**广东省高等教育自学考试《信息与网络安全管理》课程考试大纲**

**（课程代码：03344）**

**Ⅰ 课程性质与课程目标**

一、课程性质和特点

“信息与网络安全管理”是为满足计算机应用领域及相关专业对计算机应用人才的需要而开设的。通过本课程的学习，学生能够掌握信息安全和网络安全的基本原理、安全策略的制定、安全管理的方法和技术等，能够在日后的工作中为信息安全和网络安全提供保障。

“信息与网络安全管理”旨在培养学生对信息安全和网络安全的认识和理解，掌握信息安全和网络安全的基本概念和基本知识，了解信息安全和网络安全的现状和趋势，掌握信息安全和网络安全的管理方法和技术，能够进行信息安全和网络安全的风险评估和安全策略的制定。

二、课程目标

设置本课程的主要目的是使考生掌握信息与网络安全管理的基本理论、基本知识和基本技能，培养学生的信息与网络安全意识和能力，为未来从事相关工作打下坚实基础。

通过本课程的学习，考生应达到以下目标。

1.理解网络信息安全的基本概念，了解网络空间面临的信息安全问题，和网络信息安全中的主要防范技术，了解网络空间信息安全的发展趋势。

2.掌握病毒防范技术，熟悉常见病毒的特点、判别、检测和清除方法。

3.掌握远程控制与黑客入侵技术原理，熟悉网络安全防范措施。

4.掌握网络空间信息密码体系，能通过密码管理策略保护信息安全。

5.了解数字签名的实现过程和用户验证原理。

6.了解网络安全协议的分类和常见网络安全协议的原理和应用。

7.掌握无线网络通信技术，熟悉无线网络安全的防范措施。

8.理解访问控制原理和防火墙原理，掌握网络地址转换技术和防火墙部署方法。

9．了解网络入侵防御系统的原理和安全策略。

10.掌握网络数据库安全技术和数据库备份技术。

三、与相关课程的联系与区别

信息与网络安全管理是一门旨在为学生提供信息安全管理领域的理论和实践知识的课程。学生在学习本课程前需要掌握计算机网络技术、操作系统概论、数据库及其应用等相关课程的基本知识。

四、课程的重点和难点

本课程的重点是网络信息安全基础：包括网络空间面临的各种信息安全问题、以及针对各种问题进行防范的技术概念和原理；以及常见的安全协议：包括SSL/TLS、IPSec、应用层安全协议的基本原理和应用。难点是该课程是一个复杂的学科，其中包含的理论知识繁杂，需要掌握的内容较多，需要学生结合实践操作加强理解和应用。

**Ⅱ 考核目标**

本大纲是“信息与网络安全管理”课程的个人自学、社会助学和考试命题的依据，本课程的考试范围以本考试大纲所限定的内容为准。

本大纲在考核目标中，按照识记、领会、简单应用和综合应用四个层次规定其应达到的能力层次要求。四个能力层次是递进关系，各能力层次的含义是：

识记：要求学生能够识别和记忆网络信息安全的基本概念、常见的安全威胁类型、防御措施以及TCP/IP网络分层中主要的网络安全协议名称等知识，能够简单地描述这些知识点的定义和特点。

领会：要求考生在识记的基础上，领悟网络安全的重要性，能够分析网络安全问题的发生原因和影响，并掌握相关的安全策略和方法，了解网络攻击者的攻击技巧和手段，具备初步的安全管理规划能力。

简单应用：要求学生能够应用网络安全技术和工具，实现基本的安全防护策略设计，能够进行一些简单的杀毒、入侵检测和防范部署等安全工作，具备初步的安全事件响应和处理能力。

综合应用：要求学生能够综合应用所学的知识和技能，进行较复杂的网络安全问题分析和解决，能够设计和实现较为复杂的网络安全方案和体系结构，具备较高水平的安全事件响应和处理能力，能够有效地应对网络安全攻击和威胁。

**Ⅲ 课程内容与考核要求**

1. 网络空间信息安全概论

一、学习目的与要求

本章的学习目的是使学生掌握网络空间信息安全的基本概念，初步认识信息安全风险的产生和防范，理解网络空间信息安全研究的重要意义，展望网络信息安全的发展趋势，具备初步的信息安全意识和能力。

