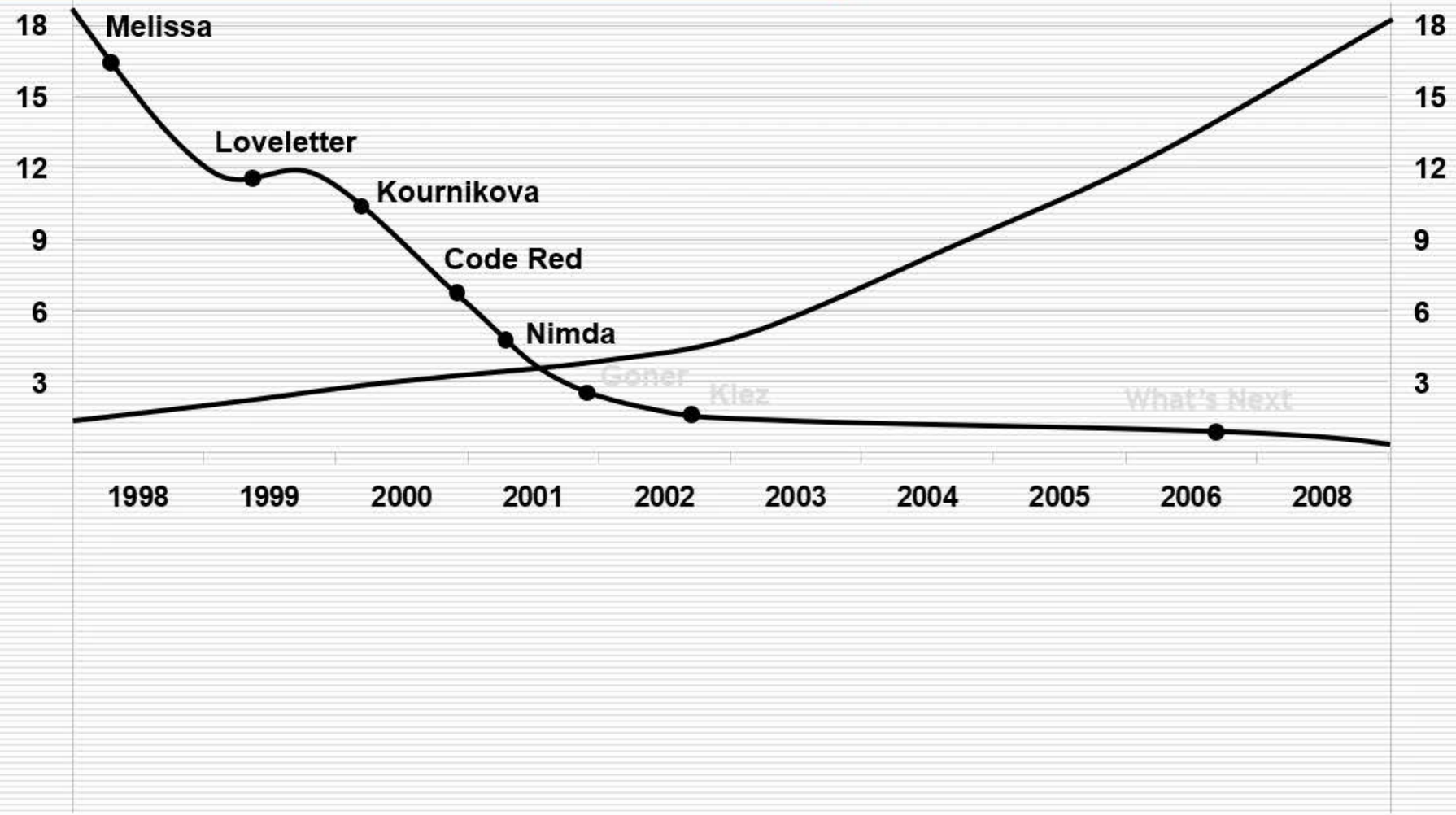
问题?

