ICS 35.110
L79

团　　体　　标　　准

T/BJCSA 01—2021

网络空间安全专业人员认证规范

Certification specification for cyberspace security professional

2021-12-30 发布　　2022-1-15 实施

北京网络空间安全协会
广东省网络空间安全协会　发布

目 次

前　言

本文件按照GB/T 1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规则起草。

本文件由网安联认证中心有限公司提出，北京网络空间安全协会、广东省网络空间安全协会归口。

本文件起草单位：网安联认证中心有限公司、广东关键信息基础设施保护中心、广州华南信息安全测评中心、网安联认证中心有限公司、联通（广东）产业互联网有限公司、深圳市计量质量检测研究院、广东计安信息网络培训中心、广东中证声像资料司法鉴定所、国源天顺科技产业集团有限公司。

本文件起草人：黄丽玲、成珍苑、吴星火、林小博、陈彦彬、姚飞、林勇忠、周绍午、李炯彬、安创文、杜守红、黄丽佳、谭祥明、杨文玲、王欢、徐伟、陈宁、贺锋、孙海申、叶婷、曾幸钦、曾炽强、谭剑成、曾灶烟、李树湖、刘泽楠、周贵招、麦世能、卢焕镇。

引　言

《中华人民共和国网络安全法》第三十四条和《中华人民共和国数据安全法》第二十条对从事网络空间安全人员安全教育、技术培训和技能考核等提出明确要求，同时鼓励相关组织、机构开展网络空间安全人员水平认证。目前对网络空间安全从业人员分级分类、专业知识和能力水平等评价认证缺乏相应的标准规范，制约了网络空间安全保障体系构建和发展。

制定统一的标准，推进权威机构的网络空间安全专业人才资质能力考核、认证工作，能够有效证明从业人员具备了相应的专业知识和能力、工作经验和业绩、以及较高的职业道德水平，从而为网络空间安全人才评价考核、选拔任用、职业进阶提供参考依据，推进网络空间安全人才的职业化和专业化发展。

网络空间安全专业人员认证（Certification Specification for Cyberspace Security 英文缩写 CSCS），针对网络空间安全从业人员进行水平认证，通过教育培训、技能考核及其他评价方式，认定获证人员具备了从事网络空间安全工作的个人素质和相应的技术知识与应用能力，规范网络安全专业人员知识、能力和行为准则，促进网络空间安全专业人才队伍建设，助力国家网络空间安全保障体系构建。

本文件规定了网络空间安全专业人员认证类别、专业方向和水平等级，明确认证要求和评价方式。

网络空间安全专业人员认证规范

1 范围

本文件规定了网络空间安全专业人员认证类别、专业方向和水平等级，明确认证要求和评价方式。

本文件适用于从事网络空间安全工作专业人员。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

3.1

网络空间安全 cyberspace security

网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

3.2

网络空间安全专业人员 cyberspace security professionals

从事网络空间安全相关工作的所有人员，包括管理人员、运营人员、技术人员。

3.3

工作经历 work experience

取得相应学历后的所有工作历史，无论是有偿的还是无偿的，全职的还是兼职的，不包括实习经历。

3.4

第三方认证机构 third-party certification bodies

具有可靠的执行网络空间安全认证制度的必要能力，并在认证过程中能够客观、公正、独立地从事认证活动的机构。

3.5

关键信息基础设施 critical information infrastructure

关键信息基础设施，是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等

3.6

重要数据 important data

是指以电子方式存在的，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的数据。

3.7

个人信息 personal information

以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息,不包括匿名化处理后的信息。

3.8

网络安全规划设计 network security planning and design

综合运用计算机软、硬件技术、网络通信技术、密码技术、信息安全技术，在企业、系统或项目的设计规划阶段，提出综合性的解决方案，以保障网络系统及其所承载的数据的保密性、完整性及可用性。

3.9

信息系统安全集成 information system security integration

按照信息系统的安全需求，采用信息系统安全工程的方法和理论，将安全单元、产品部件进行集成的统一和协调的系统之中，使资源达到充分共享，实现集中、高效、便利的管理，从而使建设完成后的信息系统满足建设方或使用方的安全需求而开展的活动。

3.10

信息系统安全运维 information system security operation and maintenance

为保障和提升服务对象的信息系统安全防护能力，及时解决出现的网络安全问题，由服务机构通过管理与技术手段提供的网络安全服务，主要包括安全巡检、病毒查杀、备份和恢复、安全审计、安全优化、渗透测试、风险评估等。

3.11

网络安全应急处理 cyberspace security emergency handling

在突发重大网络安全事件后对包括计算机运行在内的业务运行进行维持或恢复的各种技术和管理策略与规程。

3.12

软件安全开发 software security development

为解决软件产品的漏洞问题，而将安全活动集成到系统开发和软件质量保证活动中， 在软件开发的每个关键点嵌入安全要素，通过安全需求分析、安全设计、安全编码、安全测试等专业手段，解决各阶段可能出现的安全问题，有效减少软件产品潜在的漏洞数量提高软件产品安全质量的活动。

3.13

网络安全风险评估 cybersecurity risk assessment

依据有关信息安全技术与管理标准，对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行评价的过程。它要评估资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性，并结合安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响。

3.14

数据安全 data security

数据在整个系统中，从诞生到收集、清洗、存储、分析、消费、存档以及销毁这个生命周期中，其机密性、完整性和可用性不被破坏。

3.15

云计算安全 cloud computing security

云计算安全或云安全指一系列用于保护云计算数据、应用和相关结构的策略、技术和控制的集合。

3.16

网络安全审计 cyberspace security audits

网络安全审计是指按照一定的安全策略，利用记录、系统活动和用户活动等信息，检查、审查和检验操作事件的环境及活动，从而发现系统漏洞、入侵行为或改善系统性能的过程。

3.17

工业控制系统安全 industrial control system safety

通过管理与技术手段保护工业控制系统的软硬件、网络及其中数据，使其不因偶然的或者恶意原因而遭受破坏、更改泄露，保障工业控制系统连续正常的运行所提供的一系列防护策略和手段，主要包括工业控制系统调研、工业控制系统风险评估、安全解决方案设计、安全加固与防护实施、运维管理体系建设等。

3.18

渗透测试 penetration testing

模拟黑客攻击的手法，进行的非破坏性的攻击性测试，以期发现可能被黑客利用对系统进行入侵的安全漏洞和隐患及攻击路径，并将入侵的过程和漏洞细节产生报告给服务对象，提出详细、合理的修复建议，指导其进行整改，清除安全隐患，降低安全风险，为服务对象信息系统的平稳运行提供安全保障。

3.19

物联网安全　iot security

能够对物联网络的访问加以控制、确定用户（如抽象的有权限的账号、人、物联网终端、物联网端节点或物联网接入网关）身份真实有效以及私密性、保证用户行为不可抵赖、保证传输和存储数据的机密性、完整性、保证物联网的可用性、防止网络、业务遇到偶然的、被动的和主动的威胁以及病毒的扩散的技术和管理措施，以及对影响网络、业务的意外事故的应对措施。

4　认证类别和级别划分

4.1　认证类别

网络空间安全专业人员共分两个类别，包括管理类、技术类；涵盖以下方向：关键信息基础设施保护、重要数据保护、个人信息保护、网络安全管理、网络安全规划设计、软件安全开发、安全集成、安全运维、风险评估、应急处理、网络安全审计、工业控制系统安全、大数据安全、物联网安全、云计算安全、人工智能安全等。

4.2　级别划分

网络空间安全专业人员共设置四个级别，包括一级（初级）、二级（中级）、三级（高级）、四级（专家级），一级最低、四级最高。

5　认证通用要求

5.1　基本要求

获证人员应满足如下基本要求：

1)　具有独立的民事行为能力，具备承担法律责任的能力；

2)　近三年内未受过刑事处罚；

3)　遵守网络空间专业人员认证相关文件的规定；

4)　符合有关法律法规的规定，不存在法律法规禁止从业的情形。

5.2　初次申请资格要求

5.2.1　教育及工作经历

5.2.1.1　一级认证人员（初级）认证资格要求

获证人员应满足下面要求：

教育部发布的“具有普通高等学历教育招生资格的高等学校名单”中的院校的在校生、应届毕业生或全国研究生招生计划中研究生招生单位在校研究生、应届毕业生等。

5.2.1.2 二级认证人员（中级）教育及工作经历要求

专业要求：无专业要求限制。

获证人员工作经历应至少满足下面一项要求：

1) 本科（含）以上学历， 1 年以上从事网络空间安全有关工作经历；
2) 专科毕业，2 年以上从事网络空间安全有关的工作经历；
3) 中等专科毕业，4 年以上从事网络空间安全有关的工作经历；
4) 具有丰富的项目经验，5 年以上从事网络空间安全有关的工作经历。

