高等院校网络空间安全专业实战化人才培养系列教材

郭启全　丛书主编

网络安全检测评估技术与方法

袁　静　郭启全　苏艳芳　王李乐
张德馨　刘　健　高亚楠　杨晓琪　编著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书共7章，围绕“网络安全检测评估技术与方法”这一主题，系统介绍网络安全相关的基本概念、组织开展、工作要求、测评流程和方法、测评具体实施方法以及具体实例。其中，第1章概括性介绍网络安全检测评估基础知识，包括网络安全检测评估概述，各类检测评估之间的关系、发展过程等。第2章介绍网络安全等级保护测评，包括等级保护测评组织开展时涉及各方的职责，等级保护测评的要求、流程和方法、各个控制点的安全要求、测评要点、测评实施步骤，等级测评结果分析和问题整改建议编制方法。第3章介绍关键信息基础设施安全测评内容，包括关基测评工作的组织、工作要求、基本工作流程和方法，以及测评实施等。第4章介绍网络安全风险评估的组织开展、工作要求、方法流程等内容，包括不同角色的工作内容、信息系统生命周期各阶段开展风险评估的工作要点、各流程环节的实施方式等。第5章介绍数据安全检测评估内容，包括合规评估的组织开展、工作要求、流程和方法、实施、结果分析、整改建议以及有关行业领域的评估实例等。第6章介绍商用密码应用安全性评估，包括商用密码应用安全性评估工作的组织开展、评估依据和原则、流程、实施和方法、以及问题整改建议等。第7章介绍网络安全测评技术与工具，包括在等级保护测评、关键信息基础设施安全测评、风险评估、商用密码应用安全性评估中常用的网络安全测评技术与工具，涵盖漏洞扫描、渗透测试、代码安全审计和协议分析等。

本书是高等院校网络空间安全专业实战化人才培养系列教材之一，可作为网络空间安全专业的专业课教材，适合网络空间安全专业、信息安全专业以及相关专业的大学生、研究生系统学习，也适合各单位各部门从事网络安全工作者、科研机构和网络安全企业的研究人员阅读。

图书在版编目（CIP）数据

网络安全检测评估技术与方法 / 袁静等编著. 北京 : 电子工业出版社, 2025. 7. -- ISBN 978-7-121-50082-4

Ⅰ. TP393.08

中国国家版本馆CIP数据核字第20255Y6Q99号

责任编辑：桑　昀　　文字编辑：叶文涛
印　　刷：
装　　订：
出版发行：电子工业出版社
　　北京市海淀区万寿路173信箱　邮编：100036
开　　本：787×1 092　1/16　印张：22.5　字数：576千字
版　　次：2025年7月第1版
印　　次：2025年7月第1次印刷
定　　价：69.00元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

本书咨询联系方式：（010）88254554，luy@phei.com.cn。

高等院校网络空间安全专业
实战化人才培养系列教材

编委会

序 FOREWORD

在数字化智慧化高速发展的今天，网络和数据安全的重要性愈发凸显，直接关系到国家政治、经济、国防、文化、社会等各个领域的安全和发展。网络空间技术对抗能力是国家整体实力的重要方面，面对日益复杂的网络安全威胁和挑战，按照“打造一支攻防兼备的队伍，开展一组实战行动，建设一批网络与数据安全基地”的思路，培养具有实战化能力的网络安全人才队伍，已成为国家重大战略需求。

一、培养网络安全实战化人才的根本目的

在网络安全“三化六防”（实战化、体系化、常态化；动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控）理念的指引下，网络安全业务越来越贴近实战。实战行动和实战措施都离不开实战化人才队伍的支撑。培养网络安全实战化人才的根本目的，在于培养一批既具备扎实的理论基础，又掌握高新技术和前沿技术、具备攻防技术对抗能力，还能灵活运用各种技术措施和手段，应对各种网络安全威胁的高素质实战化人才，打造“攻防兼备”和具有网络安全新质战斗力的队伍，支撑国家网络安全整体实战能力的提升。

二、培养网络安全实战化人才的重大意义

习近平总书记强调：“网络空间的竞争，归根结底是人才竞争”，“网络安全的本质在对抗，对抗的本质在攻防两端能力较量”。要建设网络强国，必须打造一支高素质的网络安全实战化人才队伍。我国网络安全人才特别是实战化人才严重缺乏，因此，破解难题，从网络安全保卫、保护、保障三个方面加强实战化人才教育训练，已成为国家重大战略需求。