- 等级保护与经典安全体系结构、IATF?
- 对保护对象的划分和描述方法?
- 技术要求?
- 管理要求?
- 评测：等保 与等保2.0?

信息安全等级保护@@巨大挑战

感染一万台所需小时



布置对抗措施所需时间

什么是信息系统等级保护

对涉及国计民生的基础信息网络和重要信息系统按其重要程度及实际安全需求，合理投入，分级进行保护，分类指导，分阶段实施，保障信息系统安全正常运行和信息安全，提高信息安全综合防护能力。

讨论提纲

- 等级保护的法律与政策依据
- 各层次单位的等保工作职责和义务
- 等级保护工作的主要流程和基本要求
- 定级的8个步骤
- 定级后的后续工作
- 如何实施定级操作
- 如何写定级报告
- 如何备案

等级保护是国家意志的体现

- 中华人民共和国《网络安全法》
- 信息安全等级保护是国家信息安全保障工作的基本制度、基本策略、基本方法。开展信息安全等级保护工作是保护信息化发展、维护国家信息安全的根本保障，是信息安全保障工作中国家意志的体现。
- 公安部、国务院信息化工作办公室等四部门《关于信息安全等级保护工作的实施意见》66号文、《信息安全等级保护管理办法》43号文等政策文件
- 50多个国标和行标，初步形成了信息安全等级保护标准体系

各层次单位的等保工作职责和义务

1、国家层面

2、信息安全监管部门（包括公安机关、保密部门、国家密码工作部门）

3、信息系统主管部门

4、信息系统运营使用单位

5、安全服务机构

等级保护工作的职责分工

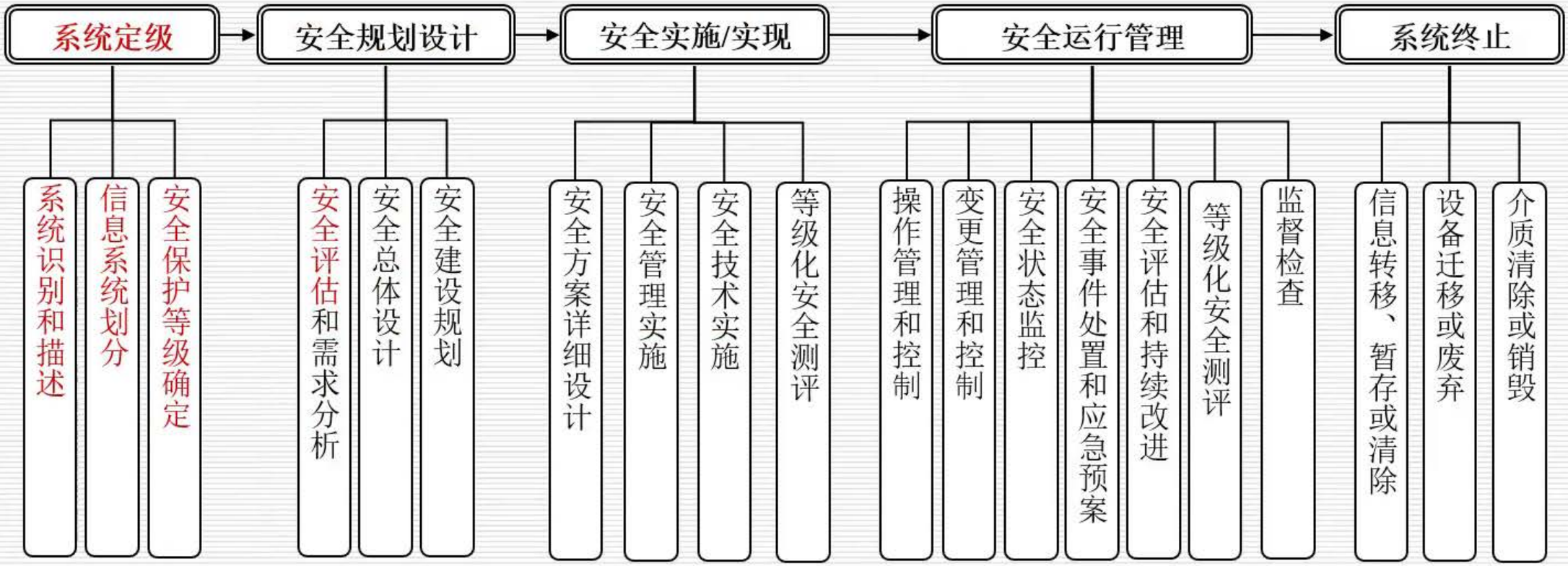
公安机关是等级保护工作的牵头部门，承担着信息安全等级保护工作的监督、检查、指导；

