高等职业教育精品示范教材　信息安全系列

信息安全等级保护与风险评估

主　编　李贺华
副主编　武春岭　鲁先志　巍　嵬　宋敦波

本书特色：

- 以就业为导向，以能力为本位
- 学习任务引领，工作需求驱动
- 通用内容为主，特殊内容为辅

中国水利水电出版社
www.waterpub.com.cn

高等职业教育精品示范教材（信息安全系列）

信息安全等级保护与风险评估

主　编　李贺华

副主编　武春岭　鲁先志　巍　嵬　宋敦波

中国水利水电出版社
www.waterpub.com.cn

内 容 提 要

本书根据高职高专教育教学特点，面向等级保护测评师岗位，以等级保护工作实施过程所需要的技术为主线选择教材内容。阐述如何对一个信息系统进行等级保护定级、安全设计、安全建设、安全测评、安全整改等有关等级保护和风险评估的相关工作。

本书内容难度适中，语言通俗易懂，适合作为计算机相关专业开设的“信息安全等级保护和风险评估”课程的配套教材，也适合作为考取国家“信息安全等级保护测评师”的学习材料，对从事网络安全管理、网络安全规划与设计的工程技术人员也有一定的参考价值。

图书在版编目（CIP）数据

信息安全等级保护与风险评估 / 李贺华主编. -- 北京 : 中国水利水电出版社, 2014.11
高等职业教育精品示范教材. 信息安全系列
ISBN 978-7-5170-2145-2

Ⅰ. ①信… Ⅱ. ①李… Ⅲ. ①信息系统－安全技术－高等职业教育－教材 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2014)第128963号

策划编辑：寇文杰　　责任编辑：樊昭然　　封面设计：李　佳

书　名	高等职业教育精品示范教材（信息安全系列） **信息安全等级保护与风险评估**
作　者	主　编　李贺华 副主编　武春岭　鲁先志　巍　嵬　宋敦波
出版发行	中国水利水电出版社 （北京市海淀区玉渊潭南路1号D座　100038） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）68367658（发行部）、82562819（万水）
经　售	北京科水图书销售中心（零售） 电话：（010）88383994、63202643、68545874 全国各地新华书店和相关出版物销售网点
排　版	北京万水电子信息有限公司
印　刷	三河市铭浩彩色印装有限公司
规　格	184mm×240mm　16开本　17.5印张　457千字
版　次	2014年11月第1版　2014年11月第1次印刷
印　数	0001—3000册
定　价	34.00元

前　言

随着我国经济的持续发展和国际地位的不断提高，我国的基础信息网络和重要信息系统面临的安全威胁和安全隐患十分严峻，计算机病毒传播和网络非法入侵猖獗，犯罪分子利用一些安全漏洞，使用黑客病毒技术、网络钓鱼技术、木马间谍程序等进行网络盗窃、网络诈骗、网络赌博等违法活动，带来了大量的社会问题。出于对信息安全的重视，国家陆续出台了信息安全等级保护和风险评估与管理的一系列文件和标准，用以促进和指导信息安全的建设。

为加强信息安全等级保护测评机构建设和管理，规范等级测评活动，保障信息安全等级保护测评工作的顺利开展，公安部下发了《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安[2010]303 号），对等级测评工作、等级测评机构建设以及等级测评人员进行了规范和要求。要求开展等级测评的人员要参加专门培训和考试，并取得由公安部信息安全等级保护评估中心颁发的“信息安全等级测评师证书”（等级测评师分为初级、中级和高级），持证上岗。

本书根据高职高专教育教学特点，面向等级保护测评师岗位，以等级保护工作实施过程所需的技术为主线选择教材内容，阐述如何对一个信息系统进行等级保护定级、安全设计、安全建设、安全测评、安全整改等有关等级保护和风险评估的相关工作。全书共分七个章节，具体内容安排如下：