5.2.1.3 三级认证人员（高级）教育及工作经历要求

专业要求：网络空间安全、信息安全、通讯、计算机相关或相近专业，非以上专业的人员，需要通过二级人员认证。

获证人员工作经历应至少满足下面一项要求：

1) 硕士研究生（含）以上学历， 2 年以上从事网络空间安全有关工作经历，其中至少 1 年以上项目经理经验；
2) 本科毕业，4 年以上从事网络空间安全相关工作经历，其中至少 2 年以上项目经理经验；
3) 专科毕业，5 年以上从事网络空间安全有关工作经历，其中至少 2 年以上项目经理经验；
4) 7 年以上从事网络空间安全有关工作经历，其中至少 2 年以上项目经理经验。

5.2.1.4 四级认证人员（专家级）申请资格要求

5.2.1.4.1 四级认证人员（专家级）教育与工作经历要求

专业要求：网络空间安全、信息安全、通讯、计算机相关或相近专业。

获证人员工作经历应至少满足下面一项要求：

1) 硕士研究生（含）以上学历， 4 年以上从事网络空间安全有关工作经历，其中至少 2 年项目经理经验；
2) 本科毕业，6 年以上从事网络空间安全相关工作经历，其中 3 年项目经理经验；
3) 专科毕业，8 年以上从事网络空间安全有关工作经历，其中至少 3 年项目经理经验；
4) 9 年以上从事网络空间安全有关工作经历，其中至少 3 年项目经理经验。

5.2.1.4.2 四级认证人员（专家级）技能、职称、学术成果要求

技能、职称、学术成果要求至少满足下面一项要求：

1) 入选全国网络空间安全领军人才、国家或省网络空间安全专家库、全国“网络空间安全人才

工程”百名高层次人才培养人选并继续从事本专业技术工作满 1 年者；

2) 担任国家、省网络空间安全专家咨询委员会专家；

3) 经国家、省、部批准的有突出贡献的中、青年科学技术专家；

4) 作为主要完成人，获得省（部）级以上科学技术奖项，或有关部门确认的相当等级的奖项；

5) 直接负责（技术负责）完成国家或省（部）级重大项目的研究、设计或生产的产品、施工技术、工艺达到当时国内领先水平，并取得明显的技术经济效益、社会效益，得到省部级有关部门的鉴定认可；

6) 具有网络空间安全、信息技术相关专业的高级技术职称（含副高）；

7) 参加省（部）级以上政府部门、省级社会组织主办的网络空间安全技能竞赛获三等奖以上。

5.2.1.5 其他要求

除 5.2.1.1-5.2.1.4 外的其他要求：

1) 满足评定要求的工作经历应在取得相应学历后获得；

2) 申请人应提交工作经历的书面证明，证明中应提供申请人从事的工作职责、岗位、级别和主要工作内容；

3) 实习经历不能包括在工作经历内；

4) 具有网络空间安全特殊能力的人才不受学历、职称、工作经历等条件限制，可直接申请相应级别认证。

5.2.2 考试要求

获证人员应满足下面要求：

1) 通过其申请的相应认证类别和级别的考试，包括笔试和实操（必要时）；

2) 必要时，通过由第三方认证或评估机构组织的专家面试；

3) 必要时，通过由第三方认证或评估机构组织的工作现场见证；

4) 一级认证人员需要掌握附录 A 网络空间安全专业人员认证通用知识要求中所要求的知识，且通过相应的考试；

5) 二级、三级认证人员分类别和专业方向，各类别专业方向人员须掌握附录（B-0）中对应方向要求的知识，且通过相应的考试；

6) 四级认证人员为资历评定，学历、工作经历、技能、职称、学术成果符合条款 5.2.1.4 的条件即可申请，无考试要求。

5.3 再认证资格要求

1) 已通过网络空间安全专业人员认证，且在认证有效期内；

2) 获证后 3 年内至少有网络空间安全、信息安全的工作经历；

3) 每年不少于 16 课时的网络空间安全相关专业的继续教育课程学习。

5.4 认证升级资格要求

获证人员应满足下面要求：

1) 已通过网络空间安全专业人员认证，且在认证有效期内；

2) 满足网络空间安全专业人员高一级别认证要求，包括工作经历、培训和考试要求。

6 认证评价

6.1 证评价方式

书面考试 + 书面评价 + 面试（必要时）。

6.2 书面考试

申请人员可参加第三方认证机构组织的相应级别的书面考试，考试大纲见附件（A-0）要求。

6.3 书面评价

6.3.1 满足一级认证要求的网络空间安全从业人员，提交认证的申请材料，包括但不限于学籍注册证明、身份证明、考试合格证明、工作经历等资格证明材料。

6.3.2 满足认证其他级别和类别要求的网络空间安全人员提交的认证申请材料，包括身份证明、学历、工作经历、书面考试合格等证明材料。

6.3.3 收到申请材料后，第三方认证机构的申请评审人员负责审查申请人提交的申请资料，若申请人提交的资料齐全、填写清楚、正确，且资料表明符合认证准则基本要求的则予以正式受理。

6.3.4 在资料审查过程中，申请评审人员应将所发现的与认证条件不符合之处通知申请人。

6.3.5 认证审核人员对申请人提交认证申请材料进行审查，并给出符合性评价结论。

6.3.6 认证审核人员对申请人的考试成绩进行核实，并给出其在所申请的专业方向和对应级别的知识水平和应用能力的评价结论。

6.3.7 认证审核人员对申请人进行综合评价，以决定直接推荐认证或需进一步面试评价。

6.4 面试评价

6.4.1 面试评价人员依据认证审核人员的建议对申请人综合素质、所申请的专业方向和级别要求的知识和能力通过面谈的方式进行考核或核实，并给出其在所申请的专业方向和对应级别的知识水平和应用能力的评价结论。

6.4.2 面试评价人员对申请人进行综合评价，以决定是否推荐认证批准。

6.5 认证批准

6.5.1 第三方认证机构认证决定人员负责审核认证书面评价和面试评价（需要时）的意见，并最终决定是否批准认证。

6.5.2 认证决定人员和审核人员不应为同一人员。

6.5.3 最终决定结果是以下三种类型之一：

1) 通过认证；

2) 不予通过认证；

3) 补充证据或信息，再行认证评定。

6.5.4 颁发证书与公告：

第三方认证机构应发布公告，公告通过认证的人员名单，并发放认证证书，认证证书有效期 3 年。

6.6 年度确认

获证人员在证书有效期内每年完成相应的再继续培训 16 个学时以上来维持认证资质的持续有效。

6.7 再认证

获证人员在证书过期前 90 天内应向第三方认证机构提交资料申请再认证申请，再认证评价需提交近三年的网络空间安全相关工作经历，应至少包括认证方向相关的经历或 2 个认证方向已完成项目。

6.8 变更

获证人员在证书有效期内提出级别、方向、类别方向的变更，如升级、降级、变更到其他方向、类别，或增加其他方向、类别的证书，均可提交变更申请，以及提供标准中要求的符合性证明材料以供评价。

6.9 暂停、恢复、撤销和注销认证

6.9.1 暂停认证

6.9.1.1 获证人员如不能持续地符合认证条件和要求，包括不提交专业持续发展课程学习的证明、不提供相关认证专业方向的工作经历证明，第三方认证机构可以暂停部分或全部认证资格。

6.9.1.2 暂停期不小于 60 天，但不大于 180 天，获证人员在暂停期间不再享有相应权利，不得使用被暂停的证书，也不得以任何明示或隐含的方式向外界表示被暂停认证的范围仍然有效。

