# 第4章

# 信息社会安全与责任

在全球信息化浪潮的推动下，计算机、网络、大数据等技术迅速发展，并渗透到政治、国防、经济及生活的各个领域，从根本上改变了社会形态及人们的生产生活方式。然而，信息系统安全问题既需要管理层重视相关法律法规的制定与完善，又需要各层面倡导与推广先进的管理手段与技术方法，更需要每一位应用者从国家、社会与合格公民的角度出发，增强信息系统安全风险防范意识,提高防范技术水平，以确保信息系统安全问题得到全面重视与高效格实,维护好国家利益及个人信息安全。

本章将通过自主、协作、探究学习让向学们认识信息系统应用过程中存在的风险，树立信息安全意识；熟悉信息系统安全风险防范的常用技术方法，养成规范的信息系统操作习惯；树立信息社会责任意识，合理使用信息系统，负责任地发布、使用与传播信息，自觉遵守信息社会中的道德准则和法律法规，从而将知识建构、技能培养与思维发展融入运用数字化工具解决问题和完成任务的过程中，促进信息技术学科核心素养达成，完成学习目标。

## 学习目标

- **认识信息系统应用中存在的安全风险，树立信息安全意识；**
- **熟悉并运用信息系统安全风险防范常用技术和方法；**
- **能够利用数字化工具解决项目中遇到的问题。**

# 一 信息系统的安全风险

## 走入情境

“在互联网上，没人知道你是一条狗”（On the Internet,nobody knows you area dog），该漫画于1993年7月由彼得·施泰纳（Peter Steiner）创作，刊登在《纽约客》上，用以描述互联网的匿名特性。今非昔比，随着大数据时代的到来，信息系统每时每刻都在记录着人们的一言一行。用户数据被各种信息系统搜集、分析甚至被交易，可以毫不夸张地说，“在如今的互联网上，每个人都知道你是一条狗”。


图1-1 大数据时代现状

**和你的小组成员一起讨论：**

（1）我们的哪些信息被互联网所记录？

（2）被互联网记录的这些信息给我们带来了哪些便利？产生了哪些安全隐患？

（3）大数据时代的“便利”和“安全”，有怎样的关系？

## 1.1 人为因素造成的安全风险

### 探究活动——认识电信架构

深圳市的张女士在接到使用改号软件假冒银行客服、公安、检察院的一系列电话后，被骗走了44万元。

电信诈骗是指犯罪分子通过电话、网络和短信方式，编造虚假信息，设置骗局，对受害人实施远程、非接触式诈骗，诱使受害人给犯罪分子汇款、转账等犯罪行为。

电信诈骗有哪些常见手段？请同学们通过网络查找，将找到的电信诈骗常见手段填入表格中，并针对电信诈骗可能带来的损失和危害进行讨论。

| 诈骗手段 | 具体实施 | 损失和危害 |
| --- | --- | --- |
| 冒充政府部门进行诈骗 | 声称根据国家政策要对事主购买的汽车、房产或农机具等进行退税、补贴，诱骗受害人持自己的银行卡在ATM上进行操作，骗取钱财 | 造成大量金钱损失 |
| 利用中奖兑换进行诈骗 | | |
| 冒充淘宝客服进行诈骗 | | |
| 利用虚假广告信息进行诈骗 | | |
| …… | …… | …… |

“人”是信息系统的使用者与管理者，是信息系统安全的薄弱环节。信息系统可以拥有最好的技术如防火墙、入侵检测系统等，但如果使用信息系统的人员没有防范意识，信息系统仍然可能面临不同层面的危险。

中国有句古语“解铃还需系铃人”。信息系统安全是个社会系统工程，除了从政府层面加强立法工作，还需要不断提高关键安全技术水平，更需要使用者全面提高道德意识与技术防范水平。

## 思考讨论

你在日常生活中是否经历过电信诈骗呢？说你是如何判别电信诈骗的？和小组同学一起讨论交流。

## 1.2 自然灾害因素造成的安全风险

2017年，美国发生的洪水、飓风、龙卷风等灾害，墨西哥发生的地震灾害，在摧毁众多信息设备和信息系统的同时，也破坏了大量的信息数据和电子文件。2016年，我国多地遭受特大暴雨的袭击，多处通信光缆被洪水冲断，电力设备被损坏，正常的手机通信受到影响。

图1-2 美国龙卷风灾害

图1-3 中国干旱灾害

水灾、火灾、雷电、地震、龙卷风等自然灾害会对信息系统的安全造成威胁，这些非人为的不可抗力可能会引起数据丢失、设备失效、线路中断等安全事件的发生。另外，静电、灰尘、温度、湿度、虫蚁鼠害等环境因素，也会导致信息系统出现故障甚至瘫痪。

图1-4 中国洪涝灾害


图1-5 美国山火灾害

## 1.3 软硬件因素造成的安全风险

### 探究活动——软硬件漏洞危害及信息系统安全

2017年10月，出现了针对物联网设备的病毒。这种病毒利用连接到互联网的路由器、摄像头等设备中的漏洞，把僵尸程序传播到互联网上，感染并控制大批在线主机,形成了一个大面积僵尸网络群，危害指数非常高。

2017年12月，利用某办公软件漏洞实施的后门攻击呈爆发趋势。恶意文档通过带有“订单”“产品购买”等垃圾邮件的附件进行传播，诱骗用户点击并盗取用户隐私。2018年1月，安全研究人员在某处理器中发现了重大的安全漏洞，攻击者可以从应用程序运行内存中窃取电子邮件、照片、文档等数据。为此，操作系统提供商也紧急发布了操作系统的相关更新补丁。

系统漏洞是指在硬件、软件、网络协议的具体实现或系统安全策略上存在的缺陷。漏洞可能来自应用软件或操作系统编码时产生的错误,也可能来自硬件设备设计时的缺陷。这些错误、缺陷一旦被有意或无意利用,就可能造成用户数据被篡改、重要资料被窃取、信息系统被攻击等事件。特别是随着物联网的广泛应用，一旦出现漏洞,危害范围非常大。

自信息系统发布的那天起,随着用户的深入使用，系统中存在的漏洞就会不断暴露出来，虽然开发者会发布补丁程序来修补已暴露的漏洞，但是很可能会引入一些新的漏洞和错误。随着时间的推移，旧的漏洞会不断消失，新的漏洞会不断出现，漏洞问题。