当前，国家在加快推进数字化智慧化建设，本质是打造数字化生态，而数字化建设面临的最大威胁是网络攻击。与此同时，国家网络安全进入新时代，新时代网络安全最显著的特征是技术对抗。因此，新时代要求我们要树立新理念、采取新举措，从网络安全、数据安全、人工智能安全等方面，大力培养实战化人才队伍，加强“网络备战”，提升队伍的技术对抗和应急处突能力，有效应对新威胁和新技术带来的新挑战，为国家经济发展保驾护航。

三、构建新型网络安全实战化人才教育训练体系

为全面提升我国网络安全领域的实战化人才培养能力和水平，按照“理论支撑技术、技术支撑实战”的理念，创新高等院校及社会差异化实战人才培养的思路和方法，建立新型实战化人才教育训练体系。遵循“问题导向、实战引领、体系化设计、督办落实”四项原则，认真落实“制定实战型教育训练体系规划、建设实战型课程体系、建设实战型师资队伍、建设实战型系列教材、建设实战型实训环境、以实战行动提升实战能力、创新实战

型教育训练模式、加强指导和督办落实”八项重大措施，形成实战化人才培养的“四梁八柱”，有力提升网络安全人才队伍的新质战斗力。

四、精心打造高等院校网络空间安全专业实战化人才培养系列教材

在有关部门的大力支持下，具有 20 多年网络安全实战经验的资深专家统筹规划和整体设计，会同 20 多位部委、高等院校、科研机构、大型企业具有丰富实战经验和教学经验的专家学者，共同打造了 14 部技术先进、案例鲜活、贴近实战的高等院校网络空间安全专业实战化人才培养系列教材，由电子工业出版社出版，以期贡献给读者最高水平、最强实战的网络安全重要知识、核心技术和能力，满足高等院校和社会培养实战化人才的迫切需要。

网络安全实战化人才队伍培养是一项长期而艰巨的任务，按照教、训、战一体化原则，以国家战略为引领，以法规政策标准为遵循，以系统化措施为抓手，政府、高校、企业和社会各界应共同努力，加快推进我国网络安全实战化人才培养，为筑梦网络强国、护航中国式现代化贡献我们的智慧和力量！

郭启全

前言 PREFACE

面对当前日益严峻和复杂的网络安全形势，各类机构面临着前所未有的挑战。无论是政府机构还是企事业单位，都可能成为网络攻击的目标，导致数据泄露、服务中断、经济损失甚至威胁国家安全和社会稳定。在这种环境下，建立一套科学严谨、实时有效的网络安全检测评估体系尤为重要。网络安全检测评估对于保护运营者的网络安全、满足法律法规要求、评估自身安全状况以及应对新型网络攻击等方面都具有重要意义，是运营者了解自身网络安全状况，防患于未然，保护网络免受恶意攻击和数据泄露的重要手段，也是网络运营者满足法律法规和行业准则的必然要求。通过网络安全检测评估，可以及时发现网络中存在的安全漏洞和风险，找出存在的安全隐患，从而采取相应的措施进行整改和防护，降低损失甚至避免损失，确保网络系统的安全稳定运行。

进入新时代，网络安全最显著的特征是技术对抗，应树立新理念，采取新举措，立足有效应对大规模网络攻击，认真落实“实战化、体系化、常态化”和“动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控”的“三化六防”措施，按照“打造一支攻防兼备的队伍，开展一组实战行动，建设一批网络与数据安全基地”这条主线，加强战略谋划和战术设计，建立完善网络安全综合防御体系，大力提升综合防御能力和技术对抗能力。从创新角度出发，按照“理论支撑技术、技术支撑实战”的理念，加强理论创新和技术突破，实施“挂图作战”；从“打造一支攻防兼备的队伍”出发，创新高等院校和企业差异化网络安全人才培养思路和方法，建立实战化人才教育训练体系，加强教育训练体系规划，强化课程体系、师资队伍、系列教材、实训环境建设和培养模式创新，培养网络安全实战型人才。

