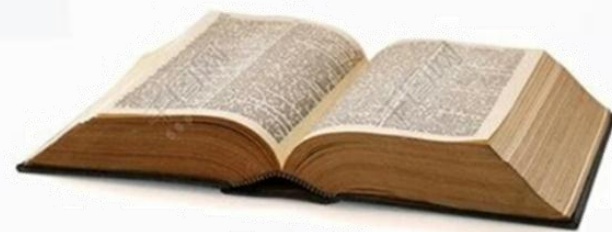


信息安全法律基础

用技术、法律、标准共建网络安全生态

——做网络安全的守护者





第3章 计算机信息系统安全法律法规

第3章 计算机信息系统安全法律法规

3.1

中华人民共和国计算机信息系
统安全保护条例

3.2

计算机病毒防治管理办法

3.3

信息安全等级保护管理办法

3.4

计算机信息系统安全专用产品检
测和销售许可证管理办法



知识点探究

- 学习“中华人民共和国计算机信息系统安全保护条例”、“计算机病毒防治管理办法”、“信息安全等级保护管理办法”等相关的计算机信息系统安全法律法规，从技术和法律角度分析相关的案件事实。
- 本章涉及的法律法规的主要立法规制方法有哪些？
- 本章涉及的法律法规哪些还需要进一步改进和完善？
- 如何加大我国信息安全法律法规的普法和执法力度？

和小伙伴们一起
为网安規制支支招



3.1 中华人民共和国计算机信息系统安全保护条例

3.1 中华人民共和国计算机信息系统安全保护条例

3.1.1 宗旨和法律地位

《中华人民共和国计算机信息系统安全保护条例》（以下简称《条例》）于1994年2月18日由中华人民共和国国务院第147号令发布，共五章三十一条。

1. 《条例》的宗旨

《条例》的宗旨是保护计算机信息系统的安全，促进计算机的应用和发展，保障社会主义现代化建设的顺利进行。（第一条）



3.1 中华人民共和国计算机信息系统安全保护条例

3.1.1 宗旨和法律地位（续）

2. 《条例》的法律地位

- 《中华人民共和国计算机信息系统安全保护条例》是我国在信息系统安全保护方面**最早**制定的一部法规，也是我国信息系统安全保护**最基本**的一部法规，它确立了我国信息系统安全保护的**基本原则**，为以后相关法规的制定奠定了基础。
- 在《条例》颁布之后，我国陆续颁布了《计算机信息网络国际联网安全保护管理办法》、《计算机病毒防治管理办法》《互联网信息服务管理办法》、《信息安全等级保护管理办法》等一系列信息安全法规，**形成了一个保护信息安全的较完善的法规体系。**



3.1 中华人民共和国计算机信息系统安全保护条例

3.1.2 适用范围

- (1) 任何组织或个人，不得利用计算机信息系统从事危害国家利益、集体利益和公民合法权益的活动，不得危害计算机信息系统的安全。《条例》适用于任何组织和个人。（第七条）
- (2) 中华人民共和国境内的计算机信息系统的安全保护适用本条例。（第五条）
- (3) 未联网的微型计算机的安全保护办法，另行制定不适用本条例。（第五条）
- (4) 军队的计算机信息系统安全保护工作，按照军队的有关法规执行。（第二十九条）



3.1 中华人民共和国计算机信息系统安全保护条例

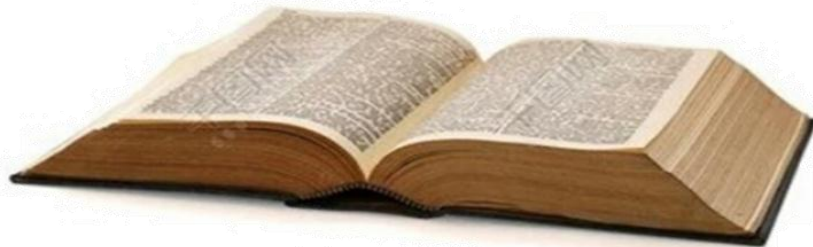
3.1.3 主要内容

1.科学界定了“计算机信息系统”的概念

本条例所称的计算机信息系统，是指由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。（第二条）—实体规制法

