**第三章习题答案**

**1.物理安全的定义？**

**要点：**（1）物理安全是系统安全的基础；（2）阻止系统遭受人为或自然的危害；（3）是针对计算机设备、设施、环境人员、系统等采取的物理防护措施。

**参考答案：**

物理安全又称实体安全，它是信息系统安全的基础。GB/T 21052-2007《信息安全技术 信息系统物理安全技术要求》中，定义的信息物理安全是：为了保证信息系统安全可靠运行，确保信息系统在对信息进行采集、处理、传输、存储过程中，不致受到人为或自然因素的危害，而使信息丢失、泄露或破坏，对计算机设备、设施（包括机房建筑、供电、空调等）、环境人员、系统等采取适当的安全措施。

**2.物理安全涉及哪些方面的内容？简单阐述。**

**要点：**（1）涉及设备安全、环境安全和系统物理安全；（2）给出三个方面的完整定义；（3）从保证整个信息系统安全的角度出发，说明这三个方面的安全需要考量的技术要求。

**参考答案：**

(1)**设备安全**

设备安全是指为保证信息系统的安全可靠运行，降低或阻止人为或自然因素对硬件设备安全可靠运行带来的安全风险，对硬件设备及部件所采取的适当安全措施。其涉及的技术要求包括：抗电磁干扰，抗电磁泄漏，电源保护，操作部件过热，以及设备的振动适应性、温度和湿度适应性、冲击适应性、碰撞适应性和可靠性。

(2)**环境安全**

环境安全是指为保证信息系统的安全可靠运行所提供的安全运行环境，使信息系统得到物理上的严密保护，从而降低或避免各种安全风险。其涉及的技术要求包括：场地的选择，机房屏蔽，防火，防辐射，稳定的供电系统，防静电，防雷，防虫鼠，防盗防毁，温湿度控制，综合布线和通信线路安全。

(3)**系统物理安全**

系统物理安全是指为保证信息系统的安全可靠运行，降低或阻止人为或自然因素从物理层面对信息系统保密性、完整性、可用性带来的安全威胁，从系统的角度采取的适当安全措施。其涉及的技术要求包括：灾难备份与恢复，设备的资源、性能、状态和故障的管理，设备鉴别和访问控制，以及边界防护等。

**3.设备的安全威胁包含哪些方面？如何保护？**

**要点：**（1）安全威胁包括被盗与被毁，电磁干扰，电磁泄漏，声光泄漏；（2）防设备被盗与被毁。提供至少3种以上的保护方法；（3）抗电磁干扰。对屏蔽、滤波、接地等抗电磁干扰手段进行简要介绍；（4）防电磁泄漏。讨论TEMPST技术手段；（5）对于声泄漏，使用物理隔声材料和结构。对于光泄漏，提供至少2中防护手段。

**参考答案：**

包含设备的被盗与被毁，电磁干扰，电磁泄漏，声光泄漏。

1. 防设备被盗与被毁

设备防盗与防毁是利用设备防盗与防毁措施保护系统设备及其部件不被盗取或毁坏。早期的防盗主要通过锁的方式进行防盗，如机箱锁扣、Kensington 锁孔等，只有打开锁才能搬运设备。这些防护措施的强度有限、安全系数低，锁扣很容易被破坏。而有些锁，如机箱电磁锁，它安装在机箱内，嵌入在 BIOS 中的子系统通过密码实现电磁锁的开关管理，这种锁美观，操作人性化，但只能防止机箱被打开，并不具有防盗功能。当前的防盗技术更趋于智能化，如设备移动报警器，将光纤电缆连接到机房的每台设备上，光束通过光纤传输，一旦连接的设备被盗，光束的传输通道就会被切断，报警器接收不到光信号，则立即报警。这种报警装置成本低，便于实施，主要用于机房的重要设备上。