为了满足培养网络安全实战型人才的需要，郭启全组织成立编委会，共同编著高等院校网络空间安全专业实战化人才培养系列教材，包括《网络安全保护制度与实施》《网络安全建设与运营》《网络空间安全技术》《网络安全威胁情报分析与挖掘技术》《数字勘查与取证技术》《恶意代码分析与检测技术》《漏洞挖掘与渗透测试技术》《网络安全事件处置与追踪溯源技术》《人工智能安全治理与技术》《数据安全管理与技术》《商用密码应用技术》《网络安全检测评估技术与方法》《网络空间安全导论》《恶意代码分析与检测技术实验指导书》。郭启全统筹规划和整体设计全套教材，组织具有丰富网络安全实战经验和教学经验的专家学者撰写这套高等院校网络空间安全专业教材，并对内容严格把关，以期贡献给读者最高水平、最强实战的网络安全、数据安全、人工智能安全等重要知识。

本书共 7 章，主要介绍网络安全检测评估的发展过程、种类；网络安全等级保护测评；关键信息基础设施安全测评；网络安全风险评估；数据安全检测评估；商用密码应用安全性评估工作的组织开展、要求、流程和方法、测评实施以及测评结果分析；网络安全

测评用到的具体技术与工具等。本书第 1 章由苏艳芳、袁静、王李乐、高亚楠、张德馨、刘健编写，第 2 章由苏艳芳编写，第 3 章由袁静编写，第 4 章由高亚楠编写，第 5 章由张德馨编写，第 6 章由刘健编写，第 7 章由王李乐编写。全书由郭启全统稿。

书中不足之处，敬请读者指正。

作者

目录 CONTENTS

第 3 章

关键信息基础设施安全测评

第 4 章

网络安全风险评估

第 1 章 网络安全检测评估概述

本章介绍网络安全检测评估的概念，各类网络安全检测评估之间的关系以及网络安全检测评估的发展过程，使读者对安全检测评估技术有初步了解和掌握。

1.1 网络安全检测评估概念

网络安全检测评估是现代信息化社会中不可或缺的关键环节，它在保障网络安全、数据安全、信息资产安全、防范网络安全风险、提升网络系统防护能力等方面发挥着至关重要的作用。

1. 法律法规对网络安全检测评估的要求

网络安全检测评估的概念和要求在国内外不同的法律、法规和标准中均有提及，如在《中华人民共和国网络安全法》中明确规定，网络运营者应当对其网络的安全性和可能存在的风险进行定期检测评估，并规定关键信息基础设施运营者的特殊保护义务，其中包括每年至少进行一次网络安全检测评估；在网络安全等级保护系列标准中详细阐述了不同安全保护等级的保护对象应达到的安全管理和技术要求，其中包含了系统建设、运行过程中的安全检测以及评估内容等。

2. 网络安全检测评估的目的

网络安全检测评估是指根据国家相关法律法规、政策标准和技术规范，对网络系统的安全性进行全面、系统和科学的检查、测试、分析和评价的过程。这一过程旨在识别网络系统的潜在安全威胁、脆弱性、风险及安全管理缺陷，并据此提出改进措施与建议，使网络和信息系统及其承载数据的保密性、完整性和可用性不受破坏。网络安全检测评估涵盖了从硬件设施到软件应用，从技术防御机制到管理策略的全方位审查与测定。网络安全检测评估旨在确保网络运营者能够及时发现并处理潜在的网络安全威胁，以保障网络系统的稳定运行和数据的安全存放。

（1）在技术层面，网络安全检测评估通过定期漏洞扫描、渗透测试以及恶意代码检测等手段，能够全面发现并量化系统存在的各种脆弱性，这些脆弱性可能源于操作系统、数据库、网络设备、应用程序等不同层面，及时识别并修复它们是预防和抵御潜在攻击的第

一道防线。在管理层面，网络安全检测评估可通过核查制度体系、组织架构、人员管理、建设管理和运维管理等方面，发现组织在管理层面是否具备有效的决策支持机制、合理的资源配置、严谨的流程管控，以及对网络安全风险的主动识别、应对和持续改善能力。

（2）威胁建模与风险评估是网络安全检测评估的核心组成部分。通过对组织面临的内外部威胁源进行分析，并结合业务连续性和数据重要性等因素，计算出潜在的安全风险等级，有助于制定有针对性的安全策略和控制措施，确保资源分配合理且有效应对高风险场景。

