第 1 章 绪论

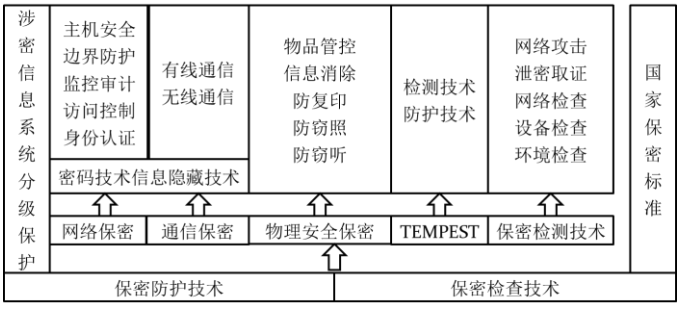
1. **秘密**，是个人、集团甚至国家在一定的时间和范围内，为保护自身的安全和利益，需要加以隐蔽、保护、限制、不让外界知悉的事项的总称。
2. 秘密根据涉及的利益不同，大体上可以分为**国家秘密、工作秘密、商业秘密**和**个人隐私**。
3. **（考）国家秘密**是关系国家安全和利益（实质要素），依照法定程序确定（程序要素），在一定时间内只限一定范围的人员知悉（时空要素）的事项。
4. **工作秘密**是指各级国家机关在其公务活动和内部管理中产生的不属于国家秘密而又不宜对外公开的事项。
5. **商业秘密**是指不为公众所知悉，能为权利人带来经济利益，具有实用性，并经权利人采取保密措施的技术信息和经营信息。
6. **商业秘密的特征：**秘密性、财产性、可分享性。
7. **个人隐私**是指公民个人生活中不愿公开或为他人知悉的秘密。
8. **保密技术**，是指保护秘密信息安全，防止秘密失窃和泄漏的所有相关保障技术。
9. **保密工作**，是指按照我国保密法的规定，为保守国家秘密而进行的工作。
10. **保密技术的基本特性：**技术对抗性、技术多样性、技术秘密性
11. **保密技术和信息安全技术的关系**

    在信息安全发展的早期，两者的根本目标一致，从信息保密角度来看，信息安全技术与保密技术具有共同的核心内容，即确保信息保密性的相关技术；但同时二者的保密对象、安全需求、保护等级等不尽相同，两者是相互关联同时又各自独立的两门技术学科。信息安全技术具有保密技术不能涵盖的内容，而保密技术更重视国家秘密和涉及国家秘密的信息安全问题，也有着信息安全技术所不能涵盖的更加宽泛的内容。总之，保密技术与信息安全技术既有共同的基础性技术，也有相互不能覆盖的技术领域，保密的目标有赖于二者的基础支撑和保障作用。
12. **保密技术的发展历程**

    通信保密发展时期：主要采用密码技术，与通信结合，提炼出保密性的要求。

    计算机极其网络保密发展时期：除保密性外，提炼出完整性、可用性，成为安全的共识。

    信息保障与全方位保密技术：关注信息保障，更加强调整体性、系统性。
13. **保密技术分类及其体系框架**



第 2 章 国家保密标准

1. **（课）“标准”**是对重复性事务和概念所作的统一规定，它以科学、技术和实践经验的综合成果为基础，经有关方面协商一致，由主管机构批准，以特定形式发布，作为共同遵守的准则和依据。
2. **（课）标准的含义**

   标准的本质属性：“一种统一规定”

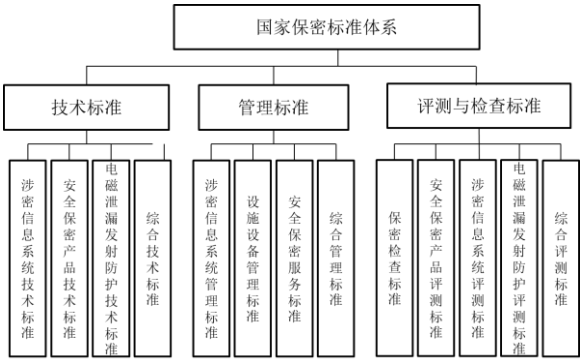
   标准制定的对象：“重复性的事物和概念”