二、课程内容

1.1 网络空间信息安全的重要意义

1.2 网络空间面临的信息安全问题

1.3 网络空间信息安全的主要内容

1.4 网络空间信息安全的七大趋势

三、考核知识点与考核要求

（一）网络空间信息安全的重要意义

识记：网络空间信息安全的概念。

领会：网络空间信息安全所包含的两部分内容。

（二）网络空间面临的信息安全问题

识记：当前网络空间面临的主要七类问题。

领会：电子邮件的安全漏洞和防范措施，文件传输协议FTP的安全漏洞和防范措施。

简单应用：根据对Web站点安全问题的理解，制定Web站点的安全防范措施。

（三）网络空间信息安全的主要内容

识记：当前网络空间信息安全主要涉及的9种技术领域。

（四）网络空间信息安全的七大趋势

领会：网络安全立法的重要性和网络信息安全对国家安全的重要意义。

四、本章重点、难点

本章的重点：网络空间信息安全面临的问题和主要技术发展内容

本章的难点：面对电子邮件安全问题、文件传输安全问题和Web站点安全问题，如果结合发现的漏洞，提出相应的防范措施。

1. 病毒防范技术

一、学习目的与要求

本章的学习目的是使学生掌握网络病毒的种类和传播方式，了解网络病毒的危害和防范措施，掌握网络病毒的检测和清除技术，提高对网络病毒的识别和应对能力。

二、课程内容

2.1 计算机病毒及病毒防范技术概述

2.2 恶意代码

2.3 典型计算机病毒的检测与清除

2.4 病毒现象与其他故障的判别

三、考核知识点与考核要求

（一）计算机病毒及病毒防范技术概述

识记：计算机病毒的特点和分类

（二）恶意代码

识记：常见恶意代码的类型。

领会：不同类型恶意代码的共同特征和各自的特点。

简单应用：掌握木马类和蠕虫类病毒的检测方法，制定防范方法和措施。

（三）典型计算机病毒的检测与清除

综合应用：U盘、手机等移动设备的病毒防范、检测和清除方法。

（四）病毒现象与其他故障的判别

简单应用：根据计算机的异常现象或运行错误提示，正确判断是计算机病毒还是软硬件故障。

四、本章重点、难点

本章的重点：网络病毒的分类、特征、传播途径和传染对象；木马和蠕虫类病毒的防治。

本章的难点：病毒和其他故障的判别，当计算机疑似病毒感染时如果结合检测手段找到病毒并进行清除，能够进行网络病毒的应急处理。

1. 远程控制与黑客入侵

一、学习目的与要求

本章的学习目的是使学生了解远程控制和黑客入侵的概念和原理，熟悉远程控制和黑客入侵的方法和工具，掌握防范远程控制和黑客入侵的技术和策略。

二、课程内容

3.1 远程控制技术

3.2 黑客入侵

3.3 日常网络及网站的安全防范措施

三、考核知识点与考核要求

（一）远程控制技术

识记：远程控制的基本概念和远程控制技术的应用范畴。

（二）黑客入侵

识记：常见恶意代码的类型。

领会：不同类型恶意代码的共同特征和各自的特点。

简单应用：掌握木马类和蠕虫类病毒的检测方法，制定防范方法和措施。

（三）日常网络及网站的安全防范措施

领会：服务器端对攻击、病毒和木马软件、故障等的防范措施。

综合应用：网站维护终端对攻击、病毒和木马软件、故障等的防范措施。

四、本章重点、难点

本章的重点：网络病毒的分类、特征、传播途径和传染对象；木马和蠕虫类病毒的防治。

本章的难点：病毒和其他故障的判别，当计算机疑似病毒感染时如果结合检测手段找到病毒并进行清除。

1. 网络空间信息密码技术

一、学习目的与要求

本章的学习目的是让学生了解密码学的基本概念和原理，掌握常用的加密算法和解密技术，以及了解密码管理和保护的相关知识。

二、课程内容

4.1 密码技术概述

4.2 对称密码体系

4.3 非对称密码体系

4.4 密码管理

三、考核知识点与考核要求

（一）密码技术概述

识记：密码技术中各种术语的概念和密码体系的分类。

领会：安全的密码体制对信息具备的功能，对称密码和非对称密码体系的优缺点比较。

（二）对称密码体系

识记：对称密码体系的概念和近现代密码体系DES和AES的名称。古典密码体系包括的密码算法。

领会：DES算法的工作原理。

简单应用：能够使用古典密码算法为明文求密文。

（三）非对称密码体系

简单应用：理解RSA算法密钥生成原理，能够根据跟定的设置计算公钥和私钥。

（四）密码管理

领会：密码管理体制的常见步骤。

四、本章重点、难点

