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：**电磁泄漏**、**芯片的脆弱性**、**数据库系统的安全漏洞**、**操作系统的安全漏洞**、**通信协议的安全漏洞**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（**CD**）**C**

A.网络攻击；B.物理攻击；C.恶意代码攻击；D.安全管理

（3）以下描述是正确的有（**C**）

A.安全风险是“绝对的”，但我们可以完全消除；

B.信息系统的安全风险一定会使系统遭受安全损失；

C.安全风险虽不能完全消除，但可以降低对系统的危害；

D.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。

3、问答题

（1）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。

**没有脆弱性的系统并不一定就没有安全风险。脆弱性主要是由系统的软、硬件缺陷导致的，是系统安全风险的主要来源，但系统的安全风险还与人的行为密切相关，人为的恶意行为、疏忽或失误也会导致系统出现安全风险。**

**比如一个在软、硬件均不存在安全缺陷的保密系统，没有脆弱性，但不能防止社会工程学攻击（比如勾结内部人员物理拷贝数据等）所带来的安全风险。**

（2）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信息系统的各个环节中的软件、硬件缺陷，这些缺陷可能被攻击者发现并利用，给信息系统带来安全风险。包括了电磁泄漏、芯片的脆弱性、数据库系统的安全漏洞、操作系统的安全漏洞、通信协议的安全漏洞和移动存储介质的安全漏洞几种类型。**

**信息系统的安全威胁体现在能够直接对信息系统造成破坏的行为上。包括了自然因素和人为因素，其中人为因素又可以分为物理攻击、网络攻击、恶意代码和安全管理。**

（3）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。

**信息系统的基本安全属性包括了保密性、完整性和可用性。除此之外我认为还应当有以下几点：**

1. **真实性。以上三点安全属性没有涵盖假冒发信人进行通信的情况，这需要身份验证来确保通信双方身份的真实性；**
2. **不可否认性。对历史通信内容应当进行记录备份存储，以防止对先前通信内容的否认抵赖。**
3. **可控性。确保信息的传播在可管制的范围内不会造成泛滥。**

（4）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”？

**信息系统的安全风险是客观存在的，不仅包含软、硬件层面上的，更与人的参与、行为密切相关，所以想要彻底消除安全风险是不可行也没有实际意义的。而安全管理能够做的就是规范化管理每一环节，尽可能降低系统所面临的安全风险。但一味地管控、降低风险同样会增加成本、或是使得流程过度繁琐。所以就需要平衡管控带来的成本与风险造成的损失，制定合理的安全管理策略，保证风险可接受的同时管理成本可控。**