   标准产生的客观基础：“科学、技术和实践经验的综合成果”

制定标准过程："经有关方面协商一致"

标准文件有其一套特定格式和制定颁布的程序

3. **（重）国家保密标准**由国家保密行政管理部门发布，在国家秘密信息的产生、处理、传输、存储和载体销毁的全过程中都应严格执行，是特殊的强制性的国家标准。**秘密性：**国家保密标准反映了我国国家秘密的安全保密防护水平，因此不能公开。
4. **（重）国家保密标准体系**

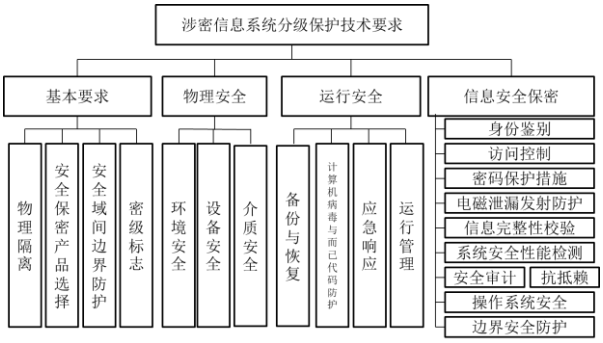


第 3 章 涉密信息系统分级保护

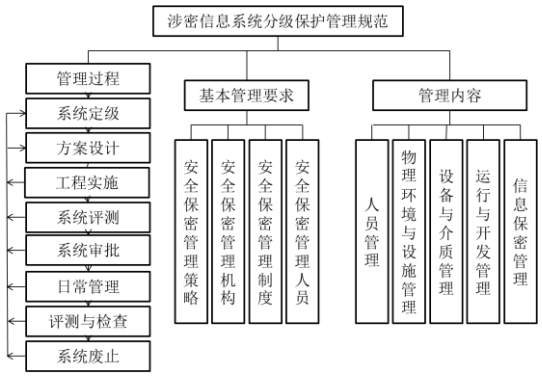
1. **（重）分级保护基本原则：**规范定密，准确定级、依据标准，同步建设、突出重点，确保核心、明确责任，加强监督。
2. **（课）涉密信息系统分级保护制度**

按照涉密信息系统所处理国家秘密信息的不同将系统划分为秘密、机密、绝密三个等级，分别采取不同强度的技术防护措施和管理模式实施保护。

3. **（课）分级保护实施过程**包括系统定级、方案设计、工程实施、系统测评、系统审批、日常管理、评测与检查、系统废止八个环节。
4. **（考）涉密信息系统分级保护技术要求**的主要内容分为基本要求、物理安全、运行安全和信息安全保密四个方面。



5. **（课）涉密信息系统分级保护管理规范**



6. **（课）涉密信息系统测评**包括资料审查、现场考察、制定测评方案、现场检测、检测结果分析、专家评估、出局检测评估结论七个步骤。

第 5 章 信息隐藏技术

1. **（课）信息隐藏技术**是指将一个信息隐藏到另外一个信息中的技术。**加密**是使信息成为不可读的密文章台，掩蔽了消息本身……
2. **（重）信息隐写原理：**掩盖通信已经存在的事实。隐写术通信双方通过交换藏有保密信息的非保密信息来实现秘密通信。
3. **（考）隐写术与数字水印技术有何异同？**

   隐写术与数字水印技术具有共同的技术基础，即都是将隐秘信息或水印嵌入到载体信息中，都利用的人类的感官特性，对冗余信息的不敏感，但前者主要用于秘密通信，后者主要用于版权保护，应用不同。
4. **数字水印的性能评价**透明性、稳健性、容量。
5. **（重）替换系统与位平面方法：**最低比特位替换、图像退化与隐蔽信道、量化。
6. **（重）基于变换域的隐写术：**变换域技术、数字音响中隐藏信息：相位编码、回波隐藏。
7. **（考）LSB 算法隐藏原理**

