国家基本职业培训包（指南包 课程包）

网络与信息安全管理员

（征求意见稿）

人力资源社会保障部职业能力建设司 编制

中国劳动社会保障出版社

目　录

1/指南包

1.1 职业培训包使用指南

1.1.1 职业培训包结构与内容

网络与信息安全管理员职业培训包由指南包、课程包、资源包三个子包构成，结构如图 1 所示。

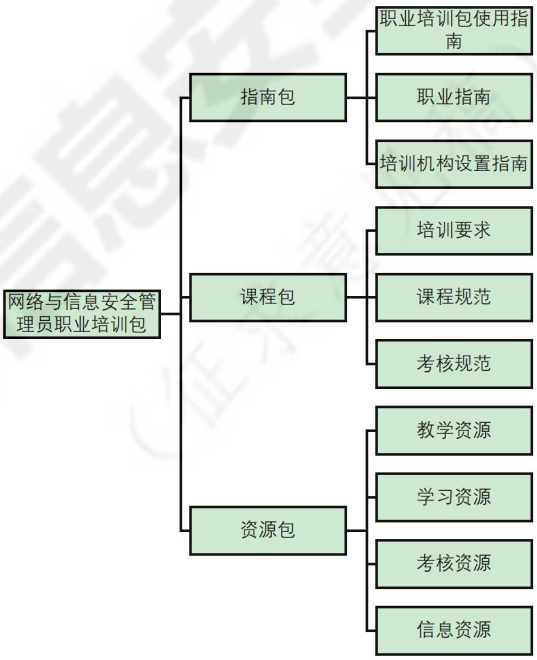

图 1 职业培训包结构图

指南包是指导培训机构、培训教师与学员开展职业培训的服务性内容总合，包括职业培训包使用指南、职业指南和培训机构设置指南。培训包使用指南是培训教师与学员了解职业培训包内容、选择培训课程、使用培训资源的说明性文本，职业指南是对职业信息的概述，培训机构设置指南是对培训机构开展职业培训提出的具体要求。

课程包是培训机构与教师实施职业培训、培训学员接受职业培训必须遵守的规范总和，包括培训要求、课程规范、考核规范。培训要求是参照国家职业技能标准、结合职业岗位工作实际需求制定的职业培训规范。课程规范是依据培训要求、结合职业培训教学规律，对课程设置、课堂学时、课程内容与培训方法等所

做的统一规定；考核规范是针对课程规范中所规定的课程内容开发的，能够科学评价培训学员过程性学习效果与终结性培训成果的规则，是客观衡量培训学员职业基本素质与职业技能水平的标准，也是实施职业培训过程性与终结性考核的依据。

资源包是依据课程包要求，基于培训学员特征，遵循职业培训教学规律，应用先进职业培训课程理念，开发的多媒介、多形式的职业培训与考核资源总和，包括教学资源、学习资源、考核资源和信息资源。教学资源是为培训教师组织实施职业培训教学活动提供的相关资源；学习资源是为培训学员学习职业培训课程提供的相关资源；考核资源是为培训机构和教师实施职业培训考核提供的相关资源；信息资源是为培训教师和学员拓宽视野提供的体现科技进步、职业发展的相关动态资源。

1.1.2 培训课程体系介绍

网络与信息安全管理员职业培训课程体系依据职业技能等级分为职业基本素质培训课程、四级/中级职业技能培训课程、三级/高级职业技能培训课程、二级/技师职业技能培训课程和一级/高级技师职业技能培训课程，每一类课程包含模块、课程和学习单元三个层级。网络与信息安全管理员职业培训课程体系均源自本职业培训包课程包中的课程规范，以学习单元为基础，形成职业层次清晰、内容丰富的“培训课程超市”。

网络与信息安全管理员职业培训课程学时分配一览表

职业技能等级	课堂学时		其他学时	培训总学时
	职业基本素质培训课程	职业技能培训课程		
四级/中级	24	56	80	160
三级/高级	24	56	80	160
二级/技师	16	40	64	120
一级/高级技师	0	40	40	80

注：课堂学时是指培训机构开展的理论课程教学及实操课程教学的建议最低学时数。除课堂学时外，培训总学时还应包括岗位实习、现场观摩、自学自练等其他学时。

（1）职业基本素质培训课程

模块	课程	学习单元	课堂学时
1.职业认知与职业道德	1-1 职业认知	职业认知	1
	1-2 职业道德基本知识	道德与职业道德	1
	1-3 职业守则	职业守则	1
2.计算机相关知识	2-1 计算机硬件基础知识	计算机硬件	1
	2-2 计算机软件基础知识	计算机软件	1
	2-3 操作系统基础知识	操作系统	1
	2-4 数据库基础知识	数据库	1
3. 网络相关知识	3-1 网络协议基础知识	网络体系结构与协议	1
	3-2 组网设备基础知识	（1）组网设备概述	1
		（2）路由器基础知识	1
		（3）交换机基础知识	1
	3-3 网络配置、故障排查常用命令和工具基础知识	网络配置、故障排查常用命令和工具	2
4.网络安全基础知识	4-1 网络安全概述	网络安全概述	2
	4-2 网络安全基础技术	网络安全基础技术	3
5. 相关法律法规、标准知识	5-1 法律、法规知识	法律、法规知识	3
	5-2 标准知识	标准知识	3
课堂学时合计			24

注：本表所列为初级职业基本素质培训课程，其他等级职业基本素质培训课程按“网络与信息安全管理员职业培训课程学时分配一览表”中相应的课堂学时要求进行必要的调整。

（2）四级/中级职业技能培训课程（网络安全管理员、信息安全管理员）

模块	课程	学习单元	课堂学时
1.网络与信息安全防护	1-1 网络安全配置与防护	（1）配置网络设备接口信息	2
		（2）配置路由协议	2
		（3）配置无线网络设备	2
		（4）配置网络设备基础安全设置	2
	1-2 系统安全配置与防护	（1）配置 Windows 操作系统密码策略与账户策略	2
		（2）配置 Linux 操作系统密码策略与账户策略	2
		（3）配置 Windows 操作系统	1

		自带的防火墙	
		（4）配置 Linux 操作系统自带的防火墙	1
		（5）安装部署防病毒软件	2
		（6）配置 Windows 系统高级安全审核	1
		（7）配置 Linux 系统审核功能	1
	1-3 应用安全配置及防护	（1）配置常见的应用服务	2
		（2）配置应用服务的基本防护	2
2.网络与信息安全管理	2-1 网络安全管理	（1）配置交换机的 VLAN	2
		（2）配置网络设备的远程管理	2
		（3）管理网络设备的用户安全级别	2
	2-2 系统安全管理	（1）管理 Windows 系统用户与组的基本配置	2
		（2）管理 Linux 系统用户与组的基本配置	2
		（3）管理 Windows 系统文件及文件夹的访问权限	1
		（4）管理 Linux 系统文件及文件夹的访问权限	1
		（5）操作系统补丁更新	2
		（6）防病毒软件安全保护策略配置和定期升级服务	2
	2-3 应用安全管理	（1）企业域名备案	2
		（2）配置企业应用域名解析	2
		（3）应用数据备份	2
3.网络与信息安全处置	3-1 网络安全事件处置	（1）使用网络诊断工具识别及处理常见网络故障	2
		（2）识别常见网络层攻击	2
	3-2 系统及应用安全事件处置	（1）常见系统安全事件识别	2
		（2）恶意代码检测与清除	4
		（3）应用数据恢复	2
课堂学时合计			56

（3）三级/高级职业技能培训课程（网络安全管理员、信息安全管理员）

模块	课程	学习单元	课堂学时
1.网络与信息安全防护	1-1 网络安全防护	（1）安全加固企业级交换机、路由器	2
		（2）部署配置边界防护设备	2
		（3）部署配置入侵检测/防御系统	2
		（4）部署配置无线网络安全	1
		（5）部署配置网络安全审计设备	1
	1-2 系统安全防护	（1）配置系统安全策略	2
		（2）配置系统自带防火墙访问控制规则	2
		（3）防范常见恶意代码	2
	1-3 应用安全防护	（1）配置数据加密传输	2
		（2）部署配置 Web 应用防火墙	2
		（3）部署配置应用安全审计	2
2.网络与信息安全管理	2-1 网络安全管理	（1）配置防火墙网络访问控制管理	2
		（2）管理各类终端接入无线网络	2
		（3）管理各类边界设备、网络节点远程访问	1
		（4）留存网络设备安全日志	1
	2-2 系统安全管理	（1）管理安全远程访问	2
		（2）管理系统漏洞和风险	2
		（3）管理应用系统备份	2
		（4）管理系统日志	1
		（5）应用系统备案	1
	2-3 应用安全管理	（1）安全管理互联网应用	2
		（2）过滤垃圾邮件等有害数据	2
		（3）管理审计互联网访问日志	2
3.网络与信息安全处置	3-1 网络安全事件监控和处置	（1）网络数据流量监控	2
		（2）攻击流量阻断	1
		（3）网络安全日志留存	1
	3-2 系统安全事件监控和处置	（1）识别、隔离被入侵或感染病毒的计算机	2
		（2）识别系统异常状态及系统后门清除	2
		（3）系统异常状态检测及恢复	1
		（4）病毒样本留存及上报	1
	3-3 应用安全事件监控和处置	（1）提取数据库、Web 服务应用访问日志	2