本章的重点：密码学基础知识、对称密码体制和常用加密算法、公钥密码体制和RSA算法

本章的难点：DES算法的加密解密原理，和RSA算法的加密和解密过程

1. 数字签名与验证技术

一、学习目的与要求

本章的学习目的是让学生了解数字签名和验证的基本原理、常见算法和应用场景，能够熟练掌握数字签名和PKI验证技术，并能在实际应用中灵活运用。

二、课程内容

5.1 数字签名

5.2 验证技术

三、考核知识点与考核要求

（一）数字签名

识记：数字签名的性质，数字签名标准中提出的数字签名算法DSA和安全散列算法SHA。

领会：数字签名的作用和意义，数字签名的实现过程。

（二）验证技术

识记：非对称密钥系统的用户验证协议，数字证书的概念和用途，PKI系统的主要功能和基本组成。

领会：口令验证协议和非对称密钥系统验证协议的优缺点，PKI技术的原理和核心。

综合应用：基于PKI的角色访问控制模型及其实现过程。

四、本章重点、难点

本章的重点：数字签名和验证的基本原理、常见算法、应用场景和安全性等方面的知识。

本章的难点：PKI技术和数字证明的原理和应用。

1. 网络安全协议

一、学习目的与要求

本章的学习目的是让学习者了解各种网络安全协议的原理、功能、应用场景及其优缺点，并能够应用这些协议解决实际网络安全问题。

二、课程内容

6.1 概述

6.2 网络安全协议的类型

6.3 网络层安全协议IPSec

6.4 传输层安全协议SSL/TLS

6.5 应用层安全协议

三、考核知识点与考核要求

（一）概述

识记：网络安全协议的概念、特点和基于功能的分类。

领会：TCP/IP协议的不安全因素有哪些。

（二）网络安全协议的类型

识记：各个网络协议下的经典安全协议。

（三）网络层安全协议IPSec

识记：IPSec协议的组成和体系结构。

领会：了解IPsec协议的功能和工作原理，以及如何使用IPsec协议进行加密、认证和数据完整性保护，SA的概念和两种工作模式

（四）传输层安全协议SSL/TLS

识记：SSL/TLS的三种基本安全功能服务。

领会：SSL握手协议、SSL记录协议，TLS在SSL上改进后的优点。

综合应用：基于SSL/TLS协议的工作原理，如何使用SSL/TLS保证数据传输的安全性。

（五）应用层安全协议

领会：安全外壳协议SSH的组成和启动方法。

简单应用： S/MIME两种安全服务数字签名和邮件加密在邮件系统中的工作流程。

综合应用：SET协议的应用系统框架设计及分析

四、本章重点、难点

本章的重点：掌握各层网络安全协议的工作原理、应用场景和优缺点。

本章的难点：各种网络安全协议的具体实现方式，以及如何使用它们解决网络安全问题。

1. 无线网络安全机制

一、学习目的与要求

本章的学习目的是帮助学生了解无线网络的安全机制，掌握无线网络安全的基本理论、技术和方法，具备独立分析和解决无线网络安全问题的能力。

二、课程内容

7.1 无线网络

7.2 短程无线通信

7.3 无线网络的安全性

三、考核知识点与考核要求

（一）无线网络

识记：无线网络的基本概念和分类。

（二）短程无线通信

识记：常见的四种短程无线通信网络技术名称。

领会：四种短程无线网络技术的适用场景和优缺点分析。

简单应用：无线网络存在的各种安全隐患。

（三）无线网络的安全性

识记：常见的无线网络安全加密技术。

领会：黑客入侵无线网络的方法。

简单应用：防范无线网络入侵的安全策制定。

四、本章重点、难点

本章的重点：无线网络安全的基本概念、无线网络安全的基本原理、常见的无线网络攻击及防范方法。

本章的难点：理解无线网络的基本原理，掌握无线网络的安全机制，学习无线网络攻击及防范方法，并应用到实际的无线网络安全问题中去。

1. 访问控制与防火墙技术

一、学习目的与要求

本章的学习目的是让学生掌握计算机网络中的访问控制和防火墙技术，理解网络安全中访问控制和防火墙的原理、技术和应用，并能够运用所学知识进行网络安全的分析和设计。

二、课程内容

8.1 访问控制技术

8.2 防火墙技术

8.3 虚拟防火墙技术

三、考核知识点与考核要求

（一）访问控制技术

识记：访问控制的概念，访问控制机制的层次，访问控制的3个要素，安全策略的实施原则，自主访问控制的实现方式，强制访问控制策略的访问模式，基于角色的访问控制策略的特点，访问控制的实现相关术语的定义。