### 拓展延伸

#### 后门程序

除了系统漏洞外，一些操作系统中还可能存在后门程序。后门程序是指留在计算机系统中，供极少数特殊使用者绕过安全性控制而获取对程序或系统访问权的程序。在软件的开发阶段，程序员常常会在软件内创建后门程序，以便及时修改程序设计中的缺陷。但是，如果这些程序被别有用心的人知道，或者在发布软件之前没有被删除，那么就容易被黑客当成漏洞进行攻击，从而引发安全风险。

保护信息系统中的硬件免受危害或窃取，通常采用的方法是:先把硬件作为物理资产处理，再严格限制对硬件的访问权限，以确保信息安全。保护好信息系统的物理位置及本身的安全是重中之重，因为物理安全的破坏可直接导致信息的丢失。软件是信息系统中最难实施安全保护的部分，主要反映在软件开发中产生的错误，如漏洞、故障、缺陷等问题。在生活中，智能手机崩溃、存在控制缺陷的汽车被召回等事件，都是软件开发过程中安全问题后置或为节省时间、资金、成本与人力等因素造成的。

### 体验探索

请咨询老师或专业人员，也可以上网查询资料，了解并梳理学校校园网的安全防护措施，填写在下列表格中。

| | 名称 | 防护功能 |
|---|---|---|
| 硬件 | | |
| 软件 | | |

## 1.4 网络因素造成的安全风险

无线网络存在巨大的安全隐患，免费Wi-Fi热点有可能就是钓鱼陷阱，家里的路由器也可能被恶意攻击者攻破。网民在毫不知情的情况下，个人敏感信息可能会遭盗取，甚至造成直接的经济损失。

### 情境探究

#### 情景一：Wi-Fi热点下的钓鱼陷阱

许多商家为招揽客户，会提供Wi-Fi接入服务，当客人发现有免费的Wi-Fi热点时，很可能会不假思索地选择接入。黑客提供一个名字与商家类似的免费Wi-Fi接入点，吸引网民接入。一旦连接到黑客设定的Wi-Fi热点，上网的所有数据包，都会经过黑客设备转发，这些信息都可以被截留下来分析，一些没有加密的通信就可以被直接查看到。

### 情景二：无线网络中的漏洞攻击

攻击者首先会使用各种黑客工具破解无线路由器的连接密码，如果破解成功，黑客就可以成功连接路由器，与用户共享一个局域网。攻击者除了免费享用网络带宽，还会尝试登录无线路由器管理后台，篡改各个用户的信息。

**讨论：**

你有在工共场所任意接入免费开放Wi-Fi的习惯吗？你认为免费开放Wi-Fi有什么存在的安全风险？

信息系统经常会受到来自犯罪组织、黑客、恶意竞争者、不怀好意者的恶意攻击。这些人通过各种方式修改或者破坏信息系统,对系统安全造成威胁。

(1) **搭线窃听。**由于连接信息系统的通信网络存在漏洞，黑客会窃听网络上传输的信息，通过信号处理和协议分析，从中获得有价值的信息。

(2) **伪装成合法用户。**黑客通过嗅探、口令猜测、撞库、诈骗等手段非法获取用户名和密码，以合法用户的身份进入信息系统，窃取需要的信息。口令猜测是利用计算机对所有密码进行猜测试验，直到找到正确的密码。诈骗则是通过电话、短信、电子邮件、钓鱼网站等手段欺骗经授权的个人，使之泄露账号或密码。

(3) **利用病毒攻击。**计算机病毒,是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。黑客等找到系统的技术漏洞后，会利用病毒进行恶意攻击，使信息设备出现中毒症状，在干扰正常工作的同时，窃取机密信息。随着手机等移动终端的日益普及，很多新型病毒被植入手机中，通过网页、邮件等网络手段传播。

图1-6 伪装合法用户


图1-7 黑客破坏信息系统

## 1.5 数据因素造成的安全风险

通过信息系统采集、存储、处理和传输的数据，是具有很高价值的资产，其安全性格外重要。

### 思考讨论

阅读以下材料，分析事件成因及处理办法，在小组中分享自己的看法。

**材料一**

某论坛的数据库对用户密码仅使用了简单的MD5加密法，黑客能够快速破解出绝大部分明文密码，这导致2300万用户数据泄漏，这些用户数据包括用户名、注册邮箱、加密后的密码等。

**材料二**

2015年，中国产业信息网公布一起重大信息泄漏事件:全国有超过多个省市的社保系统曝出高危漏洞，统计达5279.4万条，涉及人员数量达数千方，其中包括个人身份证、社保参保信息、财务、薪酬、房屋等敏感信息。市面上随处可售的个人信息，除了一部分是持有信息者主动售卖外，有接近3成的比例来自社保系统的漏洞被利用。

**材料三**

2016年，保监会发函通报某保险公司存在内控缺陷，要求进行整改。保监会指出，该公司在客户信息真实性管理、银邮渠道业务管理、团险业务管理、公司治理、财务基础管理等方面存在问题及内控缺陷。除了公司内控问题外，该公司此前还被曝出存在严重信息系统安全漏洞，面临泄露数以万计客户银行卡号、密码、开户行地址、身份证等敏感信息的风险。

### 实践探究

走访学校、社区、公司等单位，向网站管理员进行咨询，了解单位网站是否曾经遭遇过系统崩溃、信息丢失或数据破坏等的情况，都是什么原因造成的。

撰写一份简短的调查报告。

# 二 信息系统的安全风险防范措施

随着信息系统安全问题的复杂度不断提高，危害信息系统安全的手段、方法也不断变化。人们越来越深刻地认识到信息系统安全不能仅从技术入手，还得从系统的管理角度切入，才能寻找到一个较合理的解决策略。

## 2.1 P2DR安全模型

信息系统安全模型的种类很多，各有特点。下面我们介绍一种常用的安全模型——P2DR模型，如图所示。该模型包括策略（Policy）、防护（Protection）、检测(Detection)和响应（Response)四个主要部分。


图2-1 P2DR模型示意图

### 1 策略

策略指根据风险分析产生的安全策略，描述了系统中哪些资源要得到保护，以及如何实现对他们的保护等。策略是模型的核心，所有的防护、检测和响应都是依据安全策略实施的。网络安全策略一般包括：访问控制策略、加密通信策略、身份认证策略和备份恢复策略等。