		（2）日志分析、识别及定位事件	2
		（3）违法有害信息识别及处置	1
		（4）互联网安全事件记录、证据留存及上报	1
课堂学时合计			56

（4）二级/技师职业技能培训课程（网络安全管理员）

模块	课程	学习单元	课堂学时
1.网络与信息安全防护	1-1 网络安全防护	（1）网络漏洞扫描、分析及安全加固	1
		（2）安全域配置及安全策略配置	1
		（3）配置重要设备硬件冗余	1
		（4）配置虚拟专用网络（VPN）	1
	1-2 系统安全防护	（1）系统安全扫描及风险分析	2
		（2）启用数据加密策略对应用数据进行保护	1
	1-3 应用安全防护	（1）互联网应用漏洞扫描及风险分析	1
		（2）漏洞测试及验证	1
		（3）配置 Web 应用防火墙	1
		（4）规划反垃圾邮件网关实施方案	1
2.网络与信息安全管理	2-1 网络安全等级保护	（1）网络安全等级保护基础	2
		（2）网络安全基线配置检查及加固整改	2
	2-2 应用安全评估	（1）互联网服务自评估	1
		（2）信息网络安全技术方案制定	1
		（3）渗透测试工作配合	2
		（4）根据渗透测试报告进行加固	2
3.网络与信息安全处置	3-1 网络安全事件监测	（1）网络链路运行状况监测	2
		（2）网络设备运行状况监测	1
		（3）安全设备运行状况监测	1
		（4）系统运行状况监测	1
	3-2 网络安全事件分析	（1）设备监测数据清洗、汇总	2
		（2）设备监测数据分析	2
	3-3 网络安全事件响应	（1）常见网络安全事件响应	2
		（2）常见网络攻击溯源和上报	1
		（3）留存网络安全事件相关证据记录	1
4.培训指导	4-1 培训实施	（1）制订培训工作计划	1
		（2）编制和实施培训方案	1

		（3）编写培训教材、讲义、课件	1
		（4）培训宣讲	1
	4-2 技术指导	（1）技能指导	1
		（2）技能水平考核	1
课堂学时合计			40

（5）二级/技师职业技能培训课程（信息安全管理员）

模块	课程	学习单元	课堂学时
1.网络与信息安全防护	1-1 信息资产安全防护	（1）信息资产分类分级	2
		（2）安全域资源防护策略制定	2
	1-2 数据安全防护	（1）数据安全存储策略、数据加密策略配置	2
		（2）制定数据容灾策略	2
	1-3 互联网信息安全防护	（1）重要信息脆弱性评估及防护	2
		（2）员工个人信息安全策略配置	2
2.网络与信息安全管理	2-1 数据安全管理	（1）数据在存储、通信中的公私钥和证书管理	2
		（2）数据高可用管理	2
		（3）重要数据保护	1
	2-2 互联网信息安全管理	（1）履行信息安全管理义务	2
		（2）编制个人敏感信息安全保护技术方案	2
		（3）个人敏感信息脆弱性评估及防护	1
3.网络与信息安全处置	3-1 信息安全事件监测	（1）监测信息破坏事件	2
		（2）监测信息内容安全事件	2
		（3）监测其他信息安全事件	1
	3-2 信息安全事件分析	（1）信息安全监测数据清洗、汇总	2
		（2）信息安全监测数据分析	1
	3-3 信息安全事件响应	（1）常见信息安全事件响应	2
		（2）常见信息安全事件溯源和上报	1
		（3）留存信息安全事件相关证据记录	1
4.培训指导	4-1 培训实施	（1）制订培训工作计划	1
		（2）编制和实施培训方案	1
		（3）编写培训教材、讲义、课件	1
		（4）培训宣讲	1
	4-2 技术指导	（1）技能指导	1
		（2）技能水平考核	1
课堂学时合计			40

（6）一级/高级技师职业技能培训课程（网络安全管理员）

模块	课程	学习单元	课堂学时
1.网络与信息安全防护	1-1 网络安全风险评估	（1）组织整体业务系统安全风险评估	2
		（2）网络和应用系统渗透测试及漏洞验证和修补	2
	1-2 新技术、新应用安全防护	（1）云计算应用安全防护策略	2
		（2）物联网应用安全防护策略	1
		（3）移动互联应用安全防护策略	1
		（4）工业控制系统安全防护策略	1
		（5）大数据应用安全防护策略	1
		（6）区块链等其他新技术新应用安全防护策略	1
2.网络与信息安全管理	2-1 网络安全风险管理	（1）网络安全风险管理	1
		（2）漏洞评估及制定安全管理措施	2
	2-2 网络安全等级保护	（1）网络安全等级保护定级	2
		（2）网络安全等级保护备案	1
		（3）网络安全等级保护建设整改	2
		（4）网络安全自我监督检查	1
	2-3 关键信息基础设施保护	（1）关键信息基础设施安全检查	1
		（2）制定关键信息基础设施安全加固方案	2
		（3）网络安全事件应急方案编制	1
3.网络与信息安全处置	3-1 网络安全事件预警	（1）建立安全事件威胁预警机制	2
		（2）网络安全事件风险定级、设计响应级别和应急预案	1
	3-2 网络安全事件证据保存	（1）静态数据提取及固定	2
		（2）动态易失数据提取及固定	1
	3-3 网络安全事件应急响应	（1）复杂网络安全事件应急响应	2
		（2）恢复网络安全事件造成的网络或系统损坏	1
4.培训指导	4-1 培训实施	（1）培训需求分析	1
		（2）编制培训规划	1

		（3）组织编写培训教材、讲义、教案	1
		（4）进行培训宣讲	1
	4-2 技术指导	（1）技能指导	1
		（2）技能水平考核	1
		（3）组织开展技术改造、技术革新活动	1
课堂学时合计			40

（7）一级/高级技师职业技能培训课程（信息安全管理员）

模块	课程	学习单元	课堂学时
1.网络与信息安全防护	1-1 信息安全风险评估	（1）组织关键业务系统风险评估	2
		（2）出具信息安全风险评估报告	2
		（3）制定信息安全风险整改措施	2
	1-2 新技术、新应用安全防护	（1）云计算应用安全防护策略	1
		（2）物联网应用安全防护策略	1
		（3）移动互联应用安全防护策略	1
		（4）工业控制系统安全防护策略	1
		（5）大数据应用安全防护策略	1
		（6）区块链等其他新技术新应用安全防护策略	1
2.网络与信息安全管理	2-1 信息安全风险管理	（1）制定信息安全风险管理制度	2
		（2）制定风险评估方案	2
		（3）业务系统安全风险处置方案编制	1
	2-2 网络安全等级保护	（1）网络安全等级保护定级	2
		（2）网络安全等级保护备案	1
		（3）设计和制定安全管理制度	1
	2-3 关键信息基础设施保护	（1）关键信息基础设施相关数据安全保护要求	2
		（2）关键信息基础设施安全检查支持	1
3.网络与信息安全处置	3-1 信息安全事件预警	（1）信息安全事件威胁预警	2
		（2）信息安全事件风险定级	1
	3-2 信息安全事件证据保存	（1）静态数据提取及固定	2
		（2）动态易失数据提取及固定	1
	3-3 信息安全事件应急响应	（1）响应并处理复杂信息安全事件	2
		（2）恢复信息安全事件造成的信息损坏	1
4.培训指导	4-1 培训实施	（1）对培训需求进行分析	1

		（2）编制培训规划	1
		（2）组织编写培训教材、讲义、教案	1
		（3）进行培训宣讲	1
	4-2 技术指导	（1）技能指导	1
		（2）技能水平考核	1
		（3）组织开展技术改造、技术革新活动	1
课堂学时合计			40

1.1.3 培训课程选择指导

职业基本素质培训课程为必修课程，相当于本职业的入门课程。各级别职业技能培训课程由培训机构教师根据培训学员实际情况，遵循高级别涵盖低级别的原则进行选择。

原则上，初入职的培训学员应学习职业基本素质培训课程和四级/中级职业技能培训课程的全部内容，有职业技能等级提升需求的培训学员，可按照国家职业技能标准的“鉴定要求”，对照自身需求选择更高等级的培训课程。

具有一定从业经验、无职业技能等级晋升要求的培训学员，可根据自身实际情况自主选择本职业培训课程体系。具体方法为：（1）选择课程模块；（2）在模块中筛选课程；（3）在课程中筛选学习单元；（4）组合成本次培训的课程内容。

培训教师可以根据以上方法对培训学员进行单独指导。对于订单培训，培训教师可以按照如上方法，对照订单需求进行培训课程的选择。

1.2 职业指南

2.1 职业描述

网络与信息安全管理员是从事网络及信息安全管理、防护、监控工作的人员。

2.2 职业培训对象

网络与信息安全管理员职业培训的对象主要包括：城乡未继续升学的应届高中毕业生、城镇登记失业人员、转岗转业人员、退役军人、企业在职职工和高校毕业生等各类有培训需求的人员。

2.3 就业前景

网络与信息安全管理员的工作岗位有网络安全管理员、信息安全管理员、互联网信息审核员、网络安全咨询师和系统安全管理员等。可以在计算机科学与技术、信息通信、电子商务、互联网金融、电子政务等领域从事相关工作，也可以在网络与信息安全设备厂商、互联网安全公司、安全服务公司等单位工作，也可以在政府机关事业单位，银行、保险、证券等金融机构，电信、传媒等行业等从事网络与信息安全产品的研发、系统安全分析与设计、安全技术咨询服务、安全教育以及安全管理等工作。