2.明确了安全保护工作的性质

计算机信息系统的安全保护，应当保障计算机及其相关的和配套的设备、设施（含网络）的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。（第三条）



3.1 中华人民共和国计算机信息系统安全保护条例

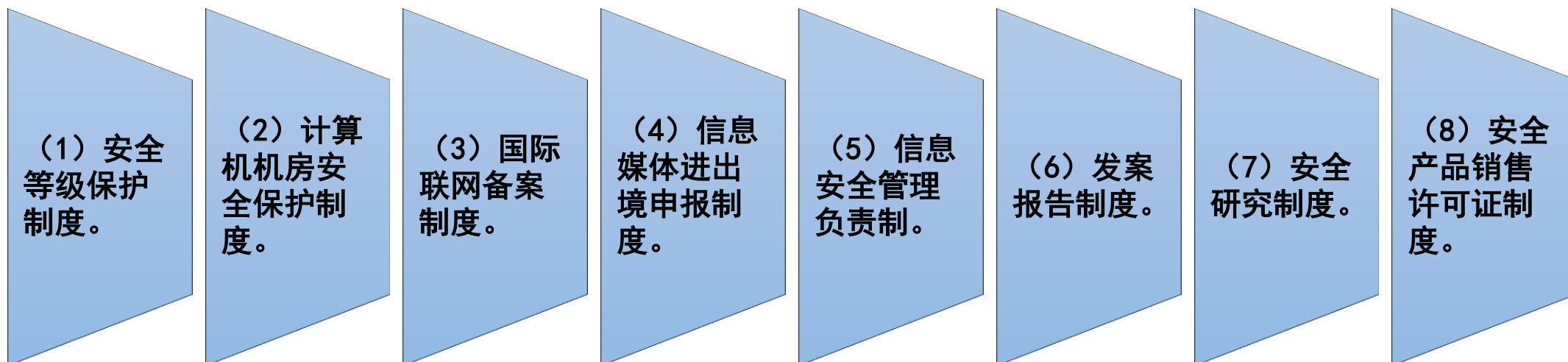
3.1.3 主要内容（续）

3.明确了计算机信息系统安全保护工作的重点

计算机信息系统的安全保护工作，重点维护国家事务经济建设、国防建设、尖端科学技术等重要领域的计算机信息系统的安全。（第四条）

4.系统设置了安全保护的制度

《条例》主要设置了以下八个方面的安全保护制度。



3.1 中华人民共和国计算机信息系统安全保护条例

3.1.3 主要内容（续）

5.明确确定了安全监督的职权和义务

（1）**公安部**主管全国计算机信息系统安全保护工作。**国家安全部、国家保密局和国务院**其他有关部门，在国务院规定的职责范围内做好计算机信息系统安全保护的有关工作。（第六条）

