、信息知识、信息能力、信息道德等涉及社会政治、经济、法律等各个领域的综合性概念。随着社会的不断发展，信息素养的内涵与外延还会不断丰富和扩大。

从上述概念描述可以发现，信息素质和信息素养的概念高度近似，主要包括信息意识、信息知识、信息能力、信息道德四个方面，强调的都是信息能力，只是信息素养是由后天养成，信息素质部分与先天因素有关。这就是为什么我们经常将两个概念混淆混用的原因。

当然，由于个人的社会地位不同，工作性质不一样，对不同的人，其信息素养水平的要求也因人而已。一般来说，根据在信息社会中与信息技术密切程度的不同可以将信息素养要求分为三个层次。

第一层次是作为一般公民所需要具有的基本信息素养即公民信息素养，这是对所有公民的最基本要求。它要求公民具有最基本的信息能力，表现为在信息意识上，是否接受信息、是否参与信息活动；在信息道德上，能判断信息行为对或错；在信息知识上，是否知道最基本的信息知识；在信息技术能力上，是否会操作最基本的信息系统、工具或软件等，如最常用的信息技术系统的操作能力、通用软件的使用、基本的信息资源利用能力，掌握基本办公软件，能够收发电子邮件，能够在网络进行基本的信息搜索等。

第二层次是作为信息技术系统应用人员所需要的信息素养即应用者信息素养。应用者信息素养比公民信息素养要求要更高一些。由于应用者的应用领域不同，其信息知识和应用能力的具体要求也不同。一般来说，要有更宽广的信息知识、更强的信息应用能力、更高的信息道德修养。具体来说，要有本专业领域的信息知识；要具有利用信息技术系统中的信息理解、选择、批判、收集、处理以及生成、表达等能力；掌握通用工具软件的应用能力；掌握本专业领域专用软件的应用能力，能够充分发挥工具的功能，制作与开发出各种各样的信息产品；由于更多地从事信息技术活动，需要更深地理解信息伦理道德，更好地遵守信息道德法律。

第三层次是针对信息技术系统开发设计人员所提出的开发设计者信息素养。系统开发人员需要掌握更多的信息技术知识，更高的信息技术能力，这样才能开发出更好的信息技术产品。他们通常在信息意识方面十分强烈，由于深知信息技术的高科技性，他们相当注意信息产业的知识产权问题和安全问题。系统开发人员需要具有高度的信息道德伦理修养和信息法律意识，才能使他们开发的产品有益于人类社会的发展而不是有害。

那么，作为中小学教师或者未来是教师的师范生，我们要具备怎样信息素养？并且怎样去努力培养学生的信息素养呢？

毫无疑问，教师作为一名公民，首先应该具有最基本的公民信息素养。即要求了解信息技术的基本知识，拥有基础信息技术系统的基本操作能力，会使用基本的信息工具，对信息技术敢想敢用，能初步辨别信息的真伪。

其次，教师的基本职责是教书育人，承担着培养人类社会的继承者与接班人、未来社会的建设者的重任。从信息技术的角度来说，教书，就是要利用信息技术的手段向学生高效率地传授知识，这就要求教师具有较高的信息技术应用能力；育人，就是要在教育活动中培养学生的信息素养。因此对教师的信息素养必然高于公民信息素养。

教师的职业特点要求教师具有独特的应用人员信息素养。

（1）从信息意识看。教师的信息意识是指教师对信息潜在的广度和敏锐度，捕捉、分析、判断、吸收和应用信息的自觉程度。教师的信息意识包括教师的教育预见能力和对教育教学环境的潜在认识等。教育预见能力是指教师能根据当前社会各领域，尤其是信息技术的发展水平和方向，预见这些发展可能带来的影响，采取具有前瞻性的教育措施和对策，制定更加科学的教育目标和教学策略。信息社会的教育，要求教师习惯于使用网络与其他信息技术来解决教育教学中的问题，教师要善于从网络纷繁复杂的信息中提取出与本学科有关的知识，不断了解和掌握本学科及相关学科的新动向，并将其与课本上的知识信息有机结合，注意信息技术与学科间的整合，以新的知识信息开阔学生视野，启迪学生思维。在具体的教学过程中，教师要有意识地借助计算机和网络，帮助学生适应、使用它们，教会学生如何查找信息、发现知识；然后，教师要能够在学生面对众多信息不知所措时，帮助他们选择和组织信息；最后教师要教会学生面对信息的态度，教会学生以一种兼有批判、创新精神的态度去对待眼前呈现出来的信息。

（2）从信息知识看。中小学教师的信息知识除包括信息技术的基本知识外，还要包括作为中小学教师应该掌握的与教育教学相关的信息技术知识。主要有以下三个方面的知识：一是了解信息技术在