1.3 培训机构设置指南

1.3.1 师资配备要求

（1）培训教师任职基本条件

1）培训四级/中级、三级/高级网络与信息安全管理员的教师应具有本职业二级/技师及以上职业资格证书或相关专业高级及以上专业技术职务任职资格。

2）培训网络与信息安全管理员二级/技师的教师应具有本职业一级/高级技师职业资格证书或相关专业高级专业技术职务任职资格。

3）培训网络与信息安全管理员一级/高级技师的教师具有本职业一级/高级技师职业资格证书 2 年以上或相关专业高级专业技术职务任职资格。

（2）培训教师数量要求（以 30 人培训班为基准）。专业课教师：2 人以上（含 2 人）；培训规模超过 30 人的，按教师与学员之比不低于 1∶20 配备教师。

1.3.2 培训场所设备配置要求

培训场所设备配置要求如下（以 30 人培训班为基准）。

（1）理论知识培训场所设备配置要求：60 平方米以上标准教室，多媒体教学设备（计算机、投影仪、幕布或显示屏、网络接入设备、音响设备）、黑板、30 套以上桌椅，符合照明、通风、安全等相关规定。

（2)操作技能培训场所设备配置要求:30 台以上 PC 机局域网集成上机环境，设备设施配套齐全，符合环保、劳保、安全、卫生、消防、通风和照明等相关规定及安全规程。

其中，网络与信息安全管理员（四级/中级、三级/高级、二级/技师、一级/高级技师）培训场所应具备教师演示和学员练习两个功能。

（3）实训设备、软件配置等要求

1）实训设备（名称、规格或型号、数量）。PC 机：4 核、主频 2.0Ghz 及以上 CPU，16G 及以上内存，500G 及以上存储，百兆及以上网卡，数量不少于 30 台。或者采用实训云平台，满足单个虚拟机 2 核 CPU 及以上，8G 内存及以上和硬盘 40G 及以上要求。

2）软件配置。需安装（具备）满足实训要求的相关软件（功能），版本包括但不限于 WindowsServer2016、Windows10、CentOS7、CiscoPacketTracer7、VMWare15。

3）其他。若培训机构使用云平台，则该云平台也需满足软件配置的功能和实训要求。

1.3.3 教学资料配备要求

（1）培训规范：《网络与信息安全管理员国家职业技能标准》《网络与信息安全管理员职业基本素质培训要求》《网络与信息安全管理员职业技能培训要求》《网络与信息安全管理员职业基本素质培训课程规范》《网络与信息安全管理员职业技能培训课程规范》《网络与信息安全管理员职业基本素质培训考核规范》《网络与信息安全管理员职业技能培训理论知识考核规范》《网络与信息安

全管理员职业技能培训操作技能考核规范》。

（2）教学资源、教材教辅、网络资源等内容必须符合“（1）培训规范”。

1.3.4 管理人员配备要求

（1）专职校长：1 人，应具有大专及以上文化程度、中级及以上专业技术职务任职资格，从事职业技术教育及教学管理 5 年以上，熟悉职业培训的有关法律法规。

（2）教学管理人员：1 人以上，专职不少于 1 人；应具有大专及以上文化程度、中级及以上专业技术职务任职资格，从事职业技术教育及教学管理 5 年以上，具有丰富的教学管理经验。

（3）办公室人员：1 人以上，应具有大专及以上文化程度。

（4）财务管理人员：2 人，应具有大专及以上文化程度。

1.3.5 管理制度要求

应建立健全完备的管理制度，包括办学章程与发展规划、教学管理、教师管理、学员管理、财务管理、设备管理等制度。

2/课程包

2.1 培训要求

2.1.1 职业基本素质培训要求

职业基本素质模块	培训内容	培训细目
1.职业认知与职业道德	1-1 职业认知	职业认知
	1-2 职业道德基本知识	道德与职业道德
	1-3 职业守则	职业守则
2.计算机相关知识	2-1 计算机硬件基础知识	计算机硬件
	2-2 计算机软件基础知识	计算机软件
	2-3 操作系统基础知识	操作系统
	2-4 数据库基础知识	数据库
3. 网络相关知识	3-1 网络协议基础知识	网络协议
	3-2 组网设备基础知识	（1）组网设备概述
		（2）路由器基础知识
		（3）交换机基础知识
	3-3 网络配置、故障排查常用命令和工具基础知识	网络配置、故障排查常用命令和工具
4.网络安全基础知识	4-1 网络安全概述	网络安全概述
	4-2 网络安全基础技术	网络安全基础技术
5. 相关法律法规、标准知识	5-1 法律、法规知识	法律、法规知识
	5-2 标准知识	标准知识

2.1.2 四级/中级职业技能培训要求（网络安全管理员、信息安全管理员）

职业功能模块	培训内容	技能目标	培训细目
1.网络与信息安全防护	1-1 网络安全配置与防护	1-1-1 能根据业务场景，规划网络地址，构建网络拓扑，配置交换机、路由器等网络设备接口信息	配置网络设备接口信息
		1-1-2 能根据网络拓扑，配置路由协议，完成互联互通	配置路由协议
		1-1-3 能根据网络拓扑，配置无线网络设备	配置无线网络设备
		1-1-4 能够对网络设备进行	配置网络设备基础安全设

		基础安全配置	置
	1-2 系统安全配置与防护	1-2-1 能配置操作系统密码策略与账户策略	（1）配置 Windows 操作系统密码策略与账户策略
			（2）配置 Linux 操作系统密码策略与账户策略
		1-2-2 能安全配置操作系统自带的防火墙功能	（1）配置 Windows 操作系统自带的防火墙
			（2）配置 Linux 操作系统自带的防火墙
		1-2-3 能安装部署防病毒软件	安装部署防病毒软件
		1-2-4 能启用系统审核功能	（1）配置 Windows 系统高级安全审核
			（2）配置 Linux 系统审核功能
	1-3 应用安全配置及防护	1-3-1 能根据业务需求，配置常见应用服务	配置常见应用服务
		1-3-2 能为常见应用场景启用基本防护	配置应用服务的基本防护
2.网络与信息安全管理	2-1 网络安全管理	2-1-1 能根据网络需求，划分交换机 VLAN	配置交换机的 VLAN
		2-1-2 能配置交换机、路由器等网络设备的远程管理方式	配置网络设备的远程管理
		2-1-3 能够管理交换机、路由器的用户安全级别	管理网络设备的用户安全级别
	2-2 系统安全管理	2-2-1 能根据组织业务需求，管理用户与组	（1）管理 Windows 系统用户与组的基本配置
			（2）管理 Linux 系统用户与组的基本配置
		2-2-2 能管理文件及文件夹的访问权限	（1）管理 Windows 系统文件及文件夹的访问权限
			（2）管理 Linux 系统文件及文件夹的访问权限
		2-2-3 能对操作系统进行定期升级更新系统补丁	操作系统补丁更新
		2-2-4 能对防病毒软件进行定期升级	防病毒软件安全保护策略配置和定期升级服务
	2-3 应用安全管理	2-3-1 能对组织应用的域名进行正确备案	企业域名备案
		2-3-2 能管理常见应用服务的域名解析	配置企业应用域名解析
		2-3-3 能对应用数据进行安全备份	应用数据备份

3.网络与信息安全处置	3-1 网络安全事件处置	3-1-1 能使用网络诊断工具识别并处理常见网络故障	识别及处理常见网络故障
		3-1-2 能识别常见网络层攻击	识别常见网络层攻击
	3-2 系统及应用安全事件处置	3-2-1 能识别常见系统安全事件	识别常见系统安全事件
		3-2-2 能使用防病毒工具清除恶意代码	恶意代码检测与清除
		3-2-3 能使用相关工具实现对恶意代码的检测和报警	
		3-2-4 能利用备份工具恢复应用数据	应用数据恢复

2.1.3 三级/高级职业技能培训要求（网络安全管理员、信息安全管理员）

职业功能模块	培训内容	技能目标	培训细目
1.网络与信息安全防护	1-1 网络安全防护	1-1-1 能对企业级交换机、路由器等网络设备进行安全加固	安全加固企业级交换机、路由器
		1-1-2 能根据网络安全需求，部署配置防火墙、安全隔离网闸等边界防护设备	部署配置边界防护设备
		1-1-3 能根据网络安全需求，部署配置入侵检测/防御系统	部署配置入侵检测/防御系统
		1-1-4 能够配置无线网络安全管理中心	部署配置无线网络安全
		1-1-5 能根据网络安全需求，部署配置网络安全审计设备	部署配置网络安全审计设备
	1-2 系统安全防护	1-2-1 能根据应用系统安全需求合理配置系统安全策略	配置系统安全策略
		1-2-2 能利用系统自带的防火墙，制定规则对网络访问进行控制	配置系统自带防火墙访问控制规则
		1-2-3 能利用补丁、安全策略等对常见恶意代码等进行有效防范	防范常见恶意代码

	1-3 应用安全防护	1-3-1 能根据网络安全需求，实现常见应用的数据加密传输	配置数据加密传输
		1-3-2 能部署 Web 应用防火墙，对 Web 应用进行安全防护	部署配置 Web 应用防火墙
		1-3-3 能根据网络安全需求，部署应用安全审计	部署配置应用安全审计
2.网络与信息安全管理	2-1 网络安全管理	2-1-1 能根据网络安全需求，通过防火墙等安全设备进行网络访问控制管理	配置防火墙网络访问控制管理
		2-1-2 能根据网络安全需求，管理各类终端接入无线网络	管理各类终端接入无线网络
		2-1-3 能安全管理各类边界设备、网络节点的远程访问	管理各类边界设备、网络节点远程访问
		2-1-4 能根据国家相关规定，正确留存网络设备安全日志	留存网络设备安全日志
	2-2 系统安全管理	2-2-1 能根据应用系统安全需求，实现安全远程访问管理	管理安全远程访问
		2-2-2 能发现系统漏洞和风险，并进行安全管理	管理系统漏洞和风险
		2-2-3 能根据应用系统要求管理备份	管理应用系统备份
		2-2-4 能根据国家相关规定，管理系统日志	管理系统日志
		2-2-5 能根据国家相关规定，对应用系统进行正确备案	应用系统备案
	2-3 应用安全管理	2-3-1 能根据国家相关规定，履行网络安全义务，安全管理互联网应用	安全管理互联网应用
		2-3-2 能利用安全设备及工具对垃圾邮件等有害数据实施过滤	过滤垃圾邮件等有害数据
		2-3-3 能根据国家相关规定，管理审计互联网访问日志	管理审计互联网访问日志
3.网络与信息安全处置	3-1 网络安全事件监控和处置	3-1-1 能利用防火墙、入侵检测等设备监控网络数据流量，识别攻击特征	网络数据流量监控
		3-1-2 能对攻击流量进行有	攻击流量阻断

