1. 信息有非常多的定义和说法，归结起来可以认为信息就是数据或事件。关于信息，下列说法错误的是（）。

A. 在一定程度上，人类社会的发展速度取决于人们感知信息、利用信息的广度和深度

B. 信息无时不在，无处不在，信息是我们行动决策的重要依据

C. 电视机、电话机、声波、光波是信息

D. 人类可以借助信息资源对自然界中的物质资源和能量资源进行有效地获取和利用

参考答案：C

难易程度：一级

解析：电视机、电话机、声波、光波不属于信息

所属知识子域：信息安全与网络空间安全

2. 信息安全问题的根源，分为内因和外因，内因主要是信息系统复杂性导致漏洞的存在不可避免。信息系统复杂性包括（）

A. 环境因素和人为因素

B. 过程复杂性，结构复杂性和应用复杂性

C. 技术因素和人为因素两个方面

D. 员工的误操作及外部攻击

参考答案：B

难易程度：一级

解析：内因方面主要是信息系统复杂性导致漏洞的存在不可避免，换句话说，漏洞是一种客观存在。这些复杂性包括过程复杂性，结构复杂性和应用复杂性等方面。

所属知识子域：信息安全与网络空间安全

3. 根据掌握的资源和具备的能力，我国面临的信息安全威胁错误的是（）

A. 黑客威胁

B. 组织威胁

C. 个人威胁

D. 国家威胁

参考答案：A

难易程度：一级

解析：根据掌握的资源和具备的能力来看，针对信息系统的攻击由低到高分别是个人威胁、组织层面威胁(犯罪团伙、黑客团体、竞争对手等)和国家层面威胁(网络战部队)。

所属知识子域：信息安全与网络空间安全

4. 对于以下列举的四种个人信息，其中不属于个人隐私的是哪个（）

A. 家庭住址

B. 手机号码

C. 身份证号

D. 单位的名称

参考答案：D

难易程度：一级

解析：单位的名称不属于个人隐私

所属知识子域：信息安全与网络空间安全

5. 购物网站通过技术手段能证明用户的确只支付了 20 元，而不是用户声称的 100 元，这是实现以下哪个属性（）

A. 不可否认性
B. 保密性
C. 可用性
D. 可靠性
参考答案：A
难易程度：一级
解析：证明要求保护的事件或动作及其发起实体的行为。

所属知识子域：信息安全与网络空间安全

6. 信息安全基本属性简称是 CIA，此外，还可以涉及其他属性，例如真实性、可问责性、不可否认性和可靠性。下面不属于信息安全基本属性的是（）

A. 机密性
B. 完整性
C. 可用性
D. 可控性
参考答案：D
难易程度：一级
解析：通常情况下，保密性、完整性和可用性(简称“CIA”)被称为信息安全基本属性

所属知识子域：信息安全与网络空间安全

7. 某网站因技术问题，受到病毒等攻击无法正常为用户提供服务，这破坏了数据的（ ）

A. 完整性
B. 可用性
C. 不可否认性
D. 可靠性
参考答案：B
难易程度：二级
解析：可用性是确保任何时候得到授权的实体在需要时，都能访问到需要的数据，信息系统必须提供相应的服务。

所属知识子域：信息安全与网络空间安全

8. 我国面临的信息安全威胁，下面不属于国家威胁的是（）

A. 恐怖组织通过网络大肆发布恐怖信息，渲染暴力活动
B. 邪教组织通过网络极力宣扬种族歧视，煽动民族仇恨，破坏民族团结，宣扬邪教理念，破坏国家宗教政策，煽动社会不满情绪，甚至暴力活动
C. 网络恐怖分子破坏公共秩序、制造社会混乱等
D. 其他国家情报机构收集我国政治、军事、经济等情报信息
参考答案：C
难易程度：一级
解析：网络恐怖分子破坏公共秩序、制造社会混乱等属于组织威胁

所属知识子域：信息安全与网络空间安全

9. 目前，信息系统面临外部攻击者的恶意攻击威胁，从威胁能力和掌握资源分，这些威胁

可以按照个人威胁、组织威胁和国家威胁三个层面划分，则下面选项中属于组织威胁的是 （ ）

A. 喜欢恶作剧、实现自我挑战的娱乐型黑客

B. 实施犯罪、获取非法经济利益网络犯罪团伙

C. 搜集政治、军事、经济等情报信息的情报机构

D. 巩固战略优势，执行军事任务、进行目标破坏的信息作战部队

参考答案：B

难易程度：一级

解析：A 属于个人威胁，C 和 D 都属于国家威胁

所属知识子域：信息安全与网络空间安全

10. 对信息资源开放范围进行控制，确保信息不被非授权的个人、组织和计算机程序访问，体现了信息安全什么属性（）

A. 真实性

B. 可用性

C. 机密性

D. 可控性

参考答案：C

难易程度：一级

解析：保密性也称机密性，是指对信息资源开放范围的控制，确保信息不被非授权的个人、组织和计算机程序访问

所属知识子域：信息安全与网络空间安全

11. 数据被破坏、非法篡改破坏了信息安全的（）属性。

A. 真实性

B. 可用性

C. 完整性

D. 不可否认性

参考答案：C

难易程度：一级

解析：完整性是保证信息系统中的数据处于完整的状态，确保信息没有遭受篡改和破坏

所属知识子域：信息安全与网络空间安全

12. 2008 年，《国家网络安全综合倡议(CNCI)》发布。CNCI 计划建立三道防线，下面不属于三道防线内容的是（）

A. 减少漏洞和隐患，预防入侵

B. 全面应对各类威胁，增强反应能力，加强供应链安全抵御各种威胁

C. 强化未来安全环境，增强研究、开发和教育，投资先进技术

D. 充分发挥国家、企业和个人的积极性，不能忽视任何一方的作用

参考答案：C

难易程度：一级

解析：2008 年，《国家网络安全综合倡议(CNCI)》发布。CNCI 计划建立三道防线：第一道防线，减少漏洞和隐患，预防入侵；第二道防线，全面应对各类威胁，增强反应能力，加强供应链安全抵御各种威胁；第三道防线，强化未来安全环境，增强研究、开发和教育，投资

先进技术。

所属知识子域：网络安全法律法规

13. 2003 年 7 月，国家信息化领导小组根据国家信息化发展的客观需求和网络与信息安全工作的现实需要，制定出台了《关于加强信息安全保障工作的意见》(中办发 27 号文件)，文件明确了加强信息安全保障工作的总体要求，坚持（）方针。

A. 积极防御、综合防范

B. 重点保障基础信息网和重要信息系统安全

C. 创建安全健康的网络环境，保障和促进信息化的发展

D. 保护公共利益，维护国家安全

参考答案：A

难易程度：一级

解析：坚持积极防御、综合防范的方针，全面提高信息安全防护能力，重点保障基础信息网和重要信息系统安全，创建安全健康的网络环境，保障和促进信息化的发展，保护公共利益，维护国家安全。

所属知识子域：网络安全法律法规

14. 2003 年 7 月，国家信息化领导小组制定出台了《关于加强信息安全保障工作的意见》(中办发 27 号文件)，这个文件是我国信息安全保障工作的纲领性文件。文件明确了加强信息安全保障工作的总体要求：坚持( )的方针，全面提高()，重点保障()安全，创建安全健康的网络环境，保障和促进信息化的发展，保护公共利益，维护国家安全。

A. 积极防御、综合防范；信息安全防护能力；基础信息网和重要信息系统

B. 积极防御、综合防范；基础信息网和重要信息系统；信息安全防护能力

C. 立足国情，以我为主，坚持管理与技术并重；信息安全防护能力；基础信息网和重要信息系统

D. 立足国情，以我为主，坚持管理与技术并重；基础信息网和重要信息系统；信息安全防护能力

参考答案：A

难易程度：一级

解析：坚持积极防御、综合防范的方针，全面提高信息安全防护能力，重点保障基础信息网和重要信息系统安全，创建安全健康的网络环境，保障和促进信息化的发展，保护公共利益，维护国家安全。

所属知识子域：网络安全法律法规

15. 网络空间作为新兴的第（）空间，已经成为新的国家竞争领域，威胁来源从个人上升到犯罪组织，甚至上升到国家力量的层面。

A. 2

B. 3

C. 4

D. 5

参考答案：D
难易程度：一级
解析：网络空间作为新兴的第五空间，已经成为新的国家竞争领域，威胁来源从个人上升到犯罪组织，甚至上升到国家力量的层面。

所属知识子域：网络安全法律法规

16. 互联网的不断发展，越来越多的设备被接入并融合，技术的融合将传统的虚拟世界与物理世界相互连接，共同构成了一个新的 IT 世界。最先把网络安全上升到国家高度的国家是（）

A. 英国

B. 美国

C. 俄罗斯

D. 中国

参考答案：B
难易程度：一级
解析：2009 年，美国的《国家网络安全综合计划》(CNCI)被披露出来，信息安全上升到国家安全高度的主张被全世界认可，网络战、关键基础设施保护在现代国防领域中凸显作用。

所属知识子域：网络安全法律法规

17. 以下那个法律被认为是我国网络空间安全的基本法（）

A. 中华人民共和国国家安全法

B. 中华人民共和国网络安全法

C. 中华人民共和国密码法

D. 中华人民共和国电子签名法

参考答案：B
难易程度：一级
解析：中华人民共和国网络安全法

所属知识子域：网络安全法律法规

18. 以下关于“网络安全为人民、网络安全靠人民”这句话的理解最准确的是（）

A. 网络安全是人民内部矛盾问题，靠人民内部解决

B. 网络安全的最终目的是为了人民更好的生活，解决上也要人民群众共同参与

C. 网络安全是为了保护人民群众使用的网络安全，因此要深入人民群众中去

D. 网络安全为了实现人民群众的自主性，因此网络安全全靠人民自己解决

参考答案：B
难易程度：二级

解析：B 选项

所属知识子域：网络安全法律法规

19. 根据《信息安全等级保护管理办法》，（ ）负责信息安全等级保护工作的监督、检查、指导。

A. 公安机关

B. 国家保密工作部门

C. 国家密码管理部门

D. 国家网信办

参考答案：A
难易程度：一级

解析：法律法规

所属知识子域：网络安全法律法规

20. 国家秘密密级分为绝密、机密、秘密三级。（）级国家秘密是最重要的国家秘密，泄露会使国家安全和利益遭受特别严重的损害

A. 绝密
B. 机密
C. 秘密
D. 公开

参考答案：A
难易程度：二级

解析：法律法规

所属知识子域：网络安全法律法规

21. 国家秘密的保密期限，除另有规定外，绝密级不超过（）年，机密级不超过（）年，秘密级不超过（）年。

A. 30、20、10
B. 50、30、20
C. 30、20、15
D. 30、15、10

参考答案：A
难易程度：三级

解析：法律法规

所属知识子域：网络安全法律法规

22. 关于国家秘密载体管理，以下说法错误的是（）

A. 制作国家秘密载体，应当由机关、单位或者经保密行政管理部门保密审查合格的单位承担，制作场所应当符合保密要求

B. 收发国家秘密载体，应当履行清点、编号、登记、签收手续

C. 传递国家秘密载体，应当通过国有邮政企业进行，而不能通过民营快递企业

D. 复制国家秘密载体或者摘录、引用、汇编属于国家秘密的内容，应当按照规定报批，不得擅自改变原件的密级、保密期限和知悉范围，复制件应当加盖复制机关、单位戳记，并视同原件进行管理

参考答案：C

难易程度：三级

解析：传递国家秘密载体，应当通过机要交通、机要通信或者其他符合保密要求的方式进行。

所属知识子域：网络安全法律法规

23. 关于涉密载体，以下说法错误的是（）

A. 机密、秘密级涉密载体应当存放在密码文件柜中；

B. 绝密级涉密载体应当存放在密码保险柜中

C. 涉密计算机应当安装双网卡、一机双网（单位内网、涉密网），且两个网络互相隔离均不与互联网相通

D. 涉密载体应存放在涉密办公场所内，涉密办公场所要相对固定和独立，应当安装门禁、视频监控、防盗报警等安防系统，实行封闭管理

参考答案：C

难易程度：二级

解析：涉密计算机禁止和外网连接

所属知识子域：网络安全法律法规

24. 《刑法》第二百八十五条【非法侵入计算机信息系统罪】违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，（）

A. 处三年以下有期徒刑或者拘役。

B. 三年以上五年以下有期徒刑或者拘役

C. 10000 元罚款

D. 1000 元罚款

参考答案：A

难易程度：二级

解析：处三年以下有期徒刑或者拘役。

所属知识子域：网络安全法律法规

25. 《刑法》第二百八十六条：违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，（）；后果特别严重的，（）。

A. 处五年以下有期徒刑或者拘役；处五年以上有期徒刑。

B. 三年以上五年以下有期徒刑或者拘役；处五年以上有期徒刑。

C. 处五年以上有期徒刑；处五年以上十年以下有期徒刑。

D. 处五年以上有期徒刑；处十年以上有期徒刑。
参考答案:A
难易程度：二级
解析：处五年以下有期徒刑或者拘役；处五年以上有期徒刑。
所属知识子域：网络安全法律法规

26. 关于涉密信息存放，以下说法正确的是（）
A. 涉密信息只能存放在涉密区
B. 涉密信息可以保存在涉密区，也可以保存在内部安全区域
C. 涉密信息进行了 AES 高强度加密以后可以通过互联网传输
D. 以上都正确
参考答案:A
难易程度：二级
解析：法律法规
所属知识子域：网络安全法律法规

27. 在企业中，（）对于信息安全管理都负有责任。
A. 高级管理层
B. 安全管理员
C. IT 管理员
D. 所有与信息系统有关人员
参考答案:D
难易程度：三级
解析：所有与信息系统有关人员
所属知识子域：网络安全法律法规

28. 网络安全法第三十五条规定关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家（）会同国务院有关部门组织的国家安全审查。

A. 公安部

B. 国家安全部

C. 网信部门

D. 国家保密局

参考答案:C
难易程度：一级
解析：网络安全法
所属知识子域：网络安全法律法规

29. 省、直辖市的人民代表大会和它们的常务委员会，在不同宪法、法律、行政法规相抵触的前提下，可以制定地方性法规，报（）备案。

A. 省人民代表大会常务委员会

B. 市人民代表大会常务委员会

C. 全国人民代表大会常务委员会

D. 国务院

参考答案:C

难易程度：一级

解析：省、直辖市的人民代表大会和它们的常务委员会，在不同宪法、法律、行政法规相抵触的前提下，可以制定地方性法规，报全国人民代表大会常务委员会备案。

所属知识子域：网络安全法律法规

30. 以宪法为根本依据，我国的立法分类分为几个层次（）

A. 3 个层次，法律、行政法规、地方性法规

B. 4 个层次，法律、行政法规、地方性法规、自治条例

C. 5 个层次，法律、行政法规、地方性法规、自治条例和单行条例、规章

D. 6 个层次，宪法、法律、行政法规、地方性法规、自治条例和单行条例、规章

参考答案:A

难易程度：一级

解析：以宪法为根本依据，分为法律、行政法规、地方性法规三个层次

所属知识子域：网络安全法律法规

31. 从立法体系而言，宪法具有最高的法律效力，一切法律、行政法规、地方性法规、自治条例和单行条例、规章都不得同宪法相抵触。则我国上位法和下位法之间的关系错误的是（）

A. 法律的效力高于行政法规、地方性法规、规章。

B. 行政法规的效力高于地方性法规、规章。

C. 法律、行政法规、地方性法规如果有超越权限或下位法违反上位法规定的情形的，将依法予以改变或者撤销。

D. 法律、行政法规、地方性法规如果有超越权限或下位法违反上位法规定的，在发现后，将依法予以改变或者撤销，发现之前实施了的维持不变。

参考答案:D

难易程度：一级

解析：从立法体系而言，宪法具有最高的法律效力，一切法律、行政法规、地方性法规、自治条例和单行条例、规章都不得同宪法相抵触。法律的效力高于行政法规、地方性法规、规章。行政法规的效力高于地方性法规、规章。法律、行政法规、地方性法规如果有超越权限或下位法违反上位法规定的情形的，将依法予以改变或者撤销。

所属知识子域：网络安全法律法规

32. 下面不属于第二百八十七条 之一 【非法利用信息网络罪】的是（）

A. 设立用于实施诈骗、传授犯罪方法、制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组的

B. 向他人出售或者提供公民个人信息，情节严重的

C. 发布有关制作或者销售毒品、枪支、淫秽物品等违禁物品、管制物品或者其他违法犯罪信息的

D. 为实施诈骗等违法犯罪活动发布信息的

参考答案:B
难易程度：一级
解析：第二百五十三条之一：【侵犯公民个人信息罪】违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金;情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

所属知识子域：网络安全法律法规

33. 信息安全主要包括信息的保密性、真实性、完整性等，当完整性受到破坏时，信息可能受到了以下哪种攻击（）

A. 篡改
B. 中断
C. 窃听
D. 以上都不正确
参考答案：A
难易程度：二级
解析：完整性是保证信息系统中的数据处于完整的状态，确保信息没有遭受篡改和破坏。
所属知识子域：信息安全与网络空间安全

34. 为保障信息系统的安全性，信息系统还需具备不可否认性，其中不可否认性指（）

A. 信息在传输、交换、存储和处理过程保持非修改、非破坏和非丢失的特性
B. 对流通在网络系统中的信息传播及具体内容能够实现有效控制的特性
C. 通信双方在信息交互过程中，所有参与者都不可能否认或抵赖本人所做的操作
D. 信息按给定要求不泄漏给非授权的个人、实体或过程
参考答案：C
难易程度：二级
解析：不可否认性：证明要求保护的事件或动作及其发起实体的行为。在法律上，不可否认意味着交易的一方不能拒绝已经接收到交易，另一方也不能拒绝已经发送的交易。

所属知识子域：信息安全与网络空间安全

35. 依据《中华人民共和国标准法》将标准级别划分为 4 个层次，不包括（）

A. 国际标准

B. 国家标准
C. 行业标准
D. 地方标准
参考答案：A
难易程度：三级
解析：标准级别是指依据《中华人民共和国标准化法》将标准划分为国家标准、行业标准、地方标准和企业标准等 4 个层次。
所属知识子域：网络空间安全政策与标准

36. 依据信息安全基本属性定义，下面数据的完整性体现为（）
A. 数据不被泄露给非授权用户、实体或过程
B. 数据源不能够否认所发送的数据
C. 数据可被授权实体访问并按需求使用
D. 数据未经授权不能进行更改
参考答案：D
难易程度：三级
解析：完整性是保证信息系统中的数据处于完整的状态，确保信息没有遭受篡改和破坏。
所属知识子域：信息安全与网络空间安全