第一章，介绍了等级保护的基础知识，内容包括：等级保护的来源、发展，等级保护的基本含义、实施原则，等级保护的相关工作部门，以及相关标准简介等。

第二章，介绍了等级保护的实施过程，主要包括等级保护五个环节：信息系统定级、总体安全规划、安全设计与实施、安全运行与维护和信息系统终止的主要工作内容和工作方法等。

第三章，介绍了信息系统定级的方法，包括信息系统定级的重要性、定级要素、主要的定级过程，并以学生最为熟悉的高校教育信息系统为例详细描述了定级的方法和应用。

第四章，介绍了信息系统等级保护测评的方法和过程，主要包括等级保护测评实施过程、测评对象的确定方法、测评内容和测评要求，以及测评方案和测评报告的编制。

第五章，介绍了基于等级保护的信息系统安全建设与整改方法，包括新建系统等级保护设计和已建系统的整改方案设计等。

第六章，介绍了根据国家对“数字海洋”应用系统的定级要求，及等级保护三级标准进行建设方案的分析与设计的过程和方法。

第七章，介绍了信息安全风险评估的基本概念、原则和要求等，给出了信息安全风险评估的一般方法和流程。

本书适合作为计算机相关专业开设的“信息安全等级保护和风险评估”课程的配套教材，

也适合作为考取“信息安全等级保护测评师”的学习材料，对从事网络安全管理、网络安全规划与设计的工程技术人员也有一定的参考价值。

本书由重庆电子工程职业学院教师李贺华任主编（编写第 1、2、3、5 和 7 章），武春岭、鲁先志、巍嵬（西安理工大学）和宋敦波（西昌学院）任副主编（编写第 4、6 章和附录），最后由巍嵬博士统稿，胡云兵、李腾、何倩、童均等老师参与部分内容的审稿和修订，对本书编写提出了宝贵意见。本书在编写过程中参考了大量的国际标准、国家标准、专著、教材和网络资源等，在此对其作者表示衷心的感谢。另外，由于编者水平有限，书中难免存在不妥甚至错误之处，请广大读者批评指正，不胜感激。编者的联系方法：lihehuacqcet@yeah.net。

目　录

1 信息安全与等级保护概述

任务描述

本章主要介绍了等级保护的基本含义、基本原则、等级保护的来源与发展、相关部门的工作责任，以及等级保护的相关标准。涵盖以下主题：

- 等级保护的基本概念
- 等级保护的来源与发展
- 等级保护主要标准的作用
- 等级保护与风险评估的关系

1.1 等级保护的基本概念

1.1.1 什么是等级保护

等级保护是对信息和信息载体按照重要性等级分级别进行保护的一种工作，在中国、美国等很多国家都存在的一种信息安全领域的技术和工作。在中国，等级保护广义上为涉及到该工作的标准、产品、系统、信息等均依据等级保护思想的安全工作；狭义上称为的一般指信息系统安全等级保护，是指对国家安全、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置的综合性工作。

1.1.2 等级保护的来源与发展

为了进一步提高信息安全的保障能力和防护水平，维护国家安全、公共利益和社会稳定，保障和促进信息化建设的健康发展，1994 年国务院颁布的《中华人民共和国计算机信息系统安全保护条例》（国务院 147 号令）中规定，“计算机信息系统实行安全等级保护。安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定”。

2002 年 7 月 18 日，公安部在 GB 17859 的基础上，又发布实施五个 GA 新标准，分别是：GA/T 387-2002《计算机信息系统安全等级保护网络技术要求》、GA 388-2002 《计算机信息系统安全等级保护操作系统技术要求》、GA/T 389-2002《计算机信息系统安全等级保护数据库管理系统技术要求》、GA/T 390-2002《计算机信息系统安全等级保护通用技术要求》、GA 391-2002《计算机信息系统安全等级保护管理要求》。这些标准是我国计算机信息系统安全保护等级系列标准的一部分。

2003 年中央办公厅、国务院办公厅转发的《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号）明确指出，“要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南”。

2004 年由公安部、国家保密局、国家密码管理局、国务院信息化工作办公室联合转发的《关于信息安全等级保护工作的实施意见》（公通字[2004]66 号）中再次强调“信息安全等级保护制度是国家在国民经济和社会信息化的发展过程中，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健康发展的一项基本制度。实行信息安全等级保护制度，能够充分调动国家、法人和其他组织及公民的积极性，发挥各方面的作用，达到有效保护的目的，增强安全保护的整体性、针对性和实效性，使信息系统安全建设更加突出重点、统一规范、科学合理，对促进我国信息安全的发展将起到重要推动作用。”