领会：自主访问控制策略和强制访问控制策略的区别和优缺点。

（二）防火墙技术

识记：网络防火墙的定义、组成和分类。

领会：对防火墙含义的理解，各类防火墙的特点和优缺点。

综合应用：防火墙的安全策略及应用。

（三）虚拟防火墙技术

领会：虚拟系统的特点。

简单应用：大中型企业的虚拟防火墙网络隔离应用和云计算的安全网关应用。

四、本章重点、难点

本章的重点：访问控制基础概念及分类、访问控制列表（ACL）和角色访问控制（RBAC）的实现和应用、防火墙的原理和应用

本章的难点：运用防火墙进行网络安全策略的设计和配置。

1. 入侵防御系统

一、学习目的与要求

本章的学习目的是让学习者了解各种网络安全协议的原理、功能、应用场景及其优缺点，并能够应用这些协议解决实际网络安全问题。

二、课程内容

9.1 入侵防御系统概述

9.2 网络入侵防御系统

9.3 主机入侵防御系统

三、考核知识点与考核要求

（一）入侵防御系统概述

识记：入侵手段、入侵防御系统的分类

领会：网络入侵防御系统的工作过程、主机入侵防御系统的工作过程。

（二）网络入侵防御系统

识记：网络入侵防御系统的结构。

领会：入侵检测机制的分类，信息捕获机制，各种入侵检测方法的原理。

简单应用：基于统计机制和基于规则机制的异常检测实施，网络入侵防御系统的安全策略制定

（三）主机入侵防御系统

识记：主机入侵防御系统的保护对象主机资源

领会：实现主机入侵防御系统的截获机制

简单应用：访问控制按全策略制定。

四、本章重点、难点

本章的重点：入侵防御系统的基本原理和分类、网络入侵防御系统和主机入侵防御系统。

本章的难点：网络入侵防御系统和主机入侵防御系统的工作流程和应用。

1. 网络数据库安全与备份技术

一、学习目的与要求

本章的学习目的是让学习者了解各种网络安全协议的原理、功能、应用场景及其优缺点，并能够应用这些协议解决实际网络安全问题。

二、课程内容

10.1 网络数据库安全技术

10.2 网络数据库访问控制模型

10.3 数据库服务器安全

10.4 网络数据库备份技术

三、考核知识点与考核要求

（一）网络数据库安全技术

识记：网络数据库的安全策略。

领会：网络数据库的安全需求。

（二）网络数据库访问控制模型

识记：强制访问控制的两种强制策略，基于完整性的强制策略的两条控制原则。

领会：多级安全模型的多实例问题，完整性锁的作用。

（三）数据库服务器安全

领会：数据库的服务器安全漏洞

（四）网络数据库备份技术

识记：系统备份方案的组成，网络数据库备份的方法和分类。

领会：应用需求和网络数据库备份方法的选择，软件备份的功能组成。

简单应用：物理热备份和热备份的实施方法和特点。

四、本章重点、难点

本章的重点：网络数据库的安全需求与安全策略，网络数据库的自主访问控制和强制访问控制，网络数据备份技术。

本章的难点：网络数据库安全策略的应用和实施。

**Ⅳ 关于大纲的说明与考核实施要求**

一、自学考试大纲的目的和作用