现代社会特别是教育领域中的地位与作用，了解信息技术发展的历史和趋势，掌握微型计算机系统的结构与组成，了解信息知识产权与信息安全等知识。二是了解信息技术在教学中应用的模式和基本理论，具有比较先进的、与信息技术相适应的教育思想和观念，掌握信息技术与学科教学整合的理论与实践知识；三是掌握现代信息技术基本操作知识，掌握将 Internet 的信息服务应用于教学工作的方法，熟悉与计算机和网络相关的其他信息技术的知识。

（3）从信息能力看。中小学教师的信息能力概括起来就是两个层面的能力：一是掌握信息知识、驾驭信息和信息化环境下终生学习的能力，具体来说表现在利用信息设备和信息渠道获取信息、加工处理信息、创造信息以及批判性地评价信息的能力；信息系统的基本操作能力；各种软件尤其是本学科的专业软件的应用能力；教育资源的开发与利用能力，体现在对教育信息的采集、传播、组织、表达及加工处理等方面的能力；通过各种网络信息渠道、运用各种信息技术工具进行终生学习和研究的能力等。二是运用信息技术进行教育教学科研的能力。在新的形势下，教师要有信息化教育观念，树立信息化环境下新的学生观，所以教师不仅要自身具有利用信息技术进行教育教学的能力，还要有教会学生利用信息技术进行学习的能力。信息社会中，一位具有很高信息素养的教师应具有现代化的教育思想、教学观念，掌握现代化的教学方法和教学手段，对信息和网络积极认同，深入了解且有良好的悟性，能熟练运用信息工具对信息资源进行有效地收集、组织、管理、运用，实现最优化的教育效果，能通过网络与学生家长或监护人交流，在教学中营造浓郁的现代信息技术运用氛围，在潜移默化的教育环境中培养学生的信息意识。其教育教学能力主要表现在：运用信息技术进行教学设计的能力；运用信息技术工具，将数字化教育教学资源融合到课程教学过程中，采用信息技术设备、手段和形式（如多媒体课件）进行数字化教学的能力；运用信息技术工具科学评价教学效果的能力；还有能运用信息技术进行教学科研、不断总结教学经验、不断提升自我的能力。

（4）从信息道德看。中小学教师不仅是教书，更重要的是育人，处处以高尚的师德示人，做遵纪守法的模范。这就要求中小学教师要具有高尚的信息道德情操，更高的信息伦理道德修养，做信息道德的表率。除个人要模范遵守信息法律法规和信息道德规范外，必须对信息的共享性及其他性质有充分的认识，在对信息的获取、加工、处理、存储、传播过程中要恪守一定的信息道德与伦理，并言传身教，以身作则地教育学生。要针对信息技术对学生的各种负面影响，在教学中渗透信息道德规范教育，必须培养学生正确的信息伦理道德修养，使他们能够遵循信息应用人员的伦理道德规范，知道信息法律法规，知道信息知识产权保护，知道如何防止计算机病毒和其他计算机犯罪活动，不做不道德或者非法、违法犯罪活动。

本章小结

信息技术是关于信息的产生、收集、交换、存储、传输、显示、识别、提取、控制、加工和利用等的技术。现代信息技术最主要的是传感技术、通信技术和计算机技术。对普通大众和一般的应用工作者，主要是要掌握计算机技术，这也就是为什么大多数人通常将信息技术等同于计算机技术的原因。信息技术的飞速发展，带给了社会各领域巨大的变化，给人们的生活、学习和工作方式带来了无穷的影响，这就是所谓的信息化社会的由来。但是，在信息化带给人类巨大利益的同时，也给人们带来了信息安全的麻烦和担忧。如何确保信息安全？在我们采取各种信息防范技术，如防火墙技术、防病毒技术等的同时，我们要重视信息法律制度的建立，还要高度重视公民信息道德素养的培养和提高，如果每一个公民都具有高尚的信息道德情操，自觉受社会道德约束，自觉规范信息行为，就可以从源头上消除信息安全隐患。

作为未来的人民教师，在自觉掌握、应用信息技术的同时，还肩负有培养下一代社会建设人才信

息技术素养的重任，要具有强烈的信息意识、高超的信息技术应用能力，更要有高尚的信息伦理道德素养。

习　题

1．什么是信息技术？什么是信息化？
2．什么是信息安全？常见的信息安全措施有哪些？
3．简述防火墙的作用。
4．什么是数字签名技术？
5．计算机病毒有哪些危害？如何防范计算机病毒？
6．我国关于信息技术活动的法律制度有哪些？
7．我国关于知识产权保护的法律制度有哪些？
8．阐述信息素养和教师应具有的信息素养要求。