		效阻断	
		3-1-3 能有效留存日志记录，并进行上报	网络安全日志留存
	3-2 系统安全事件监控和处置	3-2-1 能有效识别、隔离被入侵或感染病毒的计算机	识别、隔离被入侵或感染病毒的计算机
		3-2-2 能识别系统异常状态，利用工具清除系统后门	识别系统异常状态及系统后门清除
		3-2-3 能检测到系统异常状态，恢复系统状态	系统异常状态检测及恢复
		3-3-4 能有效留存计算机病毒、后门等样本，并进行上报	病毒样本留存及上报
	3-3 应用安全事件监控和处置	3-3-1 能提取数据库、Web 服务等应用访问日志	提取数据库、Web 服务应用访问日志
		3-3-2 能够对日志进行简单分析，识别并定位事件	日志分析、识别及定位事件
		3-3-3 能够识别违法有害信息，并进行处置	违法有害信息识别及处置
		3-3-4 能有效留存记录及证据，并进行上报	互联网安全事件记录、证据留存及上报

2.1.4 二级/技师职业技能培训要求（网络安全管理员）

职业功能模块	培训内容	技能目标	培训细目
1.网络与信息安全防护	1-1 网络安全防护	1-1-1 能对网络进行漏洞扫描，分析扫描结果，并进行安全加固	网络漏洞扫描、分析及安全加固
		1-1-2 能分析网络安全需求，进行安全域配置，启用相应的安全策略，对各个安全域资源进行有效防护	安全域配置及安全策略配置
		1-1-3 能配置重要设备硬件冗余，保证可用性	配置重要设备硬件冗余
		1-1-4 能分析网络安全需求，配置虚拟专用网络（VPN）	配置虚拟专用网络（VPN）
	1-2 系统安全防护	1-2-1 能使用工具对系统进行安全扫描，并根据扫描报告进行风险分析	系统安全扫描及风险分析
		1-2-2 能根据系统风险分	

		析结果，调整系统安全措施	
		1-2-3 能启用数据加密策略对应用数据进行有效保护	启用数据加密策略对应用数据进行保护
	1-3 应用安全防护	1-3-1 能使用工具对互联网应用进行漏洞扫描，并根据扫描报告进行风险分析	互联网应用漏洞扫描及风险分析
		1-3-2 能对扫描报告中出现的漏洞进行测试、验证	漏洞测试及验证
		1-3-3 能配置 Web 应用防火墙，拦截 Web 应用攻击	配置 Web 应用防火墙
		1-3-4 能规划反垃圾邮件网关实施方案	规划反垃圾邮件网关实施方案
2.网络与信息安全管理	2-1 网络安全等级保护	2-1-1 能根据相关网络安全等级保护要求，核查网络安全基线配置情况	网络安全等级保护基础
		2-1-2 能根据安全基线检查情况，进行加固或给出整改建议	网络安全基线配置检查及加固整改
	2-2 应用安全评估	2-2-1 能根据国家相关规定对互联网服务自行开展安全评估	互联网服务自评估
		2-2-2 能根据国家相关规定，制定信息网络安全技术方案	信息网络安全技术方案制定
		2-2-3 能配合完成渗透测试工作	渗透测试工作配合
		2-2-4 能根据渗透测试报告进行加固或给出安全加固建议	根据渗透测试报告进行加固
3.网络与信息安全处置	3-1 网络安全事件监测	3-1-1 能使用相关工具对网络链路的运行状况进行监测	网络链路运行状况监测
		3-1-2 能使用相关工具对网络设备的运行状况进行监测	网络设备运行状况监测
		3-1-3 能使用相关工具对安全设备的运行状况进行监测	安全设备运行状况监测
		3-1-4 能使用相关工具对系统的运行状况进行监测	系统运行状况监测
	3-2 网络安全	3-2-1 能对各设备上的监	设备监测数据清洗、汇总

	事件分析	测数据进行清洗、汇总	
		3-2-2 能对各设备上的监测数据进行分析，发现异常痕迹	设备监测数据分析
	3-3 网络安全事件响应	3-3-1 能对常见的网络安全事件进行响应	常见网络安全事件响应
		3-3-2 能对常见的网络攻击进行溯源和上报	常见网络攻击溯源和上报
		3-3-3 能留存网络安全事件相关证据记录	留存网络安全事件相关证据记录
4.培训指导	4-1 培训实施	4-1-1 能制订培训工作计划	制订培训工作计划
		4-1-2 能编制和实施培训方案	编制和实施培训方案
		4-1-3 能编写培训教材、讲义、课件	编写培训教材、讲义、课件
		4-1-4 能进行培训宣讲	培训宣讲
	4-2 技术指导	4-2-1 能对三级/高级工及以下级别人员进行技能指导	技能指导
		4-2-2 能对三级/高级工及以下级别人员技能水平进行考核	技能水平考核

2.1.5 二级/技师职业技能培训要求（信息安全管理员）

职业功能模块	培训内容	技能目标	培训细目
1.网络与信息安全防护	1-1 信息资产安全防护	1-1-1 能对组织信息资产进行分类分级，划分安全域	信息资产分类分级
		1-1-2 能对安全域资源制定有效的防护策略	安全域资源防护策略制定
	1-2 数据安全防护	1-2-1 能进行数据分级分类，制定数据的安全存储策略，规划、配置数据加密策略	数据安全存储策略、数据加密策略配置
		1-2-2 能根据业务需求，制定数据容灾策略	制定数据容灾策略
	1-3 互联网信息安全防护	1-3-1 能对个人用户名、密码等重要信息的使用进行脆弱性评估并给出	重要信息脆弱性评估及防护

		防护建议	
		1-3-2 能配置安全策略，审计员工对个人信息的操作	员工个人信息安全策略配置
2.网络与信息安全管理	2-1 数据安全管理	2-1-1 能安全管理数据在存储、通信中的公私钥和证书	数据在存储、通信中的公私钥和证书管理
		2-1-2 能对数据进行高可用管理	数据高可用管理
		2-1-3 能参照国家有关标准，采用数据分类、备份、加密等措施加强对重要数据保护	重要数据保护
	2-2 互联网信息安全管理	2-2-1 能根据国家相关法律法规及规定履行信息安全管理义务	履行信息安全管理义务
		2-2-2 能编制个人敏感信息的安全保护技术方案	编制个人敏感信息安全保护技术方案
		2-2-3 能对个人敏感信息进行脆弱性评估并给出防护建议	个人敏感信息脆弱性评估及防护
3.网络与信息安全处置	3-1 信息安全事件监测	3-1-1 能监测信息破坏事件	监测信息破坏事件
		3-1-2 能监测信息内容安全事件	监测信息内容安全事件
		3-1-3 能监测其他信息安全事件	监测其他信息安全事件
	3-2 信息安全事件分析	3-2-1 能对信息安全监测数据进行清洗、汇总	信息安全监测数据清洗、汇总
		3-2-2 能对信息安全监测数据进行分析	信息安全监测数据分析
	3-3 信息安全事件响应	3-3-1 能对常见的信息安全事件进行响应	常见信息安全事件响应
		3-3-2 能对常见的信息安全事件进行溯源和上报	常见信息安全事件溯源和上报
		3-3-3 能留存信息安全事件相关证据记录	留存信息安全事件相关证据记录
4.培训指导	4-1 培训实施	4-1-1 能制订培训工作计划	制订培训工作计划
		4-1-2 能编制和实施培训方案	编制和实施培训方案
		4-1-3 能编写培训教材、	编写培训教材、讲义、课件

		讲义、课件	
		4-1-4 能进行培训宣讲	培训宣讲
	4-2 技术指导	4-2-1 能对三级/高级工及以下级别人员进行技能指导	技能指导
		4-2-2 能对三级/高级工及以下级别人员技能水平进行考核	技能水平考核

2.1.6 一级/高级技师职业技能培训要求（网络安全管理员）

职业功能模块	培训内容	技能目标	培训细目
1.网络与信息安全防护	1-1 网络安全风险评估	1-1-1 能对组织整体业务系统进行安全风险评估	组织整体业务系统安全风险评估
		1-1-2 能对网络和应用系统进行渗透测试，并对测试报告中的漏洞进行验证和修补	网络和应用系统渗透测试及漏洞验证和修补
	1-2 新技术、新应用安全防护	1-2-1 能对云计算应用提出安全防护策略	云计算应用安全防护策略
		1-2-2 能对物联网应用提出安全防护策略	物联网应用安全防护策略
		1-2-3 能对移动互联应用提出安全防护策略	移动互联应用安全防护策略
		1-2-4 能对工业控制系统提出安全防护策略	工业控制系统安全防护策略
		1-2-5 能对大数据应用提出安全防护策略	大数据应用安全防护策略
		1-2-6 能对区块链等其他新技术新应用提出安全防护策略	区块链等其他新技术新应用安全防护策略
2.网络与信息安全管理	2-1 网络安全风险管理	2-1-1 能根据安全风险评估结果实施网络安全风险管理	网络安全风险管理
		2-1-2 能对漏洞进行评估，制定安全管理措施	漏洞评估及制定安全管理措施
	2-2 网络安全等级保护	2-2-1 能根据组织业务情况，对网络和信息系统进行合理定级	网络安全等级保护定级
		2-2-2 能根据网络安全	网络安全等级保护备案

