[第五章 信息安全保密基础 2](#_Toc9648)

[第六章 数据库系统 25](#_Toc24457)

[第七章 工具软件 48](#_Toc18894)

[第八章 统一工作平台 58](#_Toc253)

[第九章 广东地税“大集中”征管系统体系 82](#_Toc295)

[第十章 广东地税“大集中”数据库结构及维护技术 98](#_Toc14457)

[第十一章 广东地税“大集中模式”其他信息系统介绍 132](#_Toc12355)

[第十二章 广东地税应用系统建设与维护 143](#_Toc24593)

[第十三章 信息技术普及知识 158](#_Toc31188)

第五章 信息安全保密基础

一、单项选择题（在每个小题的备选答案中，只有一个答案最符合题意，请将其代码填在该题的括号内。）

1.信息安全的基本属性有（ ）。（D）

A.保密性 B.可用性 C.完整性 D.以上三者都是

解析：信息安全主要有保密性、完整性和可用性三个基本属性。除以上三个基本属性外，信息安全还具有可控性和不可否认性。

2.计算机网络上的通信面临的威胁不包括（ ）。（ B）

A. 截获 B. 传输 C. 篡改 D. 伪造

解析：计算机网络上的通信面临以下的四种威胁：截获、中断、篡改、伪造。(1) 截获—从网络上窃听他人的通信内容。 (2) 中断—有意中断他人在网络上的通信。(3) 篡改—故意篡改网络上传送的报文。 (4) 伪造—伪造信息在网络上传送。

3. 下列计算机网络上的通信面临的威胁属于被动攻击的是（ ）。（A）

A. 截获 B. 中断 C. 篡改 D. 伪造

解析：主动攻击会更改信息和拒绝用户使用资源的攻击，攻击者对某个连接进行各种处理。被动攻击是监听信息的攻击，攻击者只是观察和分析某一个协议数据单元而不干扰信息流。截获属于被动攻击，中断、篡改、伪造属于主动攻击。