37. 我国的（ ）主要规定了关于数据电文、电子签名与认证及相关的法律责任。
A. 《中华人民共和国宪法》
B. 《中华人民共和国网络空间安全法》
C. 《中华人民共和国电子签名法》
D. 《商用密码管理条例》
参考答案：C
难易程度：一级
解析：《中华人民共和国电子签名法》由中华人民共和国第十届全国人民代表大会常务委员会第十一次会议于 2004 年 8 月 28 日通过，自 2005 年 4 月 1 日起施行。共计 5 章，三十六条。主要内容是对电子签名的法律效力、适用范围和作为证据的真实性提出要求。
所属知识子域：网络安全法律法规

38. 保证信息不被篡改，使信息能正确生成、存储以及传输，体现了信息安全的哪个性质（）
A. 完整性
B. 即时性
C. 可控性
D. 保密性
参考答案：A
难易程度：二级
解析：完整性是保证信息系统中的数据处于完整的状态，确保信息没有遭受篡改和破坏。
所属知识子域：信息安全与网络空间安全

39. 关键信息基础设施的运营者采购涉及商用密码的网络产品和服务，可能影响国家安全的，应当按照（）的规定，通过国家网信部门会同国家密码管理部门等有关部门组织的国家安全审查。

A. 中华人民共和国网络安全法
B. 中华人民共和国密码法
C. 中华人民共和国保密法
D. 中华人民共和国国家安全法
参考答案：A
难易程度：一级
解析：关键信息基础设施的运营者采购涉及商用密码的网络产品和服务，可能影响国家安全的，应当按照《中华人民共和国网络安全法》的规定，通过国家网信部门会同国家密码管理部门等有关部门组织的国家安全审查。
所属知识子域：网络安全法律法规

40. （）是针对没有国家标准而又需要在全国某个行业范围内统一的技术要求而制定的标准。

A. 国家标准
B. 行业标准
C. 国际标准
D. 地方标准
参考答案：B
难易程度：一级
解析：行业标准是针对没有国家标准而又需要在全国某个行业范围内统一的技术要求而制定的标准。
所属知识子域：网络空间安全政策与标准

41. （）由省、自治区、直辖市标准化行政主管部门制定，并报国务院标准化行政主管部门和国务院有关行政主管部门备案。

A. 地方标准
B. 国家标准
C. 行业标准
D. 区域标准
参考答案：A
难易程度：一级
解析：地方标准由省、自治区、直辖市标准化行政主管部门制定，并报国务院标准化行政主管部门和国务院有关行政主管部门备案。
所属知识子域：网络空间安全政策与标准

42. 国际上，信息安全标准化工作兴起于（）

A. 二十世纪 50 年代中期

B. 二十世纪 60 年代中期

C. 二十世纪 70 年代中期

D. 二十世纪 80 年代初期

参考答案：C

难易程度：一级

解析：国际上，信息安全标准化工作兴起于二十世纪 70 年代中期

所属知识子域：网络空间安全政策与标准

43. 强制性国家标准代号为（）

A. GB/T

B. GB/Z

C. GA/T

D. GB

参考答案：D

难易程度：一级

解析：我国的国家标准分别有：GB 强制性国家标准、GB/T 推荐性国家标准和 GB/Z 国家标准化指导性技术文件。

所属知识子域：网络空间安全政策与标准

44. 违反强制性国家标准会造成什么后果（）

A. 不构成经济方面的责任

B. 不构成法律方面的责任

C. 构成经济或法律方面的责任

D. 以上都错

参考答案：C

难易程度：一级

解析：**强制性标准：**强制性标准具有法律属性，一经颁布必须贯彻执行，违反则构成经济或法律方面的责任。

所属知识子域：网络空间安全政策与标准

45. 国家标准化指导性技术文件在实施后 3 年内必须进行复审。复审的结果是（）

A. 再延长 3 年

B. 转为国家标准

C. 撤销

D. 以上都对

参考答案:D

难易程度：一级

解析：国家标准化指导性技术文件在实施后 3 年内必须进行复审。复审结果的可能是：再延长 3 年;转为国家标准;撤销。

所属知识子域：网络空间安全政策与标准

46. 1999 年国家强制标准《GB17859-1999 计算机信息系统安全保护等级划分准则》发布，正式细化了对计算机系统采用划分等级进行保护的要求。标准对安全保护对象划分了五个安全级别，从低到高分别为（）

A. 用户自主保护、系统审计保护、安全标记保护、结构化保护、访问验证保护

B. 用户自主保护、系统审计保护、访问验证保护、安全标记保护、结构化保护

C. 安全标记保护、系统审计保护、结构化保护、用户自主保护、访问验证保护

D. 安全标记保护、结构化保护、用户自主保护、系统审计保护、访问验证保护

参考答案：A

难易程度：一级

解析：标准对安全保护对象划分了五个安全级别，从低到高分别为用户自主保护、系统审计保护、安全标记保护、结构化保护、访问验证保护。

所属知识子域：网络空间安全政策与标准

47. 某大型企业声称自己的 ISMS 符合 ISO/IBC 27001 或 GB/T22080 标准要求，其信息安全控制措施通常在以下方面实施常规控制，不包括哪一项（）

A. 信息安全方针、信息安全组织、资产管理

B. 人力资源安全、物理和环境安全、通信和操作管理

C. 访问控制、信息系统获取、开发和维护、符合性

D. 规划与建立 ISMS

参考答案：D

难易程度：二级

解析：规划与建立 ISMS 是属于在建设信息安全管理体系前期的工作，不属于常规控制项

所属知识子域：信息安全管理体系建设

48. 《网络安全法》中的网络运营者，是指（）

A. 网络的所有者和高层管理者

B. 高层管理者和和网络服务提供者

C. 网络的所有者和网络服务提供者

D. 网络的所有者、管理者和网络服务提供者

参考答案：D

难易程度：二级

解析：网络安全法

所属知识子域：网络安全法律法规

49. 等级保护 2.0 中，等级保护对象受到破坏时所侵害的客体包括以下（）

A. 公民、法人和其他组织的合法权益

B. 社会秩序、公共利益

C. 国家安全

D. 以上都对

参考答案：D

难易程度：二级

解析：信息安全技术网络安全等级保护定级指南 GBT22240-2020

所属知识子域：网络安全法律法规

50. ISO/IEC 27002 中规定的控制措施被认为是适用于大多数组织的最佳实践，并很容易适应各种规模和复杂性的组织。在 ISO/IEC 27002：2013 中，将控制措施划分为（）个安全控制章节。

A. 11

B. 12

C. 13

D. 14

参考答案：D

难易程度：二级

解析：在 ISO/IEC 27002：2013 中，将控制措施划分为 14 个安全控制章节，35 个主要的安全类别和 113 个控制措施。

所属知识子域：信息安全管理

51. 在信息安全管理实用规则中，控制措施是指企业根据风险评估结果，结合风险应对策

略，确保内部控制目标得以实现的方法和手段。控制措施的目的是改变流程，政策，设备，实践或其他行动的风险。控制措施可以是（）

A. 预防性的

B. 检测性的

C. 纠正性的

D. 以上都对

参考答案：D

难易程度：一级

解析：控制措施是指企业根据风险评估结果，结合风险应对策略，确保内部控制目标得以实现的方法和手段。控制措施的目的是改变流程，政策，设备，实践或其他行动的风险。控制可以是预防性的，检测性或纠正性。

所属知识子域：信息安全管理

52. 信息安全管理体系(ISMS)在哪个阶段需要确立总体战略和业务目标，规模和地域分布范围，通过对信息资产及其价值的确定、信息处理，存储和通信的业务需求以及法律，监管和合同要求等方面理解来识别信息安全要求。（）

A. 规划与建立阶段

B. 实施和运行阶段

C. 监视和评审阶段

D. 维护和改进阶段

参考答案：A

难易程度：一级

解析：组织在规划与建立阶段确立总体战略和业务目标，规模和地域分布范围，通过对信息资产及其价值的确定、信息处理，存储和通信的业务需求以及法律，监管和合同要求等方面理解来识别信息安全要求。

所属知识子域：信息安全管理

53. 企业按照 ISO27001 标准建立信息安全管理体系过程中，对关键成功因素描述错误的是（）

A. 来自所有管理层级、特别是最高管理者的可见支持和承诺

B. 有效的信息安全意识、培训和教育计划

C. 只需要高层管理员和 IT 部门的人员参与建设信息安全管理体系，不需要全体员工参与

D. 所有管理者、员工及其他相关方理解企业信息安全策略、指南与标准等当中他们的信息安全义务，并遵照执行

参考答案：C

难易程度：一级

解析：信息安全管理体系成功因素

所属知识子域：信息安全管理

54. 组织首先必须能够认识到信息安全对组织所形成的必要性，信息安全关联着组织的业务命脉，在现代高度依赖信息化发展的产业链中，没有信息安全就没有成功的企业。下面不会对组织业务产生致命影响的是（）

A. 知识产权盗窃

B. 用户敏感信息泄露

C. 组织信息系统遭到勒索或拒绝服务攻击

D. 重要技术员辞职

参考答案：D

难易程度：一级

解析：信息安全管理体系成功因素

所属知识子域：信息安全管理

55. 下面对信息安全管理体系理解错误的是（）

A. 信息安全不是一个部门的工作，也不是某个人的职责

B. 最高领导不应该成为信息安全工作的第一责任人，被委托的高层管理者才是

C. 信息安全应该贯穿于整个组织

D. 组织的每个成员都需要承担相关的义务和责任

参考答案：B

难易程度：一级

解析：信息安全管理体系成功因素

所属知识子域：信息安全管理

56. 信息安全管理就是风险管理，因此，信息安全控制措施的本质就是（）

A. 风险评估

B. 信息系统审计

C. 风险处置

D. 信息安全管理体系的建设

参考答案：C

难易程度：一级

解析：信息安全管理就是风险管理，因此，信息安全控制措施的本质就是风险处置。

所属知识子域：信息安全管理

57. 在信息安全管理体系建设中，信息系统与安全之间的关系理解正确的是（）

A. 同步规划、同步建设、同步使用

B. 可以不同步规划和同步建设，但要同步使用

C. 要同步规划，但可以不同步建设和使用

D. 以上说法都错

参考答案：A

难易程度：一级

解析：信息系统与安全的“同步规划、同步建设、同步使用”已经被立法约束。

所属知识子域：信息安全管理

58. 对 PDCA 特征的理解错误的是（）

A. 按照 P-D-C-A 的顺序依次进行，周而复始，发现问题，分析问题，然后解决问题

B. 大环套小环，把安全目标的分解成多个小目标，一层层地解决问题，最终把安全目标达成

C. 信息安全风险管理的思路不符合 PDCA 的问题解决思路，两者没有关系

D. 阶梯式上升，每次循环都要进行总结，巩固成绩，改进不足，使组织的管理体系能够得到持续的改进，管理水平将随之不断提升。

参考答案：C

难易程度：一级

解析：PDCA 是管理学中常用的一个过程模型，该模型在应用时，按照 P-D-C-A 的顺序依次进行，一次完整的 P-D-C-A 可以看成组织在管理上的一个周期，每经过一次 P-D-C-A 循环，组织的管理体系都会得到一定程度的完善，同时进入下一个更高级的管理周期，通过连续不断的 P-D-C-A 循环，组织的管理体系能够得到持续的改进，管理水平将随之不断提升。

所属知识子域：信息安全管理

59. 在《ISO/IEC 27001:2013 信息安全管理体系要求》中定义了 PDCA 过程方法的四个阶段主要工作：规划与建立、实施与运行、监视与评审、（）

A. 维持与改进

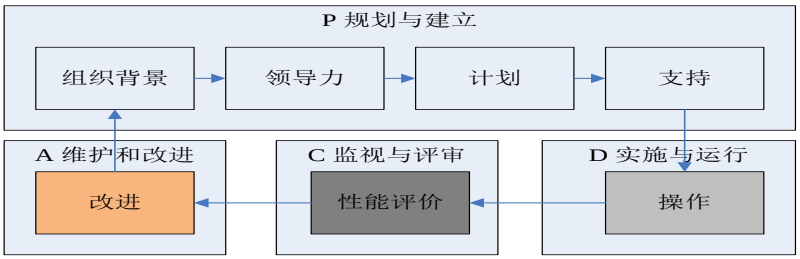
B. 维持与报告

C. 报告与监督

D. 监督与报告

参考答案：A

难易程度：一级

解析： 

所属知识子域：信息安全管理

60. 信息安全管理体系是建立在（）的基础之上，信息安全管理体系文件的建立和管理遵从质量管理体系文件规范和要求。

A. 组织持续运行

B. 文档化

C. 企业文化标准化

D. 管理者持续支持

参考答案：B

难易程度：一级

解析：信息安全管理体系是建立在文档化的基础之上，信息安全管理体系文件的建立和管理遵从质量管理体系文件规范和要求。

所属知识子域：信息安全管理

61. 信息安全管理体系文档层次化的文件结构是构成管理体系的重要内容之一，通常文件分为四个层级，下面属于三级文件的是（）

A. 方针、政策

B. 制度、流程、规范

C. 法律、政策导向、制度

D. 使用手册、操作指南、作业指导书

参考答案：D

难易程度：一级

解析：三级文件：使用手册、操作指南、作业指导书

所属知识子域：信息安全管理

62. 信息安全管理体系文档层次化的文件结构是构成管理体系的重要内容之一，通常文件分为四个层级，下面属于一级文件的是（）

A. 方针、政策

B. 方针、制度、流程

C. 法律、政策导向、制度

D. 使用手册、操作指南、作业指导书

参考答案：A

难易程度：一级

解析：一级文件：方针、政策

所属知识子域：信息安全管理

63. 信息安全管理体系文档层次化的文件结构是构成管理体系的重要内容之一，通常文件分为四个层级，下面属于四级文件的是（）

A. 制度、流程、使用手册、规范

B. 标准、制度、流程、检查表

C. 标准、制度、流程、检查表、记录

D. 日志、记录、检查表、模板、表单等

参考答案：D

难易程度：一级

解析：四级文件：日志、记录、检查表、模板、表单等

所属知识子域：信息安全管理

64. 信息安全管理体系文档层次化的文件结构是构成管理体系的重要内容之一，通常文件分为四个层级，由谁签署发布（）

A. 董事会

B. 组织管理者代表

C. 综合办公室资源管理处

D. 风险管理部

参考答案：B

难易程度：一级

解析：二级文件：由组织管理者代表签署发布，该文件针对组织宏观战略提出的目标建立组织内部的“法”。

所属知识子域：信息安全管理

65. **信息安全管理体系文档层次化中，其中第四级文件是整个组织的底层基础性文件，每个文件理论上都应该形成相应的记录，因此四级文件也是我们通常所说的审核证据。下面对四级文件理解错误的是（）**

A. 四级文件是对整个组织所形成的检查列表、表单、日志等记录性文件建立，并归类

B. 所有文件必需具有连续性、可以追溯

C. 业务表单及记录，必须贯穿整个组织业务的始终，形成一个闭环

D. 重要业务表单及记录才必须贯穿整个组织业务的始终，形成一个闭环

参考答案：D

难易程度：一级

解析：信息安全管理体系文档化

所属知识子域：信息安全管理

66. 在建立信息安全管理体系时，组织应确定管理范围，对管理范围理解正确的是（）

A. 组织的全部

B. 也可以是组织的一个系统

C. 也可以是一个部门或者一个人

D. 以上都正确

参考答案：D

难易程度：一级

解析：在建立信息安全管理体系时，组织应确定管理范围，范围可以是组织的全部，也可以是组织的一个系统，一个部门或者一个人，组织的范围依据管理的具体要求所涉及的人、事、物来建立。

所属知识子域：信息安全管理

67. （）是建立信息安全管理体系的基础，首先应该了解组织有关信息安全的内部(人员、管理、流程等)和外部(合作伙伴、供应商、外包商等)问题，以及影响组织建立体系时需要解决的内部和外部问题。

A. 建立组织背景

B. 建立组织结构

C. 文档化

D. 最高管理层的承诺

参考答案：A

难易程度：一级

解析：建立组织背景是建立信息安全管理体系的基础，首先应该了解组织有关信息安全的内部(人员、管理、流程等)和外部(合作伙伴、供应商、外包商等)问题，以及影响组织建立体系时需要解决的内部和外部问题。

所属知识子域：信息安全管理

68. 组织建立信息安全管理体系，在信息安全方针中明确描述组织的角色、职责和权限。常见的角色原则理解错误的是（）

A. 遵循最小授权

B. 知必所需

C. 岗位轮换

D. 遵循最大授权

参考答案：D

难易程度：一级

解析：在信息安全方针中明确描述组织的角色、职责和权限。常见的角色遵循最小授权、知必所需、岗位轮换等原则。

所属知识子域：信息安全管理

69. 信息安全管理体系（ISMS）的计划，是建立在风险评估基础之上，只有在组织风险不可接受的时候才需要建立控制计划。风险评估是客观，只有客观的风险评估才能为组织安全战略提供最具（）的控制。

A. 费效比

B. 有效性

C. 有价值

D. 有竞争力

参考答案：A

难易程度：一级

解析：计划的建立是在风险评估基础之上，只有在组织风险不可接受的时候才需要建立控制计划。风险评估是客观，只有客观的风险评估才能为组织安全战略提供最具费效比的控制。

所属知识子域：信息安全管理

70. 在建立信息安全管理体系的过程中，组织的计划必须符合组织的安全目标，层次化的计划通过层次化的文件体系反映在不同层级的组织机构中执行。安全目标与方针应可以（）并持续改进，通过持续改进实现组织信息安全的螺旋式上升。

A. 检测

B. 度量

C. 评审

D. 优化

参考答案：B

难易程度：一级

解析：度量

所属知识子域：信息安全管理

71. 信息安全管理体系在实施与运行过程中，选择和实施控制措施以降低风险，对控制风险理解正确的是（）

A. 确保把风险降低到可接受的水平

B. 实施控制措施后，确保风险完全消除，是风险管理的目标

C. 在风险不可能解决的情况了，组织应放弃该资产，以达到解决风险的目的

D. 风险是不可能消除的，所以要不计成本的去降低风险，杜绝风险事件的发生

参考答案：A

难易程度：一级

解析：选择和实施控制措施以降低风险。控制措施需要确保风险降至可接受的水平，同时考虑到国家和国际立法和条例的要求和限制、组织的安全目标、组织对操作的要求和限制。

所属知识子域：信息安全管理

72. 对每个信息系统的建设来说，信息安全控制在哪个阶段考虑是最合适也是成本最低的（）

A. 在系统项目需求规格和设计阶段考虑信息安全控制

B. 在信息系统编码阶段考虑

C. 在信息系统的实施阶段考虑

D. 在信息系统运行和管理阶段考虑

参考答案：A

难易程度：一级

解析：在系统项目需求规格和设计阶段考虑信息安全控制。

所属知识子域：信息安全管理

73. 在信息安全管理体系建设过程的监视和评审阶段，ISMS 审核将检查 ISMS 是否包含适用于在 ISMS 范围内处理风险的特定控制。此外，根据这些监测区域的记录，提供验证证据，以及纠正，预防和改进措施的（）。