		等级保护定级要求，进行备案指导	
		2-2-3 能根据组织业务情况，进行网络安全建设整改	网络安全等级保护建设整改
		2-2-4 能根据组织业务情况，进行网络安全自我监督检查	网络安全自我监督检查
	2-3 关键信息基础设施保护	2-3-1 能按照检查内容对关键信息基础设施进行安全检查	关键信息基础设施安全检查
		2-3-2 能制定关键信息基础设施安全加固方案	制定关键信息基础设施安全加固方案
		2-3-3 能对系统和数据库设计容灾备份方案	网络安全事件应急方案编制
3.网络与信息安全处置	3-1 网络安全事件预警	3-1-1 能监测各类网络数据，建立安全事件威胁预警机制	建立安全事件威胁预警机制
		3-1-2 能针对网络安全事件进行风险定级，设计响应级别和应急预案	网络安全事件风险定级、设计响应级别和应急预案
	3-2 网络安全事件证据保存	3-2-1 能够对静态数据进行提取及固定	静态数据提取及固定
		3-2-2 能够对动态易失数据进行提取及固定	动态易失数据提取及固定
	3-3 网络安全事件应急响应	3-3-1 能及时响应并处理复杂网络安全事件	复杂网络安全事件应急响应
		3-3-2 能恢复网络安全事件造成的网络或系统损坏	恢复网络安全事件造成的网络或系统损坏
4.培训指导	4-1 培训实施	4-1-1 能对培训需求进行分析	培训需求分析
		4-1-2 能编制培训规划	编制培训规划
		4-1-3 能组织编写培训教材、讲义、教案	组织编写培训教材、讲义、教案
		4-1-4 能进行培训宣讲	培训宣讲
	4-2 技术指导	4-2-1 能对二级/技师及以下级别人员进行技能指导	技能指导
		4-2-2 能对二级/技师及以下级别人员技能水平进行考核	技能水平考核
		4-2-3 能组织开展技术改造、技术革新活动	组织开展技术改造、技术革新活动

2.1.7 一级/高级技师职业技能培训要求（信息安全管理员）

职业功能模块	培训内容	技能目标	培训细目
1.网络与信息安全防护	1-1 信息安全风险评估	1-1-1 能对组织关键业务系统进行风险评估	组织关键业务系统风险评估
		1-1-2 能根据信息安全风险评估结果，出具评估报告	出具信息安全风险评估报告
		1-1-3 能根据信息安全风险评估报告，制定整改措施	制定信息安全风险整改措施
	1-2 新技术、新应用安全防护	1-2-1 能对云计算应用提出安全防护策略	云计算应用安全防护策略
		1-2-2 能对物联网应用提出安全防护策略	物联网应用安全防护策略
		1-2-3 能对移动互联应用提出安全防护策略	移动互联应用安全防护策略
		1-2-4 能对工业控制系统提出安全防护策略	工业控制系统安全防护策略
		1-2-5 能对大数据应用提出安全防护策略	大数据应用安全防护策略
		1-2-6 能对区块链等其他新技术、新应用提出安全防护策略	区块链等其他新技术新应用安全防护策略
2.网络与信息安全管理	2-1 信息安全风险管理	2-1-1 能根据国家相关规定，制定信息安全风险管理制度	制定信息安全风险管理制度
		2-1-2 能制定风险评估方案，组织开展风险评估工作	制定风险评估方案
		2-1-3 能够对业务系统存在的安全风险制定处置方案，对风险进行监督管理	业务系统安全风险处置方案编制
	2-2 网络安全等级保护	2-2-1 能根据组织业务情况，对网络和信息系统进行合理定级	网络安全等级保护定级
		2-2-2 能根据网络安全等级保护定级要求，进行备案指导	网络安全等级保护备案
		2-2-3 能根据组织架构和安全现状，设计和制定安全管理制度	设计和制定安全管理制度

	2-3 关键信息基础设施保护	2-3-1 能掌握关键信息基础设施相关数据安全保护要求	关键信息基础设施相关数据安全保护要求
		2-3-2 能对关键信息基础设施安全检查提供支持	关键信息基础设施安全检查支持
3.网络与信息安全处置	3-1 信息安全事件预警	3-1-1 能建立信息安全事件威胁预警机制	信息安全事件威胁预警
		3-1-2 能对信息安全事件进行风险定级，设计响应级别和应急预案	信息安全事件风险定级
	3-2 信息安全事件证据保存	3-2-1 能够对静态数据进行提取及固定	静态数据提取及固定
		3-2-2 能够对动态易失数据进行提取及固定	动态易失数据提取及固定
	3-3 信息安全事件应急响应	3-3-1 能及时响应并处理复杂信息安全事件	响应并处理复杂信息安全事件
		3-3-2 能恢复信息安全事件造成的信息损坏	恢复信息安全事件造成的信息损坏
4.培训指导	4-1 培训实施	4-1-1 能对培训需求进行分析	对培训需求进行分析
		4-1-2 能编制培训规划	编制培训规划
		4-1-3 能组织编写培训教材、讲义、教案	组织编写培训教材、讲义、教案
		4-1-4 能进行培训宣讲	进行培训宣讲
	4-2 技术指导	4-2-1 能对二级/技师及以下级别人员进行技能指导	技能指导
		4-2-2 能对本二级/技师及以下级别人员技能水平进行考核	技能水平考核
		4-2-3 能组织开展技术改造、技术革新活动	组织开展技术改造、技术革新活动

2.2 课程规范

2.2.1 职业基本素质培训课程规范

模块	课程	学习单元	课程内容	培训建议	课堂学时
1.职业认知与职业道德	1-1 职业认知	职业认知	1）网络与信息安全行业认知 2）网络与信息安全管理员的工作内容	（1）方法：讲授法 （2）重点与难点：网络与信息安全管理员的工作内容	1
	1-2 职业道德基本知识	道德与职业道德	1）道德 2）职业道德 3）网络与信息安全管理员的职业道德	（1）方法：讲授法、案例教学法 （2）重点与难点：网络与信息安全管理员的职业道德	1
	1-3 职业守则	职业守则	1）遵纪守法，爱岗敬业 2）勤奋进取，忠于职守 3）认真负责，团结协作 4）爱护设备，安全操作 5）诚实守信，讲求信誉 6）勇于创新，精益求精	（1）方法：讲授法、案例教学法 （2）重点与难点：网络与信息安全管理员的职业守则	1
2.计算机相关知识	2-1 计算机硬件基础知识	计算机硬件	1）计算机的发展 ①计算机的发展历程 ②计算机的分类	（1）方法：讲授法、案例教学法 （2）重点与难点：计算机的组成	1

			2）计算机的组成 ①中央处理器 ②主板 ③存储器 ④外部设备		
	2-2 计算机软件基础知识	计算机软件	1）计算机软件基础 2）常用计算机语言 3）常用编程算法 4）常见数据结构	（1）方法：讲授法、案例教学法 （2）重点与难点：常见数据结构	1
	2-3 操作系统基础知识	操作系统	1）操作系统概念 2）常见操作系统 3）常见文件系统 4）常见文件类型	（1）方法：讲授法、案例教学法 （2）重点与难点：常见操作系统	1
	2-4 数据库基础知识	数据库	1）数据库概述 2）数据类型 3）数据模型 4）主流数据库介绍 5）分布式数据库 6）数据库语言 SQL	（1）方法：讲授法、案例教学法 （2）重点与难点：主流数据库介绍	1
3．网络相关知识	3-1 网络协议基础知识	网络体系结构与协议	1）网络体系结构概述 2）开放系统互联参考模型 3）TCP/IP 的体系结构	（1）方法：讲授法、案例教学法 （2）重点与难点：开放系统互联参考模型、TCP/IP 的体系结构	1

			4）IP 地址 ①IP 地址介绍与分类 ②IP 地址规划与子网划分		
	3-2 组网设备基础知识	（1）组网设备概述	1）组网设备的分类	（1）方法：讲授法、案例教学法 （2）重点与难点：物理层设备	1
			2）物理层设备		
			3）数据链路层设备		
			4）网络及以上层设备		
		（2）路由器基础知识	1）路由器概述 ①路由器的概念 ②路由器的工作原理和应用场景 ③路由器的性能指标 ④路由器的分类	（1）方法：讲授法、案例教学法 （2）重点与难点：路由器的基础配置	1
			2）路由器的组成 ①路由器的硬件构成和安装 ②路由器的启动过程		
			3）路由器的基础配置 ①路由器的配置方式 ②路由器的工作模式		
		（3）交换机基础知识	1）交换机概述 ①交换机的概念 ②交换机的工作原理和应用场景 ③交换机的性能指标 ④交换机的分类	（1）方法：讲授法、案例教学法 （2）重点与难点：交换机的基础配置	1