（2）公安机关对计算机信息系统保护工作行使下列监督职权：（第十七条）

- ①监督、检查、指导计算机信息系统安全保护工作；
- ②查处危害计算机信息系统安全的违法犯罪案件；
- ③履行计算机信息系统安全保护工作的其他监督职责。

（3）公安机关发现影响计算机信息系统安全的隐患时，应当及时通知使用单位采取安全保护措施。（第十八条）



3.1 中华人民共和国计算机信息系统安全保护条例

3.1.3 主要内容（续）

6.全面规定了违法者的法律责任

7.定义了计算机病毒及专用安全产品（第二十八条）

（1）**计算机病毒**，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

（2）**计算机信息系统安全专用产品**，是指用于保护计算机信息系统安全的专用硬件和软件产品。



- **教材P30案例6**
- 倪**破坏计算机信息系统案

**请大家谈谈对该
案例的看法**



案例：恶意植入木马 非法控制计算机信息系统

- 2014 年 11 月 2 日，张某出于炫耀的目的，在江西省景德镇市的家中租用一台服务器作为主控服务器，用扫描器扫描出互联网中存在服务器管理漏洞的计算机，使用木马文件取得计算机信息系统的控制权，随后利用其租用的服务器内黑客软件生成名为“ip32.rar”的木马文件，再利用连接器将该木马上传至其控制的计算机信息系统中，致使计算机信息系统遭到 DDOS 流量攻击。
- 经过调查取证，张某非法控制腾讯云计算（北京）有限责任公司计算机系统的数量为 94 台，致使腾讯云网络瘫痪约 100 分钟，情节严重，其行为已构成非法控制计算机信息系统罪，同年 12 月 24 日，张某被公安机关抓获，判处张某有期徒刑二年零六个月。
- **案例释义**
 - （1）关于作案过程与电子取证：罪犯采取先入侵，然后用黑客手段生成密钥掌握被害服务器权限，并植入木马被控端程序，再利用被控制的服务器主机对外部主机进行流量攻击。被攻击的每一台电脑都有罪犯的登录日志或者放置的木马，通过日志或者木马可以反映出这台电脑是否被控制。
 - （2）关于罪责刑的思考：罪犯的行为涉及到信息安全基本属性的可用性，给公司的经营造成巨大的经济损失，但本罪没有附加的财产处罚。

- 杭州公安揭秘新型网络黑客犯罪 上市公司网站瘫痪损失近千万

**请大家谈谈对该
案例的看法**





3. 2计算机病毒防治管理办法

3. 2计算机病毒防治管理办法

3.2.1 目的

- 为了加强对计算机病毒的预防和治理，保护计算机信息系统安全，保障计算机的应用与发展，根据《中华人民共和国计算机信息系统安全保护条例》的规定，公安部于2000年4月26日以公安部第51号令发布了《计算机病毒防治管理办法》。



3.2计算机病毒防治管理办法

3.2.2 主要内容

1.对计算机病毒进行了准确定义

第二条 本办法所称的**计算机病毒**，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

2.为了远离计算机病毒的危害，规范了人们的行为

第五条 任何单位和个人**不得制作计算机病毒**。

第六条 任何单位和个人不得有下列**传播计算机病毒**的行为：

- （一）故意输入计算机病毒，危害计算机信息系统安全；
- （二）向他人提供含有计算机病毒的文件、软件、媒体；
- （三）销售、出租、附赠含有计算机病毒的媒体；
- （四）其他传播计算机病毒的行为。

第十二条 任何单位和个人在从计算机信息网络上下载程序、数据或者购置、维修、借入计算机设备时，应当进行**计算机病毒检测**。



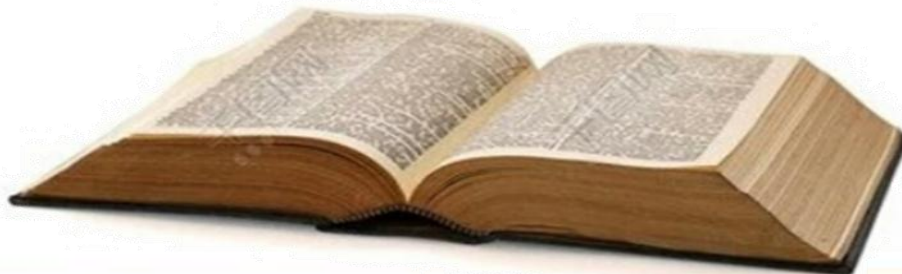
3.2 计算机病毒防治管理办法

3.2.2 主要内容（续）

3. 明确了**计算机信息系统使用单位**在计算机病毒防治工作中应当履行的职责。

第十一条 计算机信息系统的使用单位在计算机病毒防治工作中应当履行下列职责：

- （一）建立本单位的计算机病毒防治管理制度；
- （二）采取计算机病毒安全技术防治措施；
- （三）对本单位计算机信息系统使用人员进行计算机病毒**防治教育和培训**；
- （四）及时检测、清除计算机信息系统中的计算机病毒，并备有检测、清除的记录；
- （五）使用具有计算机信息系统安全**专用产品销售许可证**的计算机病毒防治产品；
- （六）对因计算机病毒引起的计算机信息系统瘫痪、程序和数据严重破坏等重大事故及时向公安机关报告，并保护现场。