   LSB 最低有效位，指二进制中最低位数值。LSB 信息隐藏，其核心思想是用秘密信息代替 LSB，即二进制数据的最低位。这是数字密写中常用的方法，并且可以相对容易地应用到图像和音频中。这种方法的优势是相当数量的信息能够被隐藏，同时也几乎不会对载体造成什么可察觉的影响。
8. **（课）隐写术面临的主要攻击**有主动攻击（较小的修改，鲁棒隐写）和恶意攻击（伪造信息或冒充通信一方，安全隐写）。
9. **（课）数字水印面临的主要攻击**有信号去除攻击、同步攻击、解释攻击和合法性攻击。
10. **（课）信息隐藏技术的应用领域**隐蔽通信、版权保护、设备控制和拷贝控制、“指纹”识别与叛逆追踪、内容真实性保护、防伪印刷、广播监视。

第 6 章 身份认证

1. **保密**用来确保信息的保密性，阻止截获、窃听等攻击；**认证**是用于确保信息的真实性、完整性和有效性，阻止冒充、篡改、重放等攻击。
2. **（课）基于口令的鉴别技术**包括**基于静态口令**和**基于动态口令**身份鉴别两种，静态口令的用户口令是由自己设定的，口令是静态的数据，而动态口令，送入计算机系统的验证数据是动态的。
3. **（课）基于生理特征的身份认证**包括手书签字、指纹、语音、视网膜、虹膜、脸型等。
4. **（课）PKI 的组成：**认证中心 CA、证书库、Web 安全通信平台、最终实体。

第 7 章 访问控制

1. **访问控制**的目的是限制主体对客体的访问权限，从而使计算机系统在合法的范围内使用。
2. **访问控制策略**主要分为自主访问控制、强制访问控制和基于角色的访问控制。
3. **（课）自主访问控制**基于对主体或主体所属的主体组的识别，来限制对客体的访问。特点：访问权限具有传递性、资源的拥有者对资源的访问具有决策权
4. **（课）强制访问控制**为所有的主体和客体指定安全级别，不同级别标记了不同重要程度和能力的实体，不同级别的主体对应不同级别的客体的访问。特点：自主访问控制较弱，强制访问控制又太强，使用不便，两者常结合在一起使用。
5. **（课）基于角色的访问控制**用户不是自始至终以同样的注册身份和权限访问系统，而是以一定的角色访问。不同角色被赋予不同的访问权限，系统的访问控制机制只看到角色，而看不到用户。**特点：**提供了三种授权管理的控制途径、系统中所有的角色关系结构可以是层次化的，便于管理、具有较好的提供最小权限的能力，从而提高了安全性、具有

责任分离的能力。

6. **最小权限**是指每个程序或系统用户所具有的完成任务所必需的最小权限集合。

第 8 章 安全监控与审计

1. **安全监控与审计**就是以主机（包括服务器、用户终端、单机、移动笔记本）和网络设备、应用系统和数据库的安全为目标，通过基本网络传输、访问控制和安全审计等技术、对受控主机、网络设备、应用系统、数据库等进行有效的监控，在出现非授权行为、违规操作等异常情况下，主动采取有效的阻断措施，并将违规操作行为记入日志，以便事后审计。
2. **（重）安全监控作用：**通过设置安全策略，对监控对象进行行为监控，对违规/异常行为告警/阻断，便于事后取证。

   （课）按照监控对象分类：主机、网络、数据库、应用系统。
3. **（重）安全监控、审计的保密性要求：**安全监控不应具有屏幕监视功能，不应具有鼠标、键盘监控功能，不应具有对监控对象的设备、服务和进程实时监控功能；安全审计产品不应在审计日志中记录口令、信息具体内容等敏感信息，不应对处理传输的信息内容进行报文回放。
4. **（重）安全监控基本组成及功能：**主机监控系统一般由服务程序、控制台程序和客户端代理程序组成。**服务程序：**用于与客户端代理程序通信，收集和存储审计日志。**控制台程序：**用于管理服务器程序，并可实现监控策略的制定、下发以及审计日志的管理。**客户端代理程序：**用于收集受控主机基本配置信息和运行状态信息，接收并执行控制台程序下发的监控与审计策略，并将有关信息发往管理主机。
5. **（重）违规外联和非授权接入的安全隐患：**1、外部攻击者能绕过内网自身的防护手段，顺利侵入违规外联的内网计算机，窃取内部敏感信息；2、利用该计算机做跳板，入侵整个网络，植入病毒和窃取信息。
6. **（重）违规外联方式：**拨号、外设、网卡。
7. **（重）网络安全审计技术**：高速抓包技术、协议分析技术、会话重组技术、优化数据库结构设计。
8. **（重）数据库审计**：数据库直接访问审计、数据库网络访问审计。
9. **（重）常见的数据库安全审计技术：基于日志的审计技术、基于代理的审计技术、基于网络监听的审计技术、基于网关的审计技术**
10. **（课）安全审计的分类：**服务器，用户终端，应用系统，网络设备，外部设备/介质的使用以及操作系统。