4.攻击者利用传输数据来冲击网络接口，使得服务器过于繁忙以至于不能应答请求的攻击方式是（ ）。（A）

A.拒绝服务攻击 B.地址欺骗攻击

C.会话劫持 D.信号包探测程序攻击

解析：常见的网络攻击手段有网络监听、端口扫描、口令入侵、特洛伊木马、拒绝服务攻击、缓冲区溢出、IP地址欺骗等。

5.网络信息未经授权不能进行改变的特性是（ ）。（A）

A．完整性 B．可用性 C．可靠性 D．保密性

解析：信息安全主要有保密性、完整性和可用性三个基本属性。完整性是指信息在存储或传输过程中保证不被未授权的、非预期的或无意的操作修改和破坏。

6.确保信息在存储、使用、传输过程中不会泄露给非授权的用户或者实体的特性是（ ）。（D）

A．完整性 B．可用性 C．可靠性 D．保密性

解析：信息安全主要有保密性、完整性和可用性三个基本属性。保密性是指保证信息不会泄漏给非授权用户、实体或者进程。

7.确保授权用户或者实体对于信息及资源的正常使用不会被异常拒绝，允许其可靠而且及时地访问信息及资源的特性是（ ）。（B）

A．完整性 B．可用性 C．可靠性 D．保密性

解析：信息安全主要有保密性、完整性和可用性三个基本属性。可用性指信息可以被授权者访问并按需求使用的特性，即网络信息服务在需要时，允许授权用户或实体使用的特性。

8. （ ）国务院发布《计算机信息系统安全保护条例》。（B）

A． 1990年2月18日 B． 1994年2月18日

C． 2000年2月18日 D． 2004年2月18日

9. 计算机实体安全中，（ ）包括计算机的防盗、防毁、防电磁泄漏以及抗电磁干扰等。（ B ）

A.环境安全 B.设备安全 C.媒体安全 D.介质安全

解析：实体安全具体内容包括环境安全、设备安全、媒体安全。设备安全主要包括计算机设备的防盗、防毁、防电磁泄漏以及抗电磁干扰等。

10. 计算机实体安全中，（ ）包括计算机介质本身的安全及介质数据的安全。（ C ）

A.环境安全 B.设备安全 C.媒体安全 D.介质安全

解析：实体安全具体内容包括环境安全、设备安全、媒体安全。媒体安全又称介质安全，包括媒体本身的安全及媒体数据的安全。

11.《计算机信息系统安全保护条例》规定，国家对计算机信息系统安全专用产品的销售实行（ ）。（A）

A.许可证制度 B.3C认证 C.IS09000认证 D.专卖制度

12.《计算机信息系统安全保护条例》规定，运输、携带、邮寄计算机信息媒体进出境的，应当如实向（ ）。（B）

A.国家安全机关申报 B.海关申报

C.国家质量检验监督局申报 D.公安机关申报

13.《计算机信息系统安全保护条例》规定，故意输入计算机病毒以及其他有害数据危害计算机信息系统安全的，或者未经许可出售计算机信息系统安全专用产品的，由公安机关处以警告或者（ ）。（A）

A． 对个人处以5000元以下的罚款，对单位处以15000元以下的罚款

B．对个人处以5000元以上的罚款，对单位处以15000元以上的罚款

C．对个人处以2000元以下的罚款，对单位处以10000元以下的罚款

D．对个人处以2000元以上的罚款，对单位处以10000元以上的罚款

14.《计算机信息系统安全保护条例》规定，任何组织或者个人违反条例的规定，给国家、集体或者他人财产造成损失的，应当依法承担 （ ）。( B )

A.刑事责任 B.民事责任 C.违约责任 D.其他责任

15.在信息安全管理中进行（ ），可以有效解决人员安全意识薄弱问题。( C )

A.内容监控 B.责任追查和惩处

C.安全教育和培训 D.访问控制

16. 信息泄密各种途径中，无知泄密属于（ ）。( D )

A.计算机电磁波辐射泄漏 B.计算机联网泄密

C.计算机媒体泄密 D.内部工作人员泄密

解析：信息泄密主要途径有计算机电磁波辐射泄漏、计算机联网泄密、计算机媒体泄密和内部工作人员泄密等。其中内部工作人员泄密包括无知泄密、违反规章制度泄密和故意泄密等。

17. 计算机信息系统实体安全是指计算机信息系统设备及相关设施的安全。设施安全属于哪种实体安全（ ）。 ( A )

A.环境安全 B.设备安全 C.媒体安全 D.介质安全

解析：实体安全具体内容包括环境安全、设备安全、媒体安全。环境安全包括机房与设施安全、环境与人员安全等。

18.信息安全等级保护制度中，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全的，该等级属于（ ）。 ( B )

A.第一级 B.第二级 C.第三级 D.第四级

解析：根据信息和信息系统在国家安全、经济建设、社会生活中的重要程度；其遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度；针对信息的保密性、完整性和可用性要求及信息系统必须要达到的基本的安全保护水平等因素，信息和信息系统的安全保护等级分为五个级别。

19.信息安全等级保护定级中，( )以上的信息系统需要到公安机关备案 。( B )

A.第一级 B.第二级 C.第三级 D.第四级

20.涉密信息系统分级保护中，（ ）等级保密要求最高。( C )

A.秘密 B.机密 C.绝密 D.加密

解析：涉密信息系统按照秘密、机密、绝密三级进行保护和管理。

21.税务系统网络与信息安全事件分级中，（ ）等级严重程度最高。( A )

A. 1级 B. 3级 C. 4级 D. 5级

解析：根据事件后果的严重程度，税务网络与信息安全事件划分为5个级别，其中1级危害程度最高，5级危害程度最低。

22. 根据事件后果的严重程度，税务网络与信息安全事件中的灾难性安全事件属于（ ）。（ A ）

A. 1级 B. 3级 C. 4级 D. 5级

解析：1级网络与信息安全事件：灾难性安全事件。对税务系统业务活动、税务单位利益或社会公共利益有灾难性的影响或危害。

23. （ ）以上的网络与信息安全事件按《税务系统重大网络与信息安全事件调查处理办法》进行处理。（ C ）

A. 1级 B. 2级 C. 3级 D. 4级

解析：根据事件后果的严重程度，税务网络与信息安全事件划分为5个级别，3级和3级以上的网络与信息安全事件称为重大网络与信息安全事件。

24.以下不符合机房防静电要求的是（ ）。（ B ）

A. 穿合适的防静电衣服和防静电鞋

B. 在机房内直接更衣梳理

C. 用表面光滑平整的办公家具

D. 经常用湿拖布拖地

解析：机房静电的防护措施：（1）机房内应严禁使用地毯、挂毯等容易产生静电的物品；（2）机房计算机系统应有一套合理的接地与屏蔽系统；（3）机房要保证安装防静电地板；（4）机房内工作台面及座椅的材料应该是导静电的，而且必须进行静电接地；（5）机房内应保持一定的湿度，在干燥季节应该加湿。