从国务院 147 号令、27 号文到 66 号文，逐步明确了信息安全等级保护是国家的一项基本制度。实施信息安全等级保护，能够有效地提高我国信息和信息系统安全建设的整体水平，有利于在信息化建设过程中同步建设信息安全设施，保障信息安全与信息化建设相协调；有利于为新信息系统安全建设和管理提供系统性、针对性、可行性的指导和服务，有效控制信息安全建设成本；有利于优化信息安全资源的配置，对信息系统分级实施保护，重点保障基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统的安全；有利于明确国家、法人和其他组织、公民的信息安全责任，加强信息安全管理；有利于推动信息安全产业的发展，逐步探索出一条适应社会主义市场经济发展的信息安全模式。

为了落实国务院 147 号令、27 号文和 66 号文的精神，作为信息安全等级保护工作的主管部门，公安部牵头会同有关部门加快了制定信息安全等级保护配套管理办法和技术标准的步伐，先后提出并组织制订了以国家标准《计算机信息系统安全保护等级划分准则》（GB 17859-

1999）为核心的一系列等级保护配套国家标准，并于2006年开展了信息安全等级保护试点工作，通过试点工作进一步了解了我国信息系统安全保护的普遍情况，完善了等级保护相关管理规范和标准体系，明确了落实信息安全等级保护的相关单位的责任，加强了信息安全等级保护监督管理队伍和技术支撑队伍的建设，扩大了信息安全等级保护的社会影响。最终，形成“一套经验”、“一套制度”、“一批标准”、“一批工程”和“一支队伍”，为国家信息安全等级保护制度全面实行打下了坚实基础。

鉴于“经验”、“制度”、“标准”、“工程”和“队伍”的逐步成熟，2007年7月公安部、国家保密局、国家密码管理局、国务院信息化工作办公室转发了《信息安全等级保护管理办法（公通字[2007]43号）》（以下简称《管理办法》）和《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安[2007]861号)文件，开始部署在全国范围内开展重要信息系统安全等级保护定级工作。

根据信息系统中处理信息的不同，信息系统分为涉密信息系统和非涉密信息系统，根据《管理办法》的要求，涉密信息系统应当依据国家信息安全等级保护的基本要求，按照国家保密工作部门有关涉密信息系统分级保护的管理规定和技术标准，结合系统实际情况进行保护。非涉密信息系统不得处理国家秘密信息。

1.1.3 安全等级的划分

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。我国把信息系统的安全保护等级分为以下五个级别：

（1）第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

（2）第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

（3）第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

（4）第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

（5）第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

特别强调的是：《关于信息安全等级保护工作的实施意见》（简称66号文）中的这种分级主要是从信息和信息系统的业务重要性及遭受破坏后的影响出发的，是系统从应用需求出发必须纳入的安全业务等级，而不是GB 17859-1999中定义的系统已具备的安全技术等级。

正是因为不同级别的信息系统受到攻击后造成的损害不同，所以对它们进行监督管理的强度也不同，因此这五个级别也分别称为：自主保护级、指导保护级、监督保护级、强制保护级和专控保护级。

（1）第一级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。

（2）第二级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行指导。

（3）第三级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行监督、检查。

（4）第四级信息系统运营、使用单位应当依据国家有关管理规范、技术标准和业务专门需求进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行强制监督、检查。

（5）第五级信息系统运营、使用单位应当依据国家有关管理规范、技术标准和业务特殊安全需求进行保护。国家指定专门部门对该级信息系统信息安全等级保护工作进行专门监督、检查。

1.1.4 等级保护基本原则

信息系统安全等级保护的核心是对信息系统分等级、按标准进行建设、管理和监督。信息系统安全等级保护实施过程中应遵循以下基本原则。

1. 自主保护原则

信息系统的安全责任主体是信息系统运营、使用单位及其主管部门，“自主”体现在运营使用单位及其主管部门按照相关标准自主定级、自主保护。在等级保护工作中，信息系统运营使用单位和主管部门按照“谁主管谁负责，谁运营谁负责”的原则开展工作，并接受信息安全监管部门对开展等级保护工作的监管。运营使用单位和主管部门是信息系统安全的第一责任人，对所属信息系统安全负有直接责任；公安、保密、密码部门对运营使用单位和主管部门开展等级保护工作进行监督、检查、指导，对重要信息系统安全负监管责任。由于重要信息系统的安全运行不仅影响本行业、本单位的生产和工作秩序，也会影响国家安全、社会稳定、公共利益，因此，国家需要对重要信息系统的安全进行监管。

