信息安全技术概述

信息安全的任务是保护信息财产，以防止偶然的故意为之的未授权者对信息的恶意修改、破坏以及泄漏，从而导致信息无法处理，不完整、不可靠。

信息安全具有以下基本属性：

（1）保密性（Confindentialy）：保证未授权者无法享用信息，信息不会被非法泄漏而扩散；

（2）完整性（Integrity）：保证信息的来源、去向、内容真实无误；

（3）可用性（Availability）：保证网络和信息系统随时可用；

（4）可控性（Controllability）：保证信息管理者能对传播的信息及内容实施必要的控制以及管理；

（5）不可否认性（Non-Repudiation）:又称不可抵赖性，保证每个信息参与者对各自的信息行为负责；

其中，前三者又称为信息安全的目标——CIA。

信息安全所面临的危险可以分为自然威胁和人为威胁两方面：

自然威胁：各种自然灾害，恶劣的场地环境，电磁干扰，电磁辐射，网络设备自然老化等；

人为威胁：人为威胁又包含无意威胁（偶然事故）和恶意攻击；

偶然事故；

操作失误：未经允许使用，操作不当，误用存储媒介等；

意外损失：电力线路漏电、搭线等；

编程缺陷：经验、水平不足，检查疏忽等；

意外丢失：数据被盗、被非法复制，设备、传输媒介失窃等；

管理不善：维护不力，管理松懈等；

恶意攻击：又分为主动攻击和被动攻击。

主动攻击：有选择性的修改、删除、伪造、添加、重放、乱序信息，冒充以及制造病毒等；

被动攻击：在不干扰网络信息系统正常工作的情况下，进行侦收，截获，窃取，破译，业务流量分析以及电磁泄漏等。

信息安全的额外信息

信息安全体系：包括信息安全服务与信息安全机制。

信息安全服务：实体鉴别，数据源鉴别，禁止抵赖，访问控制，数据完整性，数据机密性

信息安全机制：加密，访问控制，数字签名，交换鉴别，路由控制，公证机制

信息安全的主要技术包括：加密技术，认证技术，防伪技术，知识产权保护技术，网络控制技术，反病毒技术，数据库安全技术和安全审计技术等。

信息安全管理：在“安全方针政策，组织安全，资产分类与控制，人员安全，物理与环境安全，通信与运营安全、访问控制、系统开发与维护、业务持续性管理、符合法律法规要求”等十个领域建立管理控制措施，保证组织资产安全与业务的连续性。