网络安全等级保护定级指南解读

《信息安全技术 **网络安全**等级保护定级指南》

是

《信息安全技术 信息系统安全等级保护定级指南》

（GB/T 22240-2008）的修订版

主要内容

一．基本概念和定级要素

二．定级方法

三．工作流程

一、基本概念和定级要素

- 定级是开展网络安全等级保护工作的“基本出发点”
- 定级结果应当成为系统安全保护的总体安全需求之一
- 定级过程是找到系统最大风险的过程

一、基本概念和定级要素-等级定义

- 《信息安全等级保护管理办法》（公通字[2007]43号“第七条 信息系统的保护等级分为以下五级：

  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；

一、基本概念和定级要素-等级定义

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；

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。

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。

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。”

一、基本概念和定级要素

- 解决了：信息系统根据什么定级？定什么级？
  - 从信息系统对国家安全、经济建设、公共利益等方面的重要性，以及信息系统被破坏后造成危害的严重性角度对信息系统确定的等级-重要性定级
- 没有解决：定级的方法、流程

一、基本概念和定级要素

- 《信息安全技术 信息系统安全等级保护定级指南》

  （GB/T 22240-2008）

- 《信息安全技术 网络安全等级保护定级指南》

  （GB/T 22240-20**）(前者的修订版)

——主要关注等级保护定级工作开展的流程及定级的方法

8

一、基本概念和定级要素

- 概念解释
  - 安全保护等级
  - 等级保护对象
  - 客体

一、基本概念和定级要素

- 安全保护等级

  等级的确定是不依赖于安全保护措施的，具有一定的“客观性”，即该系统在存在之初便由其自身所实现的使命的重要程度决定了它的安全保护等级，而非由“后天”的安全保护措施决定。

一、基本概念和定级要素

- 等级保护对象
  - 网络安全等级保护工作的作用对象，主要包括基础网络设施、信息系统（如工业控制系统、云计算平台、物联网、使用移动互联技术的系统、其他系统）以及数字资源等。

一、基本概念和定级要素

- 客体
  - 受法律保护的、等级保护对象受到破坏时所侵害的社会关系，如国家安全、社会秩序、公共利益以及公民、法人或其他组织的合法权益。

一、基本概念和定级要素

- 定级要素一：受侵害的客体
- 定级要素二：对客体的侵害程度
- 定级要素与安全保护等级的对应关系

一、基本概念和定级要素

- 要素一　受侵害的客体
  - 公民、法人和其他组织的合法权益
  - 社会秩序和公共利益
  - 国家安全

一、基本概念和定级要素

- 公民、法人和其他组织的合法权益
  - 是法律确认的并受法律保护的公民、法人和其他组织所享有的一定的社会权利和利益。
  - 本标准中特指拥有信息系统的个体或确定组织所享有的社会权利和利益。

一、基本概念和定级要素

- 社会秩序
  - 国家机关的工作秩序；
  - 各类经济活动秩序；
  - 各行业科研、生产秩序；
  - 公众正常生活秩序等。

一、基本概念和定级要素

- 公共利益
  - 不特定社会成员所共同享有的，维持其生产、生活、教育、卫生等方面的利益，表现为：
    - 社会成员使用公共设施
    - 社会成员获取公开信息资源
    - 社会成员获取公共服务等

一、基本概念和定级要素

- 国家安全
  - 国家层面、与全局相关的国家政治安全、国防安全、经济安全、社会安全、科技安全和资源环境安全等方面利益。

一、基本概念和定级要素

- 要素二　对客体的侵害程度

  等级保护对象受到破坏后对客体造成侵害的程度归结为以下三种：

  - 造成一般损害
  - 造成严重损害
  - 造成特别严重损害

一、基本概念和定级要素

- 一般损害，是指对客体造成一定损害和影响，经采取恢复或弥补措施，可消除部分影响。
- 严重损害，是指对客体造成严重损害，经采取恢复或弥补措施，仍产生较大影响。
- 造成特别严重损害，是指对客体造成特别严重损害，后果特别严重，影响重大且无法弥补。