25. 布置计算机信息系统信号线缆的路由走向时,以下做法错误的是（ ）。（ A ）

A. 可以随意弯折

B. 转弯时,弯曲半径应大于导线直径的 10 倍

C. 尽量直线,平整

D. 尽量减小由线缆自身形成的感应环路面积

26. 下面说法错误的是（ ）。（ C ）

A. 基于主机的入侵检测系统可以监视一个主机上发生的全部事件

B. 基于主机的入侵检测可以运行在交换网络中

C. 基于主机的入侵检测系统可以检测针对网络中所有主机的网络扫描

D. 基于应用的入侵检测系统比起基于主机的入侵检测系统更容易受到攻击

解析：入侵检测系统只能是有针对性的进行监视和检测。

27. 使用漏洞库匹配的扫描方法,能发现（ ）。（ B ）

A. 未知的漏洞 B. 已知的漏洞

C. 自行设计的软件中的漏洞 D. 所有漏洞

解析：使用漏洞库匹配的扫描方法,能发现已知的漏洞，可及时进行更新系统补丁。

28. 系统安全性能检测属于（ ）信息安全保密要求的项目内容。（ B ）

A.秘密级 B.机密级 C.绝密级 D.加密级

解析：涉密信息系统按照秘密、机密、绝密三级进行保护和管理。

秘密级信息安全保密要求的项目内容包括：身份鉴别、访问控制、信息密码措施、电磁泄漏发射防护、系统安全性能检测、安全审计、边界安全防护。

29.数据库安全属于（ ）信息安全保密要求的项目内容。（ B ）

A.秘密级 B.机密级 C.绝密级 D.加密级

解析：涉密信息系统按照秘密、机密、绝密三级进行保护和管理。

秘密级信息安全保密要求的项目内容包括：身份鉴别、访问控制、信息密码措施、电磁泄漏发射防护、系统安全性能检测、安全审计、边界安全防护。机密级信息安全保密要求的项目内容，应该在秘密级的基础上，再增加信息完整性检验、操作系统安全、数据库安全等3个项目。

30. 下面关于隔离网闸的说法，正确的是（ ）。（ C ）

A. 能够发现已知的数据库漏洞

B. 可以通过协议代理的方法穿透网闸的安全控制

C. 任何时刻网闸两端的网络之间不存在物理连接

D. 在 OSI 的二层以上发挥作用

解析：物理隔离网闸在OSI的所有七层都工作。

31. 当收到你认识的人发来的电子邮件并发现其中有意外附件，应该（ ）。 （ C ）

A. 打开附件,然后将它保存到硬盘

B. 打开附件,但是如果它有病毒,立即关闭它

C. 用防病毒软件扫描以后再打开附件

D. 直接删除该邮件

32. 不能防止计算机感染病毒的措施是（ ）。( A )

A. 定时备份重要文件

B. 经常更新操作系统补丁

C. 除非确切知道附件内容,否则不要打开电子邮件附件

D. 重要部门的计算机尽量专机专用与外界隔绝

33. 假设使用一种加密算法，它的加密方法很简单：将每一个字母加5，即a加密成f。这种算法的密钥就是5，那么它属于（ ）。（A）

A. 对称加密技术 B. 分组密码技术

C. 公钥加密技术 D. 单向函数密码技术

解析：对称加密技术是一种传统加密方式，它的加密密钥和解密密钥是一样的。

34．A方有一对密钥（KA公钥，KA私钥），B方有一对密钥（KB公钥，KB私钥），A方向B方发送数字签名M，对信息M加密为： M’ = KB公钥（KA私钥（M）），则B方收到密文的解密方案是（ ）。（C）

A. KB公钥（KA私钥（M’）） B. KA公钥（KA公钥（M’））

C. KA公钥（KB私钥（M’）） D. KB私钥（KA私钥（M’））

解析：这种非对称密钥，每个人都有一对唯一对应的密钥：公开密钥和私人密钥，公钥对外公开，私钥由个人秘密保存；用其中一把密钥加密，就只能用另一把密钥解密。因为公钥是公开对外发布的，所以想给私钥持有者发送信息的人都可以取得公钥，用公钥加密后，发送给私钥持有者，即使被拦截或窃取，没有私钥的攻击者也无法获得加密后的信息，可以保证信息的安全传输。另外，先用私钥加密，再用公钥解密，可以完成对私钥持有者的身份认证，因为公钥只能解开有私钥加密后的信息。

