**第一章：**

1. 填空题

（1）信息安全包含\_\_\_系统安全\_\_\_\_\_\_ 、\_\_\_\_\_数据安全\_\_\_\_\_、\_\_\_\_\_\_\_内容安全\_\_\_ 和\_\_\_\_行为安全\_\_\_\_\_\_等四个层次。

（2）信息系统的脆弱性主要包括：\_\_\_电磁泄露\_\_\_\_\_\_\_ 、\_\_\_数据库系统的安全漏洞\_\_\_\_\_\_\_ 、\_\_\_\_\_通信协议的安全漏洞\_\_\_\_\_ 、 \_\_\_\_芯片的脆弱性\_\_\_\_\_\_ 、\_\_\_\_\_\_\_操作系统的安全漏洞\_\_\_和\_\_\_移动存储介质的安全漏洞\_\_\_\_\_\_\_ 。

（3）人为安全威胁的来源包括：\_\_\_\_\_\_物理攻击\_\_\_\_ 、\_\_\_\_\_网络攻击\_\_\_\_\_ 、\_\_\_\_\_\_恶意代码\_\_\_\_ 和 \_\_\_安全管理\_\_\_\_\_\_\_ 。

2、选择题（单选和多选）

（1）2008年，XXX国利用BGP（Border Gateway Protocol边界网关协议）劫持，破坏了 格鲁吉亚的互联网，瘫痪了所有政府的基础设施。这种攻击行为属于（A ）

A.网络攻击；B.物理攻击；C.病毒攻击；D.安全管理

（2）1982年，由工业控制软件内嵌的病毒引发泛西伯利亚天然气管道发生大爆炸。 这种攻击行为属于（C ）

1. 网络攻击；B.物理攻击；C.恶意代码攻击；D.安全管理
2. 以下描述是正确的有（C ）
3. 安全风险是“绝对的”，但我们可以完全消除；
4. 信息系统的安全风险一定会使系统遭受安全损失；
5. 安全风险虽不能完全消除，但可以降低对系统的危害；
6. 安全威胁一定会造成安全损失，因此我们必须严防安全威胁。
7. 问答题
8. 如果信息系统无任何脆弱性，是否就不存在安全风险呢？分析举例。

依旧存在安全风险。

信息系统的开放性可能会导致安全风险。当前普遍采用的网络协议是TCP/IP协议，而OSI仅用于开放网络模型。TCP/IP协议的开放性和灵活性好似一把双刃剑，在推动了互联网的迅猛发展的同时，给信息系统安全带来了极大的安全隐患，TCP报头的内容都是明文，攻击者很容易就可以破坏A和B之间的连接，并在攻击者和目的主机之间建立连接。

黑客的恶意入侵也会影响信息系统安全。2010年6月发现的“震网”病毒是第一个定向攻击基础设施的“蠕虫”病毒。2017年5月爆发勒索病毒使得近百国中招，其中英国医疗系统陷入瘫痪、大量病人无法就医，中国的高校校内网也被感染。受害者只有付费后才能解锁计算机。

1. 信息系统的脆弱性和安全威胁分别体现在哪些方面？简要阐述。

信息系统的脆弱性体现在系统会遇到辐射泄露，数据库自身存在的安全缺陷，协议的开放性，硬件安全问题，操作系统软件的缺陷。

信息系统的安全威胁体现在系统会受到来自自然和人为两方面的威胁，来自人为方面的包括物理攻击，网络攻击，恶意代码，安全管理四个方面。

1. 根据标准GA/T 708-2007，信息系统的基本安全属性包含哪些？除此之外，你认为信息系统还需要有哪些安全需求？举例说明。

保密性，完整性，可用性。

信息系统还需要有从被攻击后的状态恢复的能力，比如当系统因为受到ddos攻击而崩溃时，需要能够恢复系统的正常运行，消除ddos攻击带来的影响。

1. 如何理解：安全管理的最终目的是“使安全风险降低到用户和决策者都可以接受的程度”？

因为安全风险是绝对的，不可能完全消除，只能尽可能降低安全风险的程度，使其对系统的危害可以被用户和决策者接受。