一、基本概念和定级要素

- 侵害程度
  - 外在表现： 产生各种不良后果，包括：
    - 财产损失
    - 机构声誉损害
    - 人员伤亡
    - ……

21

一、基本概念和定级要素

- 影响行使工作职能；
- 导致业务能力下降；
- 引起法律纠纷；
- 导致财产损失；
- 造成社会不良影响；
- 对其他组织和个人造成损失；
- 其他影响。

22

一、基本概念和定级要素

- 一般损害：工作职能受到局部影响，业务能力有所降低但不影响主要功能的执行，出现较轻的法律问题，较低的财产损失，有限的社会不良影响，对其他组织和个人造成较低损害。

23

一、基本概念和定级要素

- 严重损害：工作职能受到严重影响，业务能力显著下降且严重影响主要功能执行，出现较严重的法律问题，较高的财产损失，较大范围的社会不良影响，对其他组织和个人造成较严重损害。

24

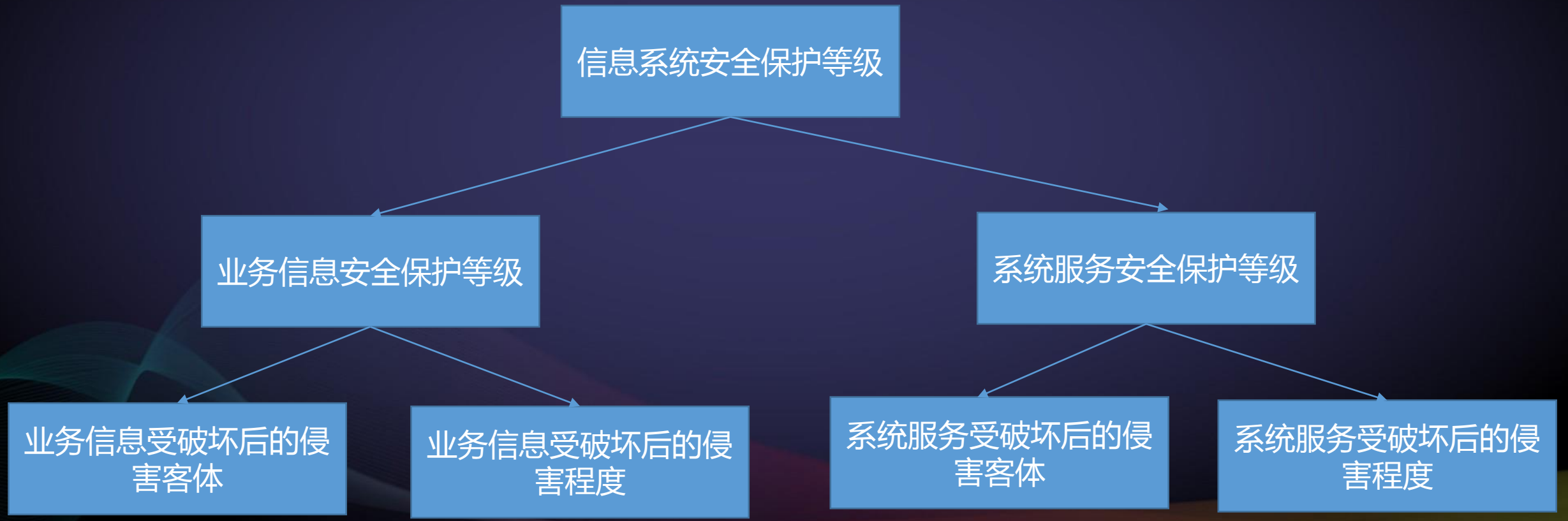
一、基本概念和定级要素

- 特别严重损害：工作职能受到特别严重影响或丧失行使能力，业务能力严重下降且或功能无法执行，出现极其严重的法律问题，极高的财产损失，大范围的社会不良影响，对其他组织和个人造成非常严重损害。