6.9.2 恢复认证

被暂停认证的，在规定的暂停期限内达到认证要求后，申请并经确认符合，可以恢复认证资格。

6.9.3 撤销认证

在下列情况下，第三方认证机构应撤销认证：

1) 被暂停认证的，超过暂停期仍不能恢复认证（部分暂停的则部分撤销）；

2) 当认证规则、认证准则变更时，在规定时间内不能满足新要求的；

3) 获证人员不能履行第三方认证机构的相关认证规则中规定的义务；

4) 获证人员被证实不再符合认证准则所规定的要求。

6.9.4 注销认证

在下列情况下，第三方认证机构应注销认证：

1) 获证人员自愿申请撤销认证；

2) 认证有效期满未申请再认证。

6.9.5 暂停、恢复、撤销和注销认证公告

在暂停、恢复、撤销和注销认证决定后，第三方认证机构将发布认证公告，部分撤销认证的同时更新原有发布的电子证书。

附 录 A
（规范性）
通用技术基础知识考试大纲

A.1 目的

为使考生达到本文件中网络空间安全专业人员通用技术基础能力要求，指导考生有效准备考试，特制定本考试大纲（以下简称大纲）。

A.2 考试内容

A.2.1 课程要求和考试比例

表 A.1 通用技术课程要求

课程名称	课程类型	选择范围
信息安全技术	基础课程	全部

A.2.2 课程知识点要求

表 A.2 信息安全技术课程内容与知识点

章节号	章节名	内容与知识点
1	密码学基础	了解密码学发展简史和基本概念 掌握密码学算法知识，如对称密码算法、非对称密码算法、哈希函数和数字签名算法
2	密码学应用	了解密码学应用基础 了解公钥基础设施 了解虚拟专用网络知识 了解特权管理基础设施 了解其他密码应用知识
3	鉴别和访问控制	掌握鉴别的类型、访问控制模型、访问控制技术
4	操作系统安全	掌握 windows 系统安全机制相关知识 掌握 Linux 系统安全机制相关知识 掌握安全操作系统设计原则
5	网络安全	掌握网络安全协议、网络安全设备、网络架构安全知识
6	数据库安全	了解数据库系统概念 了解数据库安全知识 理解数据库安全防护方法
7	应用安全	了解应用安全概念 掌握 web 应用安全、互联网服务安全、办公软件安全等知识

表 A.2　信息安全技术课程内容与知识点（续）

章节号	章节名	内容与知识点
8	安全漏洞和恶意代码	了解安全漏洞的产生和发展 掌握安全漏洞发现和修复知识 掌握恶意代码的产生和发展、实现技术、防御技术
9	安全攻击和防护	了解信息收集和分析的作用、方法和防范 了解常见攻击和防范 了解后门设置与防范、痕迹清除和防范
10	软件安全开发	了解软件安全开发背景 掌握软件开发模型知识 掌握软件安全需求和设计 掌握软件安全测试方法
11	新技术安全	了解云计算安全、物联网安全、工业控制安全、大数据安全、人工智能安全等知识

附 录 B
（规范性）
通用管理类知识考试大纲

B.1 目的

为使考生达到本认证规范中网络空间安全专业人员通用管理类能力要求，指导考生有效准备考试，特制定本考试大纲（以下简称大纲）。

B.2 考试内容

B.2.1 课程要求

表 B.1 通用管理类课程要求

课程名称	课程类型	选择范围
网络安全管理实践	专业课程	全部
关键信息基础设施保护	专业课程	全部
重要数据保护	专业课程	全部
个人信息保护	专业课程	全部

B.3 各课程知识点要求

B.3.1 网络安全管理实践

表 B.2 网络安全管理实践课程内容与知识点

章节号	章节名	内容与知识点
1	基本概念	理解网络安全基本概念和信息安全模型
2	安全管理策略	了解各国网络安全管理策略
3	安全机构和人员管理	掌握安全机构和人员管理的职责、管理方法
4	安全技术管理	掌握密码学、物理和通讯链路安全、网络安全管理、系统安全管理等基本概念和方法
5	系统建设和安全管理	掌握信息安全风险评估、信息安全工程知识 掌握信息系统获取、开发和维护管理
6	安全事件管理和应急响应	掌握信息安全事件分类分级 掌握信息安全事件处置方法、流程 掌握网络安全通报预警和应急处置知识、应急预案编制管理知识
7	连续性管理	掌握业务连续性管理知识 掌握备份技术和恢复管理知识

表 B.2　网络安全管理实践课程内容与知识点（续）

章节号	章节名	内容与知识点
8	法规和标准	了解网络信息安全相关法律法规 了解网络信息安全管理标准
9	网络安全等级保护	了解网络安全等级保护制度和标准 了解信息安全等级保护实施过程 理解安全等级保护定级和备案知识 理解安全等级保护建设知识 掌握安全等级保护测评知识 了解网络安全自查和监督检查知识

B.3.2　关键信息基础设施保护

表 B.3　关键信息基础设施保护课程内容与知识点

章节号	章节名	内容与知识点
1	基本概念	了解关键信息基础设施安全基本概念和安全现状
2	保护范围	了解关键信息基础设施安全保护范围
3	网络安全法	理解网络安全法的精髓 了解基于网络安全法的关键信息基础设施安全 掌握网络安全审查的主要内容、目的和意义
4	网络安全等级保护	了解网络安全等级保护的安全理念 掌握网络安全等级保护的基本内容 掌握实施等级保护的基本原则和常规动作
5	关键信息基础设施保护条例	了解关键信息基础设施法律政策和标准依据 掌握网络运营者的安全义务 掌握网络安全监测预警、应急处置、检测评估方法、步骤和流程 了解关保主体责任

B.3.3　个人信息安全保护

表 B.4　个人信息安全保护课程内容与知识点

章节号	章节名	内容与知识点
1	基本概念	了解个人信息安全基本概念 了解个人信息安全的法律法规

表 B.4　个人信息安全保护课程内容与知识点（续）

章节号	章节名	内容与知识点
2	重要数据出境安全评估	了解重要数据出境安全评估基本概念 理解出境数据的界定和评估内容
3	个人信息出境安全评估方法	掌握个人信息出境的评估范围和流程 掌握限制出境的个人信息
4	个人信息安全规范	掌握个人信息安全基本原则 掌握个人信息安全的收集、保存、使用和共享转让披露的规范

B.3.4　数据安全保护

表 B.5　重要数据保护课程内容与知识点

章节号	章节名	内容与知识点
1	基本概念	了解数据、数据处理和数据安全的定义 了解数据安全工作基本原则 熟悉数据安全相关国家标准
2	数据安全制度	了解数据安全的发展、数据标准体系 了解数据安全制度 了解数据安全保护义务和法律责任 了解政务数据安全与开放

附 录 C
（规范性）
网络安全规划设计考试大纲

C.1 目的

为使考生达到本文件中网络空间安全专业人员在网络安全规划设计方面能力要求，指导考生有效准备考试，特制定本考试大纲（以下简称大纲）。

C.2 考试内容

C.2.1 课程要求和考试比例

表 C.1 网络安全规划设计课程要求

课程名称	课程类型	选择范围
网络安全管理实践	基础课程	全部
信息安全技术	基础课程	全部
网络规划与设计	专业课程	全部

C.3 各课程知识点要求

C.3.1 网络规划与设计

表 C.2 网络规划与设计内容与知识点

章节号	章节名	内容与知识点
1	计算机网络原理	掌握计算机网络概念、组成、分类、体系结构知识 掌握数据通信基础知识，如数据通信系统、数据调制与编码、多路复用技术、数据交换方式、传输介质、检错与纠错等知识 掌握网络体系结构、网络设备和网络软件知识 掌握局域网、广域网与接入网知识 掌握网络互联、Internet 协议、网络管理、服务质量技术等知识
2	计算机网络规划与设计	掌握计算机网络基本元素、互联设备、网络性能、网络设计文档等知识 掌握网络分析与设计过程知识 掌握网络需求分析、通信规范、逻辑网络设计、物理网络设计、网络测试试运行和维护、网络故障分析与处理等知识
3	网络资源设备	掌握网络服务器、网络存储系统、其他资源设备等知识

表 C.2　网络规划与设计内容与知识点（续）

章节号	章节名	内容与知识点
4	网络安全	掌握恶意代码、黑客攻击及其预防、防火墙应用配置、ISA Server 应用配置知识 掌握 IDS 和 IPS、访问控制技术、VPN 技术等知识 掌握企业网络安全隔离知识 掌握公钥基础机构、文件加密和电子签章等知识 掌握网络安全应用协议、桌面安全解决方案、系统安全、安全审计、安全管理制度等知识
5	标准化和知识产权	掌握标准化概念、过程、分类、编号、标准化组织、信息技术标准等知识 掌握知识产权概念、计算机软件著作权法等知识
6	网络系统分析与设计案例	掌握网络规划、优化、配置、故障分析与处理