第 9 章 边界防护

1. **（考、重）边界防护**就是对边界进行安全防护，保证网络间和安全区域间必要的信息交流安全可靠，同时防止非法访问者对被保护网络的攻击、入侵和资源窃取等。
2. **（考）逻辑隔离：**拥有相同传输介质系统的两个网络之间，通过硬件设备或软件措施实现的某种隔离。
3. **物理隔离：**两个网络通过各自拥有独立的传输介质系统实现的隔离。
4. **安全隔离：**由安全设备和安全线路组成的系统，用于涉密网络与外网之间、涉密网之间、安全域之间的隔离
5. **（重）无线通信开放性：**由于通信信道的开放性，使得网络物理接口和数据链路通道也处于开放状态……
6. **防火墙：**运行在一台或多台计算机之上的一组特别的服务软件，用于对网络进行防护和通信控制，有时也以专用的硬件形式出现。作用：当值不希望的、未经授权的通信进出被保护的内部网络，是通过边界控制强化内部网络的安全策略。防火墙是一种逻辑隔离

部件。防火墙体系结构：包过滤、双宿网关、屏蔽主机、屏蔽子网等。

7. **入侵检测技术：**用于检测损害或企图损害网络系统的机密性、完整性或可用性等行为的一类安全技术。IDS 分为数据源、分析检测和响应三个模块。按照数据源不同可分为基于主机和基于网络两类。分析检测方法：勿用检测、异常检测、其他检测。入侵响应分为主动响应、被动响应。
8. **安全网关**一般部署在内部网络与外部网络的边界，主要用来抵御来自外部网络的安全威胁。**常见安全网关：**VPN 网关、入侵防御网关、防病毒网关、基于密级标志的保密网关。
9. 将防病毒、入侵检测和防火墙安全设备，划归**统一威胁管理（UTM）**。**定义：**通过安全策略的统一部署，融合多种安全能力，针对网络自身与应用系统进行破坏、利用网络进行非法活动、网络资源滥用等威胁，实现精度防控的高可靠、高性能、易管理的网关安全设备。
10. **（课）物理隔离技术包括：**终端隔离技术、远程传输隔离技术、网络隔离技术。
11. **（课）逻辑隔离技术包括：**防火墙、入侵检测技术、安全网关技术、UTM。
12. **安全隔离与信息交换技术**在隔离网络间建立“逻辑连接”，在保障网络安全的同时进行可控的数据交换，在保证安全保密的前提下，尽可能地实现互联互通。**（考）主要有两个特点：协议终止、数据摆渡**。代表技术是**（重）网闸技术**，是一种由带有多种控制功能专用硬件、在电路上切断网络之间的链路层连接，并能够在网络间进行安全适度的应用数据交换的网络安全设备。**单向网闸：数据泵技术**（基于通讯的基础上，只允许单向的传送数据，反方向只有控制信息可以通过）、**（考）数据二极管技术**（一方只管发送，另一方只管接收，至于数据是否有错误、是否完整都不会去理会，反向没有数据通道，也没有控制通道，完全处于盲状态）。

