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—初级

2022 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，以习近平同志为核心的党中央从进行具有许多新的历史特点的伟大斗争出发，重视互联网、发展互联网、治理互联网，统筹协调涉及政治、经济、文化、社会、军事等领域网络安全和信息化重大问题，作出一系列重大决策、实施一系列重大举措，推动我国网信事业取得历史性成就，走出一条中国特色治网之道。习近平同志围绕网络强国建设发表一系列重要论述，提出一系列新思想新观点新论断，为新时代网信事业发展提供了根本遵循。广大网络安全工程专业技术人员须学习、理解、掌握习近平同志关于网络强国的重要论述。

参考书目：《习近平关于网络强国论述摘编》

第二章 网信领域法律法规

第一节 法律

1. 掌握：《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》

2. 了解：《全国人民代表大会常务委员会关于加强网络信息保护的决定》《全国人民代表大会常务委员会关于维护互联网安全的决定》《中华人民共和国密码法》《中华人民共和国电子商务法》《中华人民共和国电子签名法》

第二节 政策法规

1. 掌握：《关键信息基础设施安全保护条例》《信息网络传播权保护条例》《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》《互联网信息服务管理办法》

2. 了解：《计算机软件保护条例》《中华人民共和国计算机信息系统安全保

护条例》《互联网上网服务营业场所管理条例》《外商投资电信企业管理规定》《计算机信息网络国际联网安全保护管理办法》《中华人民共和国计算机信息网络国际联网管理暂行规定》

第三节 部门规章

1. 掌握：《网络安全审查办法》《网络信息内容生态治理规定》《互联网新闻信息服务管理规定》《互联网用户账号信息管理规定》

2. 了解：《互联网信息服务算法推荐管理规定》《互联网信息内容管理行政执法程序规定》《区块链信息服务管理规定》《互联网文化管理暂行规定》《互联网视听节目服务管理规定》《互联网等信息网络传播视听节目管理办法》《儿童个人信息网络保护规定》《电信和互联网用户个人信息保护规定》《汽车数据安全管理若干规定（试行）》《互联网域名管理办法》《网络出版服务管理规定》《外国机构在中国境内提供金融信息服务管理规定》《规范互联网信息服务市场秩序若干规定》

第四节 司法解释

1. 了解：《最高人民法院 最高人民检察院〈关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释〉》《最高人民法院〈关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定〉》《最高人民法院 最高人民检察院〈关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释〉》《最高人民法院〈关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定〉》《最高人民法院 最高人民检察院〈关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释〉》《最高人民法院 最高人民检察院〈关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释（二）〉》

第五节 规范性文件

1. 掌握：《互联网用户公众账号信息服务管理规定》《云计算服务安全评估办法》《互联网新闻信息服务单位内容管理从业人员管理办法》《网络音视频信息服务管理规定》《微博客信息服务管理规定》《互联网群组信息服务管理规定》《互联网跟帖评论服务管理规定》《互联网论坛社区服务管理规定》《互联网直播服务管理规定》《移动互联网应用程序信息服务管理规定》《互联网信息搜索服务管理规定》《互联网新闻信息服务单位约谈工作规定》《互联网新闻信息服务新技术新应用安全评估管理规定》《互联网新闻信息服务许可管理实施细则》《互联网用户账号名称管理规定》《即时通信工具公众信息服务发展管理暂行规定》