附 录 D
（规范性）
信息系统安全集成考试大纲

D.1 目的

为使考生达到本文件中网络空间安全专业人员在信息系统安全集成方向二级、三级能力要求，指导考生有效准备考试，特制定本考试大纲（以下简称大纲）。

D.2 考试内容

D.2.1 专业课程要求

表 D.1 信息系统安全集成课程要求

课程名称	课程类型	选择范围
项目管理基础	基础课程	全部
安全集成	基础课程	全部
通信技术基础	基础课程	全部

D.3 各课程知识点要求

D.3.1 项目管理基础

表 D.2 项目管理基础课程内容与知识点

章节号	章节名	内容与知识点
1	项目管理基本概念	正确理解项目的本质 正确理解管理的本质 掌握项目管理的基本分类 熟练掌握项目管理的生命周期与流程 掌握项目管理相对其他管理的特性
2	项目管理的发展历史与现状	了解项目管理的发展过程 了解国际项目管理发展现状 了解国际国内项目管理人员认证情
3	九大项目管理知识领域	熟练掌握项目综合管 理、项目范围管理、 项目时间管理、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、 项目风险管理和项目采购管理思想与方法 掌握项目综合管理、 项目范围管理、项目 时间管理、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、项目风险管理和项目采购管理工具和实施技巧

表 D.2　项目管理基础课程内容与知识点（续）

4	集成类项目管理技巧	掌握集成类项目管理的特点 掌握集成类项目生命周期 掌握集成类项目九大管理知识领域特性 实践一个完整的集成

D.3.2　信息系统安全集成

表 D.3　信息系统安全集成课程内容与知识点

章节号	章节名	内容与知识点
1	安全集成的业界标准与实践	掌握 GB/T 20261 对安全集成的要求 掌握 ISO/IEC 21827 对安全集成的要求 掌握 SSE-CMM3.0 对安全集成的要求 掌握信息系统安全集成服务资质认证实施规则对安全集成的要求 掌握 CNCA/CTS 0052 信息安全服务资质认证技术规范
2	安全集成过程	掌握安全软件集成管理的全过程 掌握安全集成准备工作（如需求分析）的主要方法 掌握安全集成设计的主要方法 掌握安全集成实施的主要工作 掌握安全集成保证的主要内容
3	安全集成工具使用	熟悉典型的安全集成工具 熟悉需求分析工具使用 熟悉安全集成设计工具使用 熟悉安全保证工具使用
4	典型安全保障手段	熟悉典型的信息安全保障手段 熟悉常用的信息安全技术应用 熟悉常用的信息安全产品
5	安全集成实例	熟悉安全集成方案的结构 熟悉主要行业的安全集成特性 理解 1-2 个行业的典型安全集成实例

附 录 E
（规范性）
信息系统安全运维人员考试大纲

E.1 目的

为使考生达到本文件中网络空间安全专业人员信息系统安全运维方向二级、三级能力要求，指导考生有效准备考试，特制定本考试大纲。

E.2 考试内容

E.2.1 专业课程要求

表 E.1 信息系统安全运维课程要求

课程名称	课程类型	选择范围
信息安全技术	专业课程	全部
信息系统安全运维	专业课程	全部
网络安全等保 2.0 技术产品	基础课程	全部
渗透测试与攻防实战	专业课程	全部

E.3 各课程知识点要求

E.3.1 信息安全技术课程内容与知识点

表 E.2 信息安全技术课程内容与知识点

章节号	章节名	内容与知识点
1	信息安全概论	介绍了信息安全的基本概念、原理和知识体系
2	物理安全	包括物理安全概述、物理安全相关的法律、法规等内容
3	通讯和网络安全工程	包括网络结构安全分析技术及其他的安全服务和安全机制策略等。
4	密码学及其应用	包括密码学基础知识、对称加密算法、非对称加密算法、散列算法及其应用、数字签名、PKI 技术、SSL、SSH、IPSec、PGP 加密文件系统等。

E.3.2 信息系统安全运维

表 E.3 信息系统安全运维课程内容与知识点

章节号	章节名	内容与知识点
1	业界标准与实践	理解信息安全管理体系对安全软件的要求 理解服务管理体系对安全运维的要求 理解安全弱点管理相关规范

表 E.3　信息系统安全运维课程内容与知识点（续）

章节号	章节名	内容与知识点
2	安全运维机构与思想	理解安全运维的核心思想 理解安全运维管理的关系结构
3	安全运维工具使用	熟悉典型的安全运维工具 熟悉典型的安全运维手段
4	安全运维实例	熟悉主要行业的安全运维特性 熟悉 1-2 个行业的典型安全运维实例

E.3.3　网络安全等保 2.0 技术产品

表 E.4　网络安全等保 2.0 技术产品课程内容与知识点

章节号	章节名	内容与知识点
1	VPN 原理与实践	掌握 IPsec VPN、GRE Over IPsec、DMVPN、SSL VPN 等网络安全技术
2	防火墙原理与实践	掌握防火墙安装和配置实践，特定的防火墙技术、工具和技巧
3	入侵防御原理与实践	掌握入侵防御系统的功能、原理与部署、关键技术
4	漏洞扫描原理与实践	掌握漏洞扫描与防护相关理论与技术
5	信息安全审计	掌握如何根据相关标准、法规进行合规性安全审计，以及如何对计算机信息系统中的所有网络资源（包括数据库、主机、操作系统、网络设备、安全设备等）进行安全审计，记录所有发生的事件，为系统管理员提供系统维护以及安全防范的依据
6	安全设备	了解 HPS、上网行为管理，WAF 主流产品

E.3.4　渗透测试与攻防实战

表 E.5　渗透测试与攻防实战课程内容与知识点

章节号	章节名	内容与知识点
1	web 安全渗透测试与安全防御	了解渗透测试的基础知识 掌握渗透测试环境的部署 重点掌握 Web 应用、移动应用漏洞利用
2	Kali Linux 渗透测试攻防实战	掌握 Kali Linux 渗透测试的各种核心技术，涵盖从安装配置，到信息收集和漏洞扫描及利用，再到权限提升及各种渗透测试等技术
3	WHFI 无线安全攻防	掌握设备硬件以及无线电通信的威胁。

4	攻防实战	掌握攻防实战技术

附 录 F
（规范性）
软件安全开发方向考试大纲

F.1 目的

为使考生达到本文件中网络空间安全专业人员在软件安全开发方向二级、三级能力要求，指导考生有效准备考试，特制定本考试大纲（以下简称大纲）。

F.2 考试内容

F.2.1 专业课程要求

表 F.1 软件安全开发课程要求

课程名称	课程类型	选择范围
项目管理基础	基础课程	全部
软件安全开发	专业课程	全部

F.3 各课程知识点要求

F.3.1 项目管理基础

表 F.2 项目管理基础课程内容与知识点

章节号	章节名	内容与知识点
1	项目管理基本概念	正确理解项目的本质 正确理解管理的本质 掌握项目管理的基本分类 熟练掌握项目管理的生命周期与流程 掌握项目管理相对其 他管理的特性
2	项目管理的发展历史与现状	了解项目管理的发展过程 了解国际项目管理发展现状 了解国际国内项目管理人员认证情
3	九大项目管理知识领域	熟练掌握项目综合管理、项目范围管理、 项目时间管理、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、 项目风险管理和项目采购管理思想与方法 掌握项目综合管理、 项目范围管理、项目 时间管理、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、项目风险管理和项目采购管理工具和实施技巧

表 F.2　项目管理基础课程内容与知识点（续）

章节号	章节名	内容与知识点
4	开发类项目管理技巧	掌握开发类项目管理的特点 掌握开发类项目生命周期 正确掌握开发类项目九大管理知识领域特性 实践一个完整的开发类项目过程

F.3.2　软件安全开发

表 F.3　软件安全开发课程内容与知识点

章节号	章节名	内容与知识点
1	软件安全开发基础	了解软件安全开发背景 了解软件安全开发概念 了解软件安全开发方法 了解软件安全开发风险管理、信息系统安全工程、CC 标准等
2	软件安全需求分析	了解软件安全需求的定义和分类、安全需求工程 熟练掌握安全需求分析方法
3	软件安全设计	了解软件设计主要工作 熟悉软件安全设计原则和减少受攻击面知识 掌握软件安全设计方法 掌握软件架构安全性分析方法 熟练掌握威胁建模知识
4	安全编码	了解软件漏洞含义及分类 掌握软件安全编码原则和安全编程基础知识 掌握 Web 应用安全编程方法 掌握数据安全编码知识
5	软件安全测试	掌握软件安全测试基础知识 熟练掌握代码分析知识 熟练掌握模糊测试和渗透测试知识
6	软件部署和项目管理安全	掌握软件部署安全知识 掌握软件项目管理安全知识 了解软件安全编码规范检查列表、安全测试工具、测试文档模板等