25

一、基本概念和定级要素

信息系统安全保护等级=业务信息安全保护等级+系统服务安全保护等级



一、基本概念和定级要素

侵害客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

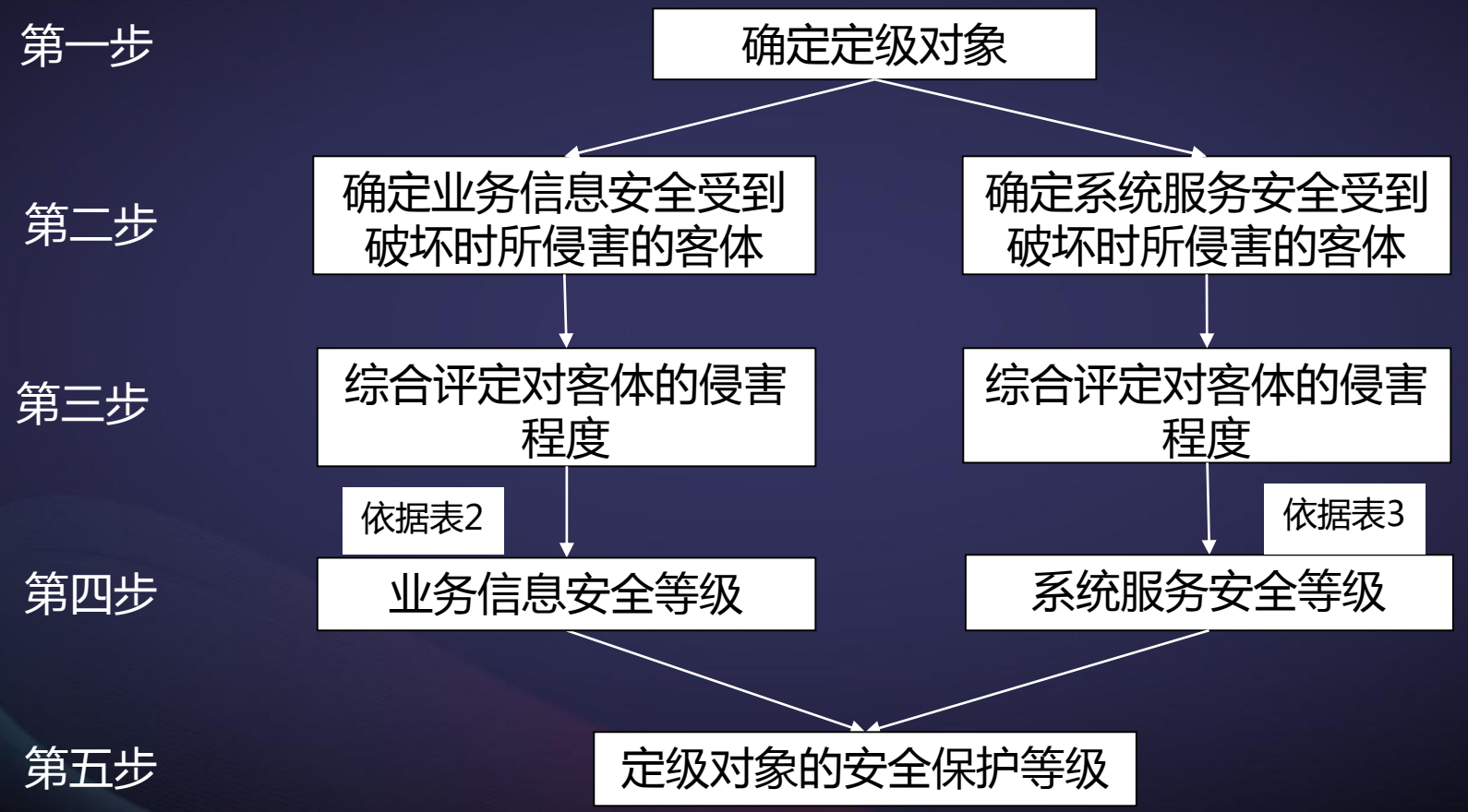
主要内容

一．基本概念和定级要素

二．定级方法

三．定级流程

二、定级方法


第一步
确定定级对象
第二步
确定业务信息安全受到破坏时所侵害的客体
确定系统服务安全受到破坏时所侵害的客体
第三步
综合评定对客体的侵害程度
综合评定对客体的侵害程度
依据表2
依据表3
第四步
业务信息安全等级
系统服务安全等级
第五步
定级对象的安全保护等级

二、定级方法

- 第一步： 确定定级对象

  定级对象应当具备以下条件：

  - 具有确定的主要安全责任主体
  - 承载相对独立的业务应用
  - 包含相互关联的多个资源

二、定级方法

确定定级对象可通过以下工作进行：

1）．系统识别和描述

- 识别基本信息
- 识别管理框架
- 识别业务种类和业务流程
- 识别信息资产
- 识别网络结构
- 识别软硬件设备
- 识别用户类型和分布

2）．信息系统划分

- 分析安全管理责任，确定管理边界
- 分析网络结构和已有内外部边界
- 分析业务流程和业务间关系
- 初步划定信息系统
- 各信息系统描述

二、定级方法

- 系统识别
  - 识别单位基本信息
  - 识别管理框架
  - 识别业务种类和业务流程
  - 识别信息
  - 识别网络结构
  - 识别主要的软硬件设备
  - 识别用户类型和分布

二、定级方法

- 系统划分
  - 分析安全管理责任，确定管理边界
  - 分析网络结构和已有内外部边界
  - 分析业务流程和业务间关系

二、定级方法

- 系统划分方法
  - 管理机构
  - 业务特点