第 10 章 基础部件安全

1. **信息系统**是由软硬件基础设备和应用软件组成的综合系统。**基础设备包括**计算机设备和网络设备。计算机设备主要由硬件平台(如：服务器、台式 PC 机、笔记本电脑)、操作系统、数据库管理系统软件等基础部件组成。
2. **从终端源头实施安全控制，是信息系统安全保密的关键。**
3. **信息安全保障的主要目的：**保护信息系统和数据不被未经授权访问、使用、泄露、中断、修改或破坏。终端安全是纵深防御体系的重要内容。
4. **终端面临的威胁来源：**缺乏终端网络准入机制；系统漏洞的广泛存在；木马、病毒等恶意软件的攻击手段层出不穷；终端用户缺乏安全意识。**解决方案：**构建全面的终端防护体系；改进 PC 机硬件结构，加强终端安全的硬件基础。
5. **（重）可信传递技术**

   信任链技术是体现终端平台可信的重要手段，是 TCG 中可信计算平台的核心机制。

   （重）信任链的传递分为两个阶段：1、加电开始直到操作系统加载完毕，此时操作系统内核已装入内存，但没有开始运行。2、从操作系统内核开始运行直到终端平台应用环境建立完毕。
6. **（考）可信执行技术提供安全特性：**分区执行保护、可验证性、安全存储、I/O 保护、内存保护。
7. **最小特权：**在完成某种操作时，所赋予系统中每个主体（用户或进程）必不可少的权限。

   （重、考）最小特权原则：应限定系统中每个主体所必须的最小特权，确保可能的事故、错误、网络部件的篡改等原因所造成的损失最小。
8. **（重）TCSEC 将计算机系统安全分为七个级别：**D 级，最低安全性。DOS, windows 3.x, windows95；C1 级，自主访问控制（DAC）；C2 级，较完善的自主访问控制、审计， Unix, windows NT； B1 级，强制访问控制（MAC）； B2 级，良好的结构化涉及、形式化安全

模型；B3 级，全面的访问控制、可信恢复；A1 级，形式化验证。

9. **（重）计算机系统保护能力的五个等级：**第一级：用户自主保护级；第二级：系统审计保护级；第三级： 安全标记保护级；第四级：结构化保护级；第五级：访问验证保护级
10. **数据库安全**

（重）基于属主的自主访问控制，其基本管理方式是对象的宿主具有对象的管理权。

（重）基于数据库的视图提供了对细粒度的基于内容的访问控制的支持。

优点：基于视图的访问控制可以非常灵活地控制对对象（表等）内容的授权访问，只向用户提供需要且有访问权限的字段。这样既方便了用户的使用，又可以保证数据库中表的安全性。

缺点：需要创建的视图较多，系统的管理和维护比较负责。

（重）基于角色的访问控制——角色的约束：RBAC 常见的还有职责分离约束，包括静态的和动态的职责分离。

11. **终端安全策略：**操作系统安全策略、分配用户权限、互联网访问策略、制定外来人员的访问策略。
12. **终端安全措施：**终端安全策略、终端数据保护、终端行为审计、终端准入控制、终端外设接口管理。
13. **（课）**可信硬件技术、可信固件技术、可信传递技术、可信执行技术。
14. **（课）操作系统安全机制：**身份认证、访问控制、安全审计、信道保护机制、最小特权原则、安全配置。
15. **（课）操作系统安全模型：**保密性模型、完整性模型、混合策略模型。

第 11 章 网络攻击技术

1. **（重、考）网络攻击的基本步骤：**漏洞挖掘与利用、信息收集与分析、网络扫描与探测、目标入侵与控制。
2. **（重）漏洞攻击步骤：**漏洞挖掘、漏洞分析、漏洞利用。
3. **（重）网络安全扫描分为三个阶段：**发现目标主机或网络、进一步搜集目标信息、根据搜集到的信息，判断或者进一步测试系统是否存在安全漏洞。
4. **（考）漏洞**是指硬件、软件或策略上的缺陷，导致非法用户未经授权而获得访问系统的权限或提高其访问权限。
5. **（重）后门**是软件作者或硬件开发者在组件的制作过程中留下的，可以绕过相应的安全访问机制来修改并改变相应组件行为的程序。
6. **（考）SQL 注入攻击**是攻击者通过把 SQL 命令插入到 Web 表单递交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的 SQL 命令。
7. **（重）弱口令攻击：**通过调用实现相关协议的口令认证模块，可以循环测试用户/密码组合，以此来破解出口令
8. **（重）恶意代码**是一种可以中断、破坏计算机及网络的程序或代码。
9. **（课）缓冲区溢出原理**