2. 了解：《国家互联网信息办公室关于开展境内金融信息服务报备工作的通知》《常见类型移动互联网应用程序必要个人信息范围规定》《互联网危险物品信息发布管理规定》

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 专业知识

第一章 网络安全数学基础

第一节 概率论与数理统计

一、概率论的基本概念

1. 掌握概率、条件概率的概念，并会简单计算

二、随机变量及其分布

1. 理解随机事件的独立性和随机变量的独立性

2. 掌握乘法公式、全概率公式、贝叶斯公式，并会简单应用

3. 掌握随机变量分布函数的概念，掌握连续型随机变量的密度函数和离散

型随机变量的分布列

4. 理解常见分布及其简单性质

（1）两点分布（2）二项分布（3）泊松分布

（4）均匀分布（5）正态分布（6）指数分布

三、随机变量的数字特征

1. 理解数学期望、方差（标准差）、相关系数的概念，并会简单计算

2. 了解多元随机变量的概念，掌握多元正态分布

3. 理解统计量、样本均值、样本方差（标准差）的概念，并会简单计算

四、参数估计

1. 理解点估计的概念，了解点估计的无偏性、相合性

第二节 密码学

一、密码学概述

1. 了解密码学发展史、密码学概念

二、密码学分类

1. 了解密码学的分类

（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）

三、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. 理解软件与硬件加密技术

四、PKI 概述

1. 了解 PKI 的作用、体系结构

2. 理解 PKI 的组成部分

（1）公钥技术（2）数字证书（3）CA（颁发机构）（4）RA（注册机构）

3. 了解常见的 PKI 证书 X.509 和 PKCS（公钥加密标准）等系列标准

五、数字证书

1. 掌握数字证书的概念、签发流程

六、认证机构的功能

1. 了解 CA 系统的组成、CA 的现状及应用

第二章 计算机软件基础知识

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概念
2. 理解结构化程序设计优缺点

二、面向对象程序设计

1. 掌握面向对象程序设计优缺点
2. 理解抽象的 5 个层次

（1）函数（2）类（3）泛型（4）模式（5）框架

3. 理解类和方法
4. 理解消息、实例和初始化
5. 了解继承和多态

第二节 数据结构

一、数据结构的基本概念

1. 掌握数据、数据元素、数据结构的概念
2. 理解程序性能分析的概念，了解时间复杂性与空间复杂性的分析方法

二、线性表

1. 掌握线性表的概念
2. 理解堆栈、队列、跳表和散列的描述方法与应用

三、树

1. 了解树和二叉树的概念
2. 掌握二叉树的性质

3. 理解二叉树的前序、中序、后序遍历

四、图

1. 了解有向图、无向图的概念
2. 掌握图的表示（矩阵、列表）
3. 理解图的遍历（深度优先遍历、广度优先遍历）
4. 理解有向图的拓扑排序

第三节 操作系统

一、操作系统概念

1. 掌握操作系统的概念

二、操作系统的五大功能（进程管理、存储管理、文件管理、设备管理、作业管理）

1. 掌握进程概念，理解进程调度、同步及死锁处理
2. 了解存储管理的原理，掌握内存管理策略和虚拟内存管理
3. 了解文件管理的概念
4. 了解设备管理的概念
5. 了解作业管理的概念