A. 可控性

B. 有效性

C. 真实性

D. 可追溯性

参考答案：D

难易程度：一级

解析：根据这些监测区域的记录，提供验证证据，以及纠正，预防和改进措施的可追溯性。

所属知识子域：信息安全管理

74. 持续改进信息安全管理系统的目的是提高实现保护信息机密性，可用性和完整性目标的可能性。下面对改进行动理解错误的是（）

A. 当不符合时，组织需要重现不符合，如适用采取行动控制，修正其事项并处理事项的后果

B. 评估消除不符合原因需要的行为，通过评审不符合项、确定不符合的原因并确认有相似的不符合存在或者潜在的不符合发生的情况以促使其不复发或在不在其他地方发生。

C. 组织需要持续改进 ISMS 的适宜性、充分性和有效性，定期的改进有助于组织形成信息安全管理水平的螺旋式上升。

D. 当不符合时，组织需要对不符合性进行适宜性、充分性和有效性进行评审，一次性解决，杜绝持续改进，以防浪费时间和成本。

参考答案：D

难易程度：一级

解析：维护和改进内容

所属知识子域：信息安全管理

75. 我国哪一部法律正式宣告在网络空间安全领域，将等级保护制度作为基本国策，同时也正式将针对信息系统的等级保护标准变更为针对网络安全的等级保护标准。

A. 中华人民共和国国家安全法

B. 信息安全等级保护管理办法

C. 中华人民共和国网络安全法

D. 1994 年国务院颁布的《中华人民共和国计算机信息系统安全保护条例》

参考答案：C

难易程度：一级

解析：2016 年 11 月发布的网络安全法第二十一条明确指出“国家实行网络安全等级保护制度”。正式宣告在网络空间安全领域，我国将等级保护制度作为基本国策。

所属知识子域：网络安全法律法规

76. 道德是法律的基础，法律是道德的延伸，道德与法律之间的关系理解正确的是（）

A. 道德规范约束范围广，法律约束范围要小

B. 道德规范具有人类共同的特性，法律具有国家地区特性

C. 科学的法律和道德规范应保持一致

D. 违反道德底线的行为一定违法，但是违法行为往往不一定违反道德的底线

参考答案：C

难易程度：一级

解析：科学的法律和道德规范是保持一致的

所属知识子域：网络安全法律法规

77. 人们在使用计算机软件或数据时，应遵照国家有关法律规定，尊重其作品的版权，这是使用计算机的基本道德规范。建议人们养成良好的道德规范，针对作品知识产权，下面说法错误的是（）

A. 应该使用正版软件，坚决抵制盗版，尊重软件作者的知识产权

B. 维护计算机的正常运行，保护计算机系统数据的安全

C. 不要为了保护自己的软件资源而制造病毒保护程序

D. 不要擅自篡改他人计算机内的系统信息资源

参考答案：B

难易程度：三级

解析：B 选项内容讲的是计算机安全，与题干知识产权无关

所属知识子域：网络安全法律法规

78. 作为国家注册信息安全专业人员应该遵循其应有的道德准则，中国信息安全测评中心为 CISP 持证人员设定了职业道德准则。下面选项正确的是（）

A. 自觉维护国家信息安全，拒绝并抵制泄露国家秘密和破坏国家信息基础设施的行为

B. 自觉维护网络社会安全，拒绝并抵制通过计算机网络系统谋取非法利益和破坏社会和谐的行为

C. 自觉维护公众信息安全，拒绝并抵制通过计算机网络系统侵犯公众合法权益和泄露个人隐私的行为

D. 以上都对

参考答案：D

难易程度：一级

解析：CISP 持证人员职业道德准则

所属知识子域：网络安全法律法规

79. 作为国家注册信息安全专业人员应该遵循其应有的道德准则，下面对“诚实守信，遵纪守法”的说法错误的是（）

A. 不通过计算机网络系统进行造谣、欺诈、诽谤、弄虚作假等违反诚信原则的行为

B. 利用日常工作、学术交流等各种方式保持和提升信息安全实践能力

C. 不利用个人的信息安全技术能力实施或组织各种违法犯罪行为

D. 不在公众网络传播反动、暴力、黄色、低俗信息及非法软件

参考答案：B

难易程度：一级

解析：B 选项内容是发展自身，维护荣誉方面，与诚实守信，遵纪守法无关

所属知识子域：网络安全法律法规

80. 信息是一种资产，与其他重要的业务资产一样，对组织业务必不可少，因此需要得到适当的保护。信息的价值一般从（）三个层面来看待。

A. 企业视角、用户视角、攻击者视角

B. 国家视角、企业视角、攻击者视角

C. 企业视角、服务视角、用户视角

D. 国际视角、国家视角、个人视角

参考答案：A

难易程度：一级

解析：信息的价值从企业视角、用户视角和攻击者视角三个层面来看待。

所属知识子域：信息安全管理

81. 安全模型是安全策略的清晰表述方式，具有以下哪些特点（）

A. 精确的、无歧义的

B. 简单的、抽象的，易于理解

C. 只涉及安全性质，不限制系统的功能及其实现

D. 以上都是

参考答案：D

难易程度：一级

解析：

所属知识子域：信息安全管理

82. CIA 指信息安全的三大要素，其中 C、I、A 依次代表（ ）

A. 机密性、完整性、可用性

B. 可控性、准确性、可靠性

C. 机密性、真实性、可用性

D. 机密性、不可否认性、可用性

参考答案：A

难易程度：一级

解析：CIA 三元组定义了信息安全的基本属性，分别是机密性，完整性和可用性，信息安全首要就是保护信息的这三个基本属性

所属知识子域：信息安全与网络空间安全

83. 信息不泄漏给非授权的个人、实体或过程，体现了信息安全哪一个性质（）

A. 完整性

B. 可用性

C. 保密性

D. 不可否认性

参考答案：C

难易程度：一级

解析：保密性也称机密性，是指对信息资源开放范围的控制，确保信息不被非授权的个人、组织和计算机程序访问

所属知识子域：信息安全与网络空间安全

84. 近年来，我国面临日趋严峻的网络安全形势，党和国家高度重视信息安全建设，关于网络安全形势的描述中，理解错误的是（ ）

A. 我国的网络安全形势差，但在党和国家高度重视的情况下，面临各种攻击、威胁都能解决，发展稳定

B. 持续性威胁常态化，我国面临的攻击十分严重

C. 大量联网智能设备遭受恶意程序攻击形成僵尸网络，被用于发起大流量 DDoS 攻击

D. 网站数据和个人信息泄露屡见不鲜

参考答案：A

难易程度：一级

解析：攻击和威胁并不是都能解决的，我国面临的网络安全态势情况十分严重

所属知识子域：信息安全与网络空间安全

85. 信息安全已经成为社会的焦点问题，以下不属于信息系统安全运营原则的是（ ）

A. 合规性与风险控制结合的原则

B. 绝对安全原则

C. 统一管控原则

D. 易操作性原则

参考答案：B

难易程度：三级

解析：信息系统安全是没有绝对安全的

所属知识子域：信息安全管理

86. 作为全方位的、整体的信息安全防范体系是分层次的，以下关于企业信息系统层次划分的描述，理解错误的是（ ）

A. 越接近内部的网络安全要求等级越低，越接近外部的网络安全要求等级越高

B. 业务专用网是企业为了特殊工作需要而建造的专用网络

C. 互联网区域用于日常的互联网业务，安全防护等级要求最低

D. 企业内网是企业的核心网络，拥有最高的安全防护等级

参考答案：A

难易程度：三级

解析：越接近内部的网络安全要求等级越高，越接近外部的网络安全要求等级越低

所属知识子域：信息安全管理

87. 随着网络空间安全重要性的不断提高，网络安全态势感知（NSSA）的研究与应用正在得到更多的关注。以下关于 NSSA 的描述，理解错误的是（）

A. 态势感知的数据来源丰富

B. 态势感知结果丰富实用

C. 态势感知适用范围十分窄

D. 态势感知能对网络安全状况的发展趋势进行预测

参考答案：C

难易程度：三级

解析：态势感知适用范围十分广

所属知识子域：信息安全管理

88. 信息系统安全策略应该全面地考虑保护信息系统整体的安全，在设计策略的范围时，主要考虑（）

A. 物理安全策略

B. 网络安全策略

C. 数据加密策略

D. 以上都是

参考答案：D

难易程度：一级

解析：物理安全、网络安全、数据安全都需要考虑

所属知识子域：信息安全管理

89. 计算机信息系统安全保护等级根据计算机信息系统在国家安全、经济建设、社会生活中的（），计算机信息系统受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（）等因素确定。

A. 经济价值；经济损失

B. 重要程度；危害程度

C. 经济价值；危害程度

D. 重要程度；经济损失

参考答案：B

难易程度：一级

解析：物理安全、网络安全、数据安全都需要考虑

所属知识子域：信息安全管理

90. 关键信息基础设施的安全保护等级应不低于等保（）

A．一级

B．二级

C．三级

D．四级

参考答案：C

难易程度：一级

解析：关键信息基础设施的安全保护等级应不低于等保三级

所属知识子域：信息安全管理

91. 信息系统被破坏后，会对国家安全造成一般损害的，应定级为（）

A．一级

B．二级

C．三级

D．四级

参考答案：C

难易程度：一级

解析：第三级，等级保护对象受到破坏后，会对社会秩序和公共利益造成严重损害，或者国家安全造成危害。只要对国家安全造成危害的，最低定级为三级

所属知识子域：信息安全管理

92. 我们可根据信息安全事件的起因、表现、结果等将信息安全事件分类，以下选项不属于信息安全事件分类的是（ ）

A. 恶意程序事件
B. 网络攻击事件
C. 信息破坏事件
D. 社会工程学攻击
参考答案：D

难易程度：一级

解析：社会工程学攻击不属于事件分类

所属知识子域：信息安全管理

93. 信息内容安全是信息安全在政治、法律、道德层次上的要求。信息内容安全领域的研究内容主要有（ ）

A. 信息内容的获取、分析与识别
B. 信息内容的管理和控制
C. 信息内容安全的法律保障
D. 以上都是
参考答案：D

难易程度：一级

解析：

所属知识子域：信息安全法律法规

94. 组织识别风险后，可采取的处理方式不合理的是（）

A. 缓解风险
B. 转移风险
C. 忽略风险
D. 规避风险
参考答案：C

难易程度：一级

解析：组织识别风险后，可采取的处理方式有：风险规避、风险缓解、风险转移

所属知识子域：信息安全管理

95. 威胁情报的出现将网络空间安全防御从传统被动式防御转换到主动式防御。以下选项中不属于安全威胁情报基本特征的是（）

A. 时效性
B. 相关性
C. 准确性
D. 不可操作性
参考答案：D

难易程度：二级

解析：信息安全威胁情报的基本特征是时效性、相关性、准确性

所属知识子域：信息安全管理

96. 参照国家标准 GB/Z20986-2007《信息安全事件分类指南》，根据信息安全事件发生的原因、表现形式等，对网络/信息安全事件进行分类，下列选项中错误的是（）

A. 恶意程序事件是指蓄意制造、传播有害程序，或是因受到有害程序性的影响而导致的信息安全事件

B. 网络攻击事件是指通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对信息系统实施攻击

C. 信息破坏事件是指利用信息网络发布、传播危害国家安全、社会稳定和公共利益的内容的安全事件

D. 设备设施故障是指由于信息系统自身故障或外围保障设施故障而导致的信息安全事件

参考答案：C

难易程度：二级

解析：信息破坏事件是指通过网络或其他技术手段，造成信息系统中的信息被篡改、假冒、泄漏、窃取等 而导致的信息安全事件。

所属知识子域：信息安全管理

97. 下面不属于违反《刑法》第二百八十五条非法侵入计算机信息系统罪的是（）

A. 违反国家规定，非法侵入计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，情节严重的

B. 违反国家规定，对计算机信息系统实施非法控制，情节严重的

C. 违反国家规定，提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的

D. 违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行

参考答案：D

难易程度：一级

解析：刑法第二百八十六条 【破坏计算机信息系统罪】违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役;后果特别严重的，处五年以上有期徒刑。

所属知识子域：信息安全法律法规

98. 有关危害国家秘密安全的行为的法律责任，下面说法正确的是（）

A. 违反保密规定行为只要发生，无论是否产生泄密实际后果，都要依法追究责任

B. 非法获取国家秘密，不会构成刑事犯罪，不需承担刑事责任

C. 过失泄露国家秘密，不会构成刑事犯罪，不需承担刑事责任

D. 承担了刑事责任，无需再承担行政责任和 / 或其他处分

参考答案：A

难易程度：一级

解析：保守国家秘密是一种国家行为,也是一种国家责任。危害到国家秘密安全的行为都必须受到法律追究。

所属知识子域：信息安全法律法规

99. 以下对于信息安全事件理解错误的是（）

A. 信息安全事件，是指由于自然或者人为以及软硬件本身缺陷或故障的原因，对信息系统造成危害，或在信息系统内发生对社会造成负面影响的事件

B. 对信息安全事件进行有效管理和响应，最小化事件所造成的损失和负面影响，是组织信息安全战略的一部分

C. 应急响应是信息安全事件管理的重要内容

D. 通过部署信息安全策略并配合部署防护措施，能够对信息及信息系统提供保护，杜绝信息安全事件的发生

参考答案：D

难易程度：一级

解析：信息安全事件无法杜绝

所属知识子域：信息安全法律法规

100. 假设一个信息系统已经包含了充分的预防控制措施，那么安装监测控制设备（）

A. 是多余的，因为它们完成了同样的功能，增加了组织成本

B. 是必须的，可以为预防控制的功效提供检测

C. 是可选的，可以实现深度防御

D. 在一个人工系统中是需要的，但在一个计算机系统中则是不需要的，因为预防控制功能已经足够

参考答案：C

难易程度：二级

解析：安装监测控制设备是可选的，实现了深层防御管理原则

所属知识子域：信息安全管理

101. 以下哪些是需要在信息安全策略中进行描述的（）

A. 组织信息系统安全架构

B. 信息安全工作的基本原则

C. 组织信息安全技术参数

D. 组织信息安全实施手段

参考答案：B

难易程度：二级

解析：安全策略是宏观的原则性要求，不包括具体的架构、参数和实施手段。

所属知识子域：信息安全管理

102. 在信息安全管理体系中，下面的角色对应的信息安全职责不合理的是（）

A. 高级管理层：最终责任

B. 信息安全部门主管：提供各种信息安全工作必须的资源

C. 系统的普通使用者：遵守日常操作规范
D. 审计人员：检查安全策略是否被遵从
参考答案：B

难易程度：二级

解析：通常由管理层提供各种信息安全工作必须的资源

所属知识子域：信息安全管理

103. 自 2004 年 1 月起，国内各有关部门在申报信息安全国家标准计划项目时，必须经由以下哪个组织提出工作意见，协调一致后由该组织申报。

A. 全国通信标准化技术委员会(TC485)
B. 全国信息安全标准化技术委员会(TC260)
C. 中国通信标准化协会(CCSA)
D. 网络与信息安全技术工作委员会
参考答案：B

难易程度：一级

解析：自 2004 年 1 月起，各有关部门在申报信息安全国家标准计划项目时，必须经信安标委提出工作意见，协调一致后由信安标委组织申报

所属知识子域：信息安全政策及标准

104. 安全事件管理和应急响应，以下说法错误的是（）

A. 应急响应是指组织为了应对突发或重大信息安全事件的发生所做的准备，以及在事件发生后所采取的措施
B. 应急响应方法，将应急响应管理过程分为遏制、根除、处置、恢复、报告和跟踪 6 个阶段
C. 对信息安全事件的分级主要参考信息系统的重要程度、系统损失和社会影响三方面因素
D. 根据信息安全事件的分级参考要素，可将信息安全事件划分为 4 个级别：特别重大事件(I级)、重大事件(II级)、较大事件(III级)和一般事件(IV级)
参考答案：B

难易程度：一级

解析：应急响应的六个阶段是准备、检测、遏制、根除、恢复、跟踪总结

所属知识子域：信息安全管理

105. 信息的存在形式说法正确的是（）

A. 借助媒体以多种形式存在

B. 存储在计算机、磁带、纸张等介质中

C. 记忆在人的大脑里

D. 以上都对

参考答案：D

难易程度：一级

解析：信息的存在形式：信息是无形的、借助媒体以多种形式存在、存储在计算机、磁带、纸张等介质中、记忆在人的大脑里

所属知识子域：信息安全与网络空间安全

106. 信息安全应该建立贯穿信息系统的整个生命周期，综合考虑（）

A. 人

B. 技术

C. 管理和过程控制

D. 以上都对

参考答案：D

难易程度：一级

解析：信息安全应该建立在整个生命周期中所关联的人、事、物的基础上，综合考虑人、技术、管理和过程控制，使得信息安全不是一个局部而是一个整体。

所属知识子域：信息安全与网络空间安全

107. 机密性保护需要考虑的问题（）

A. 信息系统中的数据是否都有标识，说明重要程度

B. 信息系统中的数据访问是否有权限控制

C. 信息系统中的数据访问是否有记录

D. 以上都对

参考答案：D

难易程度：一级

解析：信息系统中数据的标识、重要程度、权限、记录等都要考虑

所属知识子域：信息安全与网络空间安全

108. 我国信息安全保障工作的主要原则是（）

A. 技术为主，管理为辅

B. 管理为主，技术为辅

C. 技术与管理并重

D. 综合防御，自主发展

参考答案：C

难易程度：一级

解析：我国信息安全保障工作的主要原则：技术与管理并重，正确处理安全与发展的关系

所属知识子域：信息安全与网络空间安全

109. 网络空间安全理解正确的是（）

A. 网络战其作为国家整体军事战略的一个组成部分已经成为事实

B. 网络战只是作为国家整体军事战略的一个概念，没有那严重

C. 网络是个虚拟的世界，真正发生战争时，可以采取断网

D. 网络战是夸大的概念，和海、陆、空、外太空相比，还差很多

参考答案：A

难易程度：一级

解析：国家网络空间安全战略的发布及网络安全法等法律法规的出台，网络安全上升为国家整体军事战略的一个组成部分已经成为事实

所属知识子域：网络安全法律法规

110. 我国的国家网络空间安全战略主要强调了（）

A. 维护网络空间主权

B. 和平利用网络空间、依法治理网络空间

C. 统筹网络安全与发展

D. 以上都对

参考答案：D

难易程度：一级

解析：国家网络空间安全战略内容

所属知识子域：网络安全法律法规

111. ( )根据宪法和法律，规定行政措施，制定行政法规，发布决定和命令.