			2）交换机的组成 ①交换机的硬件构成和安装 ②交换机的启动过程		
			3）交换机的基础配置 ①交换机的配置方式 ②交换机的工作模式		
	3-3 网络配置、故障排查常用命令和工具基础知识	网络配置、故障排查常用命令和工具	1）网络配置、故障排查常用命令 ①ipconifg ②ping/pathping ③traceroute/tracert ④netstat	（1）方法：讲授法、案例教学法 （2）重点与难点：故障排查常用命令和工具	2
			2）网络配置、故障排查常用工具 ①Wireshark ②tcpdump ③Nmap		
4.网络安全基础知识	4-1 网络安全概述	网络安全概述	1）网络安全基础概念	（1）方法：讲授法、案例教学法 （2）重点与难点：网络安全风险	2
			2）网络安全风险		
	4-2 网络安全基础技术	网络安全基础技术	1）密码技术	（1）方法：讲授法、案例教学法 （2）重点与难点：密码技术、身份鉴别	3
			2）身份鉴别		
			3）访问控制		
			4）安全审计		
5. 相关法律法	5-1 法律、法规知	法律、法规知识	1）《中华人民共和国劳动法》的相关知识	（1）方法：讲授法、案例教学法 （2）重点与难点：《中华	3

规、标准知识	识		2）《中华人民共和国合同法》的相关知识	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》	
			3）《中华人民共和国民法典》的相关知识		
			4）《中华人民共和国网络安全法》的相关知识		
			5）《中华人民共和国数据安全法》的相关知识		
			6）《中华人民共和国个人信息保护法》的相关知识		
			7）其他网络安全相关法律、法规		
	5-2 标准知识	标准知识	1）网络安全标准体系	（1）方法：讲授法、案例教学法 （2）重点与难点：网络安全标准体系	3
			2）主要网络安全标准介绍	（1）方法：讲授法、案例教学法 （2）重点与难点：《网络安全等级保护基本要求》	
课堂学时合计					24

2.2.2 四级/中级职业技能培训课程规范（网络安全管理员、信息安全管理员）

模块	课程	学习单元	课程内容	培训建议	课堂学时
1. 网络与信息	1-1 网络安全配置与	（1）配置网络设备接口信息	1）OSI 基础知识	（1）方法：讲授法、演示法、实训（练习）法	2
			2）TCP/IP 基础知识		
			3）IP 地址基础知识		

安 全防护	防护		4）常见网络设备 5）路由器基础知识 6）交换机基础知识 7）IP 地址与子网划分操作	（2）重点与难点：路由器和交换机接口配置实例	
		（2）配置路由协议	1）静态路由协议 2）动态路由器协议 3）配置静态和动态路由协议	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：动态路由协议配置实例	2
		（3）配置无线网络设备	1）WLAN 简介 2）无线局域网安全基础知识 3）WLAN 的配置	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：WLAN 的配置实例	2
		（4）配置网络设备基础安全设置	1）交换机安全基础知识 2）路由器安全基础知识 3）配置 SSH 管理	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：路由器和交换机的基础安全配置实例	2
	1-2 系统安全配置与防护	（1）配置 Windows 操作系统密码策略与账户策略	1）Windows 系统账户策略 2）Windows 系统密码策略 3）Windows 系统账户密码策略配置操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：Windows 系统账户和密码策略	2
		（2）配置 Linux 操作系统密码策略与账户策略	1）Linux 系统账户策略 2）Linux 系统密码策略 3）Linux 系统账户密码策略配置操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：Linux 系统账户和密码策略	2
		（3）配置 Windows 操作系统自带的防火墙	1）防火墙基础知识 2）Windows 防火墙 3）Windows 自带防火墙配置操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：Windows 系统防火墙配置实例	1
		（4）配置 Linux 操作系统自带的防火墙	1）Linux 防火墙基础知识 2）Firewalld 基础知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：	1

			3）Linux 自带防火墙配置操作	Linux 系统防火墙配置实例	
		（5）安装部署防病毒软件	1）恶意代码防范基础知识 2）MicrosoftDefender 简介 3）MicrosoftDefender 安装部署操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：MicrosoftDefender 配置	2
		（6）配置 Windows 系统高级安全审核	1）审核的作用 2）Windows 中的审核策略 3）Windows 系统安全审核操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：Windows 系统安全审核策略设置	1
		（7）配置 Linux 系统审核功能	1）Linux 安全审核 2）FedoraServer 安全审核 3）Linux 系统安全审核操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：Linux 系统安全审核策略设置	1
	1-3 应用安全配置及防护	（1）配置常见的应用服务	1）HTTP 基础知识 2）DNS 基础知识 3）FTP 基础知识 4）身份验证基础知识 5）IIS 服务器搭建操作 6）FTP 服务器搭建操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：IIS 服务器搭建和 FTP 服务器搭建	2
		（2）配置应用服务的基本防护	1）Web 服务器安全配置与防护 2）DNS 服务器安全配置与防护 3）FTP 服务器安全配置与防护 4）IIS 服务器安全加固操作 5）FTP 服务器安全加固操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：IIS 服务器加固和 FTP 服务器加固	2
2. 网络与信息安全管理	2-1 网络安全管理	（1）配置交换机的 VLAN	1）VLAN 简介 2）VLAN 的创建、划分和查看 3）利用 VLAN 划分不同广播域操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：VLAN 划分	2

		（2）配置网络设备的远程管理	1）网络设备的四种登录方式 2）路由器、交换机的本地访问管理 3）路由器、交换机的远程访问管理 4）网络设备的 VTY 线路保护操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：路由器和交换机的远程访问	2
		（3）管理网络设备的用户安全级别	1）路由器、交换机的用户安全级 2）网络设备的用户安全级别管理操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：路由器和交换机的用户安全级别管理	2
	2-2 系统安全管理	（1）管理 Windows 系统用户与组的基本配置	1）用户和组基础知识 2）Windows 系统的用户和组 3）Windows 系统用户和组管理操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：Windows 系统用户和组管理	2
		（2）管理 Linux 系统用户与组的基本配置	1）Linux 用户和组基础知识 2）Linux 用户和组管理 3）Linux 系统用户和组管理操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：Linux 系统用户和组管理	2
		（3）管理 Windows 系统文件及文件夹的访问权限	1）文件访问控制 2）Windows 系统的文件访问控制 3）Windows 系统文件及文件夹访问权限管理操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：Windows 系统文件及文件夹访问权限管理	1
		（4）管理 Linux 系统文件及文件夹的访问权限	1）Linux 文件系统 2）Linux 系统的文件访问控制 3）Linux 系统文件及文件夹访问权限管理操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：Linux 系统文件及文件夹访问权限管理	1
		（5）操作系统补丁更新	1）安全漏洞基础知识 2)WSUSWindowsServer 更新服务 3)WSUSWindowsServer 更新服务操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：系统文件及文件夹访问权限管理	2

		（6）防病毒软件安全保护策略配置和定期升级服务	1）计算机病毒基础知识 2）防病毒软件的基本原理 3）防病毒软件安全保护策略配置和定期升级服务操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：防病毒软件安全保护策略配置和定期升级服务	2
	2-3 应用安全管理	（1）企业域名备案	1）域名备案相关规定 2）域名备案流程 3）域名备案操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：域名备案流程	2
		（2）配置企业应用域名解析	1）域名相关知识 2）域名解析配置流程 3）DNS 服务器搭建操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：DNS 服务器搭建操作	2
		（3）应用数据备份	1）数据备份简介 2）Windows 系统中的备份 3）Windows Server Backup 服务管理操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：应用数据备份	2
3. 网络与信息安全处置	3-1 网络安全事件处置	（1）使用网络诊断工具识别及处理常见网络故障	1）常用网络诊断工具 2）常见网络故障处理方法 3）网络故障的内容和故障排除的步骤 4）Linux 服务器网络系统诊断操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：网络故障的内容和故障排除的步骤	2
		（2）识别常见网络层攻击	1）常见网络层攻击 2）OPNsense 简介 3）OPNsense 入侵防御功能部署操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：常见网络层攻击	2
	3-2 系统及应用安全事件处置	（1）常见系统安全事件识别	1）常见系统安全事件分类 2）Windows 日志分析功能操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：常见系统安全事件	2
		（2）恶意代码检测与清除	1）恶意代码工作基本原理 2）恶意代码扫描与清除 3）使用 Windows	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：恶意代码扫描与清除	4

			Defender 查杀恶意代码操作		
		（3）应用数据恢复	1）数据恢复基本知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：恶意代码扫描与清除	2
			2）Windows 系统备份数据还原		
			3）Windows Server Backup 数据恢复操作		
课堂学时合计					56

2.2.3 三级/高级职业技能培训课程规范（网络安全管理员、信息安全管理员）

模块	课程	学习单元	课程内容	培训建议	课堂学时
1. 网络与信息安全防护	1-1 网络安全防护	（1）安全加固企业级交换机、路由器	1）交换机安全配置方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：路由器和交换机的安全配置实例	2
			2）路由器安全配置方法		
			3）企业级交换机、路由器安全加固操作		
		（2）部署配置边界防护设备	1）防火墙介绍 ①防火墙系统概述 ②防火墙的功能 ③防火墙的工作原理	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：边界防护设备的安全配置实例	2
			2）网闸介绍 ①网闸概述 ②网闸的功能		
			3）防火墙的部署配置操作		
		（3）部署配置入侵检测/防御系统	1）入侵检测系统介绍 ①入侵检测系统概述 ②入侵检测系统的分类 ③入侵检测系统的功能	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：入侵检测/防御系统的安全配置实例	2
			2）入侵防御系统介绍 ①入侵防御系统概述 ②入侵防御系统的分类 ③入侵防御系统的功		