向固定长度的缓冲区中写入超出其预告分配长度的内容，造成缓冲区中数据的溢出，从而覆盖了缓冲区周围的内存空间。可借此构造填充数据，导致原有流程的改变，让程序转而执行特殊的代码，最终获取控制权。

10. **（课）网络攻击：**狭义上来看，网络攻击是指任何试图破坏网络完全的行为和方法；广义上来看，网络攻击技术是多种计算机技术相结合的产物。

第 12 章 通信安全保密技术

1. **（重）无线通信泄密隐患：**电磁信号在空间中自由传播，任何具备接收条件的人都可以

接收。**泄密方式：**接触式（物理接触到无线通信系统，实施信息窃取）和非接触式（通过接收无线通信系统通信信号或设备辐射信号，进而还原窃取通信信息）

2. **（重）手机定位技术**会导致手机持有者暴露自己的位置，甚至引起严重的**泄密问题：**泄露涉密人员行踪、泄露保密要害部门部位位置泄露军事行动和军事目标地点。
3. **（课）无线通信防护技术：**保密手机、手机“木马”的病毒查杀技术、手机干扰技术、手机屏蔽技术、手机探测。
4. **（重）手机探测技术分为专门技术和通用技术。**专用技术：利用手机通信的特征进行探测；通用技术：基于传统的成像技术，如 X 光、红外、T 波等。
5. **（重）专门技术：通信特征检测**（被动、主动）、**非线性结探测**（探测构成手机的基本结构 PN 结）、其他探测方式。

第 13 章 物理安全保密技术

1. **（考）物理安全保密：**保护各种实体（包含信息）及其相应物理环境受各种威胁、攻击及窃密。**物理安全保密技术：**用来实现物理安全保密的各种防范与检查技术。
2. **（重）激光窃听器原理**

   依靠提取房间内的谈话声使门窗玻璃产生的轻微振动，来达到窃听的目的。若房间内有人讲话，振动信息就包含了话音信息，激光接收机接收反射的激光，转换成电信号，调解还原室内的声音信号。
3. **（重）硬盘信息消除**

   消磁技术：对磁性存储介质施加瞬间强磁场，使介质表面的磁性颗粒极性方向发生改变，失去表示数据的意义。

   优点：速度快，擦除效果好

   缺点：硬盘不能再用，成本较高

   热消除技术：根据磁性材料的特性，把磁介质温度升高到 Tc 以上，使磁介质失去铁磁性

   写覆盖技术：需要固定数据写操作和随机序列写覆盖多次
4. **（重）射频识别（RFID）技术**是一种利用射频信号通过空间耦合（交变磁场或电磁场）实现无接触信息传递，并通过所传递的信息达到识别目标的技术。
5. **（重）涉密物品门禁控制技术的系统原理：**系统基于 RFID 技术对涉密物品进行实时监控，可防止设涉密物品在未授权情况下被无意识地带出，提高涉密物品使用人的安全意识。一旦有非授权携带的涉密物品通过检测通道，系统监控端可以快速有效地检测到附着于涉密物品上的电子标签，并发送信息给系统服务器端。服务器端通过比对数据库中的标签授权信息，向监控端发出相应的报警信息。
6. **（重）涉密物品定位技术的系统原理：**系统基于 RFID 技术对涉密物品进行定位监控，可防止涉密物品在未授权情况下被带出监控区域。一旦有涉密物品脱离定位监控区域，系统监控端可以快速有效地检测到附着于涉密物品上的电子标签、并通过数据传输网络，发送给数据处理中心。数据处理中心集中处理并显示涉密物品定位信息，发出警报。
7. **（课）常见涉密物品管控方式：**人工方式、条码技术、射频识别技术。

第 14 章 电磁泄露发射

1. **（重、考）电磁泄露发射：**根据电磁场理论，由于场源的电流变化，产生的电磁能在空间或导体中进行传播，就是电磁发射信号。电磁发射信号中可能携带有秘密信息，被窃收方截取、破解就会造成泄密。
2. **（重）红信号：**能够造成敏感信息泄漏的、携带有数据内容或相关信息的信号。