### 2 防护

防护是指通过修复系统漏洞、正确设计开发和安装系统来预防安全事件的发生；通过定期检查来发现可能存在的系统脆弱性；通过教育等手段，让用户和操作员正确使用系统，防止意外威胁;通过访问控制、监视等手段来防止恶意威胁。防护技术通常包括数据加密、身份认证、访问控制、授权和虚拟专用网（VPN）技术、防火墙、安

全扫描和数据备份等。

### 3 检测

检测是动态响应和加强防护的依据，通过不断地检测和监控网络系统，来发现新的威胁和弱点，并通过循环反馈来及时做出有效的响应。当攻击者穿透防护系统时，检测功能就发挥作用，与防护系统形成互补。采用的技术一般有实时监控和IT审计。

### 4 响应

响应指在检测到安全漏洞和安全事件时，通过及时的响应措施将网络系统的安全性调整到风险最低的状态。主要方法包括：关闭服务、跟踪、反击、消除影响。

## 2.2 信息系统安全策略分析

对于以计算机及网络为主体的信息系统，其技术安全策略主要分为物理和逻辑两大方面，主要包括物理系统、操作系统、数据库系统、应用系统和网络系统五个层面。

### 1 物理方面

物理方面主要指物理系统层面，包括自然破坏防护机制、质量保护机制、人为破坏防护机制、性能匹配等。其主要措施包括环境保护、防盗、防火、防静电、防雷击、放电磁泄漏等。

| 主要措施 | 具体说明 |
| --- | --- |
| 环境维护 | 包括让硬件设备远离噪声源、振动源，远离火源和易被水淹没的地方，尽量避开强电磁场源：保持设备运行所需的温度：保持系统电源的稳定及可靠性。 |
| 防盗 | 对于重要的计算机系统及外部设备，可安装防盗报警装置及制订安全保护措施。 |
| 防火 | 经常检查重要部门各种电路的安全性，做好各种防火措施。 |
| 防静电 | 配备良好的接地系统，避免静电积储。 |
| 防雷击 | 根据被保护硬件设备的特点和雷电侵入的不同途径，采用相应的防护措施，分类分组保护 |
| 防电磁泄漏 | 包括抑制电磁发射：屏蔽隔离：对于相关干扰，可以采取各种措施使信息相关电磁发射泄漏即使被收到也无法识别。 |

### 2 逻辑方面

逻辑方面主要包括操作系统、数据库系统、应用系统和网络系统四个层面。

（1）操作系统层面：包括系统安全漏洞扫描、用户访问机制、用户身份认证、系统审计、关闭不必要的服务、病毒防护机制等。

（2）数据库系统层面：包括数据库安全漏洞扫描、用户口令管理、用户操作权限控制、数据库审计等。

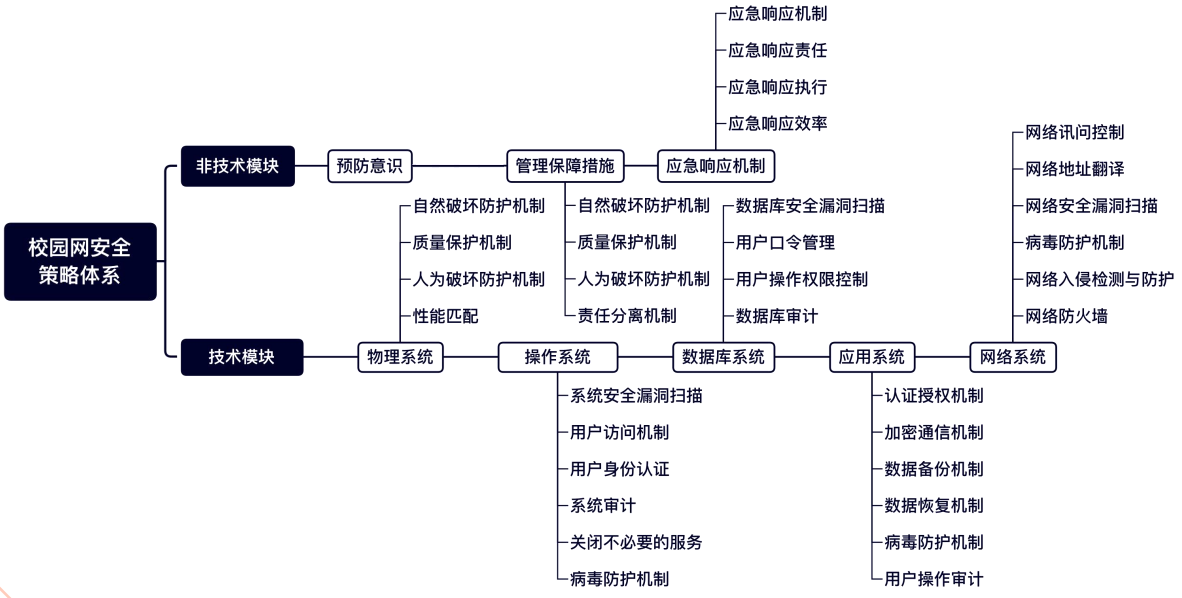
（3）应用系统层面：包括认证授权机制、加密通信机制、数据备份机制、数据恢复机制、病毒防护机制、用户操作审计等。

（4）网络系统层面：包括网络讯问控制、网络地址翻译、网络安全漏洞扫描、病毒防护机制、网络入侵检测及防护、网络防火墙等。

逻辑方面所采取的主要措施有访问控制和信息加密。访问控制是指将未经授权的非法用户拒于系统之外，使之不能进入系统。包括:通过用户身份的识别和认证，可以鉴别合法用户和非法用户，阻止非法用户的访问;通过访问权限控制，即对用户访问哪些资源、对资源的使用权限等加以控制。信息加密是指通过密钥技术，保护在通信网络中传送、交换和存储的信息的机密性、完整性和真实性不被损害。常用的方法主要有数据加密和数字签名。

## 项目实践

请各小组根据P2DR模型和信息系统安全策略分析，对校园网系统进行安全策略分析。参考模型如下：



## 2.3 信息系统安全风险防范常用技术

因为不同的信息技术发展阶段对信息系统安全的关注和需求有所不同，信息系统安全风险防范的常用技术方法总是伴随着问题的不断变化而逐步完善。信息系统安全问题，主要是确保信息在存储、处理和传输过程中免受偶然或恶意的非法泄密、转移或破坏。针对不同的信息安全风险，往往可以从身份认证、设置防火墙、数据加密、主机系统安全技术等方面进行安全防范，以确保信息系统的正常运行。