国家保密工作部门、国家密码管理部门负责等级保护工作中有关保密工作和密码工作的监督、检查、指导；

国信办及地方信息化领导小组办事机构负责等级保护工作部门间的协调。

其中，涉及国家秘密信息系统的等级保护监督管理工作由国家保密工作部门负责；非涉及国家秘密信息系统的等级保护监督管理工作由公安机关负责。

信息系统安全等级保护实施过程的主要活动



等级保护工作的主要流程和基本要求

主要流程包括六项内容：

一是自主定级与审批。

二是评审。

三是备案。

四是系统安全建设。

五是等级测评。

六是监督检查。

开展等级保护工作的总体要求

- 各基础信息网络和重要信息系统，按照**“准确定级、严格审批、及时备案、认真整改、科学测评”**的要求完成等级保护的定级、备案、整改、测评等工作 。
- 公安机关和保密、密码工作部门要及时开展监督检查，严格审查信息系统所定级别，严格检查信息系统开展备案、整改、测评等工作。
- 对故意将信息系统安全级别定低，逃避公安、保密、密码部门监管，造成信息系统出现重大安全事故的，要追究单位和人员的责任。

定级工作的主要步骤

定级是等级保护工作的首要环节，是开展信息系统建设、整改、测评、备案、监督检查等后续工作的重要基础。

第一步，摸底调查，掌握信息系统底数

第二步，确定定级对象

第三步，初步确定信息系统等级

第四步，信息系统等级评审

定级工作的主要步骤

第五步，信息系统等级的最终确定与审批

第六步：备案。

第七步：备案审核。

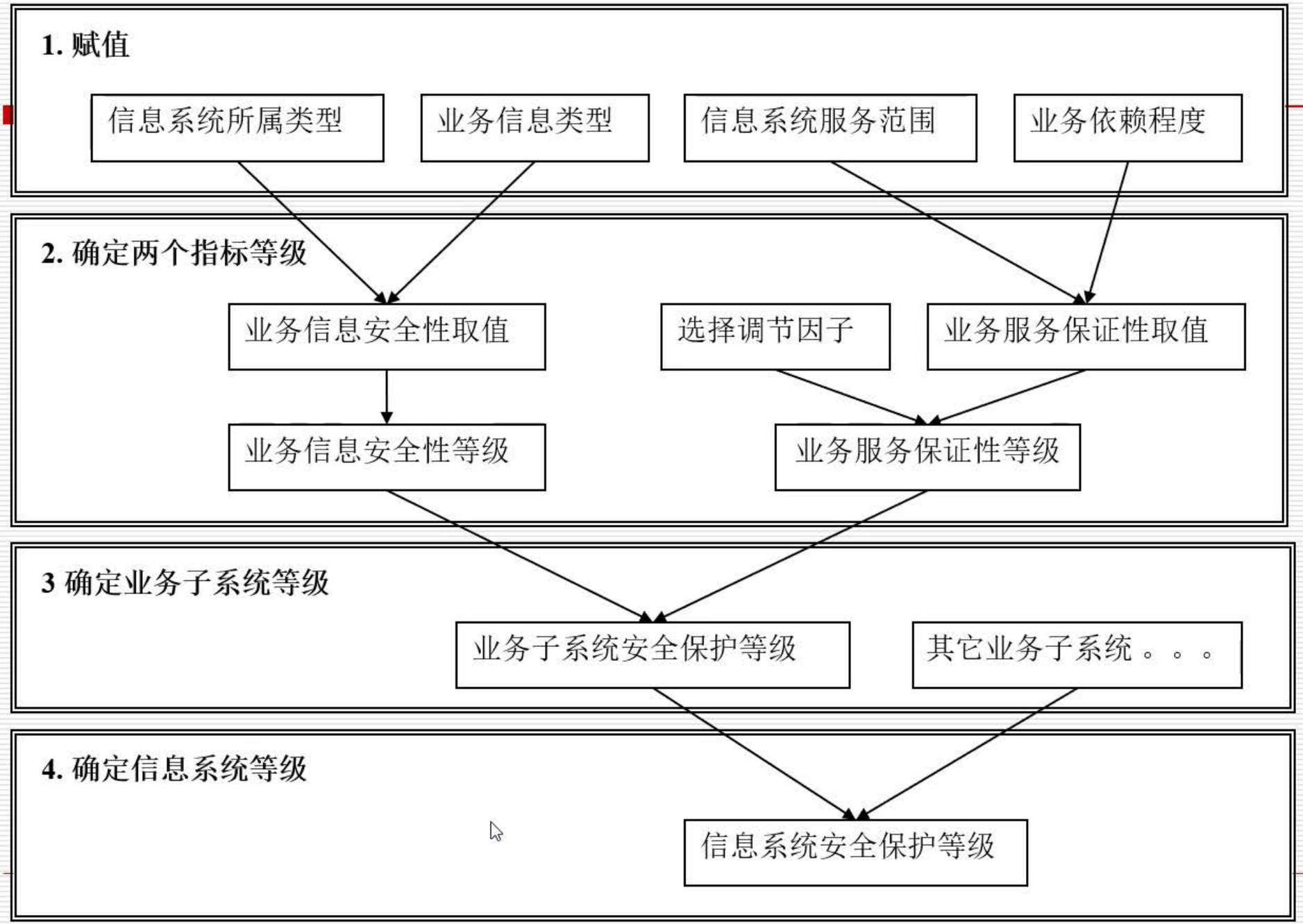
第八步：及时总结并提交总结报告。

安全保护等级的划分