35. “公开密钥密码体制”的含义是（ ）。（C）

A. 将所有密钥公开

B. 将私有密钥公开，公开密钥保密

C. 将公开密钥公开，私有密钥保密

D. 两个密钥相同

36. （ ）允许对信息进行数字签名，数字签名使用发送发送一方的专用密钥对所发送信息的某一部分进行加密。接受方收到该信息后，使用发送方的公用密钥解密数字签名，验证发送方身份。 （ C ）

A. 对称加密技术 B. 分组密码技术

C. 公钥加密技术 D. 单向函数密码技术

37. 可以被数据完整性机制防止的攻击方式是（ ）。（D）

A. 假冒源地址或用户的地址欺骗攻击

B. 抵赖做过信息的递交行为

C. 数据中途被攻击者窃听获取

D. 数据在途中被攻击者篡改或破坏

38. 身份鉴别是安全服务中的重要一环，以下关于身份鉴别叙述不正确的是（ ）。（ B ）

A. 身份鉴别是授权控制的基础

B. 身份鉴别一般不用提供双向的认证

C. 目前一般采用基于对称密钥加密或公开密钥加密的方法

D. 数字签名机制是实现身份鉴别的重要机制

39. 基于通信双方共同拥有的但是不为别人知道的密钥，利用计算机强大的计算能力，以该密钥作为加密和解密的密钥的认证是（ ）。（C）

A.公钥认证 B.零知识认证 C.共享密钥认证 D.口令认证

40. 访问控制是指确定（ ）以及实施访问权限的过程。（ A ）

A.用户权限 B.用户口令

C.系统安全性能 D.系统是否遭受入侵

解析：访问控制是按用户身份及其所归属的角色组来确定用户权限，限制用户对某些信息项的访问，或限制对某些控制功能的使用。访问控制通常用于系统管理员控制用户对服务器、目录、文件等网络资源的访问。

41. 下列对访问控制影响不大的是（ ）。（ D ）

A.主体身份 B.客体身份 C.访问类型 D.数字签名

解析：访问控制根据用户身份来确定用户权限，限制访问类型和对资源的访问权限。

42. 在访问控制中，为了简化管理，通常对访问者（ ），以避免访问控制表过于庞大。（ A ）

A.分类组织成组

B.严格限制数量

C.按访问时间排序，删除长期没有访问的用户

D.不作任何限制

43. 一般而言，Internet防火墙建立在一个网络的（ ）。（C）

A. 内部子网之间传送信息的中枢

B. 每个子网的内部

C. 内部网络与外部网络的交叉点

D. 部分内部网络与外部网络的结合处

44. 包过滤型防火墙原理上是基于（ ）进行分析的技术。（C）

A. 物理层 B. 数据链路层 C. 网络层 D. 应用层

解析：包过滤是一种内置于路由功能之上的防火墙类型，包过滤防火墙将对每一个接收到的包做出允许或拒绝的决定，包过滤是在IP层实现的，包过滤防火墙工作在网络层。

45.（ ）是在公用网络上建立专用网络的技术。（C）

A. ROUTE B. SNS C. VPN D. PNT

解析：虚拟专用网络（Virtual Private Network ，简称VPN)指的是在公用网络上建立专用网络的技术。

二、多项选择题（在每个小题的备选答案中，至少有两个或两个以上个答案最符合题意，请将其代码填在该题的括号内。）

1.信息安全的属性有（ ）。（ ABCD ）

A.保密性 B.完整性 C.可用性 D.可控性

解析：信息安全主要有保密性、完整性和可用性三个基本属性。除以上三个基本属性外，信息安全还具有可控性和不可否认性。

2.《保守国家秘密法》规定的泄密行为有（ ）。（ACD）

A.使用非涉密计算机、非涉密存储设备存储、处理国家秘密信息的

B.复制、记录、存储国家秘密的

C.邮寄托运国家秘密载体出境

D.未采取防护措施情况下，在涉密信息系统和互联网及其他公共信息网络之间进行信息交换

解析：非法复制、记录、存储国家秘密的，才属于泄密行为。

3.关于信息安全，下列说法中不正确的是（ ）。（ABD）

A．信息安全等同于网络安全

B．信息安全由技术措施实现

C．信息安全应当管理与技术并重

D．管理措施在信息安全中不重要

解析：管理与技术并重原则是信息安全管理的原则之一。

4. （ ）可能给网络和信息系统带来风险，导致安全事件。（ABCD）

A.计算机病毒 B.网络入侵 C.软硬件故障 D.人员误操作

5. （ ）安全措施可以有效降低软硬件故障给网络和信息系统所造成的风险。(ABCD)