在机箱防入侵方面，有一种 BIOS 机箱防拆卸方法，但必须与机箱侧板上的微动开关联动。在 BIOS 中有一项功能设置——Chassis Intrusion（机箱入侵） ，如果设置为Enabled，则该机箱具有防拆卸功能。一旦机箱被非法打开，系统就会报警，而且主机也不能开机，只有合上侧面板后，报警才能取消，主机才能开机。除此之外，在机房安装门禁系统、视频监控系统和红外探测系统也是非常必要的，它们能够更为可靠地保护设备，防止设备被盗或被非法拆卸。

2. 抗电磁干扰

防止计算机受到电磁干扰的主要措施有：屏蔽、滤波和接地。

（1）屏蔽。电磁屏蔽是利用金属切断电磁波的传播途径，从而消除电场波、磁场波、平面波由一个区域向另一个区域辐射和感应。当电磁波到达屏蔽体表面时，由于空气与金属的交界面上阻抗不同，从而对入射波产生反射。而未被反射掉的能量进入屏蔽体，在向前传输的过程中，被屏蔽材料吸收绝大部分能量。未被屏蔽体吸收的残余能量传导到另一表面，遇到阻抗不同的交界面时，会再次形成反射，重新返回屏蔽体。经过多次反射和吸收后，电磁波几乎全部被屏蔽体吸收。屏蔽体距离辐射源较近时，电磁波的波阻抗取决于辐射源的物理特性，因此，针对电场波、磁场波和平面波，其屏蔽体的材料是不同的。对于高阻抗的电场波，屏蔽体可以采用逆磁材料（如：铜、铝）制成，并和地连接，这样电场波将终止在屏蔽体表面，电荷被引导入地。对于低阻抗的磁场波，屏蔽体可以采用磁导率很高的强磁材料（如：钢）制成，可以把磁力线限制于屏蔽体内，频率越低的磁场越难屏蔽，有时甚至采用高导电性和高导磁性复合材料。对于阻抗为常数的平面波，则需要根据频率的大小选择不同材质的材料。但是，如果屏蔽体上出现洞穴或缝隙，将会直接降低屏蔽效果，频率愈高，这种现象愈显著。

（2）滤波。因为设备或系统上的电缆是最有效的电磁接收与发射天线，因此往往单纯采用屏蔽不能提供完整的电磁干扰防护。许多设备单独做电磁兼容实验时都没有问题，但当两台设备连接起来后，就不能满足电磁兼容的要求，这就是电缆起了天线的作用。此时采取的措施就是加滤波器，切断电磁干扰沿信号线或电源线传播的路径，与屏蔽共同构成完善的电磁干扰防护。无论是抑制干扰源、消除耦合或提高接收电路的抗干扰能力，都可以采用滤波技术。滤波的作用主要是使电子设备的内部产生的噪声不向外泄漏，同时防止电子设备外部产生的噪声进入设备。一般情况下，有害的电磁干扰频率远高于正常信号频率，电磁干扰滤波器是通过选择性地阻拦或分流有害的高频来发挥作用的，如采用 LC 电路。这样可以显著降低或衰减所有要进入或离开受保护电子器件的有害噪声信号。

（3）接地。良好的接地不仅对抑制电磁干扰有显著效果，而且可以保护设备和人身安全。常见的接地有三种：保护接地、系统接地和屏蔽接地。保护接地是将设备的金属壳与大地直接连接，防止外壳带电威胁操作人员的人身安全，如防雷地；系统接地是为系统各部分提供稳定的基准电位，要求接地回路的公共阻抗尽可能小，如交流地和直流地；屏蔽接地是将屏蔽体接地，抑制电磁阻抗。在接地设计时，交流地、直流地、防雷地和屏蔽地的接地线必须分开，不能连接在一起，而且复杂电路要采用多点接地和公共地。

3. 防电磁泄漏

与抗电磁干扰不同，防电磁泄漏是抑制信息系统和电子设备在信息处理时，向外辐射电磁信号，或采取有关技术措施使对手不能接收到辐射信号，或从辐射信号中难以提取有用的信息。国际上把电磁辐射泄漏监测与防护技术简称为 TEMPEST（Test forElectromagnetic Propagation Emission and Secure Transmission），它是 20 世纪 60 年代末 70 年代初由美国国家安全局和国防部联合研究和开发的技术。它的研究包括理论、工程和管理等方面，涉及电子、电磁、计算机、信息测量、材料和化学等多个学科领域。抑制电磁泄漏的途径有两条：一是电子隐藏，即用干扰、跳频等技术来掩盖全部计算机的工作状态和保护信息；二是物理抑制，即通过屏蔽，或优化设备与线路设计，抑制一切有用信息的电磁外泄。