A. 国务院

B. 最高人民法院

C. 最高人民检察院

D. 全国人大政协委员会

参考答案：A

难易程度：一级

解析：国务院

所属知识子域：网络安全法律法规

112. 下面不属于网络安全法第二章网络安全支持与促进内容的是（）

A. 开展经常性网络安全宣传教育

B. 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理

C. 统筹规划，扶持网络安全产业

D. 推动社会化网络安全服务体系建设

参考答案：B

难易程度：一级

解析：在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理。

是网络安全法适应范围

所属知识子域：网络安全法律法规

113. 采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于（）

A. 三个月

B. 六个月

C. 九个月

D. 十二个月

参考答案：B

难易程度：一级

解析：六个月

所属知识子域：网络安全法律法规

114. 下面属于网络运营者责任的是（）

A. 实名服务：提供服务前要求用户实名

B. 应急预案：制定网络安全事件应急预案

C. 信息发布合规：开展网络安全活动、信息发布合规

D. 以上都对

参考答案：D

难易程度：一级

解析：网络安全法

所属知识子域：网络安全法律法规

115. 关键基础设施运营中产生的数据必须（），因业务需要向外提供的，按照国家网信部门会同国务院有关部门制定的办法进行安全评估。

A. 境内存储

B. 境外存储

C. 国家存储

D. 本地存储

参考答案：A

难易程度：一级

解析：网络安全法

所属知识子域：网络安全法律法规

116. 《个人信息和重要数据出境安全评估办法（征求意见稿）》中，要求建立个人信息出境

记录并且至少保存（）年。

A. 3 年

B. 4 年

C. 5 年

D. 6 年

参考答案：C

难易程度：一级

解析：

所属知识子域：网络安全法律法规

117. 等保 2.0 一级安全区域边界的访问控制进行检查，以允许/拒绝数据包进出，以对检查的内容不包括（）

A. 源端口、目的端口

B. 源地址、目的地址

C. 协议

D. 访问控制策略

参考答案：D

难易程度：一级

解析：应对源地址、目的地址、源端口、目的端口和协议等进行检查,以允许/拒绝数据包进出。

所属知识子域：网络安全法律法规

118.（）规定网络安全等级保护指导思想、原则和要求。

A.《关于信息安全等级保护工作的实施意见的通知》2004 年 9 月 15 日发布

B.《中华人民共和国计算机信息系统安全保护条例》1994 年 2 月 18 日发布

C.《计算机信息系统安全保护等级划分准则》GB 17859-1999

D.《信息安全等级保护管理办法》2007 年 6 月 22 日

参考答案：A

难易程度：一级

解析：网络安全法

所属知识子域：网络空间安全政策与标准

119. 标准化的基本特点理解正确的是（）

A. 标准化是一项活动

B. 标准化的对象是人、事、物

C. 标准化的效益只有应用后才能体现

D. 以上都正确

参考答案：D

难易程度：一级

解析：标准化的基本特点：标准化是一项活动；标准化的对象：物、事、人；标准化是一个动态的概念；标准化是一个相对的概念；标准化的效益只有应用后才能体现

所属知识子域：网络空间安全政策与标准

120. 信息安全管理可以区分为对内和对外的组织价值，下面属于对组织内的是（）

A. 建立起文档化的信息安全管理规范，实现有“法”可依，有章可循，有据可查

B. 能够帮助界定外包时双方的信息安全责任;

C. 可以使组织更好地满足客户或其他组织的审计要求;

D. 可以使组织更好地符合法律法规的要求

参考答案：A

难易程度：一级

解析：对内：能够保护关键信息资产和知识产权，维持竞争优势;在系统受侵袭时，确保业务持续开展并将损失降到最低程度;建立起信息安全审计框架，实施监督检查;建立起文档化的信息安全管理规范，实现有“法”可依，有章可循，有据可查;

所属知识子域：信息安全管理

121. 信息安全管理可以区分为对内和对外的组织价值，下面属于对组织外的是（）

A. 能够保护关键信息资产和知识产权，维持竞争优势;

B. 在系统受侵袭时，确保业务持续开展并将损失降到最低程度;

C. 建立起信息安全审计框架，实施监督检查;

D. 能够使各利益相关方对组织充满信心

参考答案：D

难易程度：一级

解析：对外：能够使各利益相关方对组织充满信心;能够帮助界定外包时双方的信息安全责任;可以使组织更好地满足客户或其他组织的审计要求;可以使组织更好地符合法律法规的要求;若通过了 ISO27001 认证，能够提高组织的公信度;可以明确要求供应商提高信息安全水平，保证数据交换中的信息安全。

所属知识子域：网络空间安全政策与标准

122. 我国信息安全管理标准 GB/T 22080 等同采用（）

A. GB/T9000

B. ISO/IEC 27001

C. ISO/IEC 27002

D. ISO/IEC 22301

参考答案：B

难易程度：一级

解析：B 是对的

所属知识子域：网络空间安全政策与标准

123. 组织机构的信息安全管理的水平取决于管理中（）的环节

A. 脆弱性最强的

B. 技术最好的

C. 最薄弱

D. 业务最重要的

参考答案：C

难易程度：一级

解析：组织机构的信息安全管理的水平取决于管理中最薄弱的环节

所属知识子域：网络空间安全政策与标准

124. 根据《信息安全等级保护管理办法》，（ ）应当依照相关规范和标准督促、检查、指导本行业、本部门或本地区信息系统运营、使用单位的信息安全等级保护工作。

A. 公安机关

B. 国家保密工作部门

C. 国家密码管理部门

D. 信息系统的主管部门

参考答案：D

难易程度：一级

解析：信息系统的主管部门

所属知识子域：网络空间安全政策与标准

125. 信息系统建设完成后，（ ）的信息系统的运营使用单位应当选择符合国家规定的测评机构进行测评合格方可投入使用。

A. 二级及以上

B. 三级及以上

C. 四级及以上

D. 五级

参考答案：A

难易程度：一级

解析：二级及以上

所属知识子域：网络空间安全政策与标准

126. 在安全评估过程中，采取( )手段，可以模拟黑客入侵过程，检测系统安全脆弱性。

A. 问卷调查

B. 人员访谈

C. 渗透测试
D. 手工检查
参考答案：C

难易程度：二级

解析：渗透测试是通过模拟恶意黑客的攻击方法，来评估计算机网络系统安全的一种评估方法。

所属知识子域：信息安全与网络空间安全

127. 对于一个组织机构来说，资产包括（）
A. 该组织机构所拥有的座椅板凳以及办公场所
B. 该组织机构所拥有的信息系统
C. 该组织机构所拥有的著作权
D. 以上全部
参考答案 D

难易程度：二级

解析：

所属知识子域：信息安全与网络空间安全

128. 对于一个组织机构来说，信息资产包括（）
A. 该组织机构自研的信息系统
B. 该组织机构购买的正版授权的信息系统
C. 该组织机构在使用信息系统过程中所产生的数据信息
D. 以上全部
参考答案 D

难易程度：二级

解析：

所属知识子域：信息安全与网络空间安全

129. 对个人来说信息就是个人隐私，以下哪种做法是错误的（）
A. 火车票在是使用完毕后要及时粉碎或撕碎并扔进垃圾桶
B. 个人银行卡密码要尽量避免使用个人生日或身份证号中的数字，例如身份证后六位
C. 公司计算机要设置符合密码安全策略的密码，个人计算机可以不用设置密码
D. 会议讨论后要及时擦除在会议过程中书写在会议板上的信息
参考答案 C

难易程度：二级

解析：个人计算机同样需要设置符合安全策略的密码

所属知识子域：信息安全与网络空间安全

130. 哪些是关键信息基础设施（）
A. 基础信息网络，能源、金融、交通等领域和国家机关的重要信息系统，重要互联网应用系统
B. 教育、科研、水利、工业制造等领域和国家机关的重要信息系统，重要互联网应用系统
C. 医疗卫生、社会保障、公用事业等领域和国家机关的重要信息系统，重要互联网应用系统

D. 以上全部

参考答案 D

难易程度：一级

解析：关键信息基础设施定义：面向公众提供网络信息服务或支撑能源、通信、金融、交通、公共事业等重要行业运行的信息系统或工业控制系统；这些系统、服务、网络和基础设施要么提供基本商品和服务，要么构成其他关键基础设施的基础平台。

所属知识子域：网络空间安全法律法规

131. 关于信息安全，以下说法错误的是（）

A. 离开办公桌面随手将电脑锁屏

B. 重要数据经常备份，并进行加密处理

C. 避免将秘密以上文档随意放在办公桌上

D. 共享文件夹向所有用户赋予读写执行权限

参考答案 D

难易程度：一级

解析：在信息安全来说，共享文件夹只能对有权限的用户赋予读写执行权限

所属知识子域：信息安全与网络空间安全

132. 关于信息安全，以下做法正确的是（）

A. 为了不让自己忘记密码，公司小张把自己的密码写在记事本上，并保存在桌面文件框中

B. 小明电脑故障，把公司业务敏感数据备份到了自己的 U 盘里，U 盘也经常借给同事使用

C. 公司保洁阿姨文化水平不高，生活困难，因此小陈把打印错误的投标文件送予保洁阿姨

D. 小冷收到提示中奖信息来源不明的电子邮件，没有打开，直接删除

参考答案 D

难易程度：一级

解析：把密码记录在记事本上、公司业务敏感数据备份到了自己的 U 盘里、投标文件给不相关人员保管等都是错误的做法，中奖信息来源不明的电子邮件可能有木马，或是虚假、广告等信息，不要打开，直接删除

所属知识子域：信息安全与网络空间安全

133. 某信息安全公司来单位进行设备巡检维护，前台接待小张应如何接待（）

A. 将维护人员直接带到机房

B. 将维护人员带至洽谈室，并报告领导，由 IT 人员来对接

C. 将维护人员带至档案室

D. 将维护热源带至工作区等待

参考答案 B

难易程度：一级

解析：对于来公司的访客、合作人员、客户等外来人员，一律由相对应的人员接待，全程陪护，禁止外来人员到处游荡、随意进出，且带到公司敏感区域，如机房、档案室等

所属知识子域：信息安全与网络空间安全

134. 某单位需要将一批废旧电脑捐献给贫困山区的儿童，为了防止信息泄露，应采取的最合理的方法是？（）

A. 将硬盘进行格式化

B. 将硬盘进行格式化，并进行 3 次以上的硬盘痕迹擦除
C. 将硬盘进行格式化，并使用专业工具对硬盘进行消磁
D. 将硬盘拆除并进行物理破坏
参考答案 B

难易程度：一级

解析：覆盖数据三次即符合美国能源部关于安全抹掉磁性介质的标准。

所属知识子域：信息安全与网络空间安全

135. 下列关于安全下载，以下做法正确的是（）
A. 选择资源丰富的网站下载
B. 关闭杀毒软件，提高下载速度
C. 下载完成后直接打开下载的文件
D. 下载软件时，到软件官方网站或者其他正规软件下载网站下载
参考答案 D

难易程度：一级

解析：下载软件时，到软件官方网站或者其他正规软件下载网站下载，以防止计算机感染病毒

所属知识子域：信息安全与网络空间安全

136. 来访人员离开时，最优先归还哪项物品（）
A. 餐卡
B. 门禁卡
C. 公司宣传刊物
D. 公司提供的新 U 盘
参考答案 B

难易程度：一级

解析：餐卡、公司宣传刊物、公司提供的新 U 盘被来访人员带走，不影响公司的信息安全，与信息安全无关，门禁卡是公司内部物品，有了门禁卡就可以随意进出公司，从而有可能造成信息安全隐患

所属知识子域：信息安全与网络空间安全

137. 关于社交网站安全，以下说法错误的是（）
A. 不要轻易添加社交网站好友，也不要轻易相信网站微博、论坛上的信息，理性上网
B. 注册账号时，提供满足账号注册要求的最少信息
C. 充分利用社交网站的安全机制
D. 无条件信任好友转发的信息
参考答案 D

难易程度：一级

解析：社交网站上的信息不要轻易相信，哪怕是好友也一样、有可能是诈骗信息、病毒信息、不良消息等，有可能会带来恶劣影响及造成损失，严重的情况下会违法

所属知识子域：信息安全与网络空间安全

138. 以下行为符合安全原则的有（）
A. 在百度文库共享公司内部资料换取下载券

B. 重要资料需要经过互联网传输时，对重要资料进行加密传输
C. 将企业内部资料带回家中在互联网上操作
D. 在内网计算机上安装使用盗版软件
参考答案 B

难易程度：一级

解析：公司内部资料禁止泄露和带出公司，A 项涉及泄露公司资料，C 项是带出公司及有可能泄露，D 项，内网计算机禁止使用不明来历的软件，且使用盗版软件不合规、违法

所属知识子域：信息安全与网络空间安全

139. 关于移动介质使用，说法正确的是（）
A. 在同一办公室，大家都是同事，可以不经过病毒查杀，互相借用
B. 重要文件可以长期保存在移动介质中，移动介质只允许借给同办公室人使用
C. 移动介质尽量不外借，需要外借时，确保内部没有敏感资料
D. 使用移动介质从同事处拷贝的资料，可以不经过杀毒，直接在电脑上打开
参考答案 C

难易程度：一级

解析：移动介质不外借，如果确实需要外借时，确保内部没有敏感资料，且要经过病毒查杀，防止感染病毒，重要文件不能长期保存到移动介质中

所属知识子域：信息安全与网络空间安全

140. 通过病毒可以对核电站、水电站进行攻击导致其无法正常运转，对这一说法，你认为以下哪个是正确的（）
A. 核电站、水电站一般都是内网建设，不会连接互联网，所以病毒无法侵入
B. 理论上也许可行，实际上无法做到
C. 现在做不到，也许在不久的未来可以做到
D. 现在已经可以做到，并有实际案例
参考答案 D

难易程度：一级

解析：政策常识

所属知识子域：信息安全与网络空间安全

141. 李某将同学张某的小说擅自发表在网络上，这种行为（）
A. 扩大了张某的知名度，值得鼓励
B. 不影响张某在出版社出版该小说，因此合法
C. 侵犯了张某的著作权
D. 只要没有给张某造成直接经济损失，就是合法的
参考答案 C

难易程度：一级

解析：侵犯了张某的著作权

所属知识子域：信息安全与网络空间安全

142. 网络环境日益复杂，网络安全问题已然成为人们关注的重点，下列属于信息系统安全威胁的是（ ）
A. 系统的开放性

B. 系统的复杂性
C. 系统本身固有的漏洞
D. 以上都是
参考答案：D

难易程度：一级

解析：

所属知识子域：信息安全与网络空间安全

143. 应急响应通常分为准备、事件检测、抑制、根除、恢复、报告等阶段，下列选项中关于网络安全应急响应活动的说法中错误的是（ ）

A. 网络应急响应的活动应该主要包括两个方面：第一是未雨绸缪，第二是亡羊补牢
B. 事前的计划和准备为事件发生后的响应动作提供了指导框架
C. 事后的响应可能发现事前计划的不足，从而吸取教训，进一步完善安全计划
D. 目前网络安全应急响应相关工作满足实际工作需求，网络安全应急标准体系已经完善
参考答案：D

难易程度：一级

解析：D 选项错误，标准体系没有完善的说法，是不断改进的，且网络安全应急响应相关工作满足实际工作需求说法错误，不符合市场情况

所属知识子域：信息安全与网络空间安全

144. 网络安全应急管理是网络安全工作的重要内容，下列选项中关于网络安全应急能力建设的说法错误的是（ ）

A. 网络安全领域的应急保障需要依靠自动化的现代分析工具，实现对不同来源海量信息的自动采集、识别和关联分析
B. 网络安全日常管理与应急响应之间没有区别，业务类型相同，响应流程也相同
C. 在实现网络与信息安全应急指挥业务的过程中，应注重用信息化手段建立完整的业务流程
D. 研判、处置重大网络信息安全事件，需要多个单位、部门和应急队伍进行支撑和协调
参考答案：B

难易程度：一级

解析：网络安全日常管理与应急响应之间是有区别的，业务类型及响应流程都不同

所属知识子域：信息安全与网络空间安全

145. 以下哪个选项是攻击者的攻击策略？（）

A. 信息收集
B. 分析系统的安全弱点
C. 模拟攻击
D. 以上都是
参考答案：D

难易程度：一级

解析：信息收集、分析系统的弱点和模拟攻击等都属于攻击者的策略

所属知识子域：信息安全与网络空间安全

146. 以下哪个信息系统属于“国家关键信息基础设施”？（）

A. 某组织的核心管理系统
B. 国家电网调度系统
C. 某上司公司的重点业务系统
D. 某研发机构的研发系统
参考答案：B

难易程度：一级

解析：关键信息基础设施定义:面向公众提供网络信息服务或支撑能源、通信、金融、交通、公用事业等重要行业运行的信息系统或工业控制系统;且这些系统一旦发生网络安全事故，会影响重要行业正常运行，对国家政治、经济、科技、社会、文化、国防、环境以及人民生命财产造成严重损失 。

所属知识子域：网络安全法律法规

147. 网络不是法外之地，一天晚上，张某在北京昌平区回龙观一出租房内玩微信。当他使用“本·拉登”头像在某微信群聊天时，一网友说了句“看！大人物来了”。于是，张某就顺着这句话，发了一句“跟我加入 ISIS”。最终，判处有期徒刑 9 个月，并处罚金 1000 元，张某的行为属于（）

A. 已构成宣扬恐怖主义、极端主义罪
B. 拒不履行信息网络安全管理义务罪
C. 其行为致使违法信息大量传播
D. 发布有关制作或者销售毒品、枪支、淫秽物品等违禁物品、管制物品或者其他违法犯罪信息的
参考答案：A

难易程度：一级

解析：宣扬恐怖主义、极端主义罪是《中华人民共和国刑法》第一百二十条之三

所属知识子域：网络安全法律法规

148. 《中华人民共和国刑法》第二百八十六条 之一【拒不履行信息网络安全管理义务罪】网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，有下列情形之一的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金。以下属于上述行为的是（）