A．双机热备 B．多机集群 C．磁盘阵列 D．系统和数据备份

6.典型的数据备份策略包括（ ）。(ABD)

A．完全备份 B．增量备份 C．选择性备份 D．差异备份

解析：常用的数据备份策略包括完全备份，差异备份及增量备份。

7.有多种情况能够泄漏口令，这些途径包括（ ）。（ACD）

A．被猜测和发现口令 B．口令设置过于复杂

C．将口令告诉别人 D．被电子监控

8.计算机安全中，信息系统常见的危险有（ ）。（ABC）

A．软硬件设计故障导致网络瘫痪 B．黑客入侵

C．误删除数据 D．自然灾害

9.对于计算机系统，由环境因素所产生的安全隐患包括（ ）。（ABC）

A．恶劣的温度、湿度、灰尘、地震、风灾、火灾等

B．强电、磁场等

C．雷电

D．人为的破坏

10.我国信息安全等级保护的内容包括（ ）。(ABD)

A．对国家秘密信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输和处理这些信息的信息系统分等级实行安全保护

B．对信息系统中使用的信息安全产品实行按等级管理

C．对信息安全从业人员实行按等级管理

D．对信息系统中发生的信息安全事件按照等级进行响应和处置

解析：信息安全等级保护是指对信息系统的信息安全实行等级化保护和等级化管理，但没有包括对其从业人员进行分等级管理。

11.目前，我国在对信息系统进行安全等级保护时，划分了几个级别，包括（ ）。(ABCD)

A.专控保护级 B.强制保护级 C.监督保护级 D.指导保护级

解析：信息系统的安全保护等级分为五个级别：第一级为自主保护级，第二级为指导保护级，第三级为监督保护级，第四级为强制保护级，第五级为专控保护级。

12. 下列（ ）属于信息系统安全风险评估涉及的基本要素。（ABCD）

A.价值 B.资产 C.威胁 D.脆弱性

解析：信息系统安全风险评估涉及的基本要素包括资产、价值、威胁、脆弱性、风险、残余风险、安全需求、安全措施。

13. 关于信息系统安全风险评估，下列哪些说法是正确的（ ）。（ABC）

A．信息化程度越高风险越大

B．防护措施可抗击威胁，降低风险

C．风险是威胁发起的，威胁越大风险越大

D．风险防护意识越高风险越大

解析：资产都有价值，信息化的程度越高，组织机构的任务越重要，对资产的依赖度越高，资产的价值就越大；资产的价值越大风险越大；风险是威胁发起的，威胁越大风险越大；威胁都要利用脆弱性，脆弱性越大风险越大；脆弱性使资产暴露，威胁利用脆弱性，危害资产，形成风险；对风险的意识，会引出防护需求；防护需求被防护措施所满足；防护措施抗击威胁，降低风险。

14. 在信息系统安全风险评估中，以下哪些说法是正确的（ ）。 （ABCD)

A.资产价值越大风险越大 B.威胁越大风险越大

C.脆弱性越大风险越大 D.脆弱性使资产暴露

解析：资产都有价值，信息化的程度越高，组织机构的任务越重要，对资产的依赖度越高，资产的价值就越大；资产的价值越大风险越大；风险是威胁发起的，威胁越大风险越大；威胁都要利用脆弱性，脆弱性越大风险越大；脆弱性使资产暴露，威胁利用脆弱性，危害资产，形成风险；对风险的意识，会引出防护需求；防护需求被防护措施所满足；防护措施抗击威胁，降低风险。

15.通过对涉密信息系统进行风险评估，可以全面掌握涉密信息系统中（ ）。（ABCD）

A.信息资产情况 B.所采取的直接控制措施

C.所采取的相应的管理措施 D.信息资产面临的威胁

解析：通过风险评估的方式，可以全面掌握涉密信息系统中的信息资产情况、信息资产面临的威胁、存在的漏洞以及所采取的直接控制措施（包括技术措施与相应的管理措施），可以对系统的风险状态有一个相对客观的了解。