2. 重点保护原则

重点保护就是要解决我国信息安全面临的主要威胁和存在的主要问题，实行国家对重要信息系统进行重点安全保障的重大措施，有效体现“适度安全、保护重点”的目的，将有限的财力、物力、人力投入到重要信息系统安全保护中，依据相关标准建设安全保护体系，建立安全保护制度，落实安全责任，加强监督检查，有效保护重要信息系统安全，有效提高我国信息系统安全建设的整体水平。优化信息安全资源的配置，重点保障基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统的安全。

3. 同步建设原则

信息安全建设的特点要求在信息化建设中必须同步规划、同步实施，信息系统在新建、改建、扩建时应当同步规划和设计安全方案，投入一定比例的资金建设信息安全设施，保障信息安全与信息化建设相适应，避免重复建设而带来的资源浪费。因此，在《管理办法》第十二

条规定，在信息系统建设过程中，运营、使用单位应当按照《计算机信息系统安全保护等级划分准则》（GB17859-1999）、《信息安全技术　信息系统安全等级保护基本要求》等技术标准，同步建设符合该等级要求的信息安全设施。

4. 动态调整原则

跟踪信息系统的变化，调整安全保护措施。由于信息系统的应用类型、数量、范围等会根据实际需要而发生相应调整，当调整和变更的内容发生较大变化时，应当根据等级保护的管理规范和技术标准的要求，重新确定信息系统的安全保护等级，根据信息系统安全保护等级的调整情况，重新实施安全保护。同时，信息安全本身也具有动态性，不是一成不变的，当信息安全技术、外部环境、安全威胁等因素发生变化时，需要信息安全策略、安全措施进行相应的调整，以满足安全需求的变化。

1.2　等级保护主要标准介绍

1.2.1　相关标准及其体系结构

国家开始实施等级保护制度以来，为了加强等级保护的可执行性，制定一系列的标准规范来指导等级保护的具体落实工作。信息安全等级保护相关标准大致可以分为四类：基础类、应用类、产品类和其他类。不同标准在等级保护各个不同工作环节中的作用如图 1-1 所示，标准间的相互关系如图 1-2 所示。