（3）合规性也是网络安全检测评估的重要考量因素，根据国家法律法规及标准要求，如《中华人民共和国网络安全法》《关键信息基础设施安全保护条例》等，网络运营者需要对自身的系统进行全面的安全审计，确保其运营行为符合监管规定，降低因违规操作带来的法律风险和声誉损失。

（4）网络安全检测评估还强调了应急响应能力和持续改进的重要性，通过模拟演练、实战攻防测试等方式检验机构的应急预案和处置流程，找出短板并加以改进，以增强面对突发网络安全事件时的快速反应能力和恢复能力。

总之，网络安全检测评估是一个动态而持续的过程，它不仅关注当下系统的安全状态，更着眼于未来安全环境的变化与发展，旨在为构建安全稳固的网络空间提供科学依据和技术支撑，从而切实维护国家安全、社会稳定以及公民个人隐私权益不受侵犯。

3. 网络安全检测评估的种类

目前国内最常见的网络安全检测评估主要包括：网络安全等级保护测评、关键信息基础设施安全测评、商用密码应用安全性评估、数据安全检测评估、网络安全风险评估、技术检测等。

（1）网络安全等级保护测评，是指测评机构依据国家网络安全等级保护制度规定，按照有关管理规范和技术标准，对已定级备案的非涉及国家秘密的网络（含信息系统、数据资源等）的安全保护状况进行检测评估的活动。网络安全等级保护测评工作是网络安全等级保护工作的重要环节，是专门机构对网络开展的一种专业性、服务性的检测活动。

（2）关键信息基础设施安全测评，是指针对国家关键信息基础设施所进行的系统性、规范性和专业性的安全性评估活动。旨在确保关键信息基础设施的安全防护能力达到国家规定的标准和要求，能够有效抵御各种网络安全威胁，保障其正常运行，并防止对国家安全、社会稳定、经济秩序和个人隐私造成严重威胁和影响。

（3）商用密码应用安全性评估，是指对网络和信息系统中采用的商用密码技术、产品和服务集成建设的环境，从合规性、正确性和有效性三个维度进行深入且系统的评估过程。其核心目的是确保在实际应用中，密码技术能够按照国家法律法规和技术标准要求正确使用，有效抵御各种安全威胁，保障数据的安全传输、存储和处理。

（4）数据安全检测评估，是指对数据的安全问题、隐患和风险进行检测评估的活动，用于确定与数据相关的安全风险。数据安全检测评估关注的是数据在采集、存储、处理、

传输和销毁过程中的全生命周期的安全性。它需要综合运用网络安全等级保护测评和密码应用安全性评估的结果，对数据全生命周期的安全进行评估。通常数据安全检测评估包括数据安全合规评估、数据安全风险评估、数据安全检测评估认证、数据出境评估等不同类型的评估。

（5）网络安全风险评估主要关注网络系统面临的各种安全风险，通常作为单独的评估项目开展，采用定性和定量相结合的方法，分析网络威胁利用系统脆弱性的可能性和严重程度，探究系统、业务面临的风险状况。同时，网络安全风险评估也可为其他检测评估提供评估方法。

（6）技术检测是指运用技术手段对网络系统进行检测，并发现潜在的安全隐患和漏洞的过程。它是实现网络安全等级保护测评、关键信息基础设施安全测评等的基础性工作，为其他评估提供技术支持。

1.2 各类网络安全检测评估的关系

网络安全等级保护测评、关键信息基础设施安全测评、商用密码应用安全性评估、数据安全检测评估、风险评估和技术检测是相互关联而又各有侧重的检测评估活动。其中网络安全等级保护测评是基础；关键信息基础设施安全测评、商用密码应用安全性评估和数据安全检测评估是重点；而风险评估又为网络安全等级保护测评、关键信息基础设施安全测评、商用密码应用安全性评估、数据安全检测评估中发现的安全风险进行分析和评价提供支撑；技术检测是实现网络安全等级保护测评、关键信息基础设施安全测评、商用密码应用安全性评估、数据安全检测评估、风险评估的基础性工作，为其他评估提供技术支持。总之，它们共同构建了全面的网络安全检测评估体系，在这个体系中，各种评估方法相互支撑，共同作用于提升网络和信息安全防护能力，确保国家网络空间的安全与稳定。