### 1 身份认证

响应指在检测到安全漏洞和安全事件时，通过及时的响应措施将网络系统的安全性调整到风险最低的状态。主要方法包括：关闭服务、跟踪、反击、消除影响。

**情境创设** 人脸识别技术在火车站的应用

图2-2 人脸识别验票闸机

2016年，北京西站在部分通道启用自助验证验票系统，旅客持车票和身份证，通过人脸识别系统确认后，可以快速进站候车。

2018年，广州、武汉、深圳等火车站启用了人脸识别验票闸机，实现“刷脸进站”。同时，广州南站还启用了人脸识别系统，通过对人像数据的采集，实现甄别违法犯罪嫌疑人、有效寻找走失人员的功能。

身份认证是保护信息系统安全的第一道防线，用来防止未授权的用户私自访问系统。身份认证主要有以下三种方式。

第一种是“用户名+密码”的方式。这是最常见的，也是最原始、最不安全的方式，很容易由于用户无意间泄露或者遭受口令猜等恶意攻击，导致合法用户的身份被伪造。

第二种是使用用户拥有的唯一信物，如银行卡、信用卡、登录网上银行使用的U盾、网络支付时的数字证书等，由合法用户随身携带，随时进行身份验证。

第三种是利用用户自身具备的、独一无二的特征，如人脸、指纹、声音、虹膜、掌纹等生物特征的方式。以人脸识别为例，系统先利用人脸识别系统采集用户的面部特征进行数字化，把数字代码组合成特征模板存储在数据库中。当用户登录系统时，人脸识别系统会将获取的面部特征与数据库中存储的人脸特征数据进行比对，然后根

据比对的结果判断用户的身份是否合法。合法用户可以成功登录系统，不合法的用户会遭到拒绝。

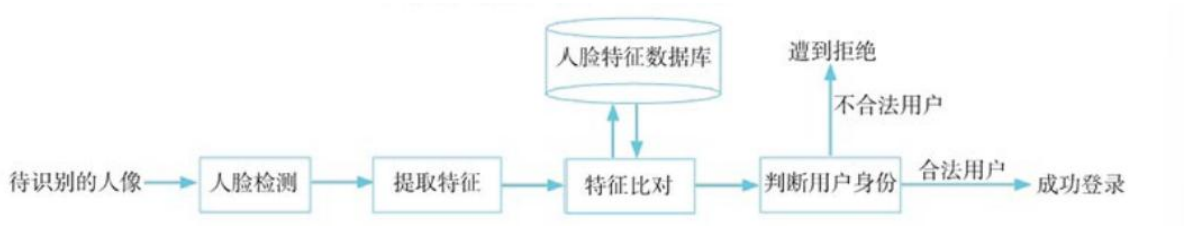



图2-3 人脸识别流程图

### 2 设置防火墙

防火墙是设置在内部网络和外部网络（如互联网）之间维护安全的系统设施。

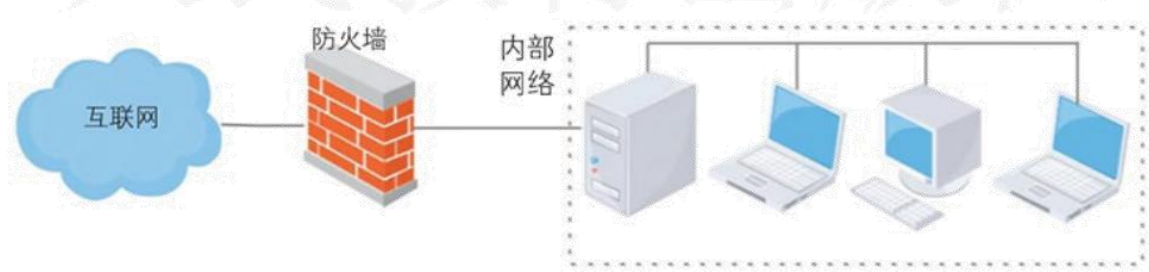



图2-4 防火墙

防火墙具有以下基本功能：过滤进出网络的数据；管理进出网络的访问行为;封堵某些禁止的业务；记录通过防火墙的信息内容和活动；遇到网络攻击时，及时显示警告信息。

随着技术的发展，新一代的防火墙集病毒扫描、人侵检测和网络监视功能于一身，可以在网关处对病毒进行初次拦截，并配合病毒库中的上亿条记录，将绝大多数病毒彻底剿灭在内部网络之外，在有效阻挡恶意攻击的同时，大大降低病毒侵袭所带来的各种威胁。

### 3 数据加密

为防止信息系统中的数据被破坏，可以采用数据加密技术，把被保护的信息转换为密文，然后再进行存储或者传输。数据加密是通过加密算法和加密密钥将明文转变为密文，保护数据在传输过程中不被非法窃取，而解密则是通过解密算法和解密密钥将密文恢复为明文。

数据加密的历史由来已久。例如，凯撒加密是一种较简单且广为人知的加密方法，其明文中的所有字母都在字母表中向后(或向前)按照一个固定数目进行偏移后被替换

成密文。在战争时期，为了防止敌对一方破获消息，即便信息技术很不发达，人们还是想到了通过电报传送消息时采用替代密码、换位密码等加密方法，保证情报的安全性。

现在常用的数据加密算法有私钥加密和公钥加密。私钥加密算法用于加密和解密的密钥是相同的，因此也称为对称密钥加密，密钥需要保密管理。公钥加密算法用于加密消息的加密密钥和用于解密消息的解密密钥不同，因此也称为非对称密钥加密。