（1）使用低辐射设备。低辐射设备即为 TEMPEST 设备，是防辐射泄露的根本措施。这些设备在设计和生产时，从线路和元器件入手，采取了防辐射措施，消除产生较强电磁波的根源，将设备的电磁泄漏抑制到最低限度。如：尽可能选用电压和功率较低的元器件；在电路布线设计时，降低耦合和辐射；在电源设计部分和信号设计部分，分别使用电源滤波器和信号滤波器；使用阻挡电磁波的透明膜；将“红”信号和“黑”信号隔离。此外，显示器是信息系统安全的一个薄弱环节，拦截显示器工作时的辐射信号已经是一项成熟的技术，因此选用低辐射显示器十分重要，如：单色显示器辐射低于彩色显示器，等离子显示器和液晶显示器也能进一步降低辐射。

（2）屏蔽。与抗电磁干扰类似，屏蔽是 TEMPEST 技术中的一项基本措施。根据用途不同，屏蔽分为：整体屏蔽、部件屏蔽和元器件屏蔽。例如，整体屏蔽最典型的案例就是屏蔽室，它是用于处理高度保密信息的场所，通过金属网将需要保护的房间包裹起来，为了达到良好的屏蔽效果，金属网必须良好接地。部件屏蔽的一个例子是使用防电磁泄漏玻璃，但必须良好接地。将该玻璃安装在电子设备显示窗上，如：早期使用的 CRT 显示器，防电磁泄漏玻璃可以将 89% 的电磁辐射通过地线导入地下，再将 10% 的电磁辐射反射掉，剩下的电磁辐射不足 1%，即使被截获也不能还原出完整的信息。

（3）滤波。正如抗电磁干扰技术描述的一样，滤波技术是屏蔽技术的一种补充。设备和元器件并不能完全密封在屏蔽体内，仍有电源线、信号线和公共地线需要与外界连接，因此，电磁波还是可以通过传导或辐射从屏蔽体内传到外部。在电源线、信号线和公共地线上加装滤波器，只允许某些频率的信号通过，而阻止其他频率范围的信号，从而起到防止信息泄露的目的。

（4）电磁干扰器。电磁干扰器是一种能够发射电磁噪声的仪器，通过辐射电磁噪声降低泄露信息的信噪比，从而达到电磁干扰的目的，使窃收方很难从泄露的信号中提取有价值的信息。利用干扰器的方法有两种：一是将一台能产生噪声的干扰器放在计算机设备旁边，干扰器产生的噪声与计算机设备产生的电磁信号一起向外辐射，要么掩盖有效电磁波的发送，要么将干扰叠加到有效电磁信号上，窃收方接收信号后，很难还原；二是将处理重要信息的计算机放在中间，四周放一些处理一般信息的设备，如打印机、传真机等，让这些设备产生的电磁信号一起向外辐射，从而起到混淆的作用，即使窃收者能够获取这些信号，也无法解调。对于第一种方法，需要注意一个问题：当干扰器发出的电磁辐射强于有效信号时，会造成保护对象的电磁污染，而且这种方式很容易通过滤波或抑制解调的方式获取有效信号，因此要求干扰器不能干扰设备的正常工作，即干扰器产生的电磁辐射不应超过 EMI（电磁干扰）标准。