A. 致使违法信息大量传播的
B. 致使用户信息泄露，造成严重后果的
C. 致使刑事案件证据灭失，情节严重的
D. 以上都是
参考答案：D

难易程度：一级

解析：刑法

所属知识子域：网络安全法律法规

149. **《中华人民共和国刑法》第二百八十七条 之一 非法利用信息网络罪，下面行为不属于该行为的是（）**

A. 设立用于实施诈骗、传授犯罪方法、制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组的
B. 发布有关制作或者销售毒品、枪支、淫秽物品等违禁物品、管制物品或者其他违法犯罪信

息的
C. 宣扬恐怖主义、极端主义
D. 为实施诈骗等违法犯罪活动发布信息的
参考答案：C

难易程度：一级

解析：宣扬恐怖主义、极端主义罪是《中华人民共和国刑法》第一百二十条之三，其它选项都是非法利用信息网络罪

所属知识子域：网络安全法律法规

150.《中华人们共和国网络安全法》正式实施的是期是（）
A. 2016 年 11 月 7 日
B. 2016 年 6 月 1 日
C. 2017 年 6 月 1 日
D. 2016 年 10 月 31 日
参考答案：C

难易程度：一级

解析：2016 年 11 月 7 日，《中华人们共和国网络安全法》正式发布，并于 2017 年 6 月 1 日实施。

所属知识子域：网络安全法律法规

151. 自 2019 年 10 月 1 日起施行《儿童个人信息网络保护规定》中，其中儿童年龄是（）
A. 是指不满十二周岁的未成年人
B. 是指不满十四周岁的未成年人
C. 是指不满十六周岁的未成年人
D. 是指不满十八周岁的未成年人
参考答案：B

难易程度：一级

解析：**第二条** 本规定所称儿童，是指不满十四周岁的未成年人。

所属知识子域：网络安全法律法规

152.《互联网新闻信息服务管理规定》，互联网新闻信息服务单位与境内外中外合资经营、中外合作经营和外资经营的企业进行涉及互联网新闻信息服务业务的合作，应当报经国家互联网信息办公室进行（）

A. 安全评估

B. 风险评估

C. 资质审查

D. 内容审查

参考答案：A

难易程度：一级

解析：安全评估

所属知识子域：网络安全法律法规

153. 软件安全问题的根本原因在于两个方面，一是内因，软件本身存在安全漏洞，二是外因，软件应用存在外部威胁，下面选项属于内因的是（）

A. 软件规模增大，功能越来越多，越来越复杂，难以避免缺陷

B. 软件模块复用，导致安全漏洞延续

C. 缺乏从设计开始安全考虑

D. 上面都对

参考答案：D

难易程度：一级

解析：内因：软件复杂性使得漏洞不可避免。软件规模增大，功能越来越多，越来越复杂，难以避免缺陷；软件模块复用，导致安全漏洞延续；缺乏从设计开始安全考虑

所属知识子域：安全漏洞与网络攻击

154. 造成开发漏洞的主要原因，下面理解正确的是（）

A. 用户出于市场和业务等因素考虑，将软件交付期和软件的新特性作为首要考虑因素，而不是软件的安全与否。

B. 开发者缺乏相关知识。软件规模越来越大，越来越复杂，开发者要想避免安全漏洞和错误，需要专门的安全技术与开发技术相结合。

C. 缺乏与安全开发的相关工具。目前已经有一些开发和测试相关的专业工具，但只有少数安全开发团队都装备了这类工具。没有专门的工具，只是凭着经验和手工管理与检测，无法有效提高所开发的软件的安全性。

D. 以上都对

参考答案：D

难易程度：一级

解析：造成开发漏洞的几个主要原因：开发者缺乏安全开发的动机；用户出于市场和业务等因素考虑，将软件交付期和软件的新特性作为首要考虑因素，而不是软件的安全与否。在没有用户的关注与压力情况下，开发商则没有足够的资源（资金、人力等）和动力去专注软件本身的安全性。开发者缺乏相关知识。软件规模越来越大，越来越复杂，开发者要想避免安全漏洞和错误，需要专门的安全技术与开发技术相结合。这涉及到安全的管理、技术和工程等方面的知识。而目前大学所传授的往往是开发技术和技能，例如编程技术（C++, VisualBasic、C#）、网络通信协议等，对于信息安全技术的传授还不够广泛。开发人员往往会认为只需要正确使用了一些安全协议（SSL 等）和加密技术来保证程序的安全，缺乏整体上的软件安全保障知识。缺乏与安全开发的相关工具。目前已经有一些开发和测试相关的专业工具，但只有少数安全开发团队都装备了这类工具。没有专门的工具，只是凭着经验和手工管理与检测，无法有效提高所开发的软件的安全性。

所属知识子域：安全漏洞与网络攻击

155. 由于“劣币驱除良币”效应的存在，对于软件的安全开发，下面理解正确的是（）

A. 企业管理层对安全开发缺乏了解，开发管理人员不了解软件安全开发的管理流程、方法和技巧

B. 软件开发人员缺乏将软件安全需求、安全特性和编程方法进行结合的能力

C. 测试人员无法以“坏人”的角度来思考软件安全问题

D. 上面都对

参考答案：D

难易程度：一级

解析：由于“劣币驱除良币”效应的存在，使得更多的软件厂商对软件安全开发缺乏动力，企业管理层和软件开发人员都缺乏相应的知识，不知道如何才能更好地实现安全的软件。公司管理层缺乏对软件安全开发的管理流程、方法和技巧，缺少正确的安全经验积累和培训教材，软件开发人员则大多数仅仅从学校学会编程技巧，不了解如何将软件安全需求、安全特性和编程方法进行结合，更无法以“坏人”的角度来思考软件安全问题。

所属知识子域：安全漏洞与网络攻击

156. 漏洞产生的应用环境原因理解错误的是（）

A. 互联网的发展使软件运行环境从传统的封闭、静态和可控变为开放、动态和难控

B. 软件安全开人员水平不够

C. 攻防信息不对称性进一步增强，攻易守难的矛盾进一步凸显

D. 强大经济利益推动漏洞挖掘产业化方向发展

参考答案：B

难易程度：一级

解析：软件安全开人员水平不够属于个人原因，不能归纳于漏洞产生的应用环境中

所属知识子域：安全漏洞与网络攻击

157. 攻击者攻击的过程（）

A. 信息收集及分析，实施攻击，设置后门，清除入侵记录

B. 信息收集及分析，实施攻击，找到需要的或破坏，清除入侵记录

C. 实施攻击，信息收集及分析，设置后门，清除入侵记录

D. 实施攻击，信息收集及分析，找到需要的或破坏，清除入侵记录

参考答案：A

难易程度：一级

解析：攻击者对系统或网络进行攻击的过程通常包括信息收集与分析、实施攻击、设置后门及清除痕迹四个步骤。

所属知识子域：安全漏洞与网络攻击

158. 攻击者做好信息收集的作用（）

A. 知己知彼 百战不殆

B. 信息是攻击的基础

C. 信息收集可以成为攻击的方式

D. 以上都对

参考答案：D

难易程度：一级

解析：

所属知识子域：安全漏洞与网络攻击

159. 攻击者信息收集的对象包括（）

A. 目标系统的 IT 相关资料，如域名、网络拓扑结构、操作系统的类型和版本、应用软件及相关脆弱性等；

B. 目标系统的组织相关资料，如组织架构及关联组织、地理位置细节、电话号码、邮件等联系方式、近期重大事件、员工简历；

C. 其他令攻击者感兴趣的任何信息，例如企业内部的部门或重要人员的独特称呼、目标组

织机构的供应商变更等。

D. 以上都对

参考答案：D

难易程度：一级

解析：信息收集的对象包括：目标系统的 IT 相关资料，如域名、网络拓扑结构、操作系统的类型和版本、应用软件及相关脆弱性等；目标系统的组织相关资料，如组织架构及关联组织、地理位置细节、电话号码、邮件等联系方式、近期重大事件、员工简历；其他令攻击者感兴趣的任何信息，例如企业内部的部门或重要人员的独特称呼、目标组织机构的供应商变更等。

所属知识子域：安全漏洞与网络攻击

160. 对于组织来说，为了防范攻击者进行信息收集与分析，下面理解错误的是（）

A. 信息展示最小化原则，不必要的信息不要发布

B. 部署网络安全设备（IDS、防火墙等）

C. 员工的个人信息和习惯不需要做防范措施

D. 设置安全设备应对信息收集（阻止 ICMP）

参考答案：C

难易程度：一级

解析：员工的个人信息和习惯是组织的敏感信息，攻击者利用这些信息入侵、破解帐户密码、诈骗等等，属于信息收集与分析的重点范畴

所属知识子域：安全漏洞与网络攻击

161. 有效对抗信息收集和分析的原则只有一个，就是“严防死守”。这句话理解正确的是（）

A. 所有不是必须向用户提供的信息，都不提供，遵循最小化原则

B. 所有不是必须向用户提供的信息，向用户提供的信息都是不重要的信息

C. 审核后确认了可以提供的信息，被攻击者收集后作用也不大，价值不高

D. 组织的任何信息都是有价值的，但报废后的信息就没有了价值，可以随便处理

参考答案：A

难易程度：一级

解析：组织的任何信息在所有过程中都是有价值的，都需要得到保护，不可以随便处理，在必须提供信息的情况下，遵循最小化原则

所属知识子域：安全漏洞与网络攻击

162. 恶意代码给计算机安全带来巨大威胁，以下属于恶意代码的特征的是（）

A. 具有恶意的目的

B. 本身不属于计算机程序

C. 不执行也能发生作用

D. 以上都不正确

参考答案：A

难易程度：一级

解析：恶意代码的特征：具有恶意的目的、本身是程序、通过执行发挥作用
所属知识子域：安全漏洞与网络攻击

163. 强口令即长度不小于 8 个字符、同时包含大写和小写字符、至少有一个数字的字符串。下列密码中，属于强口令的是（）

A. 12345678
B. 19950429
C. qwertyuiop
D. dlIgs7kn8nk2

参考答案：D

难易程度：一级

解析：强口令必须数字、字母、特殊符号，至少要两者组合，或三者组合，长度不少于 8 位数，上面符合条件的只有 D
所属知识子域：口令破解

164. 小李收到陌生中奖短信，要求其提供身份信息领奖，小明可能受到以下哪种攻击( )

A. 蠕虫病毒
B. 社会工程学
C. 勒索病毒
D. 木马

参考答案：B

难易程度：一级

解析：社会工程学充分利用了人性中的“弱点”进行攻击,攻击者可能会利用人性中的本能反应、好奇心、信任、贪婪等心理特性，通过伪装、欺骗、恐吓、威逼等种种方式以达到目的。
所属知识子域：口令破解

165. 漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷。以下属于常见的应用软件安全漏洞的是( )

A. 文件上传漏洞
B. 跨站脚本漏洞
C. SQL 注入漏洞
D. 以上都是

参考答案：D

难易程度：一级

解析：
所属知识子域：口令破解

166. 针对口令的破解攻击方式很多，下面不属于口令破解攻击方式的是（）

A. 暴力破解攻击
B. 跨站脚本攻击
C. 社会工程学攻击
D. 木马窃取

参考答案：B

难易程度：二级

解析：跨站脚本攻击(也称为 XSS)指利用网站漏洞从用户那里恶意盗取信息。不属于口令破解攻击方式

所属知识子域：口令破解

167. 注入类漏洞是一种常见的安全漏洞，其中 SQL 注入漏洞是一种危害性较大的注入类漏洞。以下不属于 SQL 注入攻击流程的是（）

A. 发送大量的数据报文导致系统死机

B. 探测 SQL 注入点

C. 判断数据库类型

D. 提升权限进一步攻击

参考答案：A

难易程度：二级

解析：SQL 注入攻击的总体思路：发现 SQL 注入位置、判断数据库类型、确定 XP-CMDSHELL 可执行情况、发现 WEB 虚拟目录、上传 ASP 木马、得到管理员权限

所属知识子域：安全漏洞与网络攻击

168. 网络攻击者经常在被侵入的计算机内留下后门，后门可以作什么（）

A. 方便下次直接进入

B. 监视用户所有行为、隐私

C. 控制用户主机

D. 以上都对

参考答案：D

难易程度：一级

解析：网络攻击者留下后门，可以方便下次直接进入、监视用户所有行为和隐私、控制用户主机等

所属知识子域：安全漏洞与网络攻击

169. 特洛伊木马程序是一种秘密潜伏的恶意程序，它不能做什么（）

A. 上传和下载文件

B. 特洛伊木马有自我复制能力

C. 窃取你的密码

D. 远程控制

参考答案：B

难易程度：一级

解析：特洛伊木马在计算机领域中指的是一种后门程序，是黑客用来盗取其他用户的个人信息，甚至是远程控制对方的计算机而加壳制作，然后通过各种手段传播或者骗取目标用户执行该程序，以达到盗取密码等各种数据资料等目的。

所属知识子域：安全漏洞与网络攻击

170. 每逢双十一购物狂欢节，网民们都会在淘宝网上抢购东西，当网民抢购商品高峰期到来时，就经常出现网站崩溃、停机等情况，这实际上可以看作是全国网民通过手动点击淘宝网址引起的一次大规模( )攻击

A. XSS

B. CSRF

C. SQL 注入

D. DDoS

参考答案：D

难易程度：一级

解析：DDoS 攻击通过大量合法的请求占用大量网络资源，以达到瘫痪网络的目的。
所属知识子域：安全漏洞与网络攻击

171. APP 应用自身的安全问题不包含哪个方面( )

A. 设计上的缺陷
B. 应用市场安全审查不严谨
C. 开发过程导致的问题
D. 配置部署导致的问题

参考答案：B

难易程度：一级

解析：应用市场安全审查不严谨不是应用自身的问题，是属于第三方监督审查方面的
所属知识子域：安全漏洞与网络攻击

172. 社会工程学攻击是利用（ ）而以获取信息或实施攻击的方式

A. 信息收集
B. 漏洞
C. 人性的弱点
D. 心理学和管理学技术

参考答案：C

难易程度：一级

解析：社会工程学攻击是利用人性的弱点而以获取信息或实施攻击的方式
所属知识子域：安全漏洞与网络攻击

173. 社会工程学的社工手段下面正确的是（）

A. 熟人好说法
B. 伪造相似的信息背景
C. 伪装成新人打入内部
D. 上面都对

参考答案：D

难易程度：二级

解析：熟人好说法、伪造相似的信息背景、伪装成新人打入内部、美人计、恶人无禁忌、他懂我就像我肚里的蛔虫、善良是善良者的墓志铭、来一场技术交流吧、外来的和尚会念经等都是社工手段
所属知识子域：安全漏洞与网络攻击

174. 社会工程学的社工手段下面正确的是（）

A. 善良是善良者的墓志铭
B. 来一场技术交流吧
C. 外来的和尚会念经
D. 上面都对

参考答案：D

难易程度：二级

解析：熟人好说法、伪造相似的信息背景、伪装成新人打入内部、美人计、恶人无禁忌、他懂我就像我肚里的蛔虫、善良是善良者的墓志铭、来一场技术交流吧、外来的和尚会念经等都是社工手段
所属知识子域：安全漏洞与网络攻击

175. 网络钓鱼欺骗是社会工程学的一种方式，下列关于社会工程学的说法中错误的是（）

A. 社会工程学利用了人性的弱点

B. 社会工程学需要结合常识

C. 社会工程学的目的是获取秘密信息

D. 谎言越多，社会工程学的欺骗效果越好

参考答案：D

难易程度：一级

解析：D 项说法错误

所属知识子域：安全漏洞与网络攻击

176. 根据恶意代码特征对恶意代码前缀命名，Worm.Sasser 病毒属于（）

A. 引导区病毒

B. 蠕虫病毒

C. 木马病毒

D. 宏病毒

参考答案：B

难易程度：三级

解析：worm，一般解释为蠕虫。一般认为蠕虫是一种通过网络传播的主动攻击的恶性计算机病毒，是计算机病毒的子类。早期恶意代码的主要形式是计算机病毒 COHE1985 COHE1989 COHE1990。

所属知识子域：安全漏洞与网络攻击

177. 耗尽网络可用资源是网络攻击的常见手段，在网络攻击中，一段代码的执行陷入无穷的循环，最终导致资源耗尽被称为（）

A. IE 炸弹

B. SQL 注入

C. 缓冲区溢出

D. 木马病毒

参考答案：A

难易程度：三级

解析：IE 炸弹是指有一段代码的执行会陷入无穷的循环，最终导致资源耗尽，影响计算机的使用。

所属知识子域：安全漏洞与网络攻击

178. 社会工程学攻击防范措施正确的是（）

A. 注重信息保护

B. 学习并了解社会工程学攻击

C. 遵循信息安全管理制度

D. 以上都对

参考答案：D

难易程度：三级

解析：在对社会工程学攻击有所了解的基础上，才能在日常工作和生活中，学会判断是否存在社会工程学攻击，这样才能更好的保护个人数据甚至组织机构的网络安全。搜集到被攻击者尽可能多的信息是实施社会工程学攻击的前提和基础，建立并完善信息安全管理体系是有效应对社会工程学攻击的方法，通过安全管理制度的建立，使得信息系统用户需要遵循规范

来实现某些操作，从而在一定程度上降低社会工程学的影响。
所属知识子域：安全漏洞与网络攻击

179. 中国互联网协会 2006 年公布了“恶意软件”定义，具有下列特征之一的软件可以被认为是恶意软件（）

A. 强制安装
B. 难以卸载
C. 恶意捆绑
D. 以上都对
参考答案：D

难易程度：一级

解析：
所属知识子域：安全漏洞与网络攻击

180. 2016 年 12 月，我国发布了《国家网络空间安全战略》，提出网络空间的发展是机遇也是挑战。下面理解正确的是（）

A. 网络渗透危害政治安全
B. 网络攻击威胁经济安全
C. 网络恐怖和违法犯罪破坏社会安全
D. 以上都对
参考答案：D

难易程度：一级

解析：国家网络空间安全战略的内容
所属知识子域：网络安全法律法规

181. 恶意代码有哪些威胁（）

A. 抢占系统资源
B. 破坏数据信息
C. 干扰系统的正常运行
D. 以上都对
参考答案：D

难易程度：一级

解析：恶意代码通过抢占系统资源、破坏数据信息等手段，干扰系统的正常运行，是信息安全的主要威胁之一
所属知识子域：恶意代码

182. 提出了最初恶意程序的概念的是（）

A. 冯·诺依曼
B. 道拉斯·麦耀莱
C. 维特·维索斯基
D. 托马斯·捷·瑞安
参考答案：A

难易程度：一级

解析：1949 年，计算机之父冯·诺依曼在《复杂自动机组织论》上提出了最初恶意程序的概念，它是指一种能够在内存中自我复制和实施破坏性功能的计算机程序。
所属知识子域：恶意代码