“信息与网络安全管理”课程自学考试大纲是根据计算机科学与技术（专升本）专业自学考试计划的要求，结合自学考试的特点而确定。其目的是对个人自学、社会助学和课程考试命题进行指导和规定。

课程自学考试大纲明确了课程学习的内容以及深广度，规定了课程自学考试的范围和标准。因此，它是编写自学考试教材和辅导书的依据，是社会助学组织进行自学辅导的依据，是自学者学习教材、掌握课程内容知识范围和程度的依据，也是进行自学考试命题的依据。

二、课程自学考试大纲与教材的关系

课程自学考试大纲是进行学习和考核的依据，教材给出了学习掌握课程知识的基本内容与范围，教材的内容还包括大纲所规定的课程知识的扩展与发挥。课程内容在教材中可以体现一定的深度或难度，但在大纲中对考核的要求一定要适当。

大纲与教材所体现的课程内容基本一致；大纲里面的课程内容和考核知识点，教材里一般也要有。反过来教材里有的内容，大纲里就不一定体现。

1. 关于自学教材

《网络空间信息安全》，苏永红、蒋天发主编，电子工业出版社，2022年第2版。

本教材第一章1.4节，第三章3.3、3.4节，第五章5.2节，第六章6.6节，第七章7.3、7.4节，第八章8.3、8.4节，第十章10.3节、10.5节、10.6节，第11章，考生可根据个人能力兴趣学习，不纳入考核范围。

四、关于自学要求和自学方法的指导

本大纲的课程基本要求是依据专业考试计划和专业培养目标而确定的。课程基本要求还明确了课程的基本内容，以及对基本内容掌握的程度。基本要求中的知识点构成了课程内容的主体部分。因此，课程基本内容掌握程度、课程考核知识点是高等教育自学考试考核的主要内容。

为有效地指导个人自学和社会助学，本大纲已指明了课程的重点和难点，在章节的基本要求中一般也指明了章节内容的重点和难点。

本课程共5学分，含实践2学分。由于成人学习的个性化特点，建议业余自学时间不低于60个学时。

建议学习本课程时注意以下几点：

1.在学习本课程教材之前，应先仔细阅读本大纲，了解本课程的性质和特点，熟知本课程的基本要求，在学习本课程时，能紧紧围绕本课程的基本要求。

2.在自学每一章的教材之前，先阅读本大纲中对应章节的学习目的与要求、考核知识点与考核要求，以使在自学时做到心中有数。

3.把学习基本理论、基本知识与分析、解决实际问题结合起来。首先，要弄懂基本理论、基本原理、基本知识和基本方法；其次，要学习运用这些知识联系实际解决有关实际问题。重点是要深刻领会教材内容，将知识转化为能力，提高运用知识分析问题和解决问题的能力。

4.考试前梳理已经学习过的内容，搞清楚一些基本概念、理论及方法之间的关系，便于记忆、加深理解，从而掌握分析计算方法。例如第六章，首先明确网络安全协议、网络层、传输层、应用层等概念，搞清楚各个层次的安全协议及其原理，即可掌握满足业务需求的协议选择和应用。

5.学习信息与网络安全管理的目的是用网络信息安全的理论知识和实践工具解决实际问题，网络安全管理能力的培养除要学习课程书本知识之外，操作和实践是学习和理解各种信息安全技术最有效的途径，为此，要求考生加强动手实践，提升安全实施能力，不仅能在计算机上解答教材中的习题，还能处理应用过程中的实际问题。