1. 基础类标准

《计算机信息系统安全保护等级划分准则》（GB17859-1999）

《信息安全技术　信息系统安全等级保护基本要求》（GB/T 22239-2008）

2. 应用类标准

（1）信息系统定级。

《信息安全技术　信息系统安全等级保护定级指南》（GB/T 22240-2008）

（2）等级保护实施。

《信息安全技术　信息系统安全等级保护实施指南》（GB/T 25058-2010）

（3）信息系统安全建设。

《信息安全技术　信息系统通用安全技术要求》（GB/T 20271-2006）

《信息安全技术　信息系统等级保护安全设计技术要求》（GB/T 25070-2010）

《信息安全技术　信息系统安全管理要求》（GB/T 20269-2006）

《信息安全技术　信息系统安全工程管理要求》（GB/T 20282-2006）

《信息安全技术　信息系统物理安全技术要求》（GB/T 21052-2007）

《信息安全技术　网络基础安全技术要求》（GB/T 20270-2006）

《信息安全技术　信息系统安全等级保护体系框架》（GA/T 708-2007）

《信息安全技术　信息系统安全等级保护基本模型》（GA/T 709-2007）
《信息安全技术　信息系统安全等级保护基本配置》（GA/T 710-2007）

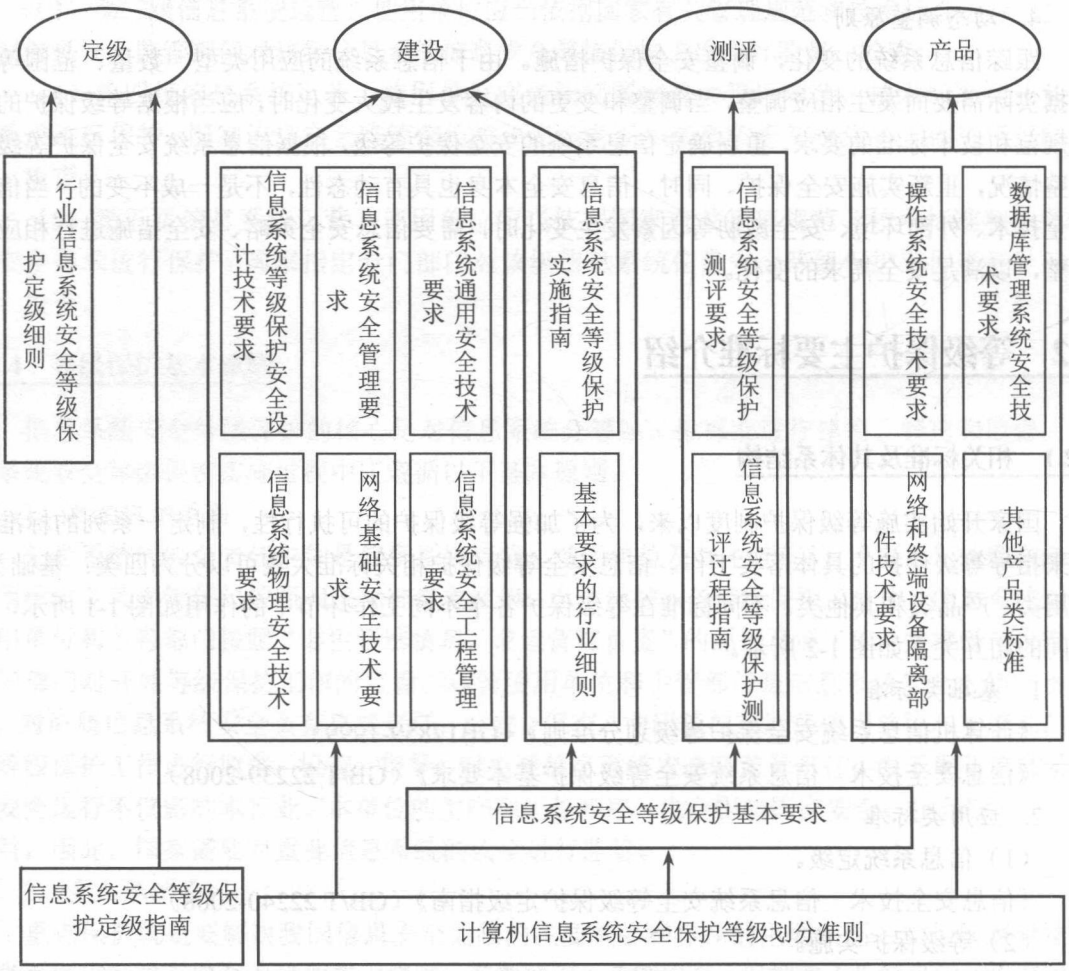

图 1-1　信息安全等级保护相关标准体系

（4）等级测评。
《信息安全技术　信息系统安全等级保护测评要求》（GB/T 28448-2012）
《信息安全技术　信息系统安全等级保护测评过程指南》（GB/T 28449-2012）
《信息安全技术　信息系统安全管理测评》（GA/T 713-2007）