附 录 G
（规范性）
网络安全风险评估考试大纲

G.1 目的

为使考生达到本文件中网络空间安全专业人员在网络安全风险评估方向二级、三级能力要求，指导考生有效准备考试，特制定本考试大纲（以下简称大纲）。

G.2 考试内容

G.2.1 专业课程要求

表 G.1 网络安全风险评估课程要求

课程名称	课程类型	选择范围
网络安全风险管理人员基本素质	基础课程	全部
网络安全风险管理意识教育	基础课程	全部
网络安全法律法规体系	基础课程	全部
网络安全风险管理基础	专业课程	全部
网络安全风险管理基础（H 级）	专业课程	全部
网络安全风险管理基础（HH 级）	专业课程	全部
信息安全风险评估实施方法	专业课程	全部
信息安全风险评估案例分析	专业课程	全部

G.3 各课程知识点要求

G.3.1 网络安全风险管理基础

表 G.2 网络安全风险管理基础课程内容与知识点

章节号	章节名	内容与知识点
1	职业素养	了解从事网络安全风险管理工作必备的职业素养
2	知识结构	理解从事网络安全风险管理工作的基础知识
3	工作技能	理解从事网络安全风险管理工作的基础技能

G.3.2 信息安全风险评估的基础理念

表 G.3　信息安全风险评估的基础理念课程内容与知识点

章节号	章节名	内容与知识点
1	信息安全风险评估的基本概念	风险评估的介绍、基本注意事项
2	信息安全风险评估相关标准	了解国际上通用的信息安全风险评估标准以及国内的风险评估标准
3	信息安全风险评估的发展与现状	了解国内信息安全风险评估的发展、现状

G.3.3　信息安全风险评估框架及流程

表 G.4　信息安全风险评估框架及流程内容与知识点

章节号	章节名	内容与知识点
1	信息安全风险评估的主要内容	掌握风险评估的依据、原则；风险评估基础模型、风险分析原理、风险评估方法介绍
2	信息系统生命周期各阶段的风险评估	掌握信息系统规划、设计、实施、运维、废弃阶段的信息安全风险评估
3	风险评估管理工具及评估工具介绍	掌握风险评估管理工具（MBSA、COBRA）、评估工具（极光远程安全评估系统、天镜脆弱性扫描与管理系统、KALH 渗透测试工具）使用方法

G.3.4　信息安全风险评估实施方法

表 G.5　信息安全风险评估实施方法内容与知识点

章节号	章节名	内容与知识点
1	信息安全风险实施 1	资产识别（资产分类、资产赋值）、威胁识别（威胁分类、威胁赋值）、脆弱性识别（脆弱性识别、脆弱性赋值）
2	信息安全风险实施 2	确认已有安全措施，对识别的风险进行分析，风险计算原理，风险结果判定，制定风险处置计划
3	信息安全风险报告编制	掌握风险评估记录方法，风险评估工作形式（自评估、检查评估），风险计算方法（矩阵法计算风险、相乘法计算风险）
4	风险评估辅助工具使用	风险评估资产调研表、人员访谈模板、基线检查模板、风险评估工作申请单、项目计划及会议纪要
5	风险评估脆弱性识别工具使用	掌握极光远程安全评估系统、天镜脆弱性扫描与管理系统、KALH 渗透测试等工具使用方法

G.3.5　网络安全风险防范

表 G.6　网络安全风险防范内容与知识点

章节号	章节名	内容与知识点
1	信息系统安全风险说明	掌握信息系统的安全属性，安全风险要素，风险评估与控制模型
2	信息系统资源分布模型及基于信息资产的风险识别与分析	掌握信息网络安全风险识别过程，信息网络系统的威胁识别，信息系统的脆弱性识别，信息系统的风险分析
3	网络安全机制设计	掌握网络安全攻防，安全等设计方法
4	网络安全访问控制策略设计	掌握网络安全访问控制策略的特点，理解当前网络安全访问控制策略的设计
5	网络云端安全设计	掌握网络安全云端安全机制，理解云计算云服务的安全策略设计
6	网络安全系统实现	掌握网络安全系统设计流程，理解安全平台使用的各种安全机制及其实施

G.3.6　网络安全风险管理

表 G.7　网络安全风险管理内容与知识点

章节号	章节名	内容与知识点
1	网络安全系统风险评估	掌握信息保护设计原则，风险属性等
2	网络安全系统统合规性监管	掌握网络安全设备合规性监管及制定网络安全合规程度的方法，掌握构建或调整网络合规性监管方法
3	网络安全风险事件管理与取证	掌握网络安全事件管理内容，理解网络安全事件响应方法的制定、规划与实施，检测与分析以及取证等解决办法
4	网络安全风险运维	掌握网络安全系统生命周期，理解网络安全与风险管理规划、部署、管理监控与检测、修复与处置等方面的运维方法

G.3.7　信息安全风险评估案例分析

表 G.8　信息安全风险评估案例分析内容与知识点

章节号	章节名	内容与知识点
1	信息安全风险评估概述	确定评估的内容、评估的依据
2	安全现状分析	对系统进行介绍、编制资产调查列表、描述网络现状
3	风险评估内容	进行安全评估综合分析，具体包括：威胁评估、网络设备安全评估、主机人工安全评估、应用安全评估、网络架构安全评估、无线网络安全评估、工具扫描、管理安全评估
4	风险分析和处理	进行综合风险分析，具体包括：综合风险评估方法、综合风险评估分析 进行风险处置，具体包括：风险处置方式、风险处置计划

附 录 H
（规范性）
网络安全应急处理考试大纲

H.1 目的

为使考生达到本文件中网络空间安全专业人员网络安全应急处理方向二级、三级能力要求，指导考生有效准备考试，特制定本考试大纲（以下简称大纲）。

H.2 考试内容

H.2.1 专业课程要求

表 H.1 网络安全应急处理课程要求

课程名称	课程类型	选择范围
项目管理基础	基础课程	全部
信息安全技术	基础课程	全部
通信技术基础	基础课程	全部
网络安全应急响应	专业课程	全部

H.3 各课程知识点要求

H.3.1 项目管理基础

表 H.2 项目管理基础课程内容与知识点

章节号	章节名	内容与知识点
1	项目管理基本概念	正确理解项目的本质 正确理解管理的本质 掌握项目管理的基本分类 熟练掌握项目管理的生命周期与流程 掌握项目管理相对其他管理的特性
2	项目管理的发展历 史与现状	了解项目管理的发展过程 了解国际项目管理发展现状 了解国际国内项目管理人员认证情

表 H.2　项目管理基础课程内容与知识点（续）

章节号	章节名	内容与知识点
3	九大项目管理知识领域	熟练掌握项目综合管理、项目范围管理、 项目时间管理、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、 项目风险管理和项目 采购管理思想与方法 掌握项目综合管理、 项目范围管理、项目 时间管理、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、项目风险管理和项目采购管理工具和实施技巧
4	开发类项目管理技巧	掌握开发类项目管理的特点 掌握开发类项目生命周期 正确掌握开发类项目九大管理知识领域特性 实践一个完整的开发类项目过程
5	集成类项目管理技巧	掌握集成类项目管理的特点 掌握集成类项目生命周期 掌握集成类项目九大管理知识领域特性 实践一个完整的集成

H.3.2　通信技术基础

表 H.3　通信技术基础课程内容与知识点

章节号	章节名	内容与知识点
1	通信的基本概念	理解通信的本质含义及电信概念 理解通信网络形成过程 了解通信网络结构 了解通信网络中的安全属性 了解通信网络应用分类 了解“网络”习惯分类 了解通信网络安全问题本质成因
2	通信协议及应用	熟悉 OSI 七层模型 熟悉 TCP/IP 协议族的基本协议及 TCP/IP 协议族存在的固有安全问题 熟悉 IPv6、移动互联网等技术及应用 了解典型的通信网络及设备