			能		
			3）入侵检测/防御系统的部署配置操作		
		（4）部署配置无线网络安全	1）无线网络安全配置方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：无线网络安全管理中心配置实例	1
			2）无线网络安全管理中心配置操作		
		（5）部署配置网络安全审计设备	1）网络安全审计设备配置方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：网络安全审计设备的安全配置实例	1
			2）网络安全审计设备部署配置操作		
	1-2 系统安全防护	（1）配置系统安全策略	1）文件系统基本知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：系统安全策略配置实例	2
			2）系统攻击知识		
			3）系统安全加固方法		
			4）系统安全策略配置操作		
		（2）配置系统自带防火墙访问控制规则	1）系统自带防火墙规则制定方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：系统自带防火墙访问控制规则配置实例	2
			2）系统自带防火墙访问控制规则配置操作		
		（3）防范常见恶意代码	1）常见恶意代码防范技术	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：制定恶意代码安全防范策略配置实例	2
			2）常见恶意代码防范配置操作		
	1-3 应用安全防护	（1）配置数据加密传输	1）传输加密知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：常见应用的加密传输配置实例	2
			2）常见应用的数据加密传输方法		
			3）数据加密传输配置操作		

		（2）部署配置Web 应用防火墙	1）Web 应用防火墙知识 2）Web 应用防火墙配置方法 3）Web 应用防火墙部署操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：Web 应用防火墙配置实例	2
		（3）部署配置应用安全审计	1）应用安全审计知识 2）应用安全审计部署方法 3）应用安全审计部署操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：应用安全审计部署实例	2
2. 网络与信息安全管理	2-1网络安全管理	（1）配置防火墙网络访问控制管理	1）网络访问权限管理知识 2）防火墙网络访问控制管理配置操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：防火墙网络访问控制管理配置实例	2
		（2）管理各类终端接入无线网络	1）无线网络接入管理知识 2）终端设备接入无线网络管理配置操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：终端设备接入无线网络管理配置操作实例	2
		（3）管理各类边界设备、网络节点远程访问	1）边界设备、网络节点的远程访问 2）边界设备、网络节点的远程访问管理配置操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：边界设备、网络节点的远程访问管理配置操作实例	1
		（4）留存网络设备安全日志	1）网络设备安全日志管理知识 2）网络设备日志按留存管理配置操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：网络设备日志按留存管理配置操作实例	1

	2-2 系统安全管理	（1）管理安全远程访问	1）系统安全远程访问方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：安全远程访问管理配置操作实例	2
			2）安全远程访问管理配置操作		
		（2）管理系统漏洞和风险	1）系统漏洞和风险知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：系统漏洞和风险安全管理配置操作实例	2
			2）系统漏洞和风险安全管理配置操作		
		（3）管理应用系统备份	1）应用系统备份知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：应用系统备份管理配置操作实例	2
			2）应用系统备份管理配置操作		
		（4）管理系统日志	1）系统日志管理知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：系统日志管理配置操作实例	1
			2）系统日志管理配置操作		
		（5）应用系统备案	1）应用系统备案知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：应用系统备案操作实例	1
			2）应用系统备案操作		
	2-3 应用安全管理	（1）安全管理互联网应用	1）互联网应用安全管理知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：互联网应用安全管理操作实例	2
			2）互联网应用安全管理操作		
		（2）过滤垃圾邮件等有害数据	1）数据过滤知识	（1）方法：讲授法、演示法、	2

			2）有害数据过滤操作	实训（练习）法 （2）重点与难点：有害数据过滤操作实例	
		（3）管理审计互联网访问日志	1）互联网访问日志管理知识 2）互联网访问日志管理操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：互联网访问日志管理操作实例	2
3. 网络与信息安全处置	3-1网络安全事件监控和处置	（1）网络数据流量监控	1）网络监控方法 2）网络数据流量监控操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：网络数据流量监控操作实例	2
		（2）攻击流量阻断	1）阻断攻击流量的方法 2）阻断攻击流量操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：阻断攻击流量操作实例	1
		（3）网络安全日志留存	1）网络安全事件处置流程 2）网络安全日志留存操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：网络安全日志留存操作实例	1
	3-2系统安全事件监控和处置	（1）识别、隔离被入侵或感染病毒的计算机	1）计算机病毒处理方法 2）识别、隔离被入侵或感染病毒的计算机操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：识别、隔离被入侵或感染病毒的计算机操作实例	2
		（2）识别系统异常状态及系统后门清除	1）系统后门处理方法 2）利用工具清除系统	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：利用工具清	2

			后门操作	除系统后门操作实例	
		（3）系统异常状态检测及恢复	1）系统安全事件处置流程 2）系统异常检测与恢复操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：系统异常检测与恢复操作实例	1
		（4）病毒样本留存及上报	1）病毒样本留存方法 2）病毒样本留存及上报操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：病毒样本留存及上报操作实例	1
	3-3 应用安全事件监控和处置	（1）提取数据库、Web 服务应用访问日志	1）日志提取方法 2）应用访问日志提取操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：应用访问日志提取操作实例	2
		（2）日志分析、识别及定位事件	1）日志分析方法 2）日志分析、识别及定位事件操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：日志分析、识别及定位事件操作实例	2
		（3）违法有害信息识别及处置	1）有害信息识别方法 2）有害信息识别及处置操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：实例	1
		（4）互联网安全事件记录、证据留存及上报	1）互联网安全事件处置流程 2）互联网安全事件记录、证据留存及上报操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：互联网安全事件记录、证据留存及上报操作实例	1
课堂学时合计					56

2.2.4 二级/技师职业技能培训课程规范（网络安全管理员）

模块	课程	学习单元	课程内容	培训建议	课堂学时
1.网络与信息安全防护	1-1网络安全防护	（1）网络漏洞扫描、分析及安全加固	1）漏洞库知识 2)网络漏洞扫描分析与安全加固操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：网络漏洞扫描分析与安全加固操作实例	1
		（2）安全域配置及安全策略配置	1）网络安全规划相关知识 2)安全域配置及策略配置操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：安全域配置及策略配置操作实例	1
		（3）配置重要设备硬件冗余	1）链路冗余、负载均衡等网络高可用性措施 2)重要设备硬件冗余配置操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：重要设备硬件冗余配置操作实例	1
		（4）配置虚拟专用网络（VPN）	1）虚拟专用网知识 2）虚拟专用网络（VPN）配置操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：虚拟专用网络（VPN）配置操作实例	1
	1-2系统安全防护	（1）系统安全扫描及风险分析	1）安全扫描知识 2）风险分析基础知识 3）系统安全措施调整方法 4）系统安全扫描、风险分析及系统安全措施调整操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：系统安全扫描及、风险分析及安全措施调整操作实例	2

		（2）启用数据加密策略对应用数据进行保护	1）数据加密策略 2)启用数据加密策略对应用数据进行有效保护操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：启用数据加密策略对应用数据进行有效保护操作实例	1
	1-3 应用安全防护	（1）互联网应用漏洞扫描及风险分析	1）漏洞测试、验证知识 2)互联网应用安全扫描及风险分析操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：互联网应用安全扫描及风险分析操作实例	1
		（2）漏洞测试及验证	1）漏洞测试、验证方法 2）漏洞测试、验证操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：漏洞测试、验证操作实例	1
		（3）配置 Web 应用防火墙	Web 应用防火墙配置方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：实例	1
		（4）规划反垃圾邮件网关实施方案	1）垃圾邮件处理高级应用 2）配置 Web 应用防火墙，拦截 Web 应用攻击操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：实例	1
2.网络与信息安全管理	2-1 网络安全等级保护	（1）网络安全等级保护基础	1）网络安全等级保护制度 2)网络安全基线配置检查操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：网络安全基线配置检查操作实例	2
		（2）网络安全基线配置检查及加固整改	1)网络安全等级保护基本要求 2)根据安全基线检查情况进行加固或给出整改建议操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难	2

				点：根据安全基线检查情况进行加固或给出整改建议操作实例	
	2-2应用安全评估	（1）互联网服务自评估	1)互联网应用安全评估技术	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：互联网服务自评估操作实例	1
			2）互联网服务自评估操作		
		（2）信息网络安全技术方案制定	1)信息网络安全技术方案制定方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：信息网络安全技术方案设计操作实例	1
			2)信息网络安全技术方案设计操作		
		（3）渗透测试工作配合	1）渗透测试知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：实例	2
			2)配合完成渗透测试工作操作		
		（4）根据渗透测试报告进行加固	根据渗透测试报告进行加固或给出安全加固建议操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：根据渗透测试报告进行加固或给出安全加固建议操作实例	2
3.网络与信息安全处置	3-1网络安全事件监测	（1）网络链路运行状况监测	1）网络监测工具介绍	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：网络链路的运行状况监测操作实例	2
			2)网络链路的运行状况监测操作		
		（2）网络设备运行状况监测	1）网络安全事件监测方法	（1）方法：讲授法、演示法、实训（练习）法	1

			2)网络设备运行状况监测操作	（2）重点与难点：实例	
		（3）安全设备运行状况监测	1)安全设备运行状况监测方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：实例	1
			2)安全设备运行状况监测操作		
		（4）系统运行状况监测	1）系统运行状况监测	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：实例	1
			2）系统运行状况监测操作		
	3-2网络安全事件分析	（1）设备监测数据清洗、汇总	1）常用数据清洗方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：对各设备上的监测数据进行清洗、汇总操作实例	2
			2)对各设备上的监测数据进行清洗、汇总操作		
		（2）设备监测数据分析	1）常用数据分析方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：各设备上的监测数据进行分析操作实例	2
			2)各设备上的监测数据进行分析操作		
	3-3网络安全事件响应	（1）常见网络安全事件响应	1）网络安全事件响应流程	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：网络安全事件响应操作实例	2
			2）网络安全事件响应操作		
		（2）常见网络攻击溯源和上报	1)网络安全事件调查与评估	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：网络安全事件调查与评估操作实例	1
			2)网络安全事件调查与评估操作		

