山东省网络安全工程职称考试知识大纲

网络安全技术研发与应用—中级

2025 年版

目 录

第一篇 公共知识

第一章 习近平总书记关于网络强国的重要思想

党的十八大以来，习近平总书记站在人类历史发展、党和国家事业全局高度，从信息化发展大势和国内国际大局出发，重视互联网、发展互联网、治理互联网，统筹推进网络安全和信息化工作，提出一系列具有开创性意义的新理念新思想新战略，系统回答了为什么要建设网络强国、怎样建设网络强国的一系列重大理论和实践问题，形成了内涵丰富、科学系统的习近平总书记关于网络强国的重要思想，为做好新时代网络安全和信息化工作指明了前进方向、提供了根本遵循。习近平总书记关于网络强国的重要思想主要体现在重要讲话、重要指示批示精神中，广大网络安全工程专业技术人员须深入学习领会、全面系统掌握。

第二章 网信领域法律法规

第一节 法律

一、《中华人民共和国网络安全法》

1. 掌握网络安全等级保护制度、监测预警和信息通报制度有关内容
2. 掌握网络产品、服务提供者及网络运营者义务
3. 掌握关键信息基础设施运行安全、网络安全事件应急预案相关内容
4. 理解违反网络安全保护义务的情形及其法律责任
5. 理解国家网信部门与行业主管机构的监管分工

二、《中华人民共和国数据安全法》

1. 掌握数据相关概念
2. 掌握数据分类分级制度
3. 掌握数据处理者义务及相关法律责任

4. 掌握数据处理活动风险评估有关内容

5. 了解数据出境安全管理要求

6. 了解政务数据的开放共享与保密义务

三、《中华人民共和国个人信息保护法》

1. 掌握处理个人信息的有关要求

2. 掌握个人信息跨境提供的规则

3. 理解个人在个人信息处理活动中的权利

4. 掌握个人信息处理者的义务及相关法律责任

5. 理解个人信息保护工作的责任部门及其保护职责

第二节 行政法规

一、《网络数据安全管理条例》

1. 掌握网络数据处理者处理个人信息的有关要求

2. 掌握重要数据处理者的网络数据安全保护责任

3. 掌握网络数据处理者向境外提供个人信息和重要数据的有关要求

4. 理解网络平台服务提供者的义务

5. 了解国家职能部门在网络数据安全监督管理方面的职责分工

二、《中华人民共和国计算机信息系统安全保护条例》

1. 掌握计算机信息系统的安全保护制度

2. 掌握计算机信息系统使用者的义务及其法律责任

三、《关键信息基础设施安全保护条例》

1. 掌握关键信息基础设施的定义

2. 掌握关键信息基础设施运营者的义务

3. 理解违反本条例的行为主体应承担的法律责任

四、《计算机软件保护条例》

1. 掌握软件著作权归属认定、保护期限及软件著作权人享有的权利

2. 理解侵犯软件著作权的行为及其法律责任

第三节 部门规章

一、《网络安全审查办法》

1. 掌握申报网络安全审查的情形
2. 掌握网络安全审查的内容
3. 理解网络安全审查的程序

二、《生成式人工智能服务管理暂行办法》

1. 掌握生成式人工智能服务提供者开展训练数据处理活动应当遵守的规定
2. 掌握生成式人工智能服务提供者应当遵守的服务规范

三、《互联网信息服务算法推荐管理规定》

1. 掌握算法推荐服务提供者的义务
2. 理解算法推荐服务提供者违反本规定应承担的法律责任

四、《互联网信息服务深度合成管理规定》

1. 掌握深度合成服务提供者和技术支持者的义务
2. 理解深度合成技术

第三章 专业技术人员职业道德

1. 掌握专业技术人员职业道德的基本要求

第二篇 基础知识

第一章 计算机基础

第一节 程序设计

一、结构化程序设计

1. 掌握结构化程序设计的基本控制结构和设计原则
2. 理解结构化程序设计的优缺点

二、面向对象程序设计

1. 理解类、对象、封装、继承、多态的概念
2. 理解抽象的五个层次（函数→类→泛型→设计模式→框架）的概念及区别
3. 理解类与方法的定义及关系，以及构造函数的概念
4. 理解实例方法、静态方法的概念及区别
5. 了解消息传递的过程
6. 了解实例化、初始化的过程及区别
7. 掌握继承与多态的实现方式及区别
8. 理解静态行为与动态行为的概念及区别