3	安全通信协议	了解典型的安全通信协议 了解典型的安全通信协议在通信过程中的应用

H.3.3 网络安全应急响应

表 H.4 网络安全应急响应课程内容与知识点

章节号	章节名	内容与知识点
1	网络安全应急响应技术概念	了解网络安全应急响应的含义和相关法规 了解网络安全应急响应技术的发展趋势 了解网络安全应急响应技术框架 了解网络安全应急响应新发展
2	网络安全应急响应技术基础知识	掌握风险评估相关概念、流程 了解风险评估与应急响应的关系 了解安全事件分级分类
3	网络安全应急响应技术流程与方法	熟练掌握应急响应准备阶段、抑制阶段、保护阶段、事件检测阶段、取证阶段、根除阶段、恢复阶段、总结报告等各阶段知识
4	应急演练	了解应急演练定义、目的、原则 了解应急演练分类及方法 了解应急演练的组织架构 了解应急演练流程和规划 掌握应急演练的实施和总结
5	网络安全事件应急处置实战	掌握常见 Web 攻击应急处置实战知识 掌握信息泄露类攻击应急处置实战知识 掌握主机类攻击应急处置实战知识 掌握有害事件应急处置实战知识
6	分析排查	掌握 windows/Linux 的分析排查知识

附 录 I
（规范性）
云计算安全考试大纲

I.1 目的

为使考生达到本文件中网络空间安全专业人员在云计算方向二级、三级能力要求，指导考生有效准备考试，特制定本考试大纲（以下简称大纲）。

I.2 考试内容

I.2.1 课程要求

表 I.1 云计算安全课程要求

课程名称	课程类型	选择范围
云计算基础	基础课程	全部
云计算信息安全及产品	基础课程	全部
云计算信息安全管理及标准	专业课程	全部
访问控制及身份鉴别	专业课程	全部
基础设施和虚拟化安全	专业课程	全部

I.3 各课程知识点要求

I.3.1 云计算基础

表 I.2 云计算基础课程内容与知识点

章节号	章节名	内容与知识点
1	云计算的定义、特点及发展历史	了解云计算的定义及基本概念、发展历史和主要特点 掌握云计算与传统 HT 的区别
2	云计算数据中心的组成	了解云计算数据中心分类和建设标准 掌握云计算数据中心的基本架构、云计算系统的组成、安全体系架构
3	云计算服务的分类	了解云计算服务的分类，各类服务包含的具体产品类别及相互关系
4	主流云计算厂商及技术	了解云计算行业内主流国内和国外厂商产品、服务及特点 了解各云计算厂商的主要技术及发展趋势
5	云存储技术及产品	了解云存储技术的种类及特点 掌握云存储产品和服务所使用的技术和特点
6	虚拟化技术及发展	了解不同层次的虚拟化技术及分类、虚拟化发展的方向 掌握典型虚拟化方案的具体实现

I.3.2 云计算信息安全及产品

表 I.3 云计算信息安全及产品课程内容与知识点

章节号	章节名	内容与知识点
1	云计算安全与传统信息安全的特点比较	了解云计算环境与传统 HT 信息安全方面的面临问题的差异
2	云计算主要的安全问题及分类	了解云计算面临在主要安全问题及分类 掌握安全威胁的种类、基本原理和防御手段
3	云计算网络安全及产品	了解云计算安全产品和服务的分类 掌握各厂商特色安全产品及特点 熟悉安全等级保护对应的安全产品

I.3.3 云计算信息安全管理及标准

表 I.4 云计算信息安全管理及标准课程内容与知识点

章节号	章节名	内容与知识点
1	云计算相关国际、国内标准及规定	了解云计算安全管理标准化工作概况 掌握 HSO27001、HSO27018 等主要安全管理标准及对应的国家标准
2	云计算安全管理的规定和要求	掌握《网络安全法》、《计算机信息系统安全保护条例》等主要法律法规对云计算的要求
3	信息安全管理体系、方法及安全评估模型	了解云计算安全管理体系及管理方法 了解云计算信息安全评估模型

I.3.4 访问控制及身份鉴别

表 I.5 访问控制及身份鉴别课程内容与知识点

章节号	章节名	内容与知识点
1	主机的访问控制	了解云计算虚拟主机的访问控制相关技术 了解访问控制模型及实现机制 掌握常用的访问控制手段和控制策略
2	SSL、VPN 及堡垒机	了解 SSL、VPN 及堡垒机涉及的相关安全技术 了解主流厂商产品及特点 掌握 SSL、VPN 及堡垒机在云资源的安全使用和运维方面的作用
3	身份鉴别及密码技术	了解云计算环境身份鉴别面临的挑战，熟悉鉴别与授权、身份管理、公钥密码体系等技术及应用 了解国家相关标准在身份鉴别方面的要求

I.3.5 基础设施和虚拟化安全

表 I.6　基础设施和虚拟化安全课程内容与知识点

章节号	章节名	内容与知识点
1	云数据中心的安全	了解云计算数据中心面临的安全问题，掌握云技术数据中心相关的安全设计及防护方法
2	主机虚拟化安全	了解虚拟化架构及安全挑战、熟悉主流虚拟化管理软件及技术特点，了解虚拟化安全相关技术及解决方案

附 录 J
（规范性）
物联网安全考试大纲

J.1 目的

为使考生达到本文件中网络空间安全专业人员在物联网安全方向二、三级级能力要求，指导考生有效准备考试，特制定本考试大纲（以下简称大纲）。

J.2 考试内容

J.2.1 课程要求

表 J.1 物联网安全课程要求

课程名称	课程类型	选择范围
物联网安全基础	基础课程	全部
物联网安全系统规划与实现	专业课程	全部
物联网安全管理与运维	专业课程	全部
物联网渗透测试	专业课程	全部
物联网安全职业素养	基础课程	全部

J.3 各课程知识点要求

J.3.1 物联网安全基础

表 J.2 物联网安全基础课程内容与知识点

章节号	章节名	内容与知识点
1	物联网安全概述	了解物联网发展过程，理解物联网生态，物联网安全模型以及安全特性
2	物联网密码学基础	掌握密钥学、密钥管理等相关知识 理解几种典型的密钥管理方案，评估方案优缺点
3	物联网设备安全开发方法	理解物联网设备安全设计和部署采用的各种工程方法
4	物联网漏洞、攻击及其应对措施	理解物联网面临的各种威胁以及应对措施

J.3.2 物联网安全系统规划与实现

表 J.3　物联网安全系统规划与实现

章节号	章节名	内容与知识点
1	物联网安全设计方法	掌握物联网设备的安全设计方法，理解物联网安全的设计目标
2	物联网接入安全设计	理解物联网身份识别和访问控制管理机制 理解物联网设备授权和访问控制的设计方法
3	物联网安全机制设计	掌握物联网安全路由、物联网安全时间同步、物联网安全数据融合等设计方法
4	物联网安全访问控制策略	掌握物联网访问控制策略的特点 理解当前物联网安全访问控制策略的设计
5	物联网云端安全设计	掌握物联网云端安全机制 理解云计算、雾计算以及物联网云服务上的安全策略设计
6	物联网安全系统实现	掌握物联网安全系统设计流程，理解物联网安全平台使用的各种安全机制及其实施

J.3.3　物联网安全管理与运维

表 J.4　物联网安全管理与运维课程内容与知识点

章节号	章节名	内容与知识点
1	物联网系统风险评估	了解物联网隐私相应评估指南，隐私保护设计原则等
2	物联网系统合规性监管	掌握物联网设备合规性监管及制定物联网合规程度的方法 掌握构建或调整物联网合规性监管方法
3	物联网安全事件管理与取证	掌握物联网安全事件管理内容，理解物联网事件响应方法的制定、规划与实施，检测与分析以及取证等解决办法
4	物联网安全运维	了解物联网系统安全生命周期，理解物联网安全规划、部署、管理、监控与检测、修复与处置等方面的运维方法

J.3.4　物联网渗透测试

表 J.5　物联网渗透测试课程内容与知识点

章节号	章节名	内容与知识点
1	IoT 渗透测试基础	掌握开展 IoT 渗透测试的基础知识 掌握 IoT 渗透测试环境的部署
2	IoT 威胁建模	掌握 IoT 威胁建模概念及方法 掌握 IoT Web 应用、移动应用、设备硬件以及无线电通信的威胁建模