  - 分析物理位置的差异

二、定级方法

- 第二步：确定受侵害客体
  - 业务信息受到破坏后的侵害客体
  - 系统服务受到破坏后的侵害客体
  - 多种信息和多种服务系统的处理

二、定级方法

- 第三步：确定对客体的侵害程度
  - 业务信息受到破坏后对客体的侵害程度
  - 系统服务受到破坏后对客体的侵害程度
  - 多种信息和多种服务系统的处理

二、定级方法

综合判定侵害程度 ：

- 如果受侵害客体是公民、法人或其他组织的合法权益，则以本人或本单位的总体利益作为判断侵害程度的基准。
- 如果受侵害客体是社会秩序、公共利益或国家安全，则应以整个行业或国家的总体利益作为判断侵害程度的基准。

二、定级方法

- 第四步：确定业务信息安全等级和系统服务安全等级
- 第五步：初步确定系统安全保护等级

主要内容

一．基本概念和定级要素

二．定级方法

三．定级流程

三、定级流程

1. 确定定级对象

2. 初步确定等级

3. 专家评审

4. 主管部门审核

5. 公安机关备案审查

三、定级流程

定级对象的运营、使用单位应组织信息安全专家和业务专家，对初步定级结果的合理性进行评审，出具专家评审意见。

定级对象的运营、使用单位应将初步定级结果上报行业主管部门或上级主管部门进行审核。

定级对象的运营、使用单位应按照相关管理规定，将初步定级结果提交公安机关进行备案审查。

三、定级流程

- 系统等级调整

  信息系统的决策者或上级主管部门可根据系统的特殊安全需求进行等级调整，可以参考以下因素：

  - 上级主管部门在政策和管理方面的特殊要求；
  - 预测业务数据可能会随着时间的变化从量变转化为质变；
  - 随着信息系统所承载的业务不断完善和稳定，各种业务的取消或合并；
  - 信息系统服务范围随着业务的发展，将会有较大的变化。

THANKS

敬 请 批 评 指 正

www.cspec.org.cn