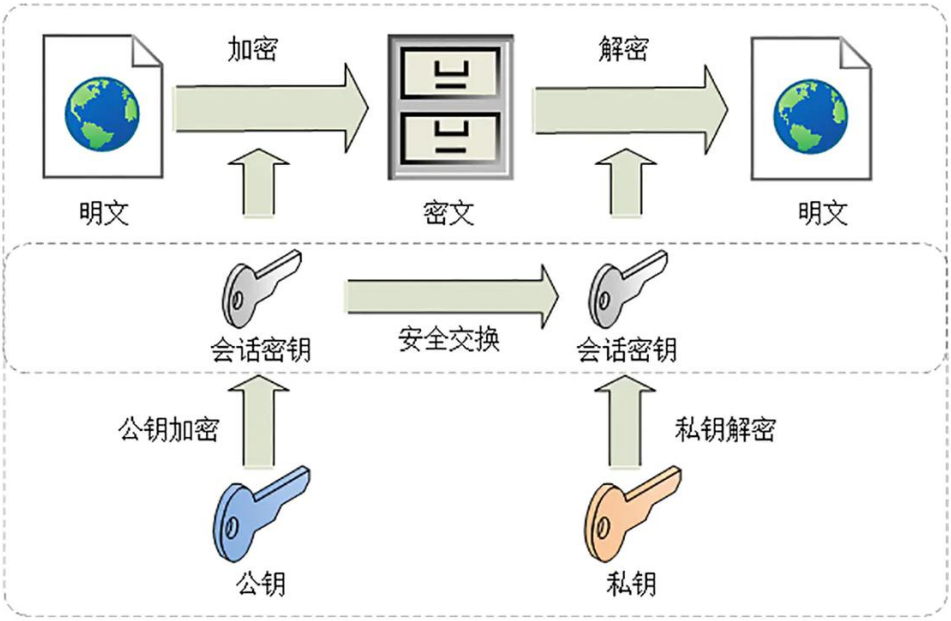



图2-5 公钥加密算法进行加密及解密操作过程图

### 4 主机系统安全技术

主机系统安全技术是指用于保护计算机操作系统和运行于其上的信息系统的技术，具体包括操作系统安全技术、数据库安全技术和可信计算技术等。例如：操作系统安全技术需要解决用户的账户控制、内存与进程保护等;而数据库安全技术需要解决业务数据的完整性、安全检索和敏感数据保护等问题。

（1）操作系统安全技术。

一般地，操作系统安全机制包括用户账号控制机制、强制完整性控制机制、用户界面特权隔离机制、网络访问保护机制等措施。用户账号控制机制的目的在于使用户能够使用标准用户权限而不是管理员权限运行系统，这样用户不会有意或无意地修改系统设置，破坏他人的敏感信息，即使受到恶意软件攻击，也不会导致系统安全设置被篡改，达到增强系统安全性的目的。

（2）数据库安全技术。

数据库安全是涉及信息安全技术领域与数据库技术领域的一个典型交叉学科，它的发展历程与同时代的数据库技术、信息安全技术的发展趋势息息相关。关于数据库安全技术中较有代表性的是安全数据库管理系统、外包数据库安全、云数据库/云存储安全等技术。其中安全数据库管理系统中，除了数据库认证、访问控制、审计等基本安全功能外，关键技术集中在数据库形式化安全模型、数据库加密、多级安全数据库事务模型及数据库隐形通道分析等，外包数据库安全包括外包数据库检索技术、查询验证技术、访问控制技术和数据库水印技术；云数据库/云存储安全主要集中在海量信息安全检索关键技术、海量数据完整性验证及海量数据隐私保护技术等方面。

### 实践探究——数字签名和数字水印认证技术

数字签名就是使用公钥加密等算法，生成别人无法伪造的一段数字串。数字水印是将特定的标记隐藏在数字照片、电子文档等数字产品中，用来保护作者对产品的所有权，防止数字产品被非法复制、传播和篡改。

请同学们尝试下载数字签名软件或数字水印软件，加密自己的文档或图片。

# 三 信息社会责任

## 3.1 树立信息安全意识

信息安全不仅影响到人们日常的生产、生活，还关系到整个国家的安全，成为日益严峻的问题。随着网络通信与互联规模的扩大、媒体信息传播方式的普及，信息安全问题日益突出。

图3-1 信息安全

维护信息安全，可以理解为确保信息内容在获取、存储、处理、检索和传送中，保持其保密性、完整性、可用性和真实性。信息的保密性是指保证信息不泄漏给未经授权的人；完整性是指防止信息被未经授权者篡改;可用性就是保证信息及信息系统确实能够为授权使用者所用;真实性是指对信息及信息系统的使用和控制是真实可靠的。

信息系统安全管理是指通过维护信息的保密性、完整性、可用性和真实性等来管理和保护信息系统资源的一项体制，也包含对信息系统安全保障进行指导、规范和管理的一系列活动和过程。对于信息系统的使用者来说，要掌握信息的特性，树立信息安全意识，负责任地发布、使用与传播信息。

### 思考辨析

查阅学习本章资源包中“信息安全管理体系”部分内容，谈谈你的看法。

作为信息社会的公民，要把国家安全放在第一位，时刻提高警惕提高安全意识，坚决避免被间谍分子所利用，给国家安全造成危害。同时，要提高保密意识，做好信息保密工作，不随意发布我国的军事装备等敏感信息,自觉维护国家安全。


图3-2 网络安全法

## 3.2 信息系统安全操作规范

### 1 获取和鉴别信息

互联网中提供了非常丰富的资源。例如，浏览新闻网站，可以及时了解时事新闻;通过搜索引擎，可以快速找到与学习相关的资料;通过下载软件，可以下载很多学习软件或文档、图片、音视频等。但是网络上也有很多虚假信息,如未经考证的生活信息、诈骗信息、谣言等，对社会稳定造成了一定的破坏。

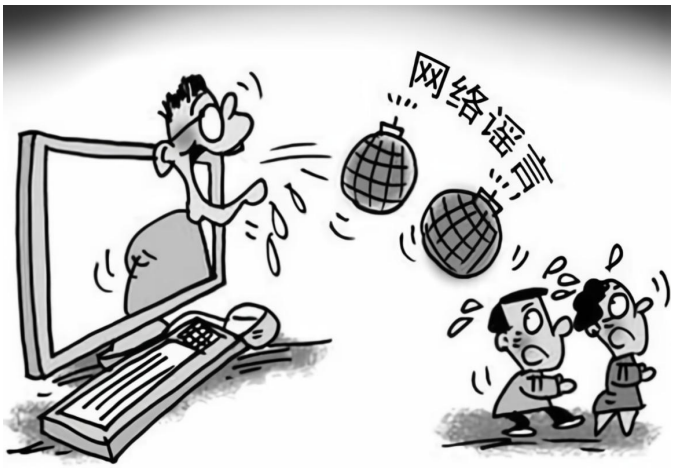



图3-3 网络谣言漫画

一般来说，来自政府机关、科研单位、大专院校、专业机构官网的信息，相对比较权威、可靠。在获取信息时，要根据信息的分类，访问相应的专业机构官方网站、官方公众号等来获取。例如，要查阅时事新闻，可以访问新华社网站;要查阅天气信息，可以访问国家气象局和各省市气象局的官方网站、微博、公众号等;要查阅地震方面的信息，可以访问国家地震局的网站;要查询学校或升学信息，可以访问教育部、