3.2计算机病毒防治管理办法

3.2.2 主要内容（续）

4.明确了对从事计算机病毒防治**产品生产单位**的要求

第八条 从事计算机病毒防治产品生产的单位，应当及时向公安部公共信息网络安全监察部门批准的计算机病毒防治产品检测机构**提交病毒样本**。

第十三条 任何单位和个人销售、附赠的计算机病毒防治产品，应当具有计算机信息系统安全专用产品销售许可证，并贴有“**销售许可**”标记。

第十四条 从事计算机设备或者媒体生产、销售、出租、维修行业的单位和个人，应当对计算机设备或者媒体进行计算机病毒检测、清除工作，并备有检测、清除的记录。



3. 2计算机病毒防治管理办法

3.2.2 主要内容（续）

5.明确了公安机关在计算机病毒防治工作中的相关职权

第四条 **公安部公共信息网络安全监察部门**主管全国的计算机病毒防治管理工作。地方各级公安机关具体负责本行政区域内的计算机病毒防治管理工作。

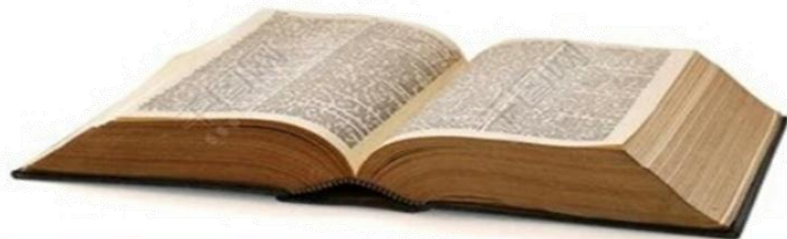
第十五条 任何单位和个人应当接受公安机关对计算机病毒防治工作的监督、检查和指导。

6.对计算机病毒的认定和疫情发布进行了规范

第二十一条 本办法所称**计算机病毒疫情**，是指某种计算机病毒爆发、流行的时间范围、破坏特点、破坏后果等情况的报告或者预报。

第七条 任何单位和个人不得向社会发布虚假的计算机病毒疫情。

第十条 对计算机病毒的**认定工作**，由公安部公共信息网络安全监察部门批准的机构承担。



3.2计算机病毒防治管理办法

3.2.2 主要内容（续）

7.明确了对计算机病毒相关违法的处罚

第十五条 任何单位和个人应当接受公安机关对计算机病毒防治工作的监督、检查和指导。

第十六条 在非经营活动中有违反本办法第五条、第六条第二、二、四项规定行为之一的，由公安机关处以一千元以下罚款。

在经营活动中有违反本办法第五条、第六条第二、三、四项规定行为之一，没有违法所得的，由公安机关对单位处以一万元以下罚款，对个人处以五千元以下罚款；有违法所得的，处以违法所得三倍以下罚款，但是最高不得超过三万元。

违反本办法第六条第一项规定的，依照《中华人民共和国计算机信息系统安全保护条例》第二十三条的规定处罚。



3.2计算机病毒防治管理办法

3.2.2 主要内容（续）

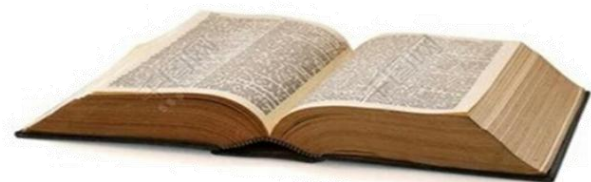
第十七条 违反本办法第七条、第八条规定行为之一的，由公安机关对单位处以一千元以下罚款，对单位直接负责的主管人员和直接责任人员处以五百元以下罚款；对个人处以五百元以下罚款。