16.信息安全等级保护制度的基本原则有（ ）。 (ABCD)

A.明确责任，共同保护 B.依照标准，自行保护

C.同步建设，动态调整 D.指导监督，重点保护

解析：实施信息安全等级保护基本应遵循自主保护原则、同步建设原则、重点保护原则、适当调整原则。

17. 根据事件后果的严重程度划分，税务网络与信息安全事件包括（ ）。（ABC）

A.灾难性安全事件 B.特别重大安全事件

C.重大安全事件 D.非安全事件

解析：根据事件后果的严重程度，税务网络与信息安全事件划分为5个级别：1级是灾难性安全事件，2级是特别重大安全事件，3级是重大安全事件，4级是较大安全事件，5级是一般安全事件。

18. 涉密信息系统按照（ ）级别进行保护和管理。（ABC）

A.秘密 B.机密 C.绝密 D.超密

解析：涉密信息系统按照秘密、机密、绝密三级进行保护和管理。

19. 在信息安全中，物理安全的管理应做到（ ）。（ABC）

A. 所有相关人员都必须进行相应的培训,明确个人工作职责

B. 制定严格的值班和考勤制度,安排人员定期检查各种设备的运行情况

C. 在重要场所的迸出口安装监视器,并对进出情况进行录像

D. 增加管理人员的经费补贴

20. 在信息安全中，场地安全要考虑的因素有（ ）。（ABCD）

A.场地选址 B.场地防火 C.场地防水防潮 D.场地温度控制

21. 火灾自动报警,自动灭火系统部署应注意（ ）。（ABCD）

A. 避开可能招致电磁干扰的区域或设备

B. 具有不间断的专用消防电源

C. 留备用电源

D. 具有自动和手动两种触发装置

22. 在信息安全防护措施中，为了减小雷电损失,可以采取的措施有（ ）。（AC）

A. 机房内应设等电位连接网络 B. 部署 UPS

C. 设置安全防护地网 D. 信息处理电路

解析：机房防雷电措施包括：直击雷的防护、电源系统的防护、信号系统的防护、等电位连接、接地防雷地网。

23. 会导致电磁泄漏的信息设备有（ ）。（ABCD）

A. 显示器 B. 开关电路及接地系统

C. 计算机系统的电源线 D. 信号处理电路

解析：电磁泄漏是指信息系统的设备在工作时能经过地线、电源线、信号线、寄生电磁信号或谐波等辐射出去，产生电磁泄漏。这些电磁信号如果被接收下来，经过提取处理，就可恢复出原信息，造成信息失密。具有保密要求的计算机信息系统必须注意防止电磁泄漏。

24. 为加强信息安全保密，磁介质的报废处理应采用（ ）。( BD )

A.直接丢弃 B.粉碎处理 C.删除内容 D.严格消磁

解析：为防止信息泄密，磁介质报废需经过严格消磁处理，或进行物理粉碎。

25. 静电的危害有（ ）。（ABCD）

A.导致磁盘读写错误,损坏磁头,引起计算机误动作

B.造成电路击穿或者毁坏

C.影响工作人员身心健康

D.吸附灰尘

解析：静电对计算机的主要危害是由于静电噪声对电子线路的干扰，引起电位的瞬间改变，导致存储器中的信息丢失或误码。静电不仅会使计算机设备的运转出故障，还对影响操作人员的身心健康。

26.防止设备电磁辐射可以采用的措施有（ ）。（ABCD）

A.屏蔽 B.滤波

C.尽量采用低辐射材料和设备 D.内置电磁辐射干扰器

解析：电磁防护措施包括：屏蔽、滤波、隔离、接地、选用低辐射设备、使用干扰器。

27. 路由器的过滤策略通常包括（ ）。（ABD）

A. 拒绝或允许来自某主机或某网段的所有连接

B. 拒绝或允许来自某主机或某网段的指定端口的连接

C. 拒绝或允许所有主机或所有网络与本地主机或网络的所有连接

D. 拒绝或允许本地主机或本地网络与其他主机或网络的所有连接

解析：路由器的通常过滤策略是不会拒绝或者允许所有主机网络的连接的，那样就失去路由器的作用了，除非有些暂时性的特殊需要。

28. 目前市场上主流防火墙提供的功能包括（ ）。（ABCD）

A.数据包状态检测过滤 B.NAT

C.策略分组 D.日志分析和流量统计分析

解析：目前的防火墙产品功能一般包括：状态检测包过滤和应用代理，IP/Mac 地址绑定，防止内部 IP 欺骗，支持 IP 映射和端口转移，网络地址转换(NAT)，策略分组，易于管理和系统升级，内置网络诊断工具，便于安装配置，有完善的日志，并能输出给用户的管理程序，具有相关的统计分析和审计功能。