第四节 数据库

一、关系数据库的基本知识

1. 掌握关系模型概念和 SQL 语言
2. 掌握关系数据库设计方法

（1）数据库需求分析（2）概念结构设计（3）逻辑设计（4）物理设计

3. 理解关系数据库索引的概念和使用方法

（1）索引创建（2）索引修改（3）索引显示（4）索引删除

4. 理解关系数据库查询处理方法

（1）查询分析（2）查询检查（3）查询优化（4）查询执行

5. 理解关系数据库查询优化方法

（1）代数优化（2）物理优化

6. 掌握关系数据库事务概念

7. 了解关系数据库事务调度方法

（1）可串行调度（2）不可串行调度

8. 了解数据库并发控制技术

（1）事务串行执行（2）交叉并发方式（3）同时并发方式

二、非关系数据库的基本知识

1. 了解非关系数据库背景

2. 了解非关系数据库分类

（1）键值存储　　（2）文档数据库

（3）分布式数据库（列式数据库）（4）图形数据库

第三章 计算机硬件基础知识

第一节 计算机体系结构

一、计算机系统结构基础

1. 了解计算机体系结构的基本概念

2. 掌握计算机体系结构的主要部件，理解其基本工作原理

（1）输入设备（2）输出设备（3）存储器（4）运算器（5）控制器

二、指令系统结构

1. 了解计算机指令集结构

2. 理解通用寄存器型指令集结构的分类（寄存器—寄存器型结构、寄存器—存储器型结构、存储器—存储器型结构）及特点

三、流水线技术

1. 掌握流水线的基本概念、分类（部件功能级流水线、处理机级流水线、处理机间级流水线）及特点

2. 了解指令级并行的概念

第二节 计算机组成原理

一、计算机组成概述

1. 了解计算机总线的基本概念

2. 掌握计算机存储器分类及分级结构

（1）按存储介质可以分类为：半导体存储器、磁表面存储器、光存储器

（2）按存储器的读写功能可以分类为：只读存储器、 随机读写存储器

（3）按信息的可保存性可以分类为：非永久记忆的存储器、永久记忆性存储器

（4）按在计算机系统中的作用可以分类为：主存储器、辅助存储器、缓冲存储器

3. 了解计算机外部设备

二、数据的表示与运算

1. 掌握计算机中有符号数和无符号数、定点数和浮点数的表示方法

2 掌握移位运算、补码加减法、补码移位乘除法运算方法及其原理

三、指令系统

1. 掌握计算机指令的基本结构

（1）操作码（2）操作数

2. 掌握数据常见的寻址方式

（1）立即寻址 （2）直接寻址 （3）隐含寻址

（4）间接寻址 （5）寄存器寻址（6）基址寻址

3. 掌握 CPU 的功能和组成

（1）寄存器（2）运算器（3）控制器（4）时钟

4. 了解指令流水

5. 了解中断系统

第四章 软件工程及项目管理

第一节 软件工程

一、软件工程的概念及其生命周期

1. 掌握软件、软件工程、软件生命周期等概念

二、软件需求分析

1. 掌握软件需求分析层次

需求分析层次：业务需求、用户需求、系统需求（功能需求、非功能需求）

2. 了解质量功能部署（QFD）的概念

3. 了解软件需求获取、分析、验证

4. 理解统一建模语言（UML）

5. 了解面向对象分析（OOA）

6. 了解需求分析的其它方法

三、软件架构设计

1. 理解软件结构化设计

2. 理解面向对象软件设计

3. 了解软件架构评估方式

4. 了解软件架构模型

四、软件测试及其管理

1. 掌握软件测试的方法

（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：桌前检查、代码走查、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 软件过程管理

一、软件工程的过程管理

1. 了解能力成熟度模型集成（CMMI）

2. 了解阶段式模型

3. 了解连续式模型

二、软件配置管理

1. 了解软件配置相关概念

三、软件的质量管理及其评估

1. 理解软件质量管理概念

2. 理解软件常见评估方法

（1）外部度量（2）内部度量

第三节 项目管理

一、项目管理的理论与体系

1. 了解项目管理基础知识

2. 掌握项目管理知识体系的构成

（1）知识领域：项目整体管理、项目范围管理、项目进度管理、项目成本管理、项目质量管理、项目人力资源管理、项目沟通管理、项目风险管理、项目采购管理、项目干系人管理

（2）过程组：启动过程组、规划过程组、执行过程组、监控过程组、收尾过程组

3. 了解 IPMP/PMP、PRINCE2 等项目管理认证体系

4. 了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

5. 了解项目管理的量化方法

二、组织结构对项目的影响

1. 了解组织结构对项目的影响

三、信息系统项目典型生命周期模型

1. 掌握瀑布模型及其瀑布模型基础上改进的模型

2. 了解原型化模型

3. 了解敏捷开发模型

四、单个项目的管理过程

1. 掌握项目整体管理的含义、作用

2. 了解项目整体管理过程

五、信息系统安全管理

1. 理解信息系统安全策略

2. 了解信息安全系统工程

3. 了解 PKI 公开密钥基础设施

4. 了解 PMI 权限（授权）管理基础

5. 了解信息系统安全管理其它方法

第五章 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. 了解计算机网络的发展历史

2. 理解计算机网络的分类、网络拓扑结构

计算机网络分类：

（1）按照网络作用范围分类：广域网、城域网、局域网、个人区域网

（2）按照网络的使用者分类：公用网、专用网

二、网络体系结构构成

1. 掌握 OSI、TCP/IP 网络参考模型

2. 了解物理层的概念，了解信道极限容量及信道最大传输速率、模拟传输和数字化传输的物理层标准

3. 了解数据链路层的概念，了解停等协议和连续 ARQ 协议、滑动窗口协议、检错和纠错机制

4. 了解介质访问控制子层的概念，了解动态多路访问控制协议，以太网，无线局域网，数据链路层的交换技术

5. 了解网络层的概念，了解常用路由协议、拥塞控制算法，服务质量，网络互连，IP 协议，子网掩码

6. 了解传输层的概念，了解传输层路由协议，TCP，UDP，拥塞控制算法

7. 了解应用层的概念，DNS，邮件系统，www，流音频与视频

第二节 网络安全监测

一、入侵检测技术

1. 了解入侵检测的概念、入侵检测系统结构

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. 了解入侵检测系统的基本模型，理解入侵检测系统的工作模式