1.2.1 关键信息基础设施安全测评与网络安全等级保护测评

关键信息基础设施安全测评是针对关键信息基础设施开展的网络安全测评，与网络安全等级保护测评存在着必然联系，但在测评目的、测评依据、测评范围、测评性质、测评内容、测评结果等方面也存在较大差异。

从联系上来看，关键信息基础设施一般由一个或多个网络系统构成，这些网络系统均依据网络安全等级保护制度要求开展了网络安全等级保护测评。因此，关键信息基础设施安全测评应在网络安全等级保护测评的基础上开展，复用网络安全等级保护测评结果。

从区别上来看，主要有以下几方面。

1. 关键信息基础设施安全测评的目的是确定关键信息基础设施的安全保护水平，及其运营者的网络安全管控能力是否满足国家网络安全的要求，发现其现存的或潜在的影响

国家网络安全的风险；而网络安全等级保护测评的目的是确定网络系统是否满足相应安全保护等级要求。

2. 关键信息基础设施安全测评依据的是 GB/T 39204—2022《信息安全技术 关键信息基础设施安全保护要求》和行业要求；而网络安全等级保护测评依据的是 GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》。

3. 关键信息基础设施安全测评的测评范围是关键信息基础设施及其运营者；而网络安全等级保护测评的测评范围是网络系统。

4. 关键信息基础设施安全测评是以网络安全等级保护测评为基础的网络安全风险和能力判定的测评；而网络安全等级保护测评是标准符合性的合规测评。

5. 关键信息基础设施安全测评重心在于分析面临的安全威胁及发现安全问题，分析威胁及问题带来的安全风险，用于运营者提升安全保护水平和能力，同时也为关键信息基础设施安全保护主管部门、保护工作部门的监管工作提供依据；而网络安全等级保护测评结果可以展现出与 GB/T 22239—2019《网络安全等级保护基本要求》相应等级要求的符合程度，用于提升运营者网络系统安全防护能力，也为网络安全等级保护主管部门的监管工作服务。

1.2.2 商用密码应用安全性评估与网络安全等级保护测评

商用密码应用安全性评估与网络安全等级保护测评是我国网络安全领域两个紧密相关但又各有侧重点的概念。《中华人民共和国密码法》第二十七条规定：“商用密码应用安全性评估应当与关键信息基础设施安全检测评估、网络安全等级测评制度相衔接，避免重复评估、测评”。这项法律规定决定了商用密码应用安全性评估与网络安全等级保护测评的衔接关系。GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》聚焦于 GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》中为密码应用安全留出的接口，形成二者既相互补充，又可相互独立实施的格局。

1. 商用密码应用安全性评估与网络安全等级保护测评的联系

从联系上看，商用密码应用安全性评估和网络安全等级保护测评之间存在着密不可分的关系，密码技术被广泛认为是维护网络与信息安全的重要手段，在进行网络安全等级保护测评过程中，对密码应用进行安全性评估是确保整个网络和信息系统符合国家安全标准的基础工作之一，特别是在保护数据传输和存储过程中的机密性、完整性和可用性方面发挥着举足轻重的作用。从一致性进行分析，主要体现在以下几个方面。

（1）对象一致性：网络安全等级保护测评与商用密码应用安全性评估的测评对象都是已定级的网络和系统。

（2）过程一致性：网络安全等级保护测评与商用密码应用安全性评估都分为四个阶段，包括测评准备、方案编制、现场测评、分析与报告编制。

（3）测评方法一致性：在测评方法上两者都是通过人员访谈、文档核查和安全测试等方式对进行测评，并且两者在身份鉴别、数据传输和存储等一些测评内容方面有所交集。

2. 商用密码应用安全性评估与网络安全等级保护测评的区别

从区别上看，主要有以下几方面。

（1）商用密码应用安全性评估主要聚焦于评估网络和信息系统中使用的商用密码产品或密码服务的合规性、正确性、有效性，是保护网络和信息系统密钥管理、数据加解密、身份认证及数据完整性等方面至关重要的部分；网络安全等级保护测评涵盖了网络和系统的全方位安全，主要关注网络和信息系统整体的安全防护情况。

（2）测评指标：网络安全等级保护测评依据 GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》，商用密码应用安全性评估依据 GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》，两者的测评指标要求不同，具有差异性。