第十八条 违反本办法第九条规定的，由公安机关处以警告，并责令其限期改正；逾期不改正的，取消其计算机病毒防治产品检测机构的检测资格。

第十九条 计算机信息系统的使用单位有下列行为之一的，由公安机关处以警告，并根据情况责令其限期改正；逾期不改正的，对单位处以一千元以下罚款，对单位直接负责的主管人员和直接责任人员处以五百元以下罚款：

- （一）未建立本单位计算机病毒防治管理制度的；
- （二）未采取计算机病毒安全技术防治措施的；
- （三）未对本单位计算机信息系统使用人员进行计算机病毒防治教育和培训的；
- （四）未及时检测、清除计算机信息系统中的计算机病毒，对计算机信息系统造成危害的；
- （五）未使用具有计算机信息系统安全专用产品销售许可证的计算机病毒防治产品对计算机信息系统造成危害的。

第二十条 违反本办法第十四条规定，没有违法所得的，由公安机关对单位处以一万元以下罚款，对个人处以五千元以下罚款；有违法所得的，处以违法所得三倍以下罚款，但是最高不得超过三万元。



- 教材P30案例10、案例11

**请大家谈谈对该
案例的看法**





3. 3信息安全等级保护管理办法

3.3信息安全等级保护管理办法

3.3.1 目的

《信息安全等级保护管理办法》（以下简称《等级保护管理办法》）于2007年6月22日由公安部、国家保密局、国家密码管理局和国务院信息化工作办公室联合发布，共七章四十四条。2006年颁布的《信息安全等级保护管理办法（试行）》（公通字[2006]7号）同时废止。）

制定《等级保护管理办法》的目的：规范信息安全等级保护管理，提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设。（第一条）



3.3信息安全等级保护管理办法

3.3.2 职能与分工

第二条 **国家**通过制定统一的信息安全等级保护管理规范和技术标准，组织公民、法人和其他组织对信息系统分等级实行安全保护，对等级保护工作的实施进行监督、管理。

第三条 **公安机关**负责信息安全等级保护工作的监督、检查、指导。**国家保密工作部门**负责等级保护工作中有关保密工作的监督、检查、指导。**国家密码管理部门**负责等级保护工作中有关密码工作的监督、检查指导。涉及其他职能部门管辖范围的事项，由有关职能部门依照国家法律法规的规定进行管理。**国务院信息化工作办公室**及地方信息化领导小组办事机构负责等级保护工作的部门间协调。

第四条 信息系统主管部门应当依照本办法及相关标准规范，督促、检查、指导本行业、本部门或者本地区信息系统运营、使用单位的信息安全等级保护工作。

第五条 信息系统的运营、使用单位应当依照本办法及其相关标准规范，履行信息安全等级保护的义务和责任。

- **实施信息系统等级保护工作的主体是信息系统运营、使用单位，公安机关是主要的监管部门。**

3.3信息安全等级保护管理办法

3.3.3 主要内容

1.明确了信息系统安全保护等级的划分原则及划分标准

第六条 国家信息安全等级保护坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全，经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。

2.明确了不同等级信息系统的监管规格的区别

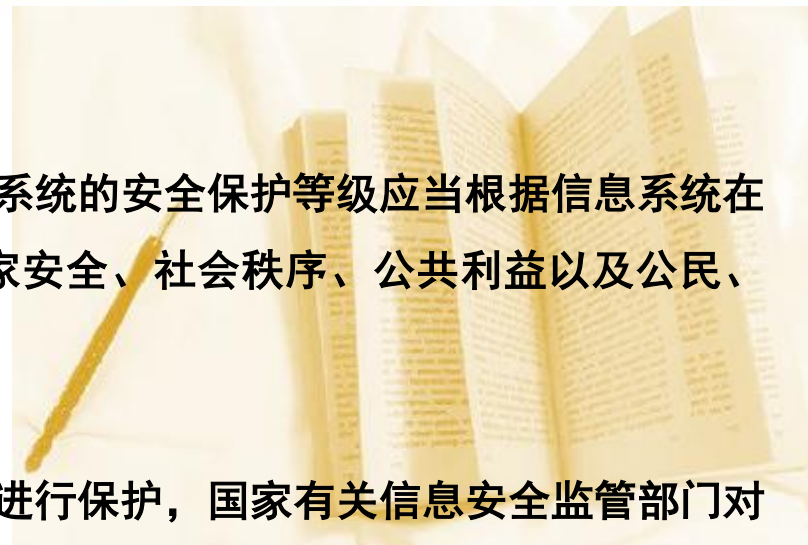
第八条 信息系统运营、使用单位依据本办法和相关术标准对信息系统进行保护，国家有关信息安全监管部门对其信息安全等级保护工作进行监督管理。