本地教育部门或各大高校的官方网站。

如果要获取的信息不好分类，只能通过搜索引擎搜索时，则要多加分析和思考，必要时请教老师或家长。“兼听则明，偏信则暗。”多渠道地获取信息，并加以比较和分析，是发现问题和疑点的有效方法。针对获取到的信息,要学会冷静、客观地分析来源渠道，多方对比查证鉴别,也可以向专业人士、权威机构求助，以去伪存真。

### 2 交流和表达信息

如今，互联网已经成为很重要的人际交流空间,大家通过聊天软件与他人交流,很多班级会建立网络聊天群，方便随时交流和沟通。在工作和学习中，也经常需要发送邮件进行沟通和交流。

在网上交流时，要使用文明语言。争论问题时，要以理服人，不能使用不文明语言辱骂或攻击对方。当前很多人喜欢使用网络语言进行交流。网络语言虽然比较简洁、生动，但是不够严谨，与我国优秀的传统语言文化有一定的差距。

在网络交流时，要少用、不用网络语言，多使用文明规范词语。对于一些网络用语，要根据场合谨慎使用。例如，给老师发送邮件、书写书面报告、展示演示文稿、发表公告等，应该使用规范的语言文字。

## 拓展延伸

**电子邮件的书写规范**

在我们的日常生活和工作中都会用到电子邮件。在写电子邮件时，首先要写清楚邮件的主题，便于收件人识别。撰写内容时，应遵照普通信件或公文所用的格式和规则，一般包括称呼、问候语、正文、祝语和署名等。邮件的正文要清晰、简洁,不要长篇大论，最好不要出现错别字;用语要文明礼貌，以示对收件人的尊重。如果邮件带有附件（如照片、作业、文档等），发送前一定要同时上传，还要在正文中对附件内容加以说明，以免收件人忽略、忘收或漏收。最后，要定期打开收件箱查看邮件，以免遗漏或耽误重要邮件的阅读和回复。收到邮件后，应及时回复，表达自己的意见。

### 3 发布和转发信息

越来越多的人利用手机、平板计算机等随时随地通过论坛、社交网站、微博、微信等自媒体平台发布、转发和评论信息。可以说，每个会使用互联网的用户都是自媒体的发布者与参与者，“个个都是通讯员，人人皆为传播者”。但是,要注意的是，网络是一个公共场所,不属于个人。个人发出的每一篇文章、每一次转发、每一条评论，都不仅仅是个人行为，更是构筑文明网络环境、和谐社会的基石。

在发布和转发信息时，要自觉遵守网络文明礼仪、道德准则以及国家的法律法规,保证内容的真实性,不能随意发布和转发虚假信息,坚决不能造谣，为营造一个充满正能量的网络空间贡献力量。

## 拓展延伸

**网络“谣”棍**

谣棍的意思是指那些专门造谣，胡说八道，没有一点依据的人。在网络这一虚拟化、匿名化、个性化、环境下，有一大部分人不会对自己的言语负责，导致网络谣言内容分散化，传播目的化。面对技术快速演进叠加复杂社会心态带来的挑战，我们急需严惩网络“谣”棍。

网络“谣”棍群体带来的社会危害非常大：

1. 扰乱人们的思想、心理和行为。人们经常是为了一个虚假的谣言而表现种种不适当的行为，尤其是面对有关自己切身利益的谣传，人们就更加失去了理智，失去了判断力，从而从内心深处觉得这就是真的，一传十，十传百，到最后，弄的人心惶惶。

2. 引发社会动荡，危害公共安全，损害公众利益。由于现在网络谣言的传播速度快，范围广，一旦一些危言耸听的谣言形成了一定规模，就会造成不良的影响，引起广大网民的慌乱，从而造成社会恐慌。

谣言的破坏力很大，危害社会，伤害个人，危害国家稳定，所以我们绝对不能胡乱造谣。网络绝不是法外之地，对屡教不改者依法从严查处！必须通过法律途径对网络谣言进行有效的规制，实现“依法治谣”。

不转发违背道德、违反法律的信息; 不转发广告类和哗众取宠类信息。例如，有的信息会以“这个一定要转发”“快看呀,不看后悔”“出大事了”“震惊内幕”等为标题，企图在人们中间造成恐慌,引起更多人的关注。对这类信息，不要随意转发。

要吸收、传播积极、正面的信息,让自己拥有健康的心理和阳光的心态，对看到、听到的信息要动脑筋思考，不盲目从众、跟风,从自我做起，杜绝不良信息的传播。


图3-2 网络安全法

### 4 信息系统规范操作

随着网络通信与互联规模的扩大、新媒体信息传播方式的普及，使得许多不可能成为可能。因此，信息的可用性、机密性、完整性问题日益突出。例如，大数据带来的个人记录保存、数据挖掘和数据匹配能力技术让个人信息处于一个危险状态，相关非法的案例层出不穷。

**信息系统规范操作的必要性**

(1) 人为因素是信息系统安全问题产生的主要原因。

人为因素是研究信息系统安全管理有效性的一个主要方面。人为因素一般是指工作生活过程中，与人发生相互作用的一切因素。随着社会的发展，任何法规、标准、流程的实现过程，人为因素都有着决定性影响。因此，提高人们的信息安全意识，加强信息安全管理，提高遵守信息安全法律、法规观念等非技术安全策略越来越引起重视，成为衡量一个优秀的安全策略的重要指标。

(2) 规范操作是消除过程因素造成的潜在安全威胁的必要策略。

所谓过程，是指运用信息系统完成特定任务所设定的流程或指令。因此，严格依照这些流程与指令规范地操作信息系统，是避免与消除过程因素造成的潜在安全威胁的必要策略。可以预测的是如果未授权的用户获得此过程，就会对信息系统的安全构成威胁。