表 J.5　物联网渗透测试课程内容与知识点（续）

3	固件分析与漏洞利用	理解固件分析方法、固件提取、固件分析文件系统分析等内容 重点掌握 IoT Web 应用、移动应用漏洞利用
4	IoT 设备攻击技术	理解 IoT 设备硬件攻击方法以及分析技术、无线电攻击技术等，理解 IoT 设备中漏洞挖掘与利用
5	IoT 自动化防护	理解 IoT 设备中高级漏洞利用技术 掌握采用自动化方法避免 IoT 设备出现漏洞

附 录 K
（规范性）
人工智能安全考试大纲

K.1 目的

为使考生达到本文件中网络空间安全专业人员人工智能安全方向二级、三级能力要求，指导考生有效准备考试，特制定本考试大纲（以下简称大纲）。

K.2 考试内容

K.2.1 课程要求和考试比例

表 K.1 人工智能安全课程要求

课程名称	课程类型	选择范围
信息安全技术	基础课程	全部
人工智能	专业课程	全部
人工智能安全	专业课程	全部

K.3 各课程知识点要求

K.3.1 人工智能

表 K.2 人工智能课程内容与知识点

章节号	章节名	内容与知识点
1	基本概念	了解人工智能的概念 了解 AI 的发展历程和现状
2	Python 入门	掌握 Python 基础知识 掌握 Python 列表、元组和字典 掌握 Python 的条件和循环、函数与模块 掌握 Python 的数据分析知识
3	人工智能数学基础	掌握人工智能的线性代数、微积分、概率论和数理统计知识
4	人工神经网络	掌握神经元知识，如人工神经网络结构、梯度消失与梯度爆炸 掌握损失函数、激活函数等知识 掌握手工搭建神经网络的知识方法
5	TensorFlow 与 PyTorch	了解 TensorFlow 的安装和使用 了解 PyTorch 的安装和使用 掌握其他深度学习框架，如 Keras、Caffe、MXNet、Sonnet、Deepleaning4j 等

表 K.2　人工智能课程内容与知识点（续）

章节号	章节名	内容与知识点
6	卷积神经网络	了解卷积神经网络的起源、发展、应用概况 掌握卷积神经网络结构 掌握训练卷积神经网络
7	目标分类	了解目标分类的概念、种类 掌握模型健壮性判断知识 掌握常用的数据集
8	目标检测	了解目标检测的基本知识 掌握区域卷积神经网络知识 掌握 YOLO 卷积神经知识 掌握单发多框检测（SSD）知识
9	图像语义分割	了解图像语义分割基本知识 掌握分割方法 掌握自然图像分割模型 FCN 掌握医学图像分割模型 U-Net
10	循环神经网络	了解循环神经网络理论基础 掌握长短期记忆网络 掌握 TensorFlow 2.0 中的 Cell 分类，通过 cell 类构建 RNN
11	自然语言处理	掌握自然语言处理基本知识，如机器翻译、信息检索、自动文摘、问答系统、信息过滤、信息抽取、文本分类、语音识别等 了解常用技术，如分词、停用词过滤、词干提取、词形还原、命名实体识别、序列标注、词向量与词嵌入 实操：手动写 word2Vec、基于 LSTM 的评论情感分析
12	生成对抗网络	了解生成对抗网络 掌握 GAN 结构的变体 掌握 GAN 的应用
13	强化学习	了解强化学习的特点和组成部分 掌握马尔可夫决策过程和动态规则 掌握基于值函数的学习方法 掌握基于策略函数的学习算法 掌握 Actor-Critic 算法

K.3.2　人工智能安全

表 K.3　人工智能安全课程内容与知识点

章节号	章节名	内容与知识点
1	人工智能安全概述	了解人工智能与安全的辩证关系 了解人工智能安全架构与分类 了解人工智能所处位置及外部关联，如人工智能安全性、可靠性和可控性的关系、人工智能安全与法律、政策和标准的关系；人工智能安全与伦理之间的关系；人工智能安全测评与防控；
2	人工智能助力安全	了解人工智能助力安全基本概念 掌握人工智能助力防御知识，如物理智能安防监控、智能入侵检测、恶意代码检测与分类、基于知识图谱的威胁猎杀、用户实体行为分析、垃圾邮件检测 掌握人工智能助力攻击知识，如自动化网络攻击、助力于网络攻击和有害信息传播、虚假信息内容的制作；智能恶意代码、神经网络后门、对抗机器学习等
3	人工智能的内生安全	掌握人工智能的内生安全知识，如数据安全、框架安全、算法安全、模型安全、运行安全等
4	人工智能衍生安全	掌握人工智能衍生安全问题，如人工智能系统失误引发的安全事故； 掌握人工智能行为体失控三要素 掌握预防人工智能技术失控的举措
5	人工智能行为体	了解人工智能行为体的定义； 了解人工智能行为体的类型 掌握人工智能行为体的特性
6	人工智能行为体的保险箍	了解保险箍的体系架构和基本功能 掌握保险箍的安全机制与安全围栏知识 掌握保险箍的增强功能、防控中心、生态环境知识
7	人工智能行为体的安全评估和检测	了解人工智能行为体的安全管理知识，如安全要素、风险评估、安全要求、功能评估等 掌握人工智能行为体安全评估和检测的目标和方法、指标 掌握人工智能行为体的检测流程
8	人工智能安全伦理准则	了解人工智能技术引发的伦理问题，如人权问题、伦理地位、责任伦理、风险问题 了解人工智能技术发展的伦理准则 了解人工智能行为体的伦理决策 了解人工智能行为体的责任归咎

附 录 L
（规范性）
大数据安全考试大纲

L.1 目的

为使考生达到本文件中网络空间安全专业人员在大数据安全方向二级、三级能力要求，指导考生有效准备考试，特制定本考试大纲（以下简称大纲）。

L.2 考试内容

L.2.1 课程要求

表 L.1 大数据安全课程要求

课程名称	课程类型	选择范围
信息安全技术	基础课程	全部
大数据技术与应用	专业课程	全部
大数据安全	专业课程	全部

L.3 各课程知识点要求

L.3.1 大数据技术与应用

表 L.2 大数据技术与应用课程内容与知识点

章节号	章节名	内容与知识点
1	了解大数据	了解大数据处理的基础技术，如大数据相关概念、处理流程、基础技术 了解主流大数据技术 了解大数据平台解决方案 了解大数据发展现状和趋势
2	大数据基础软件	掌握 Linux 基础知识 掌握 Java 基础知识 掌握 SQL 语言基础知识 了解数据库基础知识
3	大数据采集	了解大数据采集技术 了解大数据采集工具 了解八爪鱼、爬山虎采集器 了解流数据采集工具 Flume 了解数据传输工具 Sqoop 工具

表 L.2　大数据技术与应用课程内容与知识点（续）

章节号	章节名	内容与知识点
4	大数据存储	了解数据库和数据仓库基本知识 了解分布式文件系统 HDFS 了解分布式分析引擎 Kylin 基本原理、架构、特性 了解大数据仓库 Hive 的基本原理、架构和数据存储模型、应用场景 了解 NoSQL 数据库 了解键－值存储数据库 Memcached、Redis 了解面向文档数据库 MongoDB
5	Spark 内存计算框架	了解 Spark 基础知识，如技术原理、运行架构 了解 RDD 基本概念 了解 Spark SQL 实时处理技术，掌握 Spark MLlib 数据挖掘库知识 掌握机器学习知识
6	大数据分析挖掘	了解数据分析和数据挖掘的区别、常见数据分析挖掘工具 了解数据挖掘十大算法 掌握分类算法、决策树算法、推荐算法、Apriori 算法知识
7	大数据可视化	了解大数据可视化基本知识、流程、展现形式 掌握大数据可视化工具 掌握 Tableau、Power BI 大数据可视化技术知识
8	大数据应用	了解大数据在企业中的应用 了解互联网大数据的应用 了解大数据在零售、医疗领域的应用

L.3.2　大数据安全

表 L.3　大数据安全课程内容与知识点

章节号	章节名	内容与知识点
1	大数据安全挑战和现状	了解大数据的概念、特性和安全需求 了解大数据技术和平台的安全，如数据安全和个人信息保护、国家社会安全和法规标准 了解大数据安全现状，如国家安全法、网络安全法、大数据安全管理指南、数据安全能力成熟度模型、个人信息安全规范等
2	大数据治理	了解大数据治理概念和重要性 掌握大数据治理的原则和范围