（3）测评结论：网络安全等级保护测评与商用密码应用安全性评估的分值计算依据不同的公式，且分数合格线不同，网络安全等级保护测评 70 分为合格，商用密码应用安全性评估 60 分为合格。网络安全等级保护测评结论分为优、良、中、差，商用密码应用安全性评估的测评结论则分为符合、基本符合、不符合。

1.2.3　数据安全检测评估与其他评估

数据安全检测评估用于确定与数据相关的安全风险。通常数据安全检测评估包括数据安全合规评估、数据安全风险评估、数据安全检测评估认证、数据出境评估等不同类型的评估。网络安全检测评估对象主要包括网络和系统（含数据资源），而数据安全检测评估重点是围绕数据进行评估，包括数据本身、数据处理活动以及其他相关事项，但是数据的载体离不开承载其的网络和系统。数据安全检测评估与其他检测评估之间的关系主要如下。

1. 与网络安全等级保护测评的关系：在进行网络安全等级保护测评时，数据安全是其中的核心组成部分之一，涵盖了数据的保密性、完整性等方面的要求。因此，在等级保护测评的过程中，会包括对数据安全防护措施的有效性、合规性等方面的评估。

2. 与商用密码应用安全性评估的关系：商用密码应用安全性评估主要关注的是密码技术在系统中的应用安全性，尤其是数据加密环节。数据安全检测评估也会涉及数据加密策略、密码产品和密码服务的应用情况，以确保数据在传输和存储过程中的安全性。

3. 与关键信息基础设施安全测评的关系：关键信息基础设施安全测评更加侧重于国家关键领域如能源、交通、通信等行业的信息安全保障，这些领域的系统往往承载着大量敏感和重要的数据，因此其数据安全检测评估是至关重要的部分；在进行关键信息基础设施安全测评时，不仅需要考虑系统整体的安全状况，也要深入到数据层面，确保关键数据得到充分的保护。

4. 与技术检测的关系：技术检测通常是对特定系统的安全漏洞、配置错误、恶意软件等内容进行扫描或审计的过程，更多地偏向于实时性和技术性的排查。而数据安全检测评估除了包含技术检测的动作外，还可能涉及数据生命周期管理、数据分类分级、数据主体权益保护、法律法规遵循等多个非技术层面的考量。

总之，数据安全检测评估是在各类网络安全保障体系中不可或缺的一环，与其他检测评估相辅相成，共同构成了一个立体化、全方位的网络安全保障体系。同时，数据安全检测评估也因其自身的特殊性，有时作为独立模块，有时融合在其他安全检测评估活动中，确保组织机构的数据安全管理水平与法律及行业规范要求保持一致。

1.2.4 网络安全风险评估与其他评估

网络安全风险评估主要关注网络系统面临的各种安全风险，包括技术风险、管理风险、人员风险等，通常作为单独的评估项目开展，采用定性和定量相结合的方法，分析网络威胁利用系统脆弱性的可能性和严重程度，探究系统、业务面临的风险状况。同时，网络安全风险评估也可为其他检测评估提供评估方法。网络安全等级保护测评、关键信息基础设施安全测评、数据安全检测评估、商用密码应用安全性评估通常基于风险评估方法进行风险分析和评价。

总之，网络安全风险评估是其他检测评估活动的基础，它帮助组织了解风险敞口，进而有针对性地开展各类具体的检测评估和控制活动；而其他类型的检测评估则是网络安全风险评估的具体实施手段，通过它们的结果，组织可以不断调整和优化风险应对策略，形成风险管理的闭环。

1.2.5 技术检测与其他评估

技术检测主要是指在网络安全风险评估、网络安全等级保护测评、商用密码安全性评估及关键基础设施（关基）安全测评中常用的方法和工具。特别是漏洞扫描和渗透测试，它们在网络安全风险评估和网络安全等级保护测评中发挥着重要作用，用于识别安全风险，验证网络安全防护措施的有效性。在商用密码应用安全性评估中，协议分析是主要的测评方法之一，是用于对密码系统中采用的算法、协议、参数等的分析和评估。在关基设施安全测评中，通过对关基业务链的渗透测试，从攻击者视角评估关基的安全风险，检验关基的保护措施是否落实到位。

1.3 网络安全检测评估的发展过程

网络安全检测评估是一个不断演进的过程，它随着技术进步、威胁环境变化以及政策法规的要求不断发展和完善，在全球范围内经历了多个阶段的发展，每个阶段都标志着该领域的深入和成熟。