二、入侵防御技术

1. 了解入侵防御的系统功能

（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 （8）IPv6 及隧道检测（9）策略管理

（10）知识库和引擎升级 （11）设备集中管理 （12）故障监控

（13）集中软件管理 （14）系统监控 （15）日志和报表

2. 了解基于主机的入侵防御系统、基于网络的入侵防御系统、应用入侵防御系统的原理

3. 理解入侵防御系统关键技术

（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

（7）入侵防护技术 （8）应用管理技术 （9）高级威胁防御技术

三、漏洞扫描技术

1. 了解漏洞扫描的定义及原理，理解漏洞扫描的关键技术、漏洞扫描的策略和流程

漏洞扫描关键技术：

（1）端口扫描 （2）智能爬虫（3）白盒测试 （4）破解字典

漏洞扫描策略：

（1）基于网络的扫描（2）基于主机的扫描

漏洞扫描流程：

（1）目标发现 （2）信息攥取（3）漏洞检测

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

网络设备常见漏洞：

（1）防火墙漏洞 （2）交换机漏洞 （3）路由器漏洞

（4）网关设备漏洞（5）手机设备漏洞（6）网络摄像头漏洞

网络设备常见扫描技术：

（1）主机存活扫描技术（2）规避技术（3）端口扫描技术

（4）服务及系统指纹　（5）指纹技术

3. 了解操作系统的常见漏洞，理解操作系统常见安全扫描技术

操作系统常见漏洞：

（1）权限许可和访问控制漏洞　（2）信息泄露漏洞

（3）远程代码执行漏洞　（4）安全绕过漏洞

（5）GDI 组件信息泄露漏洞　（6）Kernel API 权限提升漏洞

（7）Kernel 本地信息泄露漏洞　（8）Server Message Block 权限提升漏洞

（9）输入验证漏洞　（10）WPAD 服务权限提升漏洞

（11）快捷方式漏洞　（12）SMB 协议漏洞

（13）UNIX 操作系统漏洞　（14）Linux 操作系统漏洞

操作系统常见扫描技术：

（1）ping 扫描（2）操作系统探测技术（3）端口扫描技术

4. 了解数据库的常见漏洞，理解数据库漏洞常见扫描技术

数据库常见漏洞：

（1）网络攻击的安全问题　（2）数据库引擎的安全问题

（3）内存存储对象的安全问题（4）SQL 编程组件的安全问题

数据库常见扫描技术：

（1）智能端口发现技术　（2）漏洞库的匹配技术

5. 了解 Web 常见的安全漏洞，理解 Web 漏洞常见扫描方法

Web 常见漏洞：

（1）注入　（2）失效的身份认证和会话管理

（3）跨站脚本（XSS）　（4）失效的访问控制

（5）安全配置错误　（6）敏感信息泄露

（7）攻击检测与防护不足　（8）跨站请求伪造

（9）使用含有已知漏洞的组件（10）未受有效保护的 API

Web 漏洞常见扫描方法：

（1）注入漏洞扫描　　（2）失效的身份认证和会话管理漏洞扫描

（3）跨站脚本漏洞扫描　　（4）失效的访问控制漏洞扫描

（5）安全配置错误漏洞扫描　　（6）敏感信息泄露漏洞扫描

（7）应对攻击防护不足漏洞扫描（8）跨站请求伪造漏洞扫描

（9）使用含有已知漏洞的组件漏洞扫描

（10）未受有效保护的 API 漏洞扫描

第三节 防火墙

一、防火墙的基本知识

1. 理解防火墙的作用、功能及分类

作用：

（1）提供基础组网和防护功能　（2）记录和监控网络存取与访问

（3）限定内部用户访问特殊站点（4）限制暴露用户点，防止内部攻击

（5）网络地址转换　　（6）虚拟专用网

功能：

（1）隔离　（2）访问控制

防火墙的分类方法，主要有以下 6 种：

（1）按软、硬件形式分类：软件防火墙、硬件防火墙、芯片级防火墙

（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

（4）按防火墙的应用部署位置分类：边界防火墙、个人防火墙、混合防火墙

（5）按防火墙性能分类：百兆级防火墙、千兆级防火墙

（6）按防火墙使用方法分类：网络层防火墙、物理层防火墙、链路层防火墙

2. 理解安全域的基本概念和边界防御思想

3. 掌握防火墙的技术指标

二、防火墙技术

1. 了解包过滤技术的原理、优缺点

2. 了解应用代理技术的原理、优缺点

3. 了解防火墙会话机制，掌握状态检测技术原理及优缺点

4. 了解应用识别技术 DPI 及 DFI 技术

5. 了解内容检查技术原理、优缺点

三、防火墙网络部署

1. 了解防火墙的部署模式

2. 了解 IPv4 技术及 IPv6 技术

3. 了解 VLAN 技术的原理

4. 了解静态路由协议、默认路由协议、动态路由协议、策略路由协议的概念

四、防火墙安全功能应用

1. 了解防火墙的安全策略

2. 了解防火墙边界防护技术

第四节 渗透技术