业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
	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	第二级
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

五级监管

等级	对象	侵害客体	侵害程度	监管强度
第一级	一般系统	合法权益	损害	自主保护
第二级		合法权益	严重损害	指导
		社会秩序和公共利益	损害	
第三级	重要系统	社会秩序和公共利益	严重损害	监督检查
		国家安全	损害	
第四级		社会秩序和公共利益	特别严重损害	强制监督检查
		国家安全	严重损害	
第五级	极端重要系统	国家安全	特别严重损害	专门监督检查



定级工作完成后需要开展哪些工作

一是开展安全建设和整改。

二是开展等级测评。

三是开展自查。

依据的主要标准

1、基础标准－划分准则（**GB17859**）
2、基线标准－ 《信息系统安全等级保护基本要求》
3、辅助标准－定级指南、实施指南、测评准则
4、目标标准－
《信息系统通用安全技术要求》（**GB/T20271**）
《网络基础安全技术要求》（**GB/T20270**）
《操作系统安全技术要求》（**GB/T20272**）
《数据库管理系统安全技术要求》（**GB/T20273**）
《终端计算机系统安全等级技术要求》（**GA/T671**）
《信息系统安全管理要求》（**GB/T20269**）
《信息系统安全工程管理要求》（**GB/T20282**）
5、产品标准－防火墙、入侵检测、终端设备隔离部件等