**第一章 信息安全工程基础**

**1．信息的本质是什么？它的重要性体现在哪里？**

**2．什么是信息安全？它是如何发展的？**

**3．信息安全的目标体现在哪些方面？**

**4．信息安全保障是什么？它有哪些要素和特征？**

**5．简述信息系统安全保障的生命周期。**

**6．信息保障技术框架由哪些部分组成以及各个部分有哪些作用？**

**7．请简要说明国内外信息安全保障体系的建设异同？**

**8．什么是信息安全工程？为什么需要信息安全工程？**

**9．信息安全工程是如何发展起来的？**

**10．信息安全工程涉及哪些内容？**

1.（1）信息是对客观世界中各种事物的运动状态和变化的反映，是客观事物之间相互联系和相互作用的表征，表现的是客观事物运动状态和变化的实质内容。（2）信息和信息技术改变着人们的生活和工作方式。离开计算机、电视和手机等电子信息设备，人们将无法正常生活和工作。

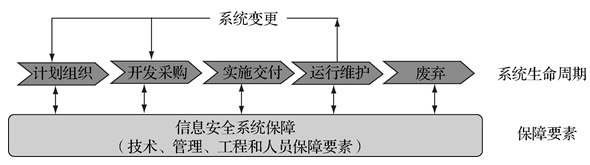
2.（1）信息安全是信息对其生存环境的基本要求，即要确保信息免受其生存环境的危害。

（2）信息安全的发展阶段大致可以分为4个时期。第一个时期为20世纪40～70年代。其主要标志是1949年香农发表的《保密系统的通信理论》。在此阶段中，通信技术不发达，人们主要使用电话、传真等进行通信，其主要的安全问题为通信过程中的信息交换，其主要的解决方法是通过密码（主要是序列密码）解决通信安全的保密问题，所以这一阶段可以称为“通信安全时期”。第二时期为20世纪70～80年代的“计算机安全时期”。这一时期半导体和集成电路技术得到飞速发展，因而推动了计算机软硬件的发展。同时网络技术的发展使数据传输可以通过计算机网络来完成，人们关注的焦点扩展为网络数据传输、处理和存储的保密性、可用性和完整性，主要保证动态信息不被窃取、解密或篡改，从而让读取信息的人能够看到准确无误的信息。第三时期是从20世纪90年代开始兴起的网络时代。这一时期被称为“信息系统安全时期”。这一阶段的安全威胁主要有网络入侵、病毒破坏、信息对抗等，其重点在于保护比“数据”更精炼的“信息”，以确保信息在存储、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，安全措施主要有防火墙、防病毒、漏洞扫描、入侵检测、PKI、VPN等。第四时期是从21世纪开始的“信息安全保障时期”。这一时期的主要标志是1998年美国国家安全局（NSA）提出的《信息保障技术框架》（IATF）。信息安全保障这一理念，不仅仅是从系统漏洞方面考虑，还要从业务的生命周期、业务流程来进行分析，其核心思想是综合技术、管理、过程、人员等，在不同的阶段进行安全保障。

3. 信息安全的总体目标是保护信息免受各种威胁的损害，以确保业务连续性，业务风险最小化，投资回报和商业机遇最大化。从纵向来看，信息安全主要包括以下4个层面：设备安全、数据安全、行为安全以及内容安全。其中数据安全即是传统的信息安全。

4.（1）信息安全保障是在信息系统的整个生命周期中，通过对信息系统的风险分析，制定并执行相应的安全保障策略，从技术、管理、工程和人员等方面提出安全保障要求，确保信息系统的保密性、完整性和可用性，降低安全风险到可接受的程度，从而保障系统实现组织机构的使命。（2）保障要素：信息安全技术体系、信息安全工程过程、信息安全管理体系和高素质的人员队伍。特征：可用性、完整性、保密性。

5. 在信息系统安全保障模型中，整个生命周期被抽象成计划组织、开发采购、实施交付、运行维护和废弃这5个阶段以及在运行维护阶段由于系统变更所产生的反馈，形成信息系统生命周期完整的闭环结构。在整个信息系统的生命周期中，任何阶段都要结合安全保障的4个要素对信息系统进行安全保障。



6. 信息保障技术框架由人员、技术和操作三部分组成。人员（People）：人员是信息保障体系的核心，拥有、管理和使用着整个信息系统，是第一位的要素，同时也是最脆弱的。技术（Technology）：完善的信息安全技术体系是实现信息保障的重要手段，信息保障体系所应具备的各项安全服务就是通过技术机制来实现的。操作（Operation）：或者叫运行，它构成了安全保障的主动防御体系。如果说技术的构成是被动的，那么操作和流程就是将各方面技术紧密结合在一起的主动的过程，其中包括风险评估、安全监控、安全审计、跟踪告警、入侵检测、响应恢复等内容。

7.同：颁布多项战略政策，推动信息安全建设。国家重视，业界共同努力。

异：我国信息安全产业的基础薄弱、起步晚，面临的挑战大、形势严峻也是必须面对的事实。我国的信息安全产业在政府引导、企业参与和用户认可的良性循环中稳步成长，产业总体规模持续扩大，企业竞争实力显著增强。但是相比发达国家而言，我国信息安全产业缺乏顶层设计和国家战略，财政投入不足，相关人才匮乏，法律机制与产业体系不健全，形势依然十分严峻。美国加强技术研发和对外渗透，美国的信息技术公司主导着全球网络和安全技术的发展。

8. （1）信息安全工程是采用工程的概念、原理、技术和方法，来研究、开发、实施与维护信息系统安全的过程，它将经过时间考验证明是正确的工程实践流程、管理技术和当前能够得到的最好的技术方法相结合，从而解决信息安全保障问题。（2）在日常生活当中，可以遇到很多需要有严格的安全保障的信息系统，如若网上支付系统出了问题，则会影响用户的利益；成绩管理系统出了问题则会影响学校的教学管理等等。

9. 信息安全工程真正作为一门现代化的学科还是从20世纪90年代后开始的。美国军方于1994年2月28日发布了《信息系统安全工程手册v1.0》，随后发布了一系列相关的军标和指令。1986年11月，美国软件工程研究所（Software Engineering Institute，SEI）在Mitre公司的协助下，着手开发过程成熟度框架，用于帮助机构改进其软件过程，并提供一种能够用来评价软件承制方能力的方法。1987年9月，SEI发布了软件过程成熟度框架的一个简短描述，不久后，该框架在被过程工程领域誉为软件过程之父的Humphrey所著的《软件过程管理》中做了扩充。CMM的1.0版在1991年8月由卡内基-梅隆大学软件工程研究所发布。虽然CMM还不够完善，但它代表了软件行业大多数人的想法，并且CMM确实能够帮助软件组织改进软件质量。

系统安全工程-能力成熟度模型SSE-CMM（Systems Security Engineering Capability Maturity Model），起源于美国国家安全局（NSA）在1993年4月提出的一个专门应用于系统工程的能力成熟模型（CMM）的构思，其目的是建立和完善一套成熟的、可度量的安全工程过程。该模型定义了一个组织的安全工程过程必须包含的本质特征，这些特征是完善的安全工程保证。1996年10月发布了SSE-CMM的1.0版本，继而在1997年春制定完成了SSE-CMM评定方法的1.0版本；1999年4月，形成了SSE-CMMV2.0和SSE-CMM评定方法V2.0；2002年3月，SSE-CMM得到了ISO的采纳，成为ISO的标准——ISO/IEC 21827。

10. 