4. 防声光泄漏

为防止光泄密事件，建议将设备摆放在远离窗户的地方，如果实在无法避免远离窗户，建议拉上窗帘。遮蔽室内灯光或用其他光源（例如蜡烛）制造散射效果。在光缆线路的维护过程中，光时域反射检测（OTDR）技术虽然广泛应用，但窃取光纤中传输的信息所引起的光纤损耗非常小，OTDR 很难将其分辨出来。为了防止光缆窃听，可以采用偏振光时域反射技术（POTDR）和迈克尔逊干涉技术。前者是测量光脉冲在光纤传输中偏振态的演变过程，一旦外界扰动，偏振态演变的速度就会发生变化。后者已在安全监测方面获得了实际应用，它利用相干光脉冲的相位对周围环境非常敏感的原理，一旦光纤中的光信号受到外界扰动，通过干涉技术输出后就可以检测出光纤受扰动的位置和程度。该方法分辨率高、测量精确。为了防止声音泄漏信息，可以采用隔声、吸声材料，其隔声性能取决于它的质量、坚硬度、阻尼性质等，如果是多层结构，还要考虑多层板的数量，每层的自身性质，与周围环境的连接情况等。常用的隔声材料和结构主要分为单层复合结构、特殊刚性板、软质隔声结构、双层板结构、各类轻型结构和高隔声量结构等，而吸声材料和结构多采用多孔吸声材料和共振吸声结构。

**4.电子信息设备所在机房的安全等级如何划分？**

**要点：**（1）应划分为A、B、C三级；（2）划分时应当根据信息系统在国民经济与社会中的重要性进行讨论；（3）对于每个等级，根据划分标准给出实例。（4）对于不同安全等级的明确配置要求。

**参考答案：**

《174 规范》根据机房的使用性质、管理要求及其在经济和社会中的重要性，将其划分为 A、B 和 C 三级。符合下列情况之一的数据中心应为 A 级：

（1）电子信息系统运行中断将造成重大的经济损失；

（2）电子信息系统运行中断将造成公共场所秩序严重混乱。

A 级是最高级别，主要是指涉及国家安全和国计民生的机房设计。其电子信息系统运行中断将造成重大的经济损失或公共场所秩序严重混乱，甚至国家安全受到威胁。如：国家气象台、国家级信息中心和计算中心、重要的军事指挥部门、大中城市的机场、广播电台、电视台、应急指挥中心、银行总行等属 A 级机房。符合下列情况之一的数据中心应为 B 级：

（1）电子信息系统运行中断将造成较大的经济损失；

（2）电子信息系统运行中断将造成公共场所秩序混乱。

如：科研院所、高等院校、三级医院、大中城市的气象台的信息中心、疾病预防与控制中心、电力调度中心、交通（铁路、公路、水运）指挥调度中心、国际会议中心、国际体育比赛场馆、省部级以上政府办公楼等属 B 级机房。不属于 A 级或 B 级的数据中心为C级。在异地建立的备份机房，设计时应与原有机房等级相同。同一个机房内的不同部分可以根据实际需求，按照不同的标准进行设计。

A 级又称为容错型，电子信息系统机房内的场地设施应按容错系统配置，在电子信息系统运行期间，场地设施不应因操作失误、设备故障、外电源中断、维护和检修而导致电子信息系统运行中断。

B 级又称为冗余型，电子信息系统机房内的场地设施应按冗余要求配置，在系统运行期间，场地设施在冗余能力范围内，不应因设备故障而导致电子信息系统运行中断。

C 级又称为基本型，电子信息系统机房内的场地设施应按基本需求配置，在场地设施正常运行情况下，应保证电子信息系统运行不中断。

**5.机房位置和设备部署的具体要求是什么？**

**要点：**（1）机房位置应当考量到电力供应、周边环境的特点、是否远离灾害隐患区域、避免物理安全威胁。（2）设备的部署需要考虑设备、人员、物料的安全，对于内部结构有具体的规范。

**参考答案：**

在机房位置的选择上，应该保证：电力供给稳定可靠，交通便捷，通信快速畅通，自然环境清洁；远离粉尘、油烟、有害气体及生产或储存具有腐蚀性、易燃、易爆物品的场所；远离水灾、地震等自然灾害隐患区域；远离强振源和强噪声源；避开强电磁场干扰。对于多层或高层建筑物内的电子信息系统机房，在确定主机房的位置时，应对设备运输、管线敷设、雷电感应和结构荷载等问题进行综合考虑和经济比较；采用机房专用空调的主机房，应具备安装室外机的建筑条件。