第二节 数据结构

一、基本概念

1. 理解数据、数据元素、数据结构的概念及区别
2. 理解程序性能分析涉及的主要性能指标、分析方法、优化策略
3. 掌握时间复杂度与空间复杂度的概念，了解其计算方法
4. 掌握常用排序算法的概念及其应用

二、线性结构

1. 理解线性表的概念、主要类型，了解其基本操作
2. 理解堆栈与队列的概念、区别，了解其应用场景
3. 了解跳表的概念、基本操作，了解其应用场景
4. 掌握散列表（哈希表）的概念、冲突解决方法，了解其应用场景

三、树与二叉树

1. 理解树、二叉树的概念及区别
2. 理解完全二叉树、满二叉树的概念
3. 掌握二叉树第 i 层最多节点数计算方法
4. 掌握二叉树前序、中序、后序的实现方法及区别

5. 了解树、二叉树的应用场景

四、图

1. 理解图的概念、分类及主要存储结构
2. 掌握图深度优先、广度优先遍历的实现方法及区别
3. 了解图的应用场景

第三节 操作系统

一、基本概念

1. 理解操作系统的定义与五大核心功能

二、进程管理

1. 理解进程的概念、特点及其与程序的区别
2. 理解进程的五种状态及转换
3. 了解进程操作原语
4. 掌握进程调度算法（FCFS、SJF、轮转法）
5. 掌握死锁的必要条件及解决方法
6. 理解线程的概念及其与进程的区别