1. 早期孤立与初步发展阶段

在 20 世纪 80 年代及以前，网络安全检测评估主要依赖于零散的、独立的安全测试方

法，如简单的漏洞扫描工具和系统审计。由于互联网普及度不高，安全问题相对有限，评估活动大多由个别组织或机构根据自身需求进行，缺乏统一的标准和流程。

2. 标准化与普及阶段

20 世纪 90 年代初至 21 世纪初，随着网络技术广泛应用和网络安全威胁增加，网络安全检测评估开始走向标准化。例如，美国国防部在 TCSEC（Trusted Computer System Evaluation Criteria）的基础上发展出了信息技术安全通用评估准则 CC（Common Criteria），为全球范围内信息安全产品和服务提供了一个国际认可的评估框架。

3. 集成化与专业化阶段

进入 21 世纪，随着入侵检测系统（IDS）、入侵防御系统（IPS）等技术兴起，网络安全检测评估从单纯的设备配置检查转变为包括实时监控、异常行为分析在内的综合评估体系。同时，出现了专门针对特定领域的安全评估标准和技术，如 Web 应用安全评估、数据库安全评估等。

4. 风险管理导向阶段

随着风险管理理念的深入人心，网络安全风险评估成为网络安全检测的核心部分。企业开始采用更全面的风险管理框架，通过结合资产识别、威胁建模、脆弱性分析以及现有控制措施的有效性评估，以量化风险并制定相应的风险管理策略。

5. 自动化与智能化阶段

近年来，随着云计算、大数据和人工智能技术的发展，网络安全检测评估更加依赖自动化工具和平台，实现持续监测和快速响应。此外，机器学习和人工智能驱动的智能分析能力也被引入到网络安全评估中，这样能够更快地发现未知威胁和模式，并进行预测性防护。

6. 法规政策推动下的规范化阶段

近年来，随着网络安全的重要性日益凸显，各国政府逐步出台严格的法律法规。如中国自 2007 年以来执行的网络等级保护制度；2016 年颁布的《中华人民共和国网络安全法》正式将网络安全等级保护写入法律，并且明确了关键信息基础设施运营者应定期进行网络安全检测评估；2019 年颁布的《中华人民共和国密码法》要求关键信息基础设施运营者对商用密码应用的合规性、正确性和有效性进行安全性评估，并且与关键信息基础设施安全检测评估、网络安全等级保护测评制度相衔接，以避免重复评估和测评；2021 年颁布的《中华人民共和国数据安全法》中明确规定重要数据处理者应当按照规定对其数据处理活动定期开展风险评估。这些法律法规的颁布也推动着相关的网络安全检测评估进入规范化阶段。

1.4 网络安全检测评估种类

依据评估对象、关注重点、评估内容等的不同，网络安全检测评估可以划分为以下类别。

根据检测评估对象不同，网络安全检测评估分为网络安全等级保护测评、关键信息基础设施安全测评和数据安全检测评估。其中，网络安全等级保护测评面向网络安全网络系统，关键信息基础设施安全测评面向关键信息基础设施，数据安全检测评估面向各类别、各级别数据。

根据检测评估关注重点的不同，网络安全检测评估分为商用密码应用安全性评估、网络安全风险评估、数据安全检测评估、漏洞扫描、代码安全审查，以及协议分析。其中，商用密码应用安全性评估关注密码应用安全性，网络安全风险评估关注风险分析，数据安全检测评估关注数据全生命周期安全，漏洞扫描关注设备和底层系统脆弱性，代码安全审查关注编码安全，协议分析关注协议安全。

根据检测评估内容的不同，可以划分为仅针对技术方面开展的检测评估以及涵盖技术和管理两个方面的检测评估。其中，技术和管理方面均涵盖的检测评估包括网络安全等级保护测评、网络安全风险评估、关键信息基础设施安全测评、数据安全检测评估、商用密码应用安全性评估，仅针对技术方面开展的检测评估包括漏洞扫描、渗透测试、代码安全审查和协议分析等。

习　题

1. 简述网络安全检测评估的概念。
2. 网络安全检测评估的目的是什么？
3. 常见的网络安全检测评估有哪些？
4. 简述各类网络安全检测评估的基本含义。
5. 简述各类网络安全检测评估之间的关系。