一、渗透测试概述

1. 了解渗透测试概念

2. 了解渗透测试的目的

（1）直观地表现网络安全漏洞的危害

（2）定量、具体地报告网络系统中存在的可能被利用的网络安全漏洞

（3）详细呈现渗透方法与过程，为设计安全解决方案提供事实依据

3. 理解渗透测试原则

（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. 掌握渗透测试常用方法

（1）应用漏洞扫描　　（2）系统结构分析

（3）隐藏文件探测　　（4）备份文件探测

（5）用户名和密码猜解　　（6）错误信息利用

（7）跨站脚本漏洞挖掘　　（8）恶意代码攻击

（9）SQL 注入漏洞挖掘　　（10）越权访问利用

（11）文件上传漏洞挖掘　　（12）任意文件读取漏洞利用

（13）目录遍历漏洞利用　　（14）功能滥用漏洞利用

（15）命令执行漏洞利用　　（16）跨站伪造请求漏洞利用

（17）文件包含漏洞利用　　（18）WebShell 检测

（19）组件泄露漏洞利用　　（20）信息泄露利用

2. 了解常用渗透测试工具

（1）信息收集工具，如端口扫描工具、目录枚举工具、网络监听工具等

（2）漏洞扫描工具，如网站漏洞扫描工具、系统层漏洞扫描工具等

（3）漏洞利用工具，如暴力破解工具、数据包拦截和篡改工具、典型高危漏洞的专用工具等

（4）测试文档管理工具

（5）缺陷管理工具

第五节 网络安全管理

一、 网络安全概述

1. 理解网络安全的概念、威胁网络安全的因素

2. 理解黑客、黑客攻击、常见的主动攻击和被动攻击

（1）主动攻击主要包含攻击者访问他所需信息的故意行为，如远程登录、伪造无效 IP 地址等

（2）被动攻击主要是收集信息而不是进行访问，包括嗅探 、信息收集等攻击方法

3. 了解恶意程序、安全漏洞、拒绝服务攻击、网站安全、云平台安全的概念

4. 理解网络空间安全的特性

（1）可用性（2）机密性（3）完整性（4）不可抵赖性

5. 了解常见的网络攻击形式

（1）逻辑炸弹　　（2）系统 Bug（3）社会工程学（4）后门和隐蔽通道

（5）拒绝服务攻击（6）病毒　　（7）蠕虫和特洛伊木马

二、 网络监控软件

1. 了解网络监控软件的概念

2. 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

3. 理解网络监控软件的监听模式和网关模式

4. 理解 Sniffer 概念、Sniffer 的软硬件两种形式方式、Sniffer 的作用

5. 了解 Sniffer Pro 软件及其使用

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. 理解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 操作系统的安全功能、Windows 认证机制、Windows 文件系统安全、Windows 加密机制、Windows 备份与还原

四、计算机病毒

1. 了解计算机病毒的定义

2. 理解计算机病毒的特点

（1）寄生（2）传染性（3）潜伏性（4）隐蔽性（5）破坏性（6）触发性

3. 了解计算机病毒按照存在的媒体、按传染的方法、按病毒的破坏能力、按病毒特有的算法的分类

4. 了解木马病毒的概念、木马病毒的防治

5. 了解蠕虫病毒的概念、蠕虫病毒的防治

6. 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）操作系统的监视和检测

（5）传统虚拟机病毒检测　（6）实时网络流量检测

（7）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

4. 理解物理安全、网络安全、主机安全、应用安全和数据安全层面的技术要求

5. 理解安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维方面的管理要求

第六章 网络安全技术发展趋势

第一节 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等

第二节 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

第三节 5G 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

第四节 人工智能

1. 了解人工智能赋能网络攻击的思想
2. 了解人工智能赋能网络攻击催生新型网络空间安全

第五节 量子密码技术

1. 了解量子密码技术
2. 了解量子技术为网络空间安全技术的发展带来的影响

第六节 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、联盟链及私有链的概念及安全问题

第七节 物联网

1. 了解物联网的概念
2. 理解物联网的应用及相关的安全风险