		了解大数据技术架构 了解大数据治理实施的目标、动力、实施过程

表 L.3　大数据安全课程内容与知识点（续）

章节号	章节名	内容与知识点
3	大数据安全创建	掌握大数据采集的分类分级、安全管理、数据源鉴别和记录知识 掌握大数据的导入导出基本原则、安全策略、制度流程 掌握大数据查询的特权账户管理、敏感数据的访问控制等知识
4	大数据的传输和存储安全	掌握大数据的传输加密知识，如大数据内容加密、网络加密、身份认证、签名与验签等 掌握网络可用性的管理指标、负载均衡、大数据方泄露知识 掌握大数据存储知识
5	大数据处理安全	掌握数据脱敏知识 掌握大数据分析安全知识 掌握大数据正当使用知识 了解大数据处理环境，如 Hadoop、Spark 等处理平台知识
6	大数据安全交换	了解大数据安全交换概念、面临的安全威胁 掌握大数据共享原则、模型、安全框架知识 掌握大数据数据接口安全限制、格式规范、异常检测应用等知识
7	大数据恢复与销毁	掌握大数据备份知识，如备份类型、加密等； 掌握大数据恢复知识 掌握大数据销毁处置知识 掌握存储媒体的销毁处置策略和方法
8	大数据安全态势感知	掌握大数据安全态势感知平台知识 掌握数据融合的技术和方法方面的知识 掌握数据挖掘技术和特征提取技术知识 掌握态势预测技术知识

附 录 M
（规范性）
工业控制系统安全考试大纲

M.1 目的

为使考生达到本文件中网络空间安全专业人员在工业控制系统安全方向二级、三级能力要求，指导考生有效准备考试，特制定本考试大纲（以下简称大纲）。

M.2 考试内容

M.2.1 课程要求

表 M.1 工业控制系统安全课程要求

课程名称	课程类型	选择范围
信息安全技术	基础课程	全部
工业控制系统安全	专业课程	全部

M.3 各课程知识点要求

M.3.1 工业控制系统安全

表 M.2 工业系统控制安全课程内容与知识点

章节号	章节名	内容与知识点
1	工业控制系统概述	了解工业控制系统的显示功能、监控功能、控制功能知识 了解工业控制系统架构，如可编程逻辑控制器、人机界面、监控和数据采集、分布式控制系统、安全仪表系统等 了解 Purdue 工业控制系统模型 掌握工业控制系统通讯介质和协议知识
2	工业控制系统安全概述	了解工业控制系统安全的历史 了解 Modbus 及其协议知识 了解 PROFINET 了解 ICS 中常见的 IT 协议
3	ICS 工具场景剖析	掌握 ICS 攻击场景知识
4	ICS 风险评估	了解 ICS 攻击、目标和结果 掌握 ICS 风险评估知识，如资产识别和系统特性、漏洞识别和威胁建模、风险计算及风险缓解等
5	Purdue 模型与全厂融合以太网	掌握 Purdue 企业参考架构知识

表 M.2　工业系统控制安全课程内容与知识点（续）

章节号	章节名	内容与知识点
6	深度防御模型	掌握 ICS 物理安全、网络安全、计算机安全、应用安全、设备安全知识 掌握 ICS 安全策略、流程和安全意识
7	ICS 物理安全	熟练掌握 ICS 物理安全知识
8	ICS 网络安全	熟练掌握 ICS 网络安全知识
9	ICS 计算机安全	熟练掌握 ICS 计算机安全知识，如终端加固、配置和变更管理、终端保护软件等
10	ICS 应用安全	熟练掌握 ICS 应用安全知识，如输入验证漏洞、软件篡改、认证漏洞、授权漏洞、非安全配置漏洞、会话管理漏洞、参数操纵漏洞等 熟练掌握应用安全测试、应用补丁等知识 了解 ICS 安全 SDLC
11	ICS 设备安全	熟练掌握 ICS 设备加固、设备补丁、设备生命周期等知识
12	ICS 网络安全计划开发过程	熟练掌握 ICS 网络安全开发过程知识，如安全策略、标准、指南和程序等

附 录 N
（规范性）
网络安全审计考试大纲

N.1 目的

为使考生达到本文件中网络空间安全专业人员在网络安全审计方向二级、三级能力要求，指导考生有效准备考试，特制定本考试大纲（以下简称大纲）。

N.2 考试内容

N.2.1 课程要求和考试比例

表 N.1 网络安全审计课程要求

课程名称	课程类型	选择范围
网络安全管理实践	基础课程	全部
信息安全技术	基础课程	全部
信息安全审计	专业课程	全部

N.3 各课程知识点要求

N.3.1 信息安全审计

表 N.2 信息安全审计课程内容与知识点

章节号	章节名	内容与知识点
1	信息安全审计概述	了解信息安全现状 了解信息系统面临的主要安全威胁 了解信息安全目标与主要安全 掌握信息系统安全设计知识，如信息系统的安全保护等级、信息系统安全风险的分析与控制等 了解信息安全事件、信息安全审计概念等
2	信息安全技术	了解信息系统安全基本概念、安全威胁与防范
3	实体访问控制的审计	掌握 IT 组织与策略的审计知识 掌握实体级控件的风险与管理的审计知识 掌握实体级控件相关的审计知识
4	数据中心和灾备机制的审计	了解数据中心的核心作用 掌握数据中心的审计过程
5	路由器/防火墙的审计	了解路由器和防火墙审计的重要性 掌握路由器和防火墙审计的知识

表 N.2　信息安全审计课程内容与知识点（续）

章节号	章节名	内容与知识点
6	Web 应用的审计	掌握主机操作系统审计知识 掌握 Web 服务器审计知识 掌握 Web 应用审计知识
7	数据库与云存储的审计	掌握数据库的审计知识 掌握与计算和外部运营的审计知识 掌握云存储的审计知识
8	信息系统的审计	掌握信息系统开发原理、基本流程和规范 掌握信息系统安全机制如身份认证、访问控制、消息认证技术 掌握信息系统安全审计知识，如审计流程和分析方法
9	信息安全审计风险、标准和法规	掌握信息安全管理和风险评估知识 掌握信息安全审计标准与法规 掌握信息安全等级保护知识
10	信息安全审计流程	掌握 COSO 知识 掌握 COBIT 知识 掌握 IT 基础架构库知识 了解美国国家安全局信息技术评估方法 了解我国的信息系统安全审计

附 录 0
（规范性）
渗透测试考试大纲

0.1 目的

为使考生达到本文件中网络空间安全专业人员在渗透测试方向二级、三级能力要求，指导考生有效准备考试，特制定本考试大纲（以下简称大纲）。

0.2 考试内容

0.2.1 课程要求

表 0.1 渗透测试课程要求

课程名称	课程类型	选择范围
信息安全技术	基础课程	全部
渗透测试	专业课程	全部

0.3 各课程知识点要求

0.3.1 渗透测试

表 0.2 渗透测试课程内容与知识点

章节号	章节名	内容与知识点
1	渗透测试基础	了解渗透测试标准、流程、方法、原则、报告等内容 了解安全政策法规、标准
2	渗透测试工具	掌握渗透测试平台、工具
3	信息收集原理与实践	了解搜索引擎技术 掌握域名信息收集、服务器信息收集、Web 信息收集、和其他信息收集知识
4	Web 攻防原理	掌握文件上传漏洞、下载漏洞、文件包含漏洞、SQL 注入漏洞、命令执行漏洞、业务逻辑漏洞等知识 掌握 XSS 跨站脚本攻击、XXE XML 实体注入、SSRF 服务端请求伪造等知识
5	中间件安全	了解中间件分类、Web 中间件知识 掌握 Apache 安全、IIS 安全、Tomcat 安全、WebLogic 安全等知识
6	操作系统安全	掌握操作系统 windows、Linux 知识
7	数据库安全	掌握 SQL Server、MySQL、Oracle、其他数据库安全等知识

表 0.2　渗透测试课程内容与知识点（续）

章节号	章节名	内容与知识点
8	高级渗透技术	掌握 Web Shell 查杀技术 掌握 WAF 鉴别与探测技术 掌握反弹 Shell 技术 掌握提权技术知识
9	实战实例	掌握企业综合网络拓扑知识 掌握综合渗透思路、实践、网络安全防护等知识

参 考 文 献

[1] GB/T 18336.1—2015 信息技术 安全技术 信息技术安全评估准则 第1 部分：简介和一般模型

[2] GB/T 27203-2016 合格评定 用于人员认证的人员能力词汇

[3] GB/T 27024-2014 合格评定 人员认证机构通用要求