**信息系统规范操作及其意义**

信息系统规范操作就是要按照信息系统既定标准、规范的要求进行操作。例如计算机信息系统管理规范中有机房突发事件处理规范、设备维护规范、文档编制规范、数据与软件归档规范等制度，其目的是加强该信息系统的运行管理，提高工作质量和管理有效性，实现计算机系统维护、操作规范化，确保计算机系统安全、可靠运作。

## 3.2 信息社会的道德准则与法律法规

### 1 信息安全道德准则

网络是个虚拟的空间，但是在实际生活中遵循的道德准则，在网络中同样要遵守。在互联网上，不能损害国家利益、公共利益和他人利益是最基本的要求。

维护清朗的网络空间。在网络上，要做到诚信友善,不恶意编造谎言、欺骗他人,更不能有辱骂网友、网络约架等道德败坏的行为。遇到问题时，要多思考、多判断、多请教,不随意跟风，不瞎起哄，从我做起,维护清朗的网络空间(图4.2.10)。同时,要擦亮眼睛,明辨是非美丑，不恶意传播低俗虚假信息，不跟谣传谣,不在朋友圈等范围发布广告和无用信息，让网络充满正面、真实的信息。

维护个人和他人隐私，要做到“三不要”。假如有人在互联网上公开我们的个人信息或者恶意毁损、玷污、丑化我们的肖像，应及时向家长、老师反映，必要时追究其违法行为，从而保护个人信息隐私权。

**拓展延伸**

**维护隐私“三不要**

(1) 不要在不安全的网站中公开自己和他人的真实姓名、身份证件、个人和家人照片、就读学校等隐私信息。

(2) 不随意打探和泄露他人隐私,不随意公开和他人的电子邮件或私聊记录。如果和朋友在同一个聊天群里，不要随意公开和传播朋友的姓名、地址、照片等个人信息。

(3) 不能恶意毁损、玷污、丑化他人的肖像，或利用他人的肖像进行人身攻击等。如果恶意毁损、玷污、丑化他人肖像,很可能为此受到法律的制裁。

保护个人和他人的知识产权。除了传统知识产权的内涵外，计算机软件、数据库、网络域名等数字化作品是开发者辛勤劳动的结晶，也都有其知识产权。作为信息社会的公民，要树立保护个人和他人知识产权的意识，遵守《中华人民共和国著作权法》，既要做到不盲目上传、不随意在网络上散发自己和他人的原创作品，又要做到合理、合法地引用他人作品。如果在自己的作品中引用了他人原创的内容，一定要注明来源。

图3-2 网络安全法

网络一旦发现网上的不良信息，应及时向相关部门或“中国互联网违法和不良信息举报中心”等网站举报。如果是一个群组的群主，要自觉遵守《互联网群组信息服务管理规定》中的要求，切实履行群组管理责任,即“谁建群谁负责”，如果群里有违法违规信息，要行使群主职责,及时进行制止。

### 2 信息安全法律法规

道德是自律的规范，法律是他律的规范。法律和道德，相辅相成，仅仅依靠道德或技术进行信息管理，规范人们在信息活动中的行为是不够的，对于一些已经造成重大危害的行为，必须通过法律的手段来制裁。

### 实践探究

查阅学习本章资源包中“信息系统法律法规清单”内容，有针对性地选择前面案例中对应的条文，上网进行详细查阅。

信息安全的法律法规是国家安全体系的重要内容，是安全保障体系建设中的必要环节。它明确信息安全的基本原则和基本制度、信息安全相关行为的规范、信息安全中各方的权利与义务、违反信息安全行为及相应的处罚。

信息安全立法能够保护国家信息主权和社会公共利益，规范信息活动，保护信息权利，协调和解决信息网络社会产生的矛盾，打击、惩治信息网络空间的违法行为

同时依托信息安全的司法和执法来实施法定程序和法律活动。

信息系统安全问题作为一项社会系统工程，既需要管理层重视相关法律法规的制定与完善，又需要各层面倡导与推广先进的管理手段与技术方法，更需要每一位应用者从国家、社会与合格公民的角度出发，提高安全防护责任意识与安全防范应用水平，以确保信息系统安全问题得到全面重视与高效落实，维护好国家利益及个人信息安全。

## 拓展延伸

**中央网络安全和信息化领导小组宣告成立**

2014年是中国接入国际互联网20周年。2014年2月27日，中共中央成立网络安全和信息化领导小组，旨在着眼国家安全和长远发展，统筹协调涉及经济、政治、文化、社会及军事等各个领域的网络安全和信息化重大问题，研究制定网络安全和信息化发展战略、宏观规划和重大政策，推动国家网络安全和信息化法治建设，不断增强安全保障能力。青少年正值人生观与价值观形成的重要时期，在这个现实空间与虚拟空间相互交织的全新社会环境中，应加强信息系统安全意识，提高信息安全风险防范水平，自觉遵守信息安全法律法规，担当起应有的信息社会责任，做信息社会的一名合格公民!

作为信息社会的高中生，我们应当清醒地认识到，不仅在现实社会中要自觉遵守法律法规，在互联网的空间中也要做一个守法公民。互联网不是超越现实、不受法律约束的空间，每一个网民需要为自己的网络行为承担法律责任。

首先，要通过多种渠道了解、学习法律法规，及时了解最新的法律法规，增强法律意识，在使用网络时做到知法、守法，不做违法的事，自觉维护网络的安全、有序。同时，在不触犯法律的情况下，保护自己在信息社会的合法权益不受侵害，为今后走向社会打好基础。


图3-2 网络安全法

其次，要树立信息社会中的法律意识，自觉履行法律规定的义务。通过前面的学习可以看出，网络中的道德准则与现实生活是相同的，都要受到法律法规的保护与监督。虽然自由和开放是互联网的生命力所在，但是网络不是一个可以为所欲为的地方。

最后，要有维权意识。学习法律法规不是为了完成学习任务，而是应该把它们作为生活中的好帮手，更好地在信息社会中保护自己和他人的权益。例如，在网购时遇到假冒伪劣商品后，不能怕麻烦而自认倒霉，在和商家沟通无果时，应及时向当地消费者协会反映，必要时通过法律手段来解决。

## 拓展延伸

### RSA算法

RSA是1977年由罗纳德·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman）一起提出的。当时他们三人都在麻省理工学院工作。RSA就是他们三人姓氏开头字母拼在一起组成的。