五、对社会助学的要求

对担任本课程自学助学的任课教师和自学助学单位提出以下几条基本要求。

1.熟知本课程考试大纲的各项要求，熟悉各章节的考核知识点。

2.辅导教学以大纲为依据，不要随意删减内容，以免偏离大纲。

3.辅导还要注意突出重点，要帮助学生对课程内容建立一个整体的概念。

4.助学者在辅导时应帮助自学者梳理重点内容和一般内容之间的关系，在他们全面掌握全部考试内容的基础上，深入病毒检测与清除、远程控制技术和黑客入侵防范、网络空间的密码体系及典型算法、网络安全协议类型和原理等重点内容，注意本课程网络信息安全问题、各种信息安全技术和网络信息安全防治等内容的系统性。

5.辅导要为考生提供足够多的上机实践机会，注意培养学生的上机操作能力，让学生能够通过上机实践进一步掌握相关知识。

本课程考纲内容建议学时如下：

|  |  |  |
| --- | --- | --- |
| 章次 | 学习内容 | 建议学时 |
| 第1章 | 网络空间信息安全概论 | 4 |
| 第2章 | 病毒防范技术 | 6 |
| 第3章 | 远程控制与黑客入侵 | 6 |
| 第4章 | 网络空间信息密码技术 | 8 |
| 第5章 | 数字签名与验证技术 | 4 |
| 第6章 | 网络安全协议 | 8 |
| 第7章 | 无线网络安全机制 | 6 |
| 第8章 | 访问控制与防火墙技术 | 6 |
| 第9章 | 入侵防御系统 | 6 |
| 第10章 | 网络数据库安全与备份技术 | 6 |

六、对考核内容的说明

1. 本课程要求考生学习和掌握的知识点内容都作为考核的内容。课程中各章的内容均由若干知识点组成，在自学考试中成为考核知识点。因此，课程自学考试大纲中所规定的考试内容是以分解为考核知识点的方式给出的。由于各知识点在课程中的地位、作用以及知识自身的特点不同，自学考试将对各知识点分别按四个认知层次确定其考核要求。

2. 在考试之日起6个月前，由全国人民代表大会和国务院颁布或修订的法律、法规都将列入相应课程的考试范围。凡大纲、教材内容与现行法律、法规不符的，应以现行法律法规为准。命题时也会对我国经济建设和科技文化发展的重大方针政策的变化予以体现。

1. 关于考试命题的若干规定

1.本课程考试采用闭卷笔试形式,考试时间为150分钟；满分100分,60分及格。

2.本大纲各章所规定的基本要求、知识点及知识点下的知识细目，都属于考核的内容。考试命题既要覆盖到章，又要避免面面俱到。要注意突出课程的重点、章节重点，加大重点内容的覆盖度。

3.不应命制超出大纲中考核知识点范围的题目，考核目标不得高于大纲中所规定的相应的最高能力层次要求。命题应着重考核自学者对基本概念、基本知识和基本理论是否了解或掌握，对基本方法是否会用或熟练。不应命制与基本要求不符的偏题或怪题。

4.本课程在试卷中对不同能力层次要求的分数比例大致为：识记占20%，领会占30%，简单应用占30%，综合应用占20%。

5.试题的难易程度分为4个等级：易、较易、较难和难四个等级。每份试卷中不同难度试题的分数比例一般为：易占20%，较易占30%，较难占30%，难占20%。

必须注意试题的难易程度与能力层次有一定的联系，但两者不是等同的概念，在各个能力层次都有不同难度的试题。

6.各种题型的具体样式参见本大纲附录。

**附录 题型举例**

一、单项选择题

1. （ ） 是非对称密码体系中的经典算法。
2. 凯撒密码 B.RSA算法

C. DES算法 D.AEA算法

二、名词解释题

1.访问控制

三、简答题

1.短距离无线通信网络的关键技术由哪些？

四、应用题

1.基于RSA算法生成密钥，若p=13,q=31,e=7，求d是多少？公钥是多少？私钥是多少？

五、案例分析题

1.某银行为信用卡电子支付设计了SET协议的应用系统框架。

（1）请补全SET协议的应用系统框架图

（2）要完成一次基于SET协议机制的信用卡安全电子支付流程，图中的各个实体要完成什么关键操作？

（3）结合信用卡电子支付过程，分析一下SET协议和SSL协议的区别。