3.明确了信息系统运营、使用单位进行信息安全等级保护工作的管理程序，管理内容和管理要求

第九条 信息系统运营、使用单位应当按照《信息系统安全等级保护实施指南》具体实施等级保护工作。

第十条 信息系统运营、使用单位应当依据本办法和《信息系统安全等级保护定级指南》确定信息系统的安全保护等级。有主管部门的，应当经主管部门审核批准。

跨省或者全国统一联网运行的信息系统可以由主管部门统一确定安全保护等级。对拟确定为第四级以上信息系统的，运营、用单位或者主管部门应当请国家信息安全保护等级专家评审委员会评审。



3.3信息安全等级保护管理办法

3.3.3 主要内容（续）

4.明确了公安机关在信息安全等级保护工作中的职责

第十七条 信息系统备案后，公安机关应当对信息系统的备案情况进行审核，对符合等级保护要求的，应当在收到备案材料之日起的10个工作日内颁发信息系统安全等级保护备案证明；发现不符合本办法及有关标准的应当在收到备案材料之日起的10个工作日内通知备案单位予以纠正；发现定级不准的应当在收到备案材料之日起的10个工作日内通知备案单位重新审核确定。

运营、使用单位或者主管部门重新确定信息系统等级后，应当按照本办法向公安机关重新备案。

5.明确了等级保护测评机构的条件和职责

第二十二条 第三级以上信息系统应当选择符合下列条件的等级保护测评机构进行测评：（一）在中华人民共和国境内注册成立（港澳台地区除外）；（二）由中国公民投资、中国法人投资或者国家投资的企事业单位（港澳台地区除外）；（三）从事相关检测评估工作两年以上，无违法记录；（四）工作人员仅限于中国公民；（五）法人及主要业务、技术人员无犯罪记录；（六）使用的技术装备设施应当符合本办法对信息安全产品的要求；（七）具有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度；（八）对国家安全、社会秩序、公共利益不构成威胁。

3.3信息安全等级保护管理办法

3.3.3 主要内容（续）

6.明确了对于涉及国家秘密的信息系统的保密管理要求

这些要求主要体现在第二十四条到第三十三条的规定中。如：

第二十七条 涉密信息系统建设使用单位应当选择具有涉密集成资质的单位承担或者参与涉密信息系统的设计与实施。

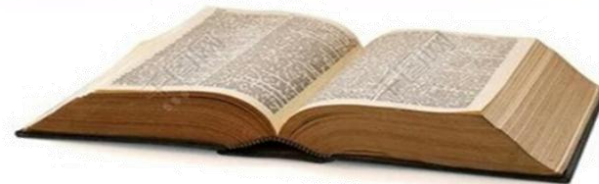
涉密信息系统建设使用单位应当依据涉密信息系统分级保护管理规范和技术标准，按照秘密、机密、绝密三级的不同要求，结合系统实际进行方案设计，实施分级保护，其保护水平总体上不低于国家信息安全等级保护第三级、第四级、第五级的水平。