三、存储管理

1. 理解存储管理的概念和主要分配策略（分区、分页、分段）
2. 掌握虚拟内存概念和实现方式
3. 掌握页面置换算法（FIFO、LRU、OPT）

四、文件管理

1. 理解文件管理的概念
2. 理解系统的目录结构（树形、层次）

五、设备管理

1. 理解设备管理的概念
2. 理解 I/O 控制方式（轮询、中断、DMA）的工作原理

六、云操作系统

1. 了解云操作系统的概念和特点

2. 了解分布式系统的概念和特点

3. 理解虚拟化、容器化的概念

第四节 数据库

一、关系数据库

1. 理解数据模型的概念及数据模型三要素

2. 理解概念模型（E-R 模型）的概念及设计方法

3. 掌握关系概念模型及组成要素（关系、元组、属性、域、候选键、主键、外键等）的概念

4. 理解数据库设计的六个步骤

（1）需求分析（2）概念结构设计（3）逻辑结构设计

（4）物理结构设计（5）数据库实施（6）数据库运行与维护

5. 掌握数据库索引的作用及创建、修改、显示、删除索引的方法

6. 了解代数优化与物理优化的基本原理，理解其实现步骤

7. 理解事务的概念和特性

8. 掌握数据定义、数据操纵、数据控制 SQL 语句的使用

二、非关系数据库

1. 理解非关系数据库的概念及特点

2. 理解非关系数据库的分类，了解其应用场景

3. 掌握键值存储数据库 Redis 的插入、查询、更新、删除操作方法

4. 理解列族存储数据库 Hbase 的插入、查询、更新、删除操作方法

第五节 计算机硬件基础

一、计算机系统结构基础

1. 理解计算机系统的五个层次结构

2. 掌握计算机系统的五大功能部件，了解其基本工作原理

3. 结合对计算机系统工作原理的理解，了解主流服务器相关硬件参数及适

用场景

二、数据表示与运算

1. 掌握原码、反码、补码的转换规则

2. 理解定点数与浮点数基本概念，了解 IEEE 754 的存储格式及运算方法（加减乘除）

三、指令系统

1. 理解 CPU 主要组成和基本工作原理

2. 理解指令格式和指令执行的基本过程

3. 了解指令流水的概念、分类及其特点

4. 掌握中断的基本概念及其基本工作过程

四、存储系统

1. 理解计算机存储系统的层次结构

2. 了解存储器的主要类型

第二章 密码学基础

一、密码学概述

1. 了解密码学概念

2. 掌握密码学的分类

（1）按时间分类：古典密码、现代密码

（2）按密钥分类：受限制的算法、基于密钥的算法

（3）按密码体制分类：对称密码体制、非对称密码体制

（4）按明文处理方法分类：分组密码、流密码

二、加密技术

1. 了解古典密码学、对称密码算法、非对称密码算法、哈希算法、散列函数（MD5 算法）、数字签名技术

2. 了解软件与硬件加密技术

三、PKI 概述

1. 掌握 PKI 的概念及作用

2. 掌握 PKI 的组成部分

（1）PKI 安全策略（2）公钥技术（3）数字证书

（4）CA（颁发机构）（5）RA（注册机构）

3. 理解常见的 PKI 证书 X.509 的内容

4. 掌握数字证书的签发流程

四、国密算法与商密算法

1. 了解国密算法、商密算法的概念

2. 理解国密算法 SM1、SM2、SM3、SM4、SM7、SM9、祖冲之密码算法的作用

3. 理解常用商密算法的作用

第三篇 专业知识

第一章 软件工程及项目管理

第一节 软件工程

一、软件工程概述

1. 理解软件的定义

2. 掌握软件生命周期

3. 理解软件工程的定义

4. 了解软件危机

二、软件过程模型

1. 掌握瀑布模型原理及其特点

2. 理解增量模型原理及其特点

3. 理解螺旋模型原理及其特点

4. 理解原型模型原理及其特点

5. 掌握敏捷模型原理及其特点

三、需求工程

1. 了解需求工程的发展、内容和特点

2. 掌握需求工程的主要活动

（1）需求获取（2）需求分析（3）形成需求规格

（4）需求确认与验证（5）需求管理

3. 理解软件需求分析层次

（1）业务需求（2）用户需求（3）系统功能需求（4）系统非功能需求

四、系统分析与设计

1. 了解系统分析与设计的目标、意义和范围

2. 掌握 UML 的用例图、时序图、活动图和类图的表示方法

3. 掌握面向对象分析的层次、活动、基本原则和步骤

4. 掌握面向对象设计的内涵、类型（实体类、边界类和控制类）和步骤

5. 理解软件架构的概念

6. 掌握软件架构视图方法

（1）逻辑视图（2）物理视图（3）开发视图（4）过程视图

五、软件测试

1. 理解软件测试阶段

（1）单元测试（2）集成测试（3）系统测试（4）验收测试

2. 掌握软件测试类型

静态测试：（1）桌前检查（2）代码走查（3）代码审查

动态测试：（1）黑盒测试（功能测试）（2）白盒测试（结构测试）

第二节 软件项目管理

一、项目管理概述

1. 了解项目管理的发展历史、目标

2. 理解软件项目进度、配置、质量和风险管理的主要内容

3. 理解项目管理成熟度模型

（1）软件能力成熟度模型 CMM

（2）组织级项目管理成熟度模型 OPM3

（3）项目管理成熟度模型 K-PMMM

（4）软件能力成熟度集成模型 CMMI

二、单个项目的管理过程

1. 了解项目整体管理的含义、作用

2. 理解项目整体管理过程

3. 理解项目单个项目管理的其它方法

三、信息系统安全管理

1. 掌握信息系统安全策略

2. 了解信息系统安全工程

3. 理解信息系统安全管理流程

（1）风险评估（2）策略制定（3）实施控制

（4）监控与审计（5）持续改进

4. 了解信息安全管理体系的国际标准 ISO/IEC 27001

第二章 计算机网络与网络安全技术

第一节 计算机网络

一、计算机网络基本知识

1. 掌握计算机网络定义和主要功能，了解计算机网络发展历史

2. 掌握局域网、广域网和城域网的概念及区别

3. 了解星型、总线型、环型等常见拓扑结构及其优缺点

4. 掌握计算机网络协议与标准的概念，了解网络协议的三个要素

二、数据通信基础知识

1. 掌握有线（如双绞线、光纤）和无线（如微波、卫星）等各类传输介质及其优缺点

2. 掌握传输速率和带宽的概念，掌握传输速率的计算方式

三、网络体系结构

1. 掌握 OSI、TCP/IP 网络参考模型，理解两种参考模型的区别及联系

2. 掌握 OSI 七层模型中物理层的概念，了解信道极限容量及信道最大传输速率

3. 掌握 OSI 七层模型中数据链路层的概念，了解停等协议和连续 ARQ 协议、滑动窗口协议

4. 掌握 OSI 七层模型中介质访问控制子层的概念，了解动态多路访问控制协议、数据链路层的交换技术

5. 掌握 OSI 七层模型中网络层的概念，了解常用路由协议和拥塞控制算法，掌握 IP 协议并了解 IPv4 和 IPv6 的区别，能够利用 IP 地址（IPv4）进行子网划分