   （重）黑信号：不含敏感信息的信号。
3. **（课）红黑信号识别方法：**频域（红信号 T 值，增加谱线根数，改变谱线位置）、时域

（时域特征分析，红信号相关检测）、典型信息设备（显示器视频信号、串行口信号）。

4. **（重）安全距离与分级：**安全距离指信息设备至可控边界的距离。我国标准中按距离远近分为 A,B,C 三级，A 级最远（最好）。
5. **（重）HIJACK 主要研究与密码设备有关的电磁泄漏。**密码设备的电磁泄露，往往使构造密码算法的努力前功尽弃，使窃收者不必大费力气去破解高强度的密码吗，就可通过接收电磁泄漏发射信号，轻而易举地得到信息内容或密钥数据。
6. **（重）**按照多极子展开理论，信息设备信息电磁泄漏场可用红信号电流经电偶极子产生的发射场来等效。
7. **电偶极子发射场的主要特性**

   在频率，远区辐射场强随频率增加而线性增强

   在时域，远区辐射场时域波形正比于电流波形的时间导数

   近场区与远场区的空间衰减规律不同：在远场区，电场与磁场皆按 1/r 规律衰减；在近场区，电场按 1/r3 规律衰减，磁场按 1/r2 规律衰减
8. **（重）传导发射分为差模和共模两种。差模发射信号：**在两导线之间传输，属于对称性信号；**共模发射信号：**在导线与地之间传输，属于非对称信号。
9. **（重）减少差模传导发射的方法：**在信号线和电源线上串联差模扼流圈，并联电容或用电容和电感组成低通滤波器，减少发射强度。
10. **（重）减少共模传导发射的方法：**在信号线和电源线上串联共模扼流圈，在地与导线之间并联电容器、组成 LC 滤波器进行滤波。
11. **（重、课）电磁泄露发射防护技术方法：**低泄射技术、屏蔽技术、干扰技术、**红黑隔离防护措施**(红设备的隔离,红信号线、红电源线的隔离,红信号与无线发射装置的隔离)。
12. **（课）电磁泄露发射检测方法：**实验室检测、现场检测。**检测设备：**TEMPEST 测试接收机、天线、PLISN。

第 15 章 保密检查技术

1. **（重）涉密计算机网络检查方法：**

   物理隔离：涉密网络终端（含服务器）与互联网等公共信息网络物理隔离检查、涉密网络设备与互联网等公共信息网络物理隔离检查、涉密网络与互联网等公共信息网络物理隔离检查、涉密办公自动化设备与互联网等公共信息网络物理隔离检查

   安全域与边界防护、身份认证、访问控制、安全审计、违规外联监控、入侵检测监控、病毒防护措施、操作系统安全、数据库安全、可移动设备管控、现场技术检查。
2. **（重、考）移动存储介质检查方法：**移动存储介质是否交叉使用、涉密介质是否有密级标志和记录、审批、非涉密移动存储介质是否存储涉密信息。
3. **（重）互联网涉密信息保密检查技术**，就是对互联网及其他公共信息网络是否存在违反国家保密法律法规行为的检查。**（重）检查方法：**一是选取搜索引擎（选择信息量大、网页更新速度快，同时使用多种公共搜索引擎，使用其他搜索功能）；二是输入关键词检索（根据公文特征，涉密文件标题，涉密事项为关键词，从检查结果重提炼关键词）。
4. **场所和信息设备的保密检查技术检查方法**

   （重）涉密信息设备电磁泄漏发射检查：涉密信息设备是指用于处理涉密信息的计算机、打印机、复印机、电话机、传真机、网络设备和扩音设备等设备。在保密检查中，用频谱分析仪对的电磁波频谱进行分析。

   有线通信设备检查：电话机电磁泄漏/电话线串音/电话搭线和并极检查/电话机伪挂机检查

   涉密场所检查：异常无线信号检查、周边保密环境检查、隐藏电子设备检查、隐藏摄像设备检查、电源检查

5. **（重）保密检查取证原则：**及时性、真实性、科学性。
6. **（考）保密技术检查：**保密行政管理部门依据国家有关保密法规标准，运用技术手段，对有关机关、单位的保密技术防范情况进行检查的活动。