183. 一般来说，恶意代码的传播方式不包括（）

A. 利用文件传播

B. 利用服务器传播

C. 利用网络服务传播

D. 利用系统漏洞传播

参考答案：B

难易程度：一级

解析：一般来说，恶意代码的传播方式包括利用文件传播、利用网络服务传播、利用系统漏洞传播三种方式。

所属知识子域：恶意代码

184. 恶意代码传播速度最快、最广的途径是（）

A. 安装系统软件时

B. 通过 U 盘复制来传播文件时

C. 通过网络来传播文件时

D. 通过移动硬盘来传播文件时

参考答案：C

难易程度：二级

解析：网络传播文件时

所属知识子域：恶意代码

185. 使用漏洞库匹配的扫描方法，能发现（）

A. 未知的漏洞

B. 已知的漏洞

C. 所有漏洞

D. 自行设计的软件中的漏洞

参考答案：B

难易程度：二级

解析：已知的漏洞

所属知识子域：恶意代码

186. 下面哪一项最好地描述了风险分析的目的（）

A. 识别用于保护资产的责任义务和流程

B. 识别资产、脆弱性并计算潜在的风险

C. 识别资产以及保护资产所使用的控制措施

D. 识别同责任义务有直接关系的威胁

参考答案：B

难易程度：二级

解析：识别资产、脆弱性并计算潜在的风险，其它与风险分析的目的无关

所属知识子域：恶意代码

187. 随着互联网的发展及上网人数的不断增长，网页逐渐成为恶意代码传播的主要方式。网页嵌入恶意代码的主要方式有（）

A. 将木马伪装为页面元素

B. 利用脚本运行的漏洞

C. 利用网页浏览中某些组件漏洞

D. 以上都对

参考答案：D

难易程度：一级

解析：网页嵌入恶意代码的主要方式有：将木马伪装为页面元素、利用脚本运行的漏洞、伪装为缺失的组件、通过脚本运行调用某些 com 组件、利用网页浏览中某些组件漏洞。

所属知识子域：恶意代码

188. 缓冲区溢出攻击指利用缓冲区溢出漏洞所进行的攻击行为。以下对缓冲区溢出攻击描述正确的是（ ）

A. 缓冲区溢出攻击不会造成严重后果

B. 缓冲区溢出攻击指向有限的空间输入超长的字符串

C. 缓冲区溢出攻击不会造成系统宕机

D. 以上都不正确

参考答案：B

难易程度：一级

解析：缓冲溢出攻击是通过向程序的缓冲区写入超过预定长度的数据，从而破坏程序的堆栈，导致程序执行流程的改变。

所属知识子域：恶意代码

189. 计算机病毒会破坏计算机数据或功能，并能寄生于其他程序，其中被寄生的程序称为（ ）

A. 更新程序

B. 不可执行程序

C. 宿主程序

D. 修改程序

参考答案：C

难易程度：一级

解析：

所属知识子域：恶意代码

190. 有效的应对攻击者进行痕迹清除的方法，首先是要确保攻击者的攻击过程被记录在日志中，通常采取的方法是对日志进行设置，下面正确的是（）

A. 记录尽可能多的信息

B. 将日志的保留时间设置更长

C. 日志的存储空间设置更大

D. 上面都对

参考答案：D

难易程度：一级

解析：有效的应对攻击者进行痕迹清除的方法，首先是要确保攻击者的攻击过程被记录在日志中，通常采取的方法是对日志进行设置，记录尽可能多的信息、将日志的保留时间设置更长、日志的存储空间设置更大等。

所属知识子域：恶意代码

191. 计算机系统一般有其相应的日志记录系统。其中，日志指系统所指定对象的某些操作和其操作结果按时间有序的集合，下列对其的叙述不正确的是（　）

A. 它是由各种不同的实体产生的“事件记录”的集合

B. 日志只在维护系统稳定性方面起到非常重要的作用

C. 它可以记录系统产生的所有行为并按照某种规范将这些行为表达出来

D. 日志信息可以帮助系统进行排错、优化系统的性能

参考答案：B

难易程度：一级

解析：B 选项错，日志不只在维护系统稳定性方面起到非常重要的作用，还有审计、监督和追踪等重要的作用

所属知识子域：恶意代码

192. 计算机系统一般具有相应的日志记录系统，并且其日志文件记录具有许多作用，以下关于日志文件记录功能的描述不正确的是（　）

A. 可以提供监控系统资源

B. 可以审计用户行为

C. 不能为计算机犯罪提供证据来源

D. 可以确定入侵行为的范围

参考答案：C

难易程度：一级

解析：日志是计算机犯罪提供证据来源之一，具有非常重要的作用

所属知识子域：恶意代码

193. 日常生活中经常使用口令加短消息验证的验证方式，属于（）

A. 双因素认证

B. 实体所知认证

C. 实体所有认证

D. 实体特征认证

参考答案：A

难易程度：一级

解析：帐户口令属于实体所知，短消息验证属于实体所有，把两个要素结合起来的身份认证的方法就是“双因素认证”。

所属知识子域：恶意代码

194. 在信息收集与分析中，攻击者最轻易获取的信息的方式是（）

A. 搜索引擎、媒体广告等
B. 向同行了解
C. 亲自到攻击点附近
D. 收买信息系统相关人员
参考答案：A

难易程度：一级

解析：公开渠道是攻击者最轻易获取的信息的方式，由于缺乏足够的安全意识，很多信息系统对公开信息没有审核或审核宽松，使得攻击者可以通过公开渠道获得目标系统大量有价值的信息。公开信息收集方式包括搜索引擎、媒体广告等方式。

所属知识子域：恶意代码

195. 下列关于用户口令说法错误的是（）

A. 口令不能设置为空
B. 口令长度越长，安全性越高
C. 复杂口令安全性足够高，不需要定期修改
D. 口令认证是最常见的认证机制
参考答案：C

难易程度：一级

解析：理论上再复杂的口令，只要给足够的时间和支持，都是可以被破解，所以需要定期修改

所属知识子域：口令破解

196. 在安全评估过程中，采取（）手段，可以模拟黑客入侵过程，检测信息系统安全的脆弱性。

A. 问卷调查
B. 渗透测试
C. 人员访谈
D. 手工检查
参考答案：B

难易程度：一级

解析：问卷调查、人员访谈、手工检查、渗透测试是安全评估的方法，但只有渗透测试手段可以模拟黑客入侵过程，检测信息系统安全的脆弱性。

所属知识子域：信息安全管理

197. 对个人来说个人信息就是个人隐私，以下哪种做法是错误的（）

A. 火车票在是使用完毕后要及时粉碎或撕碎并扔进垃圾桶
B. 个人银行卡密码要尽量避免使用个人生日或身份证号中的数字，例如身份证后六位
C. 公司计算机要设置符合密码安全策略的密码，个人计算机可以不用设置密码
D. 会议讨论后要及时擦除在会议过程中书写在会议板上的信息
参考答案 C

难易程度：一级

解析：个人计算机也要设置符合密码安全策略的密码

所属知识子域：信息安全管理

198. 下列密码中，哪个密码是最安全的（）

A. database

B. !qaz@wsx

C. !@#$%^&*

D. #*kong43Za

参考答案 D

难易程度：一级

解析：A 是全英文，且是英文单词，B 和 C 都有健盘轨迹，D 项有符号、字母、数字及大小写，在四个选项中最符合安全要求

所属知识子域：口令破解

199. 网页病毒的主要传播途径是（）

A. 文件交换

B. 网页浏览

C. 邮件

D. 光盘

参考答案 B

难易程度：一级

解析：网页浏览

所属知识子域：口令破解

200. 关于用户密码，以下做法正确的是（）

A. 自己的电脑自己用，每次输入开机密码太麻烦，就不设置密码了

B. 由于公司规定将密码设置为 123456、admin、111111 等容易记忆的密码

C. 长期使用同一个密码

D. 应用系统、邮箱登陆等登录密码设置为非自动保存

参考答案 D

难易程度：一级

解析：ABC 选项安全意识差，D 选项正确，系统登录密码设为自动保存密码，容易被他人登录，带来信息安全隐患

所属知识子域：口令破解

201. 关于办公室信息安全意识正确的是（）

A. 使用办公计算机中途外出时，只关掉了显示器

B. 虽然在内网计算机上安装了桌面管理系统，但管理员不会 24 小时监控，管理员休息了可以上会外网

C. 先把计算机的内网网线拔掉，在接入外网网线，这样就实现了两网分离，不属于违规外联

D. 在内网使用专用的内网移动介质，专用介质不能在连接外网的电脑中使用

参考答案 D

难易程度：一级

解析：内网设备禁止连接外网，BC 错，A 选项信息安全意识差，D 项符合要求

所属知识子域：网络攻击与防护

202. 关于计算机木马、病毒说法正确的是（）

A. word 文档不会感染病毒

B. 尽量访问知名网站可以避免感染木马、病毒
C. 杀毒软件能防止所有木马及病毒的侵害
D. 只要不连接互联网，就能避免受到木马、病毒的侵害
参考答案 B

难易程度：一级

解析：word 文档会感染宏病毒，杀毒软件能预防已知病毒，对未知病毒作用不大，不连接互联网也会中病毒，如存储介质连接，存储介质可能带病毒
所属知识子域：网络攻击与防护

203. 关于密码安全的说法，以下正确的是（）

A. 11 位的密码一定比 8 位的安全
B. 容易被记住的密码一定不安全
C. 任何密码在理论上都有被破解的可能
D. 密码位数越多越好
参考答案 C

难易程度：一级

解析：ABC 项说法太绝对
所属知识子域：网络攻击与防护

204. 主要用于加密机制的协议是（）

A. FTP
B. SSL
C. TELNET
D. HTTP
参考答案 B

难易程度：一级

解析：用于加密机制的协议是 SSL。SSL 协议位于 TCP 和 IP 协议与各种应用层协议之间，为数据通讯提供安全支持。
所属知识子域：网络攻击与防护

205. HTTPS 是以安全为目标的 HTTP 通道，简单讲是 HTTP 的安全版。HTTPS 的安全基础是（）

A. TELNET
B. FTP
C. SSL
D. AES
参考答案 C

难易程度：一级

解析：用于加密机制的协议是 SSL。SSL 协议位于 TCP 和 IP 协议与各种应用层协议之间，为数据通讯提供安全支持。HTTPS 的安全基础是 SSL
所属知识子域：安全漏洞与网络攻击

206. 欺骗是指伪造可信身份，并向目标系统发起攻击的行为。例如 TCP/IP 协议连接时主要认证目的 IP 地址，而源地址是可以伪造的。常见的欺骗方式有( )

A. IP 欺骗(IP spoof)
B. ARP 欺骗和 DNS 欺骗

C. TCP 会话劫持(TCP Hijack)

D. 以上都对

参考答案 D

难易程度：一级

解析：常见的欺骗方式有：IP 欺骗(IP spoof)，ARP 欺骗、DNS 欺骗，以及 TCP 会话劫持(TCP Hijack)等。

所属知识子域：安全漏洞与网络攻击

207. 攻击者进行系统入侵的最后一步是清除攻击痕迹，攻击痕迹包括攻击过程中产生的各类（）

A. 系统日志

B. 应用日志

C. 攻击过程中生成的临时文件和临时账户等

D. 以上都对

参考答案 D

难易程度：一级

解析：攻击者进行系统入侵的最后一步是清除攻击痕迹，攻击痕迹包括攻击过程中产生的各类系统日志、应用日志，攻击过程中生成的临时文件和临时账户等。

所属知识子域：安全漏洞与网络攻击

208. **删除日志会导致日志的缺少，在审计时会被发现，因此部分高明的攻击者可能会（）**

A. 篡改日志文件中的审计信息

B. 删除或停止审计服务进程

C. 修改完整性检测标签

D. 以上都对

参考答案 D

难易程度：一级

解析：例如：篡改日志文件中的审计信息，改变系统时间造成日志文件数据紊乱，删除或停止审计服务进程，修改完整性检测标签等等。

所属知识子域：安全漏洞与网络攻击

209. 下面不属于 Unix 操作系统日志文件的是（）

A. wtmp/wtmpx

B. SecEvent.Evt

C. utmp/utmpx

D. Lastlog

参考答案 B

难易程度：一级

E. 解析：以 Unix 操作系统为例，它包含 wtmp/wtmpx、utmp/utmpx 和 lastlog 三个主要日志文件，SecEvent.Evt 是 windows 操作系统

所属知识子域：安全漏洞与网络攻击

210. 下面方法能有效防范口令穷举的措施是（）

A. 随机验证码

B. 滑动填图验证

C. 手机验证码

D. 以上都对

参考答案 D

难易程度：一级

解析：随机验证吗、滑动填图验证、手机验证码、系统账户安全策略、智力挑战等都属于有效防范口令穷举方法，有力的防范了攻击者进行口令暴力破解

所属知识子域：安全漏洞与网络攻击

211.（ ）是信息系统安全防护体系中最不稳定也是最脆弱的环节

A. 员工

B. 技术

C. 管理

D. 以上都错

参考答案 A

难易程度：一级

解析：人是信息系统安全防护体系中最不稳定也是最脆弱的环节

所属知识子域：安全漏洞与网络攻击

212. 防病毒软件是目前恶意代码防护最主要的技术措施，防病毒软件是通过什么来发现病毒的（）

A. 病毒名称

B. 病毒特征码

C. 病毒特征

D. 病毒类型

参考答案 B

难易程度：一级

解析：每种恶意代码中都包含某个特定的代码段，即特征码，在进行恶意代码扫描时，扫描引擎会将系统中的文件与特征码进行匹配，如果发现系统中的文件存在与某种恶意代码相同的特征码，就认为存在恶意代码。

所属知识子域：安全漏洞与网络攻击

213. 所有防病毒软件需要定期更新的主要原因是（）

A. 防病毒软件功能的升级

B. 防病毒软件技术的迭代

C. 发现新的病毒的特征码

D. 增加防病毒软件更多的功能

参考答案 C

难易程度：一级

解析：确保计算机终端上的防病毒软件具备良好的病毒检测能力，就需要不断更新病毒库的特征码，这也是所有防病毒软件需要定期更新病毒定义码的主要原因。

所属知识子域：安全漏洞与网络攻击

214.（ ）是保护数据安全的最后手段，也是防止恶意代码攻击信息系统的最后一道防线。

A. 数据备份与数据恢复
B. 建立信息安全管理体系
C. 定期进行信息系统审计
D. 购买最先进的病毒防护软件

参考答案 A

难易程度：一级

解析：数据备份与数据恢复是保护数据安全的最后手段，也是防止恶意代码攻击信息系统的最后一道防线。

所属知识子域：安全漏洞与网络攻击

215. 哪些不属于 Windows 系统上存在的日志文件？（）

A. AppEvent.Evt
B. SecEvent.Evt
C. utmp/utmpx
D. SysEvent.Evt

参考答案 C

难易程度：一级

解析：AppEvent.Evt、SecEvent.Evt、SysEvent.Evt、W3C 扩展日志，属于 Windows 系统上存在的日志文件

所属知识子域：安全漏洞与网络攻击

216. 木马可以实现的功能是（）

A. 执行程序
B. 键盘记录
C. 屏幕监视
D. 以上都对

参考答案 D

难易程度：一级

解析：

所属知识子域：安全漏洞与网络攻击

217. 下面哪种方式不可以发现扫描痕迹（）

A. 查看系统日志
B. 查看 web 日志
C. 查看注册表
D. 查看 IDS 记录

参考答案 C

难易程度：一级

解析：

所属知识子域：安全漏洞与网络攻击

218. 为了保证系统日志可靠有效，以下哪一项不是日志必需具备的特征（）

A. 统一而精确地的时间

B. 全面覆盖系统资产

C. 包括访问源、访问目标和访问活动等重要信息

D. 可以让系统的所有用户方便的读取

参考答案 D

难易程度：一级

解析：日志只有授权用户可以读取。

所属知识子域：安全漏洞与网络攻击

219. 以下对异地备份中心的理解最准确的是（）

A. 与生产中心不在同一城市

B. 与生产中心距离 30 公里以上

C. 与生产中心距离 150 公里以上

D. 与生产中心面临相同区域性风险的机率很小

参考答案 D

难易程度：一级

解析：建立异地备份中心的核心思想是减少相同区域性风险

所属知识子域：安全漏洞与网络攻击

220.“在因特网上没有人知道对方是一个人还是一条狗”，这个故事最能说明（）

A. 身份认证的重要性和迫切性

B. 网络上所有的活动都是不可见的

C. 网络应用中存在不严肃性

D. 计算机网络是一个虚拟的世界

参考答案：A

难易程度：一级

解析：对方是男是女，是好人坏人，没人能够准确知道，身份认证也称为"身份验证"或"身份鉴别"，是指在计算机及计算机网络系统中确认操作者身份的过程，从而确定该用户是否具有对某种资源的访问和使用权限，进而使计算机和网络系统的访问策略能够可靠、有效地执行，防止攻击者假冒合法用户获得资源的访问权限，保证系统和数据的安全，以及授权访问者的合法利益。

所属知识子域：安全漏洞与网络攻击

221. 社会工程学攻击的理解正确的是（）

A. 永远有效的攻击方法

B. 人是最不可控的因素

C. 人才是最大的信息安全漏洞

D. 以上都对

参考答案 D

难易程度：一级

解析：社会工程学利用人的弱点，以顺从你的意愿、满足你的欲望的方式，让你上当的一些方法、一门艺术与学问。

所属知识子域：社会工程学攻击

222. 社会工程学攻击中，常有“电信诈骗中的公安局来电”、“我是系统管理员”等诈骗方式，是利用了人性中的（）

A. 权威

B. 好奇心
C. 贪便宜
D. 信任
参考答案 A
难易程度：一级
解析：电信诈骗中的公安局、我是系统管理员等都属于权威人士，普通人都会下意识的服从和信任，故选 A
所属知识子域：社会工程学攻击

223. 某公司技术人员利于自己的技术入侵了某电商数据库，将其中的用户数据下载后在暗网中进行售卖，该行为的处置最适用的是以下那部法律？（ ）

A. 刑法
B. 网络安全法
C. 电子签名法
D. 劳动法
参考答案 A
难易程度：一级
解析：入侵他人网站，触犯的是刑法，不属于民事责任
所属知识子域：社会工程学攻击

224. 小张在某网站上找到了一篇他需要的资料，可以免费下载，但是下载要求在网站上使用邮箱进行注册，以下哪个做法是最正确的？（ ）

A. 使用自己常用的邮箱地址用户名和密码进行注册，这样方便管理
B. 申请一个仅用于注册不常用网站的邮箱进行注册，密码单独设一个
C. 不注册了，另外到别的网站去寻找,不用注册就能下载的
D. 不注册了，也不下载了
参考答案 B
难易程度：一级
解析：根据题干，小张需要下载资料，但要使用邮箱，网站可能有病毒或木马等，为保证安全，不能使用常用邮箱，故 A、D 不符合，C 选项浪费时间，且别的网站不一定有，也不符合，故 B 选项是合适的，也是最正确的
所属知识子域：安全漏洞与网络攻击