6. 掌握 OSI 七层模型中传输层的概念，了解拥塞控制算法和 TCP、UDP 协议

四、计算机网络应用

1. 掌握局域网设计的基本原则和方法

2. 了解交换机和路由器的基本配置命令

3. 掌握网络地址转换（NAT）的工作原理

4. 了解网络应用协议中的超文本传输协议（HTTP）、文件传输协议（FTP）、简单邮件传输协议（SMTP）工作原理

5. 了解网络服务与管理中的域名系统（DNS）、动态主机配置协议（DHCP）、网络管理协议（SNMP）工作原理

6. 掌握网络服务搭建与配置，主要包括常见的 Web 服务器（如 Apache、IIS）的搭建和配置方法、FTP 服务器的搭建和配置方法、邮件服务器的搭建和配置方法

第二节 网络安全监测

一、入侵检测技术

1. 理解入侵检测的概念，了解入侵检测系统的基本模型和工作模式

2. 掌握基于主机、网络的入侵检测系统和分布式入侵检测系统的工作原理

3. 掌握异常检测、误用检测和入侵响应等入侵检测机制和技术

4. 了解入侵检测系统的部署位置选择及考虑因素

5. 了解新兴技术（如深度学习、人工智能等）在入侵检测领域的应用前景及潜在影响

二、入侵防御技术

1. 理解基于主机、网络入侵防御系统的原理

2. 掌握入侵防御常见的系统功能

（1）实时监视和拦截攻击（2）虚拟补丁（3）保护客户端

（4）协议异常检测（5）Web 应用防护（6）流量安全防护

（7）应用识别和控制

3. 掌握入侵防御系统常见的关键技术

（1）原始数据包分析（2）IP 分片重组技术（3）TCP 状态检测技术

（4）TCP 流重组技术（5）SA 应用识别技术（6）DDoS 防范技术

4. 掌握入侵防御系统具体工作流程

（1）安全策略匹配（2）报文重组（3）应用协议识别和解析

（4）签名匹配（5）响应处理

三、漏洞扫描技术

1. 理解漏洞扫描的定义及原理，并掌握以下内容：

（1）漏洞扫描关键技术：端口扫描、智能爬虫、白盒测试、破解字典

（2）漏洞扫描策略：基于网络的扫描、基于主机的扫描

（3）漏洞扫描流程：目标发现、信息攥取、漏洞检测

2. 了解交换机、路由器、防火墙等网络设备常见漏洞，了解网络设备常见的扫描技术

3. 了解操作系统的常见漏洞，了解操作系统常见安全扫描技术

4. 了解数据库的常见漏洞，了解数据库漏洞常见扫描技术

5. 了解 Web 常见的安全漏洞，了解 Web 漏洞常见扫描方法

6. 掌握常见漏洞扫描工具 Nmap、Nessus 和 OpenVAS 的使用方法

7. 掌握漏洞扫描结果的解读和分析

第三节 防火墙

一、防火墙的基本知识

1. 了解防火墙的作用及功能

2. 了解防火墙的分类方法：

（1）按软、硬件形式分类：软件防火墙、硬件防火墙

（2）按防火墙技术分类：包过滤型防火墙、应用代理型防火墙

（3）按防火墙结构分类：单一主机防火墙、路由器集成式防火墙、分布式防火墙

二、防火墙技术

1. 了解基础防火墙中的包过滤技术、状态检测技术、网络地址转换技术（NAT）、代理服务技术的原理

2. 掌握 Web 防火墙、工控防火墙等特定领域防火墙技术的基本原理

3. 了解下一代防火墙技术（NGFW）和深度包检测技术等新型防火墙技术

三、防火墙网络部署

1. 理解防火墙部署的基本步骤

（1）需求分析（2）选择防火墙设备（3）规划网络拓扑

（4）配置防火墙策略（5）测试和优化（6）监控和维护

2. 理解影响防火墙选择的因素

3. 理解访问控制列表（ACL）、网络地址转换（NAT）、虚拟专用网络（VPN）等防火墙配置策略

第四节 渗透技术

一、渗透测试概述

1. 了解渗透测试的目的

2. 理解渗透测试的原则

（1）标准性原则（2）规范性原则（3）可控性原则

（4）整体性原则（5）最小影响原则（6）保密性原则

二、渗透测试方法及流程

1. 了解渗透测试常用方法，掌握应用漏洞扫描、用户名和密码猜解、SQL 注入漏洞挖掘、越权访问利用等四种渗透测试方法

2. 了解常用渗透测试工具，掌握信息收集工具和漏洞扫描工具

（1）信息收集工具：端口扫描工具、目录枚举工具、网络监听工具等