设备的布置应满足机房管理、人员操作和安全、设备和物料运输、设备散热、安装和维护的要求。产生尘埃及废物的设备需要远离对尘埃敏感的设备，并布置在有隔断的单独区域内。当机柜或机架上的设备为前进风/后出风方式冷却时，机柜和机架的布置应采用面对面和背对背的方式。用于搬运设备的通道净宽不应小于 1.5m；面对面布置的机柜或机架正面之间的距离不应小于 1.2m；背对背布置的机柜或机架背面之间的距离不应小于 1m；当需要在机柜侧面维修测试时，机柜与机柜、机柜与墙之间的距离不应小于 1.2m；成行排列的机柜，其长度超过 6m 时，两端应设有出口通道；当两个出口通道之间的距离超过 15m 时，在两个出口通道之间还应增加出口通道；出口通道的宽度不应小于 1m，局部可为 0.8m。

**6.TEMPEST 技术的发展历史？阐述美国和中国的 TEMPEST 技术的发展现状。**

**要点：**（1）TEMPEST技术所涉及的内容；（2）TEMPEST技术的起源及其发展；（2）介绍美国的TEMPST标准发展历程，目前所达到的程度。（3）我国TEMPST标准体系的完善。

**参考答案：**

早在 20 世纪 50 年代，美国就开始研究 TEMPEST 技术，TEMPEST 最早的含义是瞬时电磁脉冲发射标准（Transient Electromagnetic Pulse Emanation Standard），现在已经演变成了电磁泄漏发射和声光泄漏发射的总称。在 20 世纪 50 年代，美国发布了第一个 TEMPEST 标准——NAG-1A“通信和信息设备的发射标准”，后在 20 世纪 60年代被 FS222 标准替代。20 世纪80年代之后，又陆续发布了国家的 TEMPEST 标准NACSIM 5100A“关于TEMPEST设备的要求”，NACSIM 5101“泄漏发射实验室测试标准技术原理”，NACSIM 5102“泄漏发射测试标准管理指南”，NACSIM 5103“关于红黑工程”和 NACSIM 5104“关于屏蔽室要求”。随后，NACSIM 5100A 标准被NACSIM TEMPEST 1 - 92标准替代，NACSIM5101和NACSIM 5102 标准被NACSIM TEMPEST 2-93标准替代，NACSIM5103标准被NACSIM TEMPEST2-95标准替代，NACSIM 5104标准被 NACSIM TEMPEST 1-95标准替代。2000年后，美国对 TEMPEST的相关标准做过一次修订。同时，美国军方也发布了相关的技术标准，如：美国陆军的 AR（C）530-4“泄密发射控制”、FM32-6“信号保密技术”等，美国空军的 AFR100-45“控制泄密发射”、AFNAG-9A“空军贯彻NACSIM 5100 系列标准 ”等 ，以 及 美 国 国 防 部 颁 发 的 DoD5200.28“ 国防部可信计算机系统评价准则 ”、CSC-STD003-85“国防部计算机安全保密要求”和 NCSC-TG-005“可信计算机网络说明”等。此外，一些西方发达国家和组织也制定了 TEMPEST 的类似标准，如：加拿大 的 CID / 09 / 12A 和 CID / 09 / 7A 标准 ，澳大利亚的ACSI71标准 ，以及北约AMSG720B、AMSG784 和 AMSG788 标准。与民用和军用电磁兼容标准相比，TEMPEST 技术标准对电子信息设备的电磁发射要求更为严格和苛刻。例如：满足 TEMPEST 标准 NACSIM 5100 的设备，其电磁辐射水平比满足电磁兼容标准 MIL-STD-461/462D“子系统和设备电磁干扰特性的控制要求”的同类设备低 40~60dB，即相当于 100~1000 倍的衰减量。假设一台满足电磁兼容标准的设备其危险半径（可窃取的电磁泄漏区域）为 1500m，那么，一旦该台设备满足TEMPEST 标准后，其危险半径将降为 1.5~15m，从而大大降低了电磁波泄漏其有用信息的可能。