225. 你需要打印一份报价材料给合作伙伴，可部门打印机缺墨无法打印，以下哪个选择从安全角度最合理？（ ）

A. 给别的部门人员帮忙打印
B. 去外面文印室打印
C. 联系相关人员尽快维修后打印
D. 微信发给合作伙伴让对方自己打印
参考答案 C
难易程度：一级
解析：从安全角度出发，ABD 选项都有可能泄露资料
所属知识子域：安全漏洞与网络攻击

226. 您突然收到一个自称公安局的人员，说您牵涉到一桩案件，要求提供身份证及银行账户等信息以证明自己清白，以下哪个做法是正确的？（ ）

A. 对方是公安局的，立即提供
B. 无法证明电话那头是否公安部门人员，可以拒绝提供

C. 要求对方报出警号后提供
D. 要求对方提供一个回拨号码，回拨后提供
参考答案:B
难易程度：一级
解析：诈骗信息，从题干中，突然、案件、公安人员、身份证及银行账户可以看出，不符合公安办案程序
所属知识子域：安全漏洞与网络攻击

227. 以下行为不属于违反国家涉密规定的是（）
A. 以不正当手段获取商业秘密
B. 在私人交往中涉及国家秘密
C. 通过普通邮政等无保密及措施的渠道传递国家秘密载体
D. 将涉密计算机、涉密存储设备接入互联网及其他公共信息网络
参考答案 A
难易程度：一级
解析：国家秘密禁止通过普通邮政渠道传输、接入互联网和私人交往中涉及，所以，BCD 违反国家涉密规定，A 项是商业秘密，不属于国家秘密
所属知识子域：网络安全法律法规

228. 为防止病毒感染和传播，日常应用中应做到( )
A. 不点击或打开来源不明的邮件和链接
B. 安装国网规定的防病毒软件
C. 使用安全移动存储介质前先杀毒
D. 以上都是
参考答案 D
难易程度：一级
解析：常识
所属知识子域：安全漏洞与网络攻击

229. 如果您住的小区外有人派发小礼品，只要登记一下手机号码就可用免费领取，以下哪个做法最恰当？( )
A. 扭送公安机关
B. 不予理会，会泄露自己个人信息
C. 免费的不要白不要，填写手机号码领一个
D. 这是好事，我帮朋友也填了领一个
参考答案：B
难易程度：一级
解析：常识
所属知识子域：安全漏洞与网络攻击

230. 网络空间成为国家竞争新的领域，关于这个说法错误的是( )
A. 网络空间已经得到国家高度重视，纳入国家战略
B. 网络空间中的产品已经全面实现国产化
C. 网络空间已经成为国家技术研发重点方向
D. 网络空间已经纳入我国海陆空三军作战范畴
参考答案：B
难易程度：一级
E. 解析：ACD 正确，B 错误，网络空间中的产品已经全面实现国产化的说法是错误的

所属知识子域：网络安全法律法规

231. 网络空间安全问题影响到我们每一个人，对于这个说法理解错误的是( )

A. 信息化技术已经与我们的生活息息相关，密不可分

B. 信息系统支撑了电力、交通等基础设施的运转

C. 没有信息系统，不仅很多企业无法运营，我们每个人的生活都会受到极大影响

D. 网络空间是虚拟空间，网络安全问题目前对普通百姓来说仅仅是信息泄露问题

参考答案：D

难易程度：一级

解析：不仅仅是信息泄露问题，严重可影响人身安全

所属知识子域：网络安全法律法规

232. 维护国家网络空间安全的基本要求和重要任务是( )

A. 实施等级保护

B. 全面落实国产化

C. 保护关键信息基础设施

D. 实施风险评估

参考答案：C

难易程度：一级

解析：常识

所属知识子域：网络安全法律法规

233. 设置复杂的口令，并安全管理和使用口令，其最终目的是（）

A. 攻击者不能获得口令

B. 规范用户操作行为

C. 增加攻击者破解口令的难度

D. 防止攻击者非法获得访问和操作权限

参考答案：D

难易程度：一级

解析：防止攻击者非法获得访问和操作权限

所属知识子域：网络安全法律法规

234. 刘某在自家的小汽车上安装伪基站设备，长期不定时的在各人口密集区利用小汽车上的伪基站强行向不特定用户手机发送虚假广告信息，干扰公用电信网络信号，局部阻断公众移动通信网络信号，陈某的行为属于（）

A. 民事侵权行为

B. 违法犯罪行为

C. 行政违法行为

D. 违反道德的行为

参考答案：B

难易程度：一级

解析：常识

所属知识子域：网络安全法律法规

235. 小区、商场、车站、广场等地方，都有各种来源不明的二维码，你认为乱扫二维码说法错误的是（）

A. 扫二维码没有风险，还可以领福利

B. 有可能造成财产的损失

C. 中木马和病毒

D. 个人隐私的泄露
参考答案：A
难易程度：一级
解析：安全意识
所属知识子域：网络安全法律法规
236. 信息安全已经成为社会的焦点问题，以下不属于信息系统安全运营原则的是（）
A. 标准化与一致性原则
B. 绝对安全原则
C. 统筹规划与分步实施原则
D. 同步规划建设原则
参考答案：B
难易程度：一级
解析：信息系统安全运营原则包括标准化与一致性原则、技术与管理并重原则、统筹规划与分步实施原则和同步规划建设原则。
所属知识子域：网络空间安全政策与标准化
237. 信息安全管理岗位属于关键岗位，以下属于对全体员工的信息安全要求的是（）
A. 禁止利用计算机资源制造、传播违反国家法律法规的信息
B. 掌握所在岗位需要的计算机信息安全知识
C. 妥善保管计算机
D. 以上都是
参考答案：D
难易程度：一级
解析：对全体员工的信息安全要求包括禁止利用计算机资源制造、传播违反国家法律法规的信息；掌握所在岗位需要的计算机信息安全知识；妥善保管计算机；妥善保管身份认证凭据（如用户帐号、密码、数字证书等）；严禁自行更改所使用计算机系统的软硬件配置等。因此本题选 D。
所属知识子域：信息安全管理
238. 业务连续性是组织对事故和业务中断的规划和响应，下列关于业务连续性描述中正确的是（）
A. 业务连续性使业务可能在预先定义的级别上持续运行的组织策略和战略上的能力
B. 是组织计算机容灾技术的升华概念
C. 其目的是保证企业信息流在任何时候以及任何需要的状况下都能保持业务连续运行
D. 以上都对
参考答案：D
难易程度：一级
解析：业务连续性是组织对事故和业务中断的规划和响应，使业务可能在预先定义的级别上持续运行的组织策略和战略上的能力，是组织计算机容灾技术的升华概念，其目的是为了保证企业包括生产、销售、市场、财务、管理以及其他各种重要的功能完全在内的运营状况百分之百可用。可以这样说，业务连续性是覆盖整个企业的技术以及操作方式的集合，其目的是保证企业信息流在任何时候以及任何需要的状况下都能保持业务连续运行。因此本题选 D。
所属知识子域：信息安全管理
239. 以下关于业务连续性和灾难备份说法不正确的是（）
A. 灾难备份只是一种尽可能减少宕机损失的工具或者策略
B. 业务连续性是灾难备份的基础

C. 缩短灾难备份系统使数据恢复正常的时间就是业务连续性的目标，消除这个时间，则是业务连续性的终极目标
D. 业务连续性是组织计算机容灾技术的升华概念
参考答案：B
难易程度：一级
解析：灾难备份只是一种尽可能减少宕机损失的工具或者策略。不过，灾难备份是业务连续性的基础，没有前者，后者就是空中楼阁，但是如果一个灾难备份系统使数据恢复正常的时间过长，那也就不存在所谓的业务连续性了，缩短这个时间，就是业务连续性的目标，消除这个时间，则是业务连续性的终极目标。因此本题选 B。
所属知识子域：信息安全管理

240. 在本地故障情况下，能继续访问应用的能力，体现了业务连续性的（）

A. 高可用性
B. 连续操作
C. 灾难恢复
D. 以上都不是
参考答案：A
难易程度：一级
解析：高可用性指提供在本地故障情况下，能继续访问应用的能力。故障包括业务流程、物理设施和 IT 软硬件故障。因此本题选 A。
所属知识子域：信息安全管理

241. 信息系统在什么阶段要评估风险（）。

A. 只在运行维护阶段进行风险评估，以识别系统面临的不断变化的风险和脆弱性，从而确定安全措施的有效性，确保安全目标得以实现
B. 只在规划设计阶段进行风险评估，以确定信息系统的安全目标
C. 只在建设验收阶段进行风险评估，以确定系统的安全目标达到与否
D. 信息系统在其生命周期的各个阶段都要进行风险评估
参考答案：D
难易程度：一级
解析：信息系统在其生命周期的各阶段都要进行风险评估。包括规划设计阶段、运行维护阶段、建设验收阶段都要进行风险评估。因此本题选 D。
所属知识子域：信息安全管理

242. 企业信息安全管理为企业信息和企业信息系统提供的服务不包括（）

A. 保密性
B. 完整性
C. 可控性
D. 不可否认性
参考答案：C
难易程度：一级
解析：企业信息安全管理为企业信息和企业信息系统提供保密性、完整性、真实性、可用性、不可否认性服务。因此本题选 C
所属知识子域：信息安全管理

243. 渗透测试与恶意入侵区别是（）

A. 采用不同思维方式

B. 渗透测试过程可控

C. 都是合法的

D. 都会对系统造成破坏

参考答案：B

难易程度：一级

解析：渗透测试必须是合法的，也就是说在渗透测试之前，需要客户签署书面授权委托，而且整个渗透测试过程必须在可控的状态下进行，这也是渗透测试和恶意攻击的本质区别。因此本题选 B。

所属知识子域：安全漏洞与网络攻击

244. 发生信息安全紧急事件时，可采取（ ）措施。

A. 事件分析

B. 抑制、消除和恢复

C. 切断不稳定因素

D. 以上采取的措施都对

参考答案：D

难易程度：一级

解析：当发生风险时，需要对出现的风险进行分析、防范和规避，且事先要对待测试系统中的数据做好备份以防止数据丢失，造成损失。因此本题选 D。

所属知识子域：安全漏洞与网络攻击

245. 以下哪一个漏洞属于数据库漏洞（）

A. XSS

B. SQL 注入

C. CSRF

D. SSRF

参考答案：B

难易程度：一级

解析：SQL 注入是最常见的数据库漏洞之一，SQL 注入到数据库后，应用程序将会被注入恶意的字符串，从而达到欺骗服务器执行命令的恶意攻击效果。因此本题选 B。

所属知识子域：安全漏洞与网络攻击

246. 渗透测试大致可分为信息收集、漏洞发现和（）三个阶段

A. 目标确立

B. 威胁建模

C. 漏洞验证

D. 漏洞利用

正确答案：D

难易程度：一级

解析：渗透测试大致可分为信息收集、漏洞发现和漏洞利用等三个阶段，更细致可划分为目标确立、信息收集、威胁建模、漏洞探测、漏洞验证、漏洞分析和漏洞利用等七个阶段，并最终形成渗透测试报告。因此本题选 D。

所属知识子域：安全漏洞与网络攻击

247. 信息收集的原则是准确性、时效性和（）

A. 必要性

B. 全面性
C. 针对性
D. 局域性
正确答案：B
难易程度：一级
解析：信息收集应遵守一定的原则，即准确性、全面性和时效性。因此本题选 B。
所属知识子域：安全漏洞与网络攻击

248. 以下关于情报收集说法错误的是（）

A. 渗透测试最重要的阶段就是情报收集
B. 情报收集是信息得以利用的第一步
C. 情报收集是一个综合过程
D. 情报收集在渗透测试中不是必要的
正确答案：D
难易程度：一级
解析：渗透测试最重要的阶段就是信息收集。信息收集是指通过各种方式获取所需要的信息，是必须要进行的步骤。因此本题选 D。
所属知识子域：安全漏洞与网络攻击

249. 以下不是社会工程学利用的心理的是（）

A. 好奇
B. 贪婪
C. 防范
D. 信任
正确答案：C
难易程度：一级
解析：社会工程学是一种通过对受害者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱进行诸如欺骗、伤害等危害手段，取得自身利益的手法。因此本题选 C。
所属知识子域：安全漏洞与网络攻击

250. 身份冒充的攻击原理是（）

A. 一个实体声称是另一个实体。
B. 诱使工作人员或网络管理人员透露或者泄漏信息
C. 声称来自于银行或其他知名机构的欺骗性垃圾邮件
D. 以上都不对
正确答案：A
难易程度：一级
解析：身份冒充指的是一个实体声称是另一个实体。这是最常见的一种攻击方式，对于最简单的口令认证方式，只要能获得别人的口令，就能轻而易举的冒充他人。因此本题选 A。
所属知识子域：安全漏洞与网络攻击

251. 数据库安全非常重要，一旦恶意 SQL 语句注入到数据库后，会产生什么后果（）

A. 读取敏感数据
B. 修改数据
C. 执行管理操作
D. 以上都是
正确答案：D
难易程度：一级

解析：SQL 注入到数据库后，应用程序将会被注入恶意的字符串，从而达到欺骗服务器执行命令的恶意攻击效果，如读取敏感数据、修改数据和执行管理操作等。
所属知识子域：安全漏洞与网络攻击

252. 用户收到了一封可疑的电子邮件要求用户提供银行账户及密码,这是属于下列攻击手段（）

A. 缓存溢出攻击
B. 钓鱼攻击
C. 暗门攻击
D. DDOS 攻击
正确答案：B
难易程度：一级
解析：网络钓鱼攻击者利用欺骗性的电子邮件和伪造的 Web 站点来进行网络诈骗活动，受骗者往往会泄露自己的私人资料，如信用卡号、银行卡账户、身份证号等内容。诈骗者通常会将自己伪装成网络银行、在线零售商和信用卡公司等可信的品牌，骗取用户的私人信息。因此本题选 B。
所属知识子域：安全漏洞与网络攻击

253. 端口扫描的目的是（）

A. 判断其运行的服务
B. 判断其存活状态
C. 发现漏洞
D. 以上都不是
正确答案：A
难易程度：一级
解析：端口扫描通过扫描目标主机端口来判断其运行的服务，是信息收集阶段的必要步骤。因此本题选 A。
所属知识子域：安全漏洞与网络攻击

254. 漏洞扫描的主要功能是()

A. 扫描目标主机的服务端口
B. 扫描目标主机的操作系统
C. 扫描目标主机的漏洞
D. 扫描目标主机的 IP 地址
正确答案：C
难易程度：一级
解析：漏洞扫描是指基于漏洞数据库，通过扫描等手段对指定的远程或者本地计算机系统的安全脆弱性进行检测，从而发现可利用漏洞的一种安全检测（渗透攻击）行为。因此本题选 C。
所属知识子域：安全漏洞与网络攻击

255. 漏洞扫描一般采用的技术是（）

A. 基于异常检测技术
B. 基于特征的匹配技术
C. 基于协议分析技术
D. 基于操作系统的分析技术
正确答案：B
难易程度：一级

解析：漏洞扫描技术是在端口扫描后得知目标主机开启的端口以及端口上的网络服务，将这些相关信息与网络漏洞扫描系统提供的漏洞库进行匹配，查看是否存在满足匹配条件的漏洞，通过模拟攻击者的攻击手法，对目标主机系统进行攻击性的安全漏洞扫描，若模拟攻击成功，则表明目标主机系统存在安全漏洞。因此本题选 B。

所属知识子域：安全漏洞与网络攻击

256. 可以获取远程主机操作系统类型的工具是（）

A. Nmap

B. Net

C. Whisker

D. Nbstat

正确答案：A

难易程度：一级

解析：Nmap 是一个网络连接端扫描软件，用来扫描网上电脑开放的网络连接端。确定哪些服务运行在哪些连接端，并且推断计算机运行哪个操作系统。因此本题选 A。

所属知识子域：安全漏洞与网络攻击

257. 网络嗅探的目的是（）

A. 随时掌握网络的实际情况

B. 查找网络漏洞

C. 检测网络性能

D. 以上都是

正确答案：D

难易程度：一级

解析：网络嗅探对于网络管理员来说可以随时掌握网络的实际情况，查找网络漏洞和检测网络性能。因此本题选 D。

所属知识子域：安全漏洞与网络攻击

258. 网络嗅探技术是一种（）技术

A. 物理层

B. 数据链路层

C. 网络层

D. 应用层

正确答案：B

难易程度：一级

解析：网络嗅探技术是一种数据链路层技术，利用了共享式网络传输介质的特性，即网络中的一台机器可以嗅探到传递给本网络中其他机器的报文。因此本题选 B。

所属知识子域：安全漏洞与网络攻击

259. 网络嗅探利用的原理是（）

A. 广播原理

B. 交换共享

C. TCP 连接

D. UDP 连接

正确答案：B

难易程度：一级

解析：网络嗅探指通过嗅探工具窃听网络上流经的数据包，其利用的是交换共享原理。因此本题选 B。

所属知识子域：安全漏洞与网络攻击

260. 下列设备中，是网络与网络连接的桥梁，是因特网中最重要的设备是（）

A. 中继器

B. 集线器

C. 路由器

D. 服务器

正确答案：C

难易程度：一级

解析：路由器（Router）是连接因特网中各局域网或广域网的设备，构成了 Internet 的骨架。因此本题选 C。

所属知识子域：安全漏洞与网络攻击

261. 端口映射的作用是（）

A. 将 MAC 地址解析成 IP 地址

B. 将内网的服务端口映射到路由器的外网地址

C. 将端口划分广播域

D. 实现点对点将本地主机加入到目标路由器所在的内网

正确答案：B

难易程度：一级

解析：端口映射，即将内网的服务端口映射到路由器的外网地址，从而实现对内网服务的访问。因此本题选 B。

所属知识子域：安全漏洞与网络攻击

262. 端口映射理论上可以提供多少端口的映射（）

A. 65535

B. 64511

C. 1024

D. 64

正确答案：B

难易程度：一级

解析：理论上可以提供 65535（总端口数）-1024（保留端口数）=64511 个端口的映射。因此本题选 B。

所属知识子域：安全漏洞与网络攻击

所属知识子域：安全漏洞与网络攻击

263. 黑客们编写的扰乱社会和他人的计算机程序，这些代码统称为（）

A. 恶意代码

B. 计算机病毒

C. 蠕虫

D. 后门

正确答案：A

难易程度：一级
解析：恶意代码是指为达到恶意目的而专门设计的程序或代码，包括一切旨在破坏计算机或者网络系统可靠性、可用性、安全性和数据完整性或者消耗系统资源的恶意程序。因此本题选 A。
所属知识子域：恶意代码