（2）漏洞扫描工具：网站漏洞扫描工具、系统层漏洞扫描工具等

3. 掌握策划、设计、执行、总结、评审等互联网渗透测试流程

第五节 网络安全管理

一、网络安全概述

1. 了解威胁网络安全的主要因素，掌握可用性、机密性、完整性、不可抵赖性等网络空间安全特性

2. 了解恶意程序、安全漏洞、拒绝服务攻击等三种网络安全威胁的概念、产生的原因

3. 掌握网络攻击的主要步骤和常见形式，掌握拒绝服务攻击、病毒防范策略

二、网络监控软件

1. 了解网络监控软件的目标

（1）有效防止员工通过网络以各种方式泄密

（2）防止并追查重要资料、机密文件的外泄渠道

（3）实现对网络计算机及网络资源的统一管理和有效监控

2. 理解网络监控软件的监听模式和网关模式

3. 了解 Sniffer 的作用，掌握 Sniffer 软硬件两种形式

4. 掌握 Sniffer Pro 软件及其使用方法

三、操作系统安全

1. 了解计算机安全评价的国际通用准则（CC 标准）

2. 理解我国信息安全评价的用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级、访问验证保护级的内容

3. 掌握安全操作系统的基本特征

（1）最小特权原则（2）自主访问控制

（3）安全审计功能（4）安全域隔离功能

4. 理解 Windows、Linux 以及常见国产操作系统在安全功能、认证机制和文件系统安全等方面的异同

四、计算机病毒

1. 掌握计算机病毒的定义和计算机病毒的特点

2. 掌握按照存在媒体、传染方法、病毒破坏能力等计算机病毒的分类方式

3. 掌握木马病毒和蠕虫病毒的概念、特点以及防治方法

4. 理解常规病毒的检测技术

（1）程序和数据完整性检测（2）病毒特征码检测

（3）启发式规则病毒检测（4）实时网络流量检测

（5）异常流量分析检测

五、网络安全等级保护 2.0 标准

1. 了解等级保护 1.0、等级保护 2.0 的发展历程

2. 理解等级保护 2.0 特点

3. 掌握等级保护一至五级的划分

（1）自主保护级（2）指导保护级（3）监督保护级

（4）强制保护级（5）专控保护级

第三章 网信技术发展趋势

一、零信任网络架构

1. 了解零信任网络架构的概念

2. 理解零信任网络架构的理念

（1）以身份为中心（2）环境感知

（3）动态的权限控制（4）严格的业务安全访问控制

二、可信网络架构

1. 了解可信网络架构的概念

2. 理解可信网络架构的特征

（1）网络中的行为总是可以预知与可控的

（2）网络内的系统符合指定的安全策略并且安全策略是可信安全的

（3）随着端点系统的动态接入，具备动态扩展性

三、移动互联网

1. 理解 5G 移动互联网的概念

2. 掌握 5G 移动互联网的特点

（1）高速率（2）低时延（3）大连接（4）低功耗（5）高安全性

3. 了解 6G 网络的基本原理

四、物联网与云计算

1. 了解云计算、物联网的概念和架构

2. 理解云计算服务的主要类型，即 IaaS、PaaS 和 SaaS

3. 理解物联网的应用及相关的安全风险

4. 理解云、边、端一体化架构及安全问题

五、区块链

1. 了解区块链的概念

2. 理解区块链的系统架构

（1）数据层（2）网络层（3）共识层

（4）激励层（5）合约层（6）应用层

3. 理解区块链的公有链、联盟链、私有链的概念及安全问题

六、人工智能

1. 了解神经网络、深度学习、大模型等概念

2. 了解国内外主流生成式人工智能大模型及其特点，了解智能体的概念

3. 了解人工智能赋能网络安全应用

4. 了解人工智能催生的新型网络空间安全风险

七、量子密码技术

1. 了解量子技术的量子计算、量子通信、量子与人工智能算法的概念

2. 了解量子密码技术的概念

3. 了解量子密码的应用，包括量子密钥分发、量子安全直接通信等

4. 了解量子技术为网络空间安全技术发展带来的影响

八、国产替代及信创技术

1. 了解信创技术对国家安全的重要意义
2. 了解芯片、操作系统、数据库、中间件等国产主流信创产品的名称、特点
3. 了解相关国产网络安全设备的种类、功能