29. 网络攻击利用网络存在的漏洞和安全缺陷对系统进行攻击，常见的网络攻击手段有（ ）。（ABCD）

A. 拒绝服务攻击

B. 端口扫描

C. 网络监听

D. 缓冲区溢出

解析：常见的网络攻击手段有网络监听、端口扫描、口令入侵、特洛伊木马、拒绝服务攻击、缓冲区溢出、IP地址欺骗等。

30. 防火墙的性能的评价方面包括（ ）。（ABCD）

A. 并发会话数 B. 吞吐量 C. 延时 D. 平均无故障时间

31. 入侵防御技术面临的挑战主要包括（ ）。（BCD）

A. 不能对入侵活动和攻击性网络通信进行拦截

B. 性能 " 瓶颈 "

C. 误报和漏报

D. 单点故障

解析：IPS技术需要面对很多挑战，其中主要有三点：一是单点故障，二是性能瓶颈，三是误报和漏报。

32. 网络安全扫描能够（ ）。（ABCD）

A.确认开放的端口 B.判断操作系统类型

C.识别网络和拓扑结构 D.测试系统是否存在安全漏洞

解析：网络安全扫描技术是一类重要的主动防御型的网络安全技术。通过对网络的扫描，网络管理员可以了解网络的安全配置和运行的应用服务，及时发现安全漏洞，客观评估网络风险等级。

33. 可能和计算机病毒有关的现象有（ ）。（ACD）

A. 可执行文件大小改变了

B. 在向写保护的 U 盘复制文件时屏幕上出现 U 盘写保护的提示

C. 系统频繁死机

D. 内存中有来历不明的进程

34.计算机病毒利用（ ）方式进行传染和破坏。（ABC）

A.读写文件 B.驻留内存 C.截取中断向量 D.加密解密

35. 下面哪些算法属于公钥加密算法（ ）。 ( CD )

A. AES B. DES C. RSA D. ECC

解析：AES和DES是分组密码算法，RSA和ECC属于公钥加密算法。

三、判断辨析题（正确的在题后的括号内划“√”；错误的在题后的括号内划“×”，改正并简述理由。）

1.网络安全应具有以下四个方面的特征：保密性、完整性、可用性、可查性。 （×）

解析：信息安全主要有保密性、完整性和可用性三个基本属性，另外还具有可控性和不可否认性

2.网络与信息安全事件分为信息系统类和信息数据类两大类。 （√）

3.安全是永远是相对的，永远没有一劳永逸的安全防护措施。 （√）

4.拒绝服务攻击属于被动攻击的一种。 （×）

5.入侵检测系统是网络信息系统安全的第一道防线。 （×）

6.根据《保守国家秘密法》，信息泄密行为可被行政处分、罚款或警告，但不会追究刑事责任。 （×）

解析：依据《保守国家秘密法》修订草案，信息泄密行为可被行政处分、罚款或警告，构成犯罪的，依法追究刑事责任。

7.涉密计算机或涉密存储设备经过安全处理后才可以接入互联网。 （×）

解析：涉密计算机或涉密存储设备不得接入互联网及其他公共信息网络。

8.复制、记录、存储国家秘密属于信息泄密行为。 （×）

解析：非法复制、记录、存储国家秘密才是属于信息泄密行为

9.风险评估是确认安全风险及其大小的过程，即利用适当的风险评估工具，确定信息资产的风险等级和优先风险控制顺序 （√ ）

10.风险控制能力相关信息获取可通过对用户发放调查问卷的形式获取。 （×）

11. 涉密信息系统分级保护中，机密等级保密要求最高。 （×）

解析：涉密信息系统分级保护中，绝密等级保密要求是最高的。

12. 税务系统网络与信息安全事件分级中，第五级的严重程度最高。 （×）

解析：税务系统网络与信息安全事件分为五级，第一级的严重程度最高。

13.对信息系统支持设施、信息系统设施造成影响而导致的网络与信息安全事件属于信息数据类安全事件。 ( × )