在我国，国家 863 计划、国家计委重大专项都曾将电磁泄漏发射防护技术列入了信息安全主题，投入了大量的研发资金。从 1991 年起，由国家保密局牵头，联合国内有关部门和科研院所，先后制定和颁布了具有 TEMPEST 性质的系列国家保密标准，初步建立了我国 TEMPEST 产业科学管理体系，并在 2001 年，国家保密局建立了电磁泄漏发射防护产品检测中心，负责相关产品的评测。相关的 TEMPEST 技术标准有：BMB1-1994“电话机电磁泄漏发射限值和测试方法”、BMB2-1998“使用现场的信息设备电磁泄漏发射检测方法和安全判据”、BMB3-1999“处理涉密信息的电磁屏蔽室的技术要求和测试方法”、GGBB1-1999“信息设备电磁泄漏发射限值”、GGBB2-1999“信息设备电磁泄漏发射测试方法”、BMB4-2000“电磁干扰器技术要求和测试方法”、BMB5-2000“涉密信息设备使用现场的电磁泄漏发射防护要求”、BMB6-2001“密码设备电磁泄漏发射限值”、BMB7-2001“密码设备电磁泄漏发射测试方法（总则）”、BMB8-2004“国家保密局电磁泄漏发射防护产品检测实验室认可要求”和 BMB17-2006“涉及国家秘密的信息系统分级保护技术要求”等二十多项标准，初步形成了满足我国实际需要的 TEMPEST标准体系。目前，这些标准还在不断地修改、完善和加强。

**7.TEMPEST 技术的主要研究内容有哪些？**

**要点：**（1）设备的电磁泄漏机理；（2）研究电磁泄漏的防护技术；（3）有用电磁信息的提取技术；（4）电磁泄漏测试技术和标准；（5）TEMPEST 材料、元器件和设备的研制。

**参考答案：**

TEMPEST 技术作为美国国家安全局和国防部联合研究与开发的一个非常重要的项目，其研究内容主要有：研究信息处理设备的电磁泄漏机理，分析有用信息是通过何种途径，以何种方式加载到辐射信号上的，以及电子信息处理设备的电气特性和物理结构对电磁泄漏的影响；研究电磁泄漏的防护技术，分析电磁泄漏中，元器件、电路设计和印刷电路板的布局、设备结构、连线和接地所起的作用，研究各种屏蔽材料、屏蔽结构对电磁的屏蔽效果；研究有用电磁信息的提取技术，即电磁信号接收技术和电磁信号还原技术；研究电磁泄漏测试技术和标准，涉及测试的内容、测试方法、测试要求和测试条件设计和制定，测试仪器设备研制和测试结果分析；TEMPEST 材料、元器件和设备的研制。

**8.信息系统物理安全如何划分等级？每个等级的相关内容有哪些？**

**要点：**（1）根据适度保护划分为五个级别，对不同级别提出相应的物理安全技术要求；（2）在每个级别内分为设备物理安全、环境物理安全和系统物理安全；（3）阐述每个级别的物理安全要求，并将所有相邻的两个等级进行技术要求的对比。

**参考答案：**

以 GB/T 17859-1999 对计算机信息系统五个安全等级的划分为基础，依据 GB/T 20271-2006 五个安全等级中对于物理安全技术的不同要求，结合当前我国计算机、网络和信息安全技术发展的具体情况，根据适度保护的原则，将物理安全技术分为五个不同级别，并对信息系统安全提出了物理安全技术方面的要求。每一级别中又分为设备物理安全、环境物理安全和系统物理安全。不同安全等级的物理安全平台为相对应安全等级的信息系统提供应有的物理安全保护能力。不同安全等级的物理安全平台为相对应安全等级的信息系统提供应有的物理安全保护能力。随着物理安全等级的依次提高，信息系统物理安全的可信度也随之增加，信息系统所面对的物理安全风险也逐渐减少。第一级物理安全平台为第一级用户自主保护级提供基本的物理安全保护。在设备物理安全方面，为保证设备的基本运行，对设备提出了抗电强度、泄漏电流、绝缘电阻等要求，并要求对来自静电放电、电磁辐射、电快速瞬变脉冲群等的初级强度电磁干扰有基本的抗扰能力。在环境物理安全方面，为保证信息系统支撑环境的基本运行，提出了对场地选择、防火、防雷电的基本要求。在系统物理安全方面，为保证系统整体的基本运行，对灾难备份与恢复、设备管理提出了基本要求，系统应利用备份介质以降低灾难带来的安全威胁，对设备信息、软件信息等资源信息进行管理。