RSA公开密钥密码体制是一种使用不同的加密密钥与解密密钥，“由已知加密密钥推导出解密密钥在计算上是不可行的”密码体制。

在公开密钥密码体制中，加密密钥（即公开密钥）PK是公开信息，而解密密钥（即秘密密钥）SK是需要保密的。加密算法E和解密算法D也都是公开的。虽然解密密钥SK是由公开密钥PK决定的，但却不能根据PK计算出SK。

正是基于这种理论，1978年出现了著名的RSA算法，它通常是先生成一对RSA密钥，其中之一是保密密钥，由用户保存；另一个为公开密钥，可对外公开，甚至可在网络服务器中注册。

为提高保密强度，RSA密钥至少为500位长，一般推荐使用1024位。这就使加密的计算量很大。为减少计算量，在传送信息时，常采用传统加密方法与公开密钥加密方法相结合的方式，即信息采用改进的DES或IDEA对话密钥加密，然后使用RSA密钥加密对话密钥和信息摘要。对方收到信息后，用不同的密钥解密并可核对信息摘要。

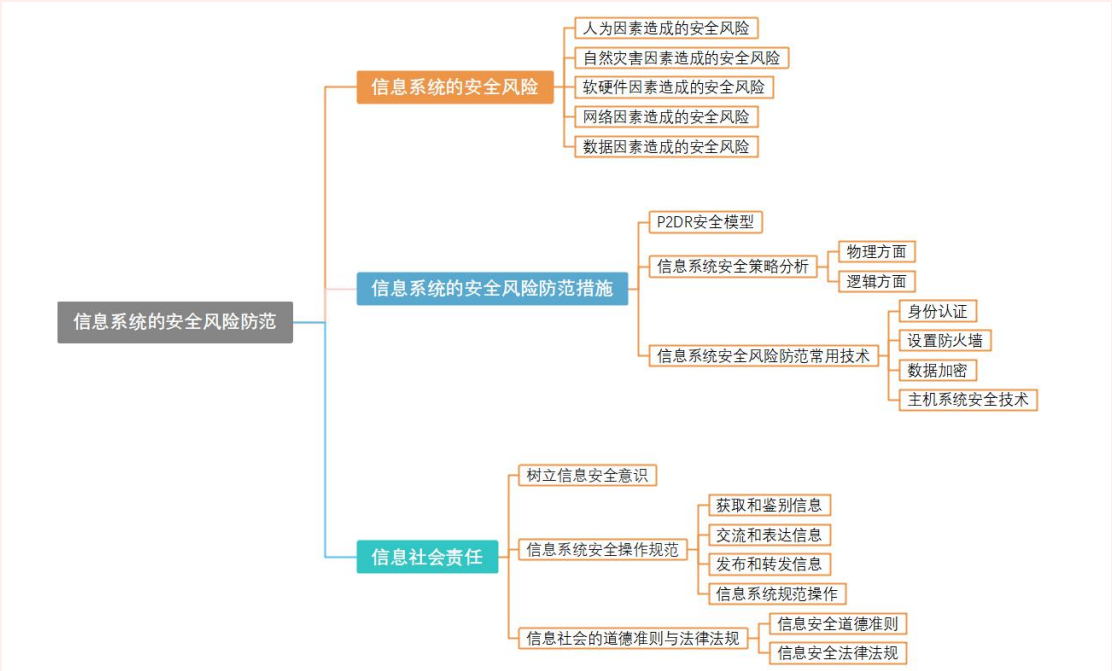
RSA是被研究得最广泛的公钥算法，从提出到现在已近三十年，经历了各种攻击的考验，逐渐为人们接受，普遍认为是目前最优秀的公钥方案之一。

# 章末小结

请同学们完成下列测试题（更多的测试题可以在教科书的配套学习资源包中查看），并通过“本章扼要回顾”，综合评价自己在信息技术知识与技能、解决实际问题的过程与方法，以及相关情感态度与价值观的形成等方面，是否达到了本章的学习目标。

## 一、本章扼要回顾

下图展示了本章的核心概念与关键能力，请同学们对照图中的内容进行总结。




## 二、单元练习

### 1、单选题

（1）小明和朋友在一家餐厅聚会后，发现手机账户信息被盗，最可能的原因是()。

A. 采用了二维码付款

B. 在餐厅里用APP播放视频

C. 添加了朋友的微信

D. 连接不安全的Wi-Fi被盗取信息

(2) 影响信息系统安全的三大因素是( )造成的潜在安全威胁、过程因素造成的潜在安全威胁、网络因素造成的潜在安全威胁。

A.人员　B.过程　C.网络　D.数据

(3) ( ) 是指通过密钥技术，保护在通信网络中传送、交换和存储的信息的机密性、完整性和真实性不被损害。

A.环境维护　B.访问控制　C.信息加密　D.以上全不正确

(4) () 是指通过维护信息的保密性、完整性、 ( ) 和真实性等来管理和保护信息系统资源的一项体制，也包含对信息系统安全保障进行 ( ) 、规范和管理的一系列活动和过程。

A、信息系统安全管理　B、可用性　C、指导　D、培训

2. 思考题

信息社会飞速发展，网络交流及表达工具不断更新（如QQ、博客、微博、微信和短视频等）。我们如何才能在虚实共存的网络社会中始终保持独立思辨的头脑?怎样才能成为有道德、守法律的网络公民?

3. 情境题——家庭网络与安全

(1) 分析《中华人民共和国网络安全法》第三十九条内容对应信息系统安全模型的哪一层?应如何做好安全防范?

阅读材料

第三十九条，国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施:

(一) 对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估;

(二)定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力;

(三)促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享;

(四) 对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

（2）阅读下列案例，分析其存在的安全问题，谈谈应采取什么操作规范才能较好地规避风险

阅读材料

**257万条公民银行个人信息被泄露**

2016年10月14日，某银行支行行长出售自己的查询账号给中间商，中间商将账号卖给有银行关系的“出单渠道”团伙，再由另外一家银行的员工进入该银行内网系统，大肆窃取个人信息贩卖获利。最后公安局网络安全保卫支队破获此案，抓获了包括银行管理层在内的犯罪团伙骨干分子15人。

强大的防御往往是从内部被攻陷，内鬼是信息系统安全中较难防范的环节，利欲熏心的内鬼总能利用职权的便利，让传统的杀毒软件、防火墙，甚至内部权限等形同虚设。