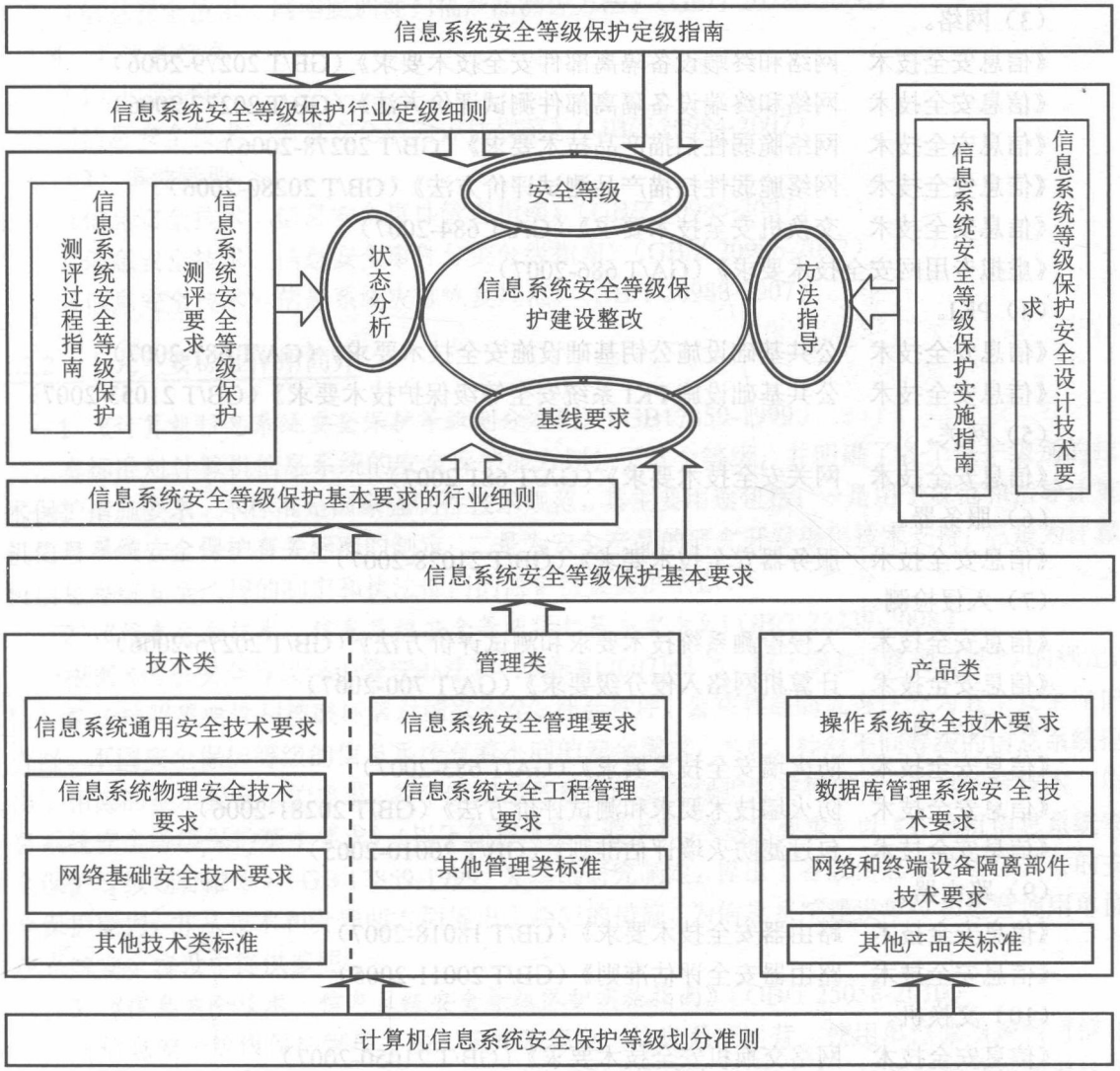

图 1-2　等级保护标准间相互关系

3. 产品类标准

（1）操作系统。

《信息安全技术　操作系统安全技术要求》（GB/T 20272-2006）

《信息安全技术　操作系统安全评估准则》（GB/T 20008-2005）

（2）数据库。

《信息安全技术　数据库管理系统安全技术要求》（GB/T 20273-2006）

《信息安全技术　数据库管理系统安全评估准则》（GB/T 20009-2005）

（3）网络。

《信息安全技术　网络和终端设备隔离部件安全技术要求》（GB/T 20279-2006）

《信息安全技术　网络和终端设备隔离部件测试评价方法》（GB/T 20277-2006）

《信息安全技术　网络脆弱性扫描产品技术要求》（GB/T 20278-2006）

《信息安全技术　网络脆弱性扫描产品测试评价方法》（GB/T 20280-2006）

《信息安全技术　交换机安全技术要求》（GA/T 684-2007）

《虚拟专用网安全技术要求》（GA/T 686-2007）

（4）PKI。

《信息安全技术　公共基础设施公钥基础设施安全技术要求》（GA/T 687-2007）

《信息安全技术　公共基础设施 PKI 系统安全等级保护技术要求》（GB/T 21053-2007）

（5）网关。

《信息安全技术　网关安全技术要求》（GA/T 681-2007）

（6）服务器。

《信息安全技术　服务器安全技术要求》（GB/T 21028-2007）

（7）入侵检测。

《信息安全技术　入侵检测系统技术要求和测试评价方法》（GB/T 20275-2006）

《信息安全技术　计算机网络入侵分级要求》（GA/T 700-2007）

（8）防火墙。

《信息安全技术　防火墙安全技术要求》（GA/T 683-2007）

《信息安全技术　防火墙技术要求和测试评价方法》（GB/T 20281-2006）

《信息安全技术　包过滤防火墙评估准则》（GB/T 20010-2005）

（9）路由器。

《信息安全技术　路由器安全技术要求》（GB/T 18018-2007）

《信息安全技术　路由器安全评估准则》（GB/T 20011-2005）

（10）交换机。

《信息安全技术　网络交换机安全技术要求》（GB/T 21050-2007）

《信息安全技术　交换机安全评估准则》（GA/T 685-2007）

（11）其他产品。

《信息安全技术　终端计算机系统安全等级技术要求》（GA/T 671-2006）

《信息安全技术　审计产品技术要求和测评方法》（GB/T 20945-2006）

《信息安全技术　虹膜识别系统技术要求》（GB/T 20979-2007）

《信息安全技术　虚拟专用网安全技术要求》（GA/T 686-2007）

《信息安全技术　应用软件系统安全等级保护通用技术指南》（GA/T 711-2007）