解析：对信息系统支持设施、信息系统设施造成影响而导致的网络与信息安全事件属于信息系统类安全事件；信息数据类安全事件是指数据安全属性破坏或通过网络传播不良信息导致的网络与信息安全事件。

14.信息系统安全保密管理，首先要确立安全目标与策略。 ( √ )

15. VPN的加密手段为VPN内的各台主机对各自的信息进行相应的加密。 ( √ )

四、简答题

1.请简述信息安全的定义。

答：信息安全是指对信息系统的硬件、软件以及数据信息实施安全防护，保证在意外事故或恶意攻击情况下系统不会遭到破坏，敏感数据信息不会被篡改和泄漏，保证信息的机密性、完整性、可用性和可控性，并保证系统能够正常运行，信息服务功能不中断。

2. 请简述信息保密的定义。

答：信息保密是指为了防止泄密、窃密和破坏，对计算机信息系统及其所存储的信息和数据、相关坏境与场所、安全保密产品进行安全防护，确保以电磁信号为主要形式的信息之产生、存储、传递和处理等过程中的保密性、完整性、可用性和抗抵赖性。

3. 请简述信息安全的基本属性，并请解释这几个基本属性。

答：信息安全主要有保密性、完整性、可用性三个基本属性。保密性是指保证信息不会泄漏给非授权用户、实体或者进程；完整性是指信息在存储或者传输过程中保证不被未授权的、非预期的或者无意的操作修改和破坏；可用性是指信息可以被授权者访问并按需求使用的特性，即网络信息服务在需要时，允许授权用户或实体使用的特性。

4. 请简述计算机信息系统实体安全的概念。

答：计算机信息系统实体安全是指计算机信息系统设备及相关设施的安全，即保护计算机设备、设施（含网络）以及其他媒体免遭地震、水灾、火灾、有害气体和其他环境事故（如电磁污染等）的破坏。

5. 请简述计算机运行安全的概念。

答：运行安全是指为保障系统功能的安全实现，提供一套安全措施（如风险分析、审计跟踪、备份与恢复、应急等）来保护信息处理过程的安全。

6.请简答物理安全的概念和包含的内容。

答：物理安全涉及在物理层面上保护企业资源和敏感信息所遭遇的威胁、并针对可能存在的缺陷和所采取的相应对策。物理安全主要包括：①机房环境安全②通信线路安全③设备安全④电源安全。

7.请简述环境安全、设备安全以及媒体安全的具体内容。

答：（1）环境安全包括机房与设施安全、环境与人员安全等。

（2）设备安全主要包括计算机设备的防盗、防毁、防电磁泄漏以及抗电磁干扰等。

（3）媒体安全又称介质安全，包括媒体本身的安全及媒体数据的安全。

8．保障通信线路安全技术的主要技术措施有哪些？

答：①电缆加压技术②对光纤等通信线路的防窃听技术（距离大于最大长度限制的系统之间，不采用光纤线通信；加强复制器的安全，如用加压电缆、警报系统和加强警卫等措施）

9．请简述电磁辐射对网络通信安全的影响主要体现在哪些方面，防护措施有哪些？

答：影响主要体现在：计算机系统可能会通过电磁辐射使信息被截获而失密，计算机系统中数据信息在空间中扩散。

防护措施：一类是对传导发射的防护，主要采取对电源线和信号线加装性能良好的滤波器，减小传输阻抗和导线间的交叉耦合；另一类是对辐射的防护，又分为两种：一种是采用各种电磁屏蔽措施，第二种是干扰的防护措施，主要措施有①屏蔽②滤波③隔离④接地，其中屏蔽是应用最多的方法。

10．请简答保障信息存储安全的主要措施有哪些？

答：①存放数据的盘，应妥善保管；②对硬盘上的数据，要建立有效的级别、权限，并严格管理，必要时加密，以确保数据的安全；③存放数据的盘，管理须落实到人，并登记；④对存放重要数据的盘，要备份两份并分两处保管；⑤打印有业务数据的打印纸，要视同档案进行管理；⑥凡超过数据保存期的，须经过特殊的数据清除处理；⑦凡不能正常记录数据的盘，需经测试确认后由专人进行销毁，并做好登记；⑧对需要长期保存的有效数据，应质量保证期内进行转存，并保证转存内容正确。