264. 关于恶意代码，计算机感染恶意代码的现象不包括（）

A. 鼠标或键盘不受控制
B. 计算机运行速度明显变慢
C. 文件无法正确读取、复制或打开
D. 计算机开机无响应

正确答案：D
难易程度：一级
解析：计算机感染了病毒后的症状很多，其中有：计算机系统运行速度明显减慢；经常无缘无故地死机或重新启动；文件无法正确读取、复制或打开；浏览器自动链接到一些陌生的网站；鼠标或键盘不受控制等。因此本题选 D。
所属知识子域：恶意代码

265. 宏病毒是一种专门感染微软 office 格式文件的病毒，下列不可能感染该病毒的文件是（）

A. *.exe
B. *.doc
C. *.xls
D. *.ppt

正确答案：A
难易程度：一级
解析：.exe 是可执行文件，不属于 office 格式文件。因此本题选 A。
所属知识子域：恶意代码

266. 一种可以驻留在对方服务器系统中的程序指的是（）

A. 后门
B. 跳板
C. 木马
D. 终端服务系统

正确答案：C
难易程度：一级
解析：木马是一种附着在正常应用程序中或者单独存在的一类恶意程序。因此本题选 C。
所属知识子域：恶意代码

267. 关于特洛伊木马程序，下列说法不正确的是（）

A. 特洛伊木马程序能与远程计算机建立连接
B. 特洛伊木马程序能够通过网络控制用户计算机系统
C. 特洛伊木马程序包含有控制端程序、木马程序和木马配置程序
D. 特洛伊木马程序能够通过网络感染用户计算机系统

正确答案：D
难易程度：一级
解析：木马与病毒不同，它在主机间没有感染性。因此本题选 D。
所属知识子域：恶意代码

268. 关于计算机病毒，计算机病毒是（）

A. 一种芯片

B. 一种生物病毒

C. 具有远程控制计算机功能的一段程序

D. 具有破坏计算机功能或毁坏数据的一组程序代码

正确答案：D

难易程度：一级

解析：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。因此本题选 D。

所属知识子域：恶意代码

269. 关于木马，下列关于计算机木马的说法错误的是（）

A. 杀毒软件对防止木马病毒泛滥具有重要作用

B. Word 文档也会感染木马

C. 只要不访问互联网，就能避免受到木马侵害

D. 尽量访问知名网站能减少感染木马的概率

正确答案：C

难易程度：一级

解析：木马可以通过软盘、光盘、移动存储设备等进行传播。因此本题选 C。

所属知识子域：恶意代码

270. 某公司的网络管理员在数据库中预留了某个程序，使得他在被解雇时执行该程序并删除公司整个数据库，此类程序属于（）

A. 木马

B. 蠕虫

C. 逻辑炸弹

D. 僵尸网络

正确答案：C

难易程度：一级

解析：当发生特定事件时，逻辑炸弹会执行某个程序或某段代码。因此本题选 C。

所属知识子域：恶意代码

271. 僵尸网络的最大危害是，攻击者可以利用网络发起（）

A. 入侵攻击

B. DDOS 攻击

C. 网络监听

D. 心理攻击

正确答案：B

正确答案：C

难易程度：一级

解析：攻击者通常利用僵尸网络发起各种恶意行为，比如对任何指定主机发起分布式拒绝服务攻击（DDoS）、发送垃圾邮件（Spam）、获取机密、滥用资源等。因此本题选 B。

所属知识子域：恶意代码

272. 通过分布式网络来扩散特定的信息或错误，进而造成网络服务器遭到拒绝并发生死锁或系统崩溃的恶意代码是（）

A. 恶意脚本

B. 蠕虫

C. 宏病毒
D. 僵尸网络
正确答案：B
难易程度：一级
解析：蠕虫病毒是自包含的程序（或者一套程序），它能传播它自身功能的拷贝或它的某些部分到其他的计算机系统中，它通过分布式网络来扩散传播特定的信息或错误，进而造成网络服务遭到拒绝并发生死锁或系统崩溃。因此本题选 B。
所属知识子域：恶意代码

273. 关于恶意代码清除，下列不属于杀毒软件的是（）

A. IDS
B. 卡巴斯基
C. KV2005
D. 小红伞
正确答案：A
难易程度：二级
解析：IDS 是入侵检测系统，不属于杀毒软件。因此本题选 A。所属知识子域：恶意代码
所属知识子域：恶意代码

274. 发现恶意代码后，比较彻底的清除方式是（）

A. 用查毒软件处理
B. 用杀毒软件处理
C. 删除磁盘文件
D. 格式化磁盘
正确答案：D
难易程度：一级
解析：格式化磁盘通常会导致现有的磁盘或分区中所有的文件被清除，同时所有的恶意代码也可以被彻底删除。因此本题选 D。
所属知识子域：恶意代码

275. 随着新型技术应用范围日益拓展，安全漏洞的数量将持续（）

A. 减少
B. 不变
C. 增加
D. 无法确定
正确答案：C
难易程度：二级
解析：格式化磁盘通常会导致现有的磁盘或分区中所有的文件被清除，同时所有的恶意代码也可以被彻底删除。因此本题选 D。
所属知识子域：安全漏洞与网络攻击

276. 身为软件用户，当安全软件提醒自己的电脑有系统漏洞时，最恰当的做法是（）

A. 重启电脑
B. 不与理睬，继续使用电脑
C. 暂时搁置，一天之后再提醒修复漏洞
D. 立即更新补丁，修复漏洞
正确答案：D
难易程度：二级

解析：为避免攻击者利用漏洞攻击用户计算机，应及时更新系统补丁，修复漏洞。因此本题选 D。
所属知识子域：安全漏洞与网络攻击

277. 中国国家信息安全漏洞库属于（）

A. 政府类漏洞管理机构
B. 企业漏洞研究机构
C. 软件厂商
D. 软件用户

正确答案：A
难易程度：二级
解析：中国国家信息安全漏洞库（China National Vulnerability Database of Information Security，CNNVD）属于政府类漏洞管理机构。因此本题选 A。
所属知识子域：安全漏洞与网络攻击

278. 隶属于中国信息安全测评中心的中国国家信息安全漏洞库的英文缩写是（）

A. NVD
B. CNVD
C. CNCVE
D. CNNVD

正确答案：D
难易程度：二级
解析：中国国家信息安全漏洞库（China National Vulnerability Database of Information Security，CNNVD）是中国信息安全测评中心为切实履行漏洞分析和风险评估的职能，负责建设运维的国家信息安全漏洞库。因此本题选 D。
所属知识子域：安全漏洞与网络攻击

279. 为信息安全漏洞在不同对象之间的传递和表达提供一致的方法的是（）

A. 漏洞标识管理
B. 漏洞补丁管理
C. 漏洞信息管理
D. 漏洞评估管理

正确答案：A
难易程度：三级
解析：漏洞标识方面的规范是为信息安全漏洞在不同对象之间的传递和表达提供一致的方法。因此本题选 A。
所属知识子域：安全漏洞与网络攻击

280. 在漏洞处理过程中应维护的原则不包括（）

A. 公平、公开、公正
B. 及时处理
C. 安全风险最小化
D. 保密，防止漏洞被泄漏

正确答案：D
难易程度：二级
解析：在漏洞处理过程中应维护公平、公开、公正、及时处理原则和安全风险最小化原则。因此本题选 D。
所属知识子域：安全漏洞与网络攻击

281. 许多黑客攻击都是利用软件实现中的缓冲区溢出的漏洞，对于这一威胁，最可靠的解决方案是（）

A. 安装 IDS

B. 安装防火墙

C. 安装反病毒软件

D. 安装系统最新补丁

正确答案：D

难易程度：二级

解析：修复漏洞最基本的方法就是安装系统最新补丁。因此本题选 D。

所属知识子域：安全漏洞与网络攻击

282. 口令安全不取决于（）

A. 口令的更换周期

B. 口令复杂度

C. 口令是否合理存放

D. 口令是否便于记忆

正确答案：D

难易程度：二级

解析：为保证口令安全，应尽可能设置复杂口令，定期更换口令，将口令文件存放隐秘处等。因此本题选 D。

所属知识子域：口令破解

283. 后门是一种恶意代码，下列关于后门的描述中不正确的是（）

A. 后门程序是绕过安全性控制而获取对程序或系统访问权的程序

B. Windows Update 实际上就是一个后门软件

C. 后门程序能绕过防火墙

D. 后门程序都是黑客留下来的

正确答案：D

难易程度：二级

解析：后门最初是软件编程人员在编写软件时，为便于调试、修改程序中可能的缺陷和问题而创建出来的。因此本题选 D。

所属知识子域：安全漏洞与网络攻击

284. 后门与其它恶意代码比较而言是有区别的，下列描述中正确的是（）

A. 后门是一个完整的程序软件

B. 后门具有“传染性”

C. 后门和木马类似，但隐蔽性不如木马

D. 后门的主要功能是隐藏在系统中搜集信息或便于攻击者连接使用

正确答案：D

难易程度：二级

解析：后门不一定具有“传染性”；木马是一个完整的程序软件，后门相对而言功能单一、体积较小，但隐蔽性更强，主要功能是隐藏在系统中搜集信息或便于攻击者连接使用。因此本题选 D。

所属知识子域：安全漏洞与网络攻击

285. 通过“计算机管理”来清除时间日志也可以达到清除痕迹的目的，具体操作是（）

A. 禁用“event system”服务

B. 禁用“net logon”服务

C. 禁用“event log”服务
D. 禁用“secondary logon”服务
正确答案：C
难易程度：三级
解析：通过“计算机管理”来清除时间日志也可以达到清除痕迹的目的，如果禁用“event log”服务，则该主机就不会对任何操作进行日志记录了。因此本题选 C。
所属知识子域：安全漏洞与网络攻击

286. 对于信息安全管理，风险评估的方法比起基线的方法，主要的优势在于它确保（）

A. 信息资产被过度保护
B. 不考虑资产的价值，基本水平的保护都会被实施
C. 对信息资产实施适当水平的保护
D. 对所有信息资产保护都投入相同的资源
正确答案：C
难易程度：三级
解析：风险评估确定了给定风险的最适当的保护，基线的方法仅仅提供了一套保护方法，没有注意风险的存在。不仅没有过度保护的信息资产，而且更大的好处是能够确定没有信息资产保护过度或保护不够。风险评估提供了和资产价值适当的保护水平。基线方法不是从资产本身的风险考虑，而是所有资产投入相同的资源。因此本题选 C。
所属知识子域：安全漏洞与网络攻击

287. 信息系统审计在企业管理中的重要性上升到了一个新高度，具体表现不包括哪些方面（）

A. 企业的生存与发展越来越依赖信息系统
B. 企业的潜在风险主要是来自互联网的威胁
C. 外部审计离不开信息系统审计
D. 董事长成为内部控制的主要参与者
正确答案：D
难易程度：三级
解析：具体表现包括信息系统审计师成为内部控制的主要参与者
所属知识子域：信息安全管理内部管理

288. 关于恶意代码，网页恶意代码通常利用（）来实现植入并进行攻击。

A. U 盘工具
B. 口令攻击
C. 拒绝服务攻击
D. 浏览器的漏洞
正确答案：D
难易程度：三级
解析：网页恶意代码通常利用浏览器的漏洞来实现植入并进行攻击。因此本题选 D。
所属知识子域：信息安全管理内部管理

289. 信息系统是指由（）组成，按照一定的应用模板和规则对信息进行存储、传输和处理的系统或者网络。

A. 计算机
B. 计算机及其相关的配套设备
C. 网络中的所有计算机
D. 网络中的所有路由器

正确答案：B
难易程度：三级
解析：信息系统是指由计算机及其相关的配套设备组成，按照一定的应用模板和规则对信息进行存储、传输和处理的系统或者网络。因此本题选 B。
所属知识子域：信息安全管理内部管理

290. 描述从源代码层修复或避免漏洞产生的方法属于修复措施类的（）

A. 检测特征
B. 防范操作
C. 补丁信息
D. 安全编程

正确答案：D
难易程度：三级
解析：修复措施类的安全编程用来描述从源代码层修复或避免漏洞产生的方法。因此本题选 D。
所属知识子域：信息安全管理内部管理

291. 关于计算机取证描述不正确的是（ ）

A. 计算机取证是使用先进的技术和工具，按照标准规程全面的检查计算机系统，已提取和保护有关计算机犯罪的相关证据的活动
B. 取证的目的包括：通过证据查找肇事者、通过证据推断犯罪过程、通过证据判断受害者损失程度及收集证据提供法律支持
C. 电子证据是计算机系统运行过程中产生的各种信息记录及储存的电子化资料及物品，对于电子证据，取证工作主要围绕两方面进行：证据的获取和证据的保护
D. 计算机取证的过程可以分为准备、保护、提取、分析和提交 5 个步骤

参考答案：C
难易程度：三级
解析：电子证据是计算机系统运行过程中产生的各种信息记录及储存的电子化资料及物品，对于电子证据，取证工作主要围绕两方面进行：证据的获取和证据的分析。
所属知识子域：网络空间安全法律法规

292. http 协议的默认端口号是（）

A. 80
B. 443
C. 53
D. 3306

参考答案：A
难易程度：三级
解析：http 的默认端口是 80 端口，是网页服务器的访问端口，用于网页浏览
所属知识子域：网络空间安全法律法规

293. 信息系统安全防护体系中最不稳定也是最脆弱的环节是 ( )

A. 防火墙
B. 管理制度
C. 系统管理员或用户
D. 服务器

参考答案：C
难易程度：二级

解析：人是信息安全管理体系中最脆弱的环节，所以选 C
所属知识子域：信息安全与网络空间安全

294. 以下关于防范钓鱼网站的做法哪个是错误的（）

A. 通过查询网站备案信息等方式核实网站资质的真伪
B. 安装安全防护软件
C. 警惕中奖、修改网银密码的通知邮件、短信，不轻意点击未经核实的陌生链接
D. 为了更好的玩游戏，关闭杀毒软件等耗资源的软件

参考答案：D
难易程度：二级
解析：关闭杀毒软件是错误的做法
所属知识子域：信息安全与网络空间安全

295. 我们在日常生活和工作中，为什么需要定期修改电脑、邮箱、网站的各类密码( )

A. 遵循国家的安全法律
B. 降低电脑受损的几率
C. 确保不会忘掉密码
D. 确保个人数据和隐私安全

参考答案：D
难易程度：一级
解析：日常生活和工作中使用的各类密码要定期修改，就是为了防止密码被他人破解和泄露，导致数据和个人隐私泄露
所属知识子域：信息安全与网络空间安全

296. 王同学喜欢在不同的购物和社交网站进行登录和注册，但他习惯于在不同的网站使用相同的用户名和密码进行注册登录，某天，他突然发现，自己在微博和很多网站的账号同时都不能登录了，这些网站使用了同样的用户名和密码，请问，王同学可能遭遇了以下哪类行为攻击。( )

A. 拖库
B. 撞库
C. 建库
D. 洗库

参考答案：B
难易程度：二级
解析：撞库是黑客通过收集互联网已泄露的用户和密码信息，生成对应的字典表，尝试批量登陆其他网站后，得到一系列可以登录的用户。很多用户在不同网站使用的是相同的帐号密码，因此黑客可以通过获取用户在 A 网站的账户从而尝试登录 B 网址，这就可以理解为撞库攻击。
所属知识子域：信息安全与网络空间安全

297.《互联网新闻信息服务单位内容管理》第四章从业人员监督管理，国家和地方互联网信息办公室职能有（）

A. 依法建立从业人员信用档案和黑名单
B. 指导互联网新闻信息服务单位建立健全从业人员准入、奖惩、考评、退出等制度
C. 国家互联网信息办公室建立从业人员统一的管理信息系统，对从业人员基本信息、从业培训经历和奖惩情况等进行记录，并及时更新、调整。地方互联网信息办公室负责对属地从业人员建立管理信息系统，并将更新、调整情况及时上报上一级互联网信息办公室
D. 以上都对

参考答案：D
难易程度：二级
解析：《互联网新闻信息服务单位内容管理》第四章从业人员监督管理
所属知识子域：信息安全与网络空间安全

298.“会话侦听和劫持技术”是属于（）的技术

A. 密码分析技术
B. 协议漏洞渗透
C. 应用漏洞分析与渗透
D. DDOS 攻击

参考答案：B
难易程度：三级
解析：
所属知识子域：信息安全与网络空间安全

299. 涉密信息系统工程监理工作需要（）的单位或组织实施监督管理

A. 涉密信息系统工程建设不需要监理
B. 具有信息系统工程监理资质的单位
C. 具有涉密信息系统工程监理资质的单位
D. 国家保密行政管理部门

参考答案：C
难易程度：三级
解析：涉密信息系统工程监理是指依法设立且具备涉密信息系统工程监理资质的单位，受建设方单位委托，依据国家有关法律法规、保密标准和工程监理合同，对涉密信息系统工程实施监督管理。
所属知识子域：信息安全与网络空间安全

300. 信息技术安全性评估通用标准用于评估信息系统、信息产品的安全性，其又被称为（）

A. ISO 标准
B. HTTP 标准
C. IEEE 标准
D. CC 标准

参考答案：D
难易程度：三级
解析：1993 年 6 月，美国政府同加拿大及欧共体共同起草单一的通用准则(CC 标准)并将其推到国际标准。制定 CC 标准的目的是建立一个各国都能接受的通用的信息安全产品和系统的安全性评估准则。
所属知识子域：信息安全与网络空间安全

301. 安全测试用于提高软件系统的安全性，以下关于安全测试的描述中错误的是（）

A. 黑盒测试主要针对程序所展现给用户的功能
B. 白盒测试是针对被测单元内部是如何工作进行的测试
C. 灰盒测试是介于黑盒测试和白盒测试之间的一种测试
D. 黑盒测试可以完全取代白盒测试

参考答案：D
难易程度：三级
解析：软件的黑盒测试意味着测试要在软件的接口处进行。软件的白盒测试是对软件的过程性细节做细致的检查。

所属知识子域：信息安全与网络空间安全

302. 网络爬虫是搜索引擎的重要组成部分，但网络爬虫也带来了一定的安全风险。爬虫被非法利用可能带来的危害包括（）

A. 核心文本被爬

B. 破坏数据和系统

C. 影响正常用户的访问

D. 以上都是

参考答案：D

难易程度：三级

解析：

所属知识子域：信息安全与网络空间安全