第二级物理安全平台为第二级系统审计保护级提供适当的物理安全保护。在设备物理安全方面，为支持设备的正常运行，本级在第一级物理安全技术要求的基础上，增加了设备对电源适应能力要求，增加了对来自电磁辐射、浪涌（冲击）的电磁干扰具有基本的抗扰能力要求，以及对设备及部件产生的电磁辐射干扰具有基本的限制能力要求。在环境物理安全方面，为保证信息系统支撑环境的正常运行，本级在第一级物理安全技术要求的基础上，增加了机房建设、记录介质、人员要求、机房综合布线、通信线路的适当要求，机房应具备一定的防火、防雷、防水、防盗防毁、防静电、电磁防护、温湿度控制、一定的应急供配电能力。在系统物理安全方面，为保证系统整体的正常运行，本级在第一级物理安全技术要求的基础上，增加了设备备份、网络性能监测、设备运行状态监测、告警监测的要求，系统对易受到损坏的计算机和网络设备应有一定的备份，对网络环境进行监测以具备网络、设备告警的能力。

第三级物理安全平台为第三级安全标记保护级提供较高程度的物理安全保护。在设备物理安全方面，为支持设备的稳定运行，本级在第二级物理安全技术要求的基础上，增加了对来自感应传导、电压变化产生的电磁干扰具有一定的抗扰能力要求，以及对设备及部件产生的电磁传导干扰具有一定的限制能力要求，并增加了设备防过热能力，温湿度、振动、冲击、碰撞适应性能力的要求。在环境物理安全方面，为保证信息系统支撑环境的稳定运行，本级在第二级物理安全技术要求的基础上，增加了出入口电子门禁、机房屏蔽、监控报警的要求，机房应具备较高的防火、防雷、防水、防盗防毁、防静电、电磁防护、温湿度控制、较强的应急供配电能力，提出了对安全防范中心的要求。在系统物理安全方面，为保证系统整体的稳定运行，本级在第二级物理安全技术要求的基础上，对灾难备份与恢复增加了灾难备份中心、网络设备备份的要求，对设备管理增加了网络拓扑、设备部件状态、故障定位、设备监控中心的要求，并对设备物理访问、网络边界保护、设备保护、资源利用提出了基本要求。

第四级物理安全平台为第四级结构化保护级提供更高程度的物理安全保护。在设备物理安全方面，为支持设备的可靠运行，本级在第三级物理安全技术要求的基础上，增加了对来自工频磁场、脉冲磁场的电磁干扰具有一定的抗扰能力要求，并要求应对各种电磁干扰具有较强的抗扰能力，增加了设备对防爆裂的能力要求。在环境物理安全方面，为保证信息系统支撑环境的可靠运行，本级在第三级物理安全技术要求的基础上，要求机房应具备更高的防火、防雷、防水、防盗防毁、防静电、电磁防护能力，温湿度控制能力，更强的应急供配电能力，并建立完善的安全防范管理系统。在系统物理安全方面，为保证系统整体的可靠运行，本级在第三级物理安全技术要求的基础上，对灾难备份与恢复增加了异地灾难备份中心、网络路径备份的要求，对设备管理增加了性能分析、故障自动恢复以及建立多层次分级设备监控中心的要求，并对设备物理访问、网络边界保护、设备保护、资源利用提出了较高要求。

第五级物理安全平台为第五级访问验证保护级提供最高程度的物理安全保护。但标准 GB/T 21052-2007 没有对该级信息系统物理安全技术进行描述。