《信息安全技术　应用软件系统安全等级保护通用测试指南》（GA/T 712-2007）

《信息安全技术　网络和终端设备隔离部件测试评价方法》(GB/T 20277-2006)
《信息安全技术　网络脆弱性扫描产品测评方法》(GB/T 20280-2006)

4. 其他类标准

(1) 风险评估。

《信息安全技术　信息安全风险评估规范》(GB/T 20984-2007)

(2) 事件管理。

《信息安全技术　信息安全事件管理指南》(GB/Z 20985-2007)
《信息安全技术　信息安全事件分类分级指南》(GB/Z 20986-2007)
《信息安全技术　信息系统灾难恢复规范》(GB/T 20988-2007)

1.2.2 十大主要标准作用简介

1.《计算机信息系统安全保护等级划分准则》(GB17859-1999)

本标准对计算机信息系统的安全保护能力划分了五个等级，并明确了各个保护级别的技术保护措施要求。本标准是国家强制性技术规范，其主要用途包括：一是用于规范和指导计算机信息系统安全保护有关标准的制定；二是为安全产品的研究开发提供技术支持；三是为计算机信息系统安全法规的制定和执法部门的监督检查提供依据。

2.《信息安全技术　信息系统安全等级保护基本要求》(GB/T 22239-2008)

根据《信息安全等级保护管理办法》(公通字[2007]43号，以下简称《管理办法》)的规定，信息系统按照重要性和被破坏后对国家安全、社会秩序、公共利益的危害性分为五个安全保护等级。不同安全保护等级的信息系统有着不同的安全需求，为此，针对不同等级的信息系统提出了相应的基本安全保护要求，各个级别信息系统的安全保护要求构成了《信息安全技术　信息系统安全等级保护基本要求》(以下简称《基本要求》)。《基本要求》以《计算机信息系统安全保护等级划分准则》(GB 17859-1999)为基础研究制定，提出了各级信息系统应当具备的安全保护能力，并从技术和管理两方面提出了相应的措施，为信息系统建设单位和运营使用单位在系统安全建设中提供参照。

3.《信息安全技术　信息系统安全等级保护实施指南》(GB/T 25058-2010)

《信息安全等级保护管理办法》第九条规定，信息系统运营、使用单位应当按照《信息安全技术　信息系统安全等级保护实施指南》具体实施等级保护工作。信息系统从规划设计到终止运行要经历几个阶段，《信息安全技术　信息系统安全等级保护实施指南》(以下简称《实施指南》)用于指导信息系统运营、使用单位，在信息系统从规划设计到终止运行的过程中如何按照信息安全等级保护政策、标准要求实施等级保护工作。

4.《信息安全技术　信息系统安全等级保护定级指南》(GB/T 22240-2008)

《信息安全等级保护管理办法》对信息系统的安全保护等级给出了明确定义。信息系统定级是等级保护工作的首要环节，是开展信息系统安全建设整改、等级测评、监督检查等后续工作的重要基础。《信息安全技术　信息系统安全等级保护定级指南》(以下简称《定级指南》)