7.明确了信息安全等级保护的密码管理要求

这些要求主要体现在第四十四条到第三十九条的规定中。如：

第三十四条 国家密码管理部门对信息安全等级保护的密码实行分类分级管理。根据被保护对象在国家安全、社会稳定、经济建设中的作用和重要程度，被保护对象的安全防护要求和涉密程度，被保护对象被破坏后的危害程度以及密码使用部门的性质等，确定密码的等级保护准则。

信息系统运营、使用单位采用密码进行等级保护的，应当遵照《信息安全等级保护密码管理办法》、《信息安全等级保护商用密码技术要求》等密码管理规定和相关标准。



3.3信息安全等级保护管理办法


3.3.3 主要内容（续）

8.明确了信息安全等级保护工作的相关法律责任

第四十条 第三级以上信息系统运营、使用单位违反本办法规定，有下列行为之一的，由公安机关、国家保密工作部门和国家密码工作管理部门按照职责分工责令其限期改正；逾期不改正的，给予警告，并向其上级主管部门通报情况，建议对其直接负责的主管人员和其他直接责任人员予以处理，并及时反馈处理结果：

- （一）未按本办法规定备案、审批的；
- （二）未按本办法规定落实安全管理制度、措施的；
- （三）未按本办法规定开展系统安全状况检查的；
- （四）未按本办法规定开展系统安全技术测评的；
- （五）接到整改通知后，拒不整改的；
- （六）未按本办法规定选择使用信息安全产品和测评机构的；
- （七）未按本办法规定如实提供有关文件和证明材料的；
- （八）违反保密管理规定的；
- （九）违反密码管理规定的；
- （十）违反本办法其他规定的。





3.4 计算机信息系统安全专用产品检测和销售 许可证管理办法

3.4 计算机信息系统安全专用产品检测和销售许可证管理办法

3.4.1 目的和意义

《计算机信息系统安全专用产品检测和销售许可证管理办法》于1997年6月28日由公安部部长办公会议通过，从1997年12月12日起施行，共五章二十六条。

第一条 为了加强计算机信息系统安全专用产品（以下简称安全专用产品）的管理，保证安全专用产品的安全功能，维护计算机信息系统的安全，根据《中华人民共和国计算机信息系统安全保护条例》第十六条的规定，制定本办法。

第二条 本办法所称计算机信息系统安全专用产品，是指用于保护计算机信息系统安全的专用硬件和软件产品。

3.4.2 检测机构的申请与批准

第六条 经省级以上技术监督行政主管部门或者其授权的部门考核合格的检测机构，可以向公安部计算机管理监察部门提出承担安全专用产品检测任务的申请。

第七条 公安部计算机管理监察部门对提出申请的检测机构的检测条件和能力进行审查，经审查合格的，批准其承担安全专用产品检测任务。

第九条 公安部计算机管理监察部门对承担检测任务的检测机构每年至少进行一次监督检查。

第十条 被取消检测资格的检测机构，两年后方准许重新申请承担安全专用产品的检测任务。

3.4 计算机信息系统安全专用产品检测和销售许可证管理办法

3.4.3 销售许可证制度

第十五条 安全专用产品的生产者申领销售许可证，应当向公安部计算机管理监察部门提交以下材料：

- （一）营业执照（复印件）；
- （二）安全专用产品检测结果报告；
- （三）防治计算机病毒的安全专用产品须提交公安机关颁发的计算机病毒防治研究的备案证明。

第十六条 公安部计算机管理监察部门自接到申请之日起，应当在十五日内对安全专用产品作出审核结果，特殊情况可延至三十日；经审核合格的，颁发销售许可证和安全专用产品“销售许可”标记；不合格的，书面通知申领者，并说明理由。

3.4.4 罚则

第二十一条 检测机构违反本办法的规定情节严重的，取消检测资格。

第二十二条 安全专用产品中含有有害数据危害计算机信息系统安全的，依据《中华人民共和国计算机信息系统安全保护条例》第二十三条的规定处罚；构成犯罪的，依法追究刑事责任。

第二十三条 依照本办法作出的行政处罚，应当由县级以上（含县级）公安机关决定，并填写行政处罚决定书，向被处罚人宣布。



感谢聆听