		（3）留存网络安全事件相关证据记录	1)留存网络安全事件相关证据记录的方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：留存网络安全事件相关证据记录操作实例	1
			2)留存网络安全事件相关证据记录操作		
4.培训指导	4-1培训实施	（1）制订培训工作计划	培训工作计划的制订要求和方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：培训工作计划的制订要求和方法	1
		（2）编制和实施培训方案	培训方案编制和实施的要求和方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：培训方案编制和实施的要求和方法	1
		（3）编写培训教材、讲义、课件	培训教材、讲义、课件的编写知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：培训教材、讲义、课件的编写知识	1
		（4）培训宣讲	教学教法知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：教学教法知识	1
	4-2技术指导	（1）技能指导	操作经验和技能总结方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：操作经验和技能总结方法	1
		（2）技能水平考核	技能和理论基础知识水平考核的要求和方法	（1）方法：讲授法、演示法、实训（练习）法	1

				（2）重点与难点：技能和理论基础知识水平考核的要求和方法	
课堂学时合计					40

2.2.5 二级/技师职业技能培训课程规范（信息安全管理员）

模块	课程	学习单元	课程内容	培训建议	课堂学时
1.网络与信息安全防护	1-1信息资产安全防护	（1）信息资产分类分级	1）信息资产分类分级知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：信息资产进行分类分级，划分安全域操作实例	2
			2）网络安全规划相关知识		
			3）信息资产进行分类分级，划分安全域操作		
		（2）安全域资源防护策略制定	1)安全域资源防护策略制定方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：安全域资源防护策略制定操作实例	2
			2)安全域资源防护策略制定操作		
	1-2数据安全防护	（1）数据安全存储策略、数据加密策略配置	1）数据分类级别知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：数据安全存储策略、数据加密策略配置实例	2
			2）数据安全存储策略		
			3）数据安全存储策略、数据加密策略配置		
		（2）制定数据容灾策略	1）数据容灾策略知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：数据容灾策略制定实例	2
			2）数据容灾策略制定		

	1-3 互联网信息安全防护	（1）重要信息脆弱性评估及防护	1）脆弱性评估方法 2）重要信息脆弱性评估及防护操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：对个人用户名、密码等重要信息的使用进行脆弱性评估并给出防护建议操作实例	2
		（2）员工个人信息安全策略配置	1）个人信息的定义 2）员工个人信息安全策略配置操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：员工个人信息安全策略配置操作实例	2
2.网络与信息安全管理	2-1 数据安全管理	（1）数据在存储、通信中的公私钥和证书管理	1）证书管理知识 2）数据在存储、通信中的公私钥和证书管理操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：数据在存储、通信中的公私钥和证书管理实例	2
		（2）数据高可用管理	1）数据高可用知识 2）对数据进行高可用管理配置操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：对数据进行高可用管理配置操作实例	2
		（3）重要数据保护	1）数据分类、备份、加密保护知识 2）采用数据分类、备份、加密等措施加强对重要数据保护操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：采用数据分类、备份、加密等措施加强对重要数据保护操作实例	1
	2-2 互联网信息安全管	（1）履行信息安全管理义务	信息安全管理义务	（1）方法：讲授法、演示法、实训（练习）法	2

	理			（2）重点与难点：信息安全管理义务	
		（2）编制个人敏感信息安全保护技术方案	1）个人敏感信息的定义	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：个人敏感信息的安全保护技术方案编制操作实例	2
			2)个人敏感信息的安全保护技术方案编制操作		
		（3）个人敏感信息脆弱性评估及防护	1)个人敏感信息安全保护技术	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：对个人敏感信息进行脆弱性评估并给出防护建议操作实例	1
			2)对个人敏感信息进行脆弱性评估并给出防护建议操作		
3.网络与信息安全处置	3-1信息安全事件监测	（1）监测信息破坏事件	1）信息破坏事件的分类	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：监测信息破坏事件操作实例	2
			2）监测信息破坏事件操作		
		（2）监测信息内容安全事件	1)信息内容安全事件的分类	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：监测信息内容安全事件操作实例	2
			2)监测信息内容安全事件操作		
		（3）监测其他信息安全事件	1）常用数据清洗方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：监测其他信息安全事件操作实例	1
			2)监测其他信息安全事件操作		

	3-2信息安全事件分析	（1）信息安全监测数据清洗、汇总	1）常用数据分析方法 2)对信息安全监测数据进行清洗、汇总操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：对信息安全监测数据进行清洗、汇总操作实例	2
		（2）信息安全监测数据分析	1)信息安全监测数据分析方法 2)信息安全监测数据分析操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：信息安全监测数据分析操作实例	1
	3-3信息安全事件响应	（1）常见信息安全事件响应	1）信息安全事件响应流程 2）信息安全事件响应操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：信息安全事件响应操作实例	2
		（2）常见信息安全事件溯源和上报	1)信息安全事件调查与评估 2)常见的信息安全事件进行溯源和上报操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：常见的信息安全事件进行溯源和上报操作实例	1
		（3）留存信息安全事件相关证据记录	1)留存信息安全事件相关证据记录方法 2)留存信息安全事件相关证据记录操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：留存信息安全事件相关证据记录操作实例	1
4.培训指导	4-1培训实施	（1）制订培训工作计划	培训工作计划的制订要求和方法	（1）方法：讲授法、演示法、实训（练习）法	1

				（2）重点与难点：培训工作计划的制订要求和方法	
		（2）编制和实施培训方案	培训方案编制和实施的要求和方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：培训方案编制和实施的要求和方法	1
		（3）编写培训教材、讲义、课件	培训教材、讲义、课件的编写知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：培训教材、讲义、课件的编写知识	1
		（4）培训宣讲	教学教法知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：教学教法知识	1
	4-2 技术指导	（1）技能指导	操作经验和技能总结方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：操作经验和技能总结方法	1
		（2）技能水平考核	技能和理论基础知识水平考核的要求和方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：技能和理论基础知识水平考核的要求和方法	1
课堂学时合计					40

2.2.6 一级/高级技师职业技能培训课程规范（网络安全管理员）

模块	课程	学习单元	课程内容	培训建议	课堂学时
1.网络与信息安全防护	1-1网络安全风险评估	（1）组织整体业务系统安全风险评估	1）风险评估知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：2）组织整体业务系统安全风险评估操作实例	2
			2)组织整体业务系统安全风险评估操作		
		（2）网络和应用系统渗透测试及漏洞验证和修补	1)网络信息系统渗透测试知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：对网络和应用系统进行渗透测试，并对测试报告中的漏洞进行验证和修补操作实例	2
			2)对网络和应用系统进行渗透测试，并对测试报告中的漏洞进行验证和修补操作		
	1-2新技术、新应用安全防护	（1）云计算应用安全防护策略	1）云计算安全防护知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：云计算应用提出安全防护策略方案设计操作实例	2
			2)云计算应用安全防护策略		
			3)云计算应用提出安全防护策略方案设计操作		
		（2）物联网应用安全防护策略	1）物联网安全防护知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：物联网安全防护策略设计操作实例	1
			2）物联网安全防护策略		
			3)物联网安全防护策略设计操作		
		（3）移动互联应	1)移动互联网安全防护知识	（1）方法：讲	1

		用安全防护策略	2)移动互联网安全防护策略	授法、演示法、实训（练习）法 （2）重点与难点：移动互联网安全防护策略设计操作实例	
			3)移动互联网安全防护策略设计操作		
		（4）工业控制系统安全防护策略	1)工业控制系统安全防护知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：工业控制系统安全防护策略设计操作实例	1
			2)工业控制系统安全防护策略		
			3)工业控制系统安全防护策略设计操作		
		（5）大数据应用安全防护策略	1)大数据应用安全防护知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：大数据应用安全防护策略设计操作实例	1
			2)大数据应用安全防护策略		
			3)大数据应用安全防护策略设计操作		
		（6）区块链等其他新技术新应用安全防护策略	1)区块链等新技术安全防护知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：区块链等新技术安全防护策略设计操作实例	1
			2)区块链等新技术安全防护策略		
			3)区块链等新技术安全防护策略设计操作		
2.网络与信息安全管理	2-1网络安全风险管理	（1）网络安全风险管理	1)网络安全风险管理基础知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难	1

			2）网络安全风险管理操作	点：网络安全风险管理操作实例	
		（2）漏洞评估及制定安全管理措施	1）漏洞评估技术	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：漏洞安全管理措施操作实例	2
			2）漏洞安全管理措施操作		
	2-2网络安全等级保护	（1）网络安全等级保护定级	1)网络安全等级保护定级知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：网络和信息系统定级操作实例	2
			2)网络和信息系统定级操作		
		（2）网络安全等级保护备案	1)网络安全等级保护备案知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：网络安全等级保护备案操作实例	1
			2)网络安全等级保护备案操作		
		（3）网络安全等级保护建设整改	1)网络安全等级保护建设整改知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：网络安全等级保护建设整改操作实例	2
			2)网络安全等级保护建设整改操作		
		（4）网络安全自我监督检查	1)关键信息基础设施的定义	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：网络安全自我监督检查操作实例	1
			2)网络安全自我监督检查操作		

	2-3 关键信息基础设施保护	（1）关键信息基础设施安全检查	1)关键信息基础设施安全要求 2)关键信息基础设施安全检查操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：关键信息基础设施安全检查操作实例	1
		（2）制定关键信息基础设施安全加固方案	1）网络安全事件预警机制 2)关键信息基础设施安全加固方案设计操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：关键信息基础设施安全加固方案设计操作实例	2
		（3）网络安全事件应急方案编制	1)网络安全事件应急方案编制方法 2)网络安全事件应急方案编制操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：网络安全事件应急方案编制操作实例	1
3.网络与信息安全处置	3-1 网络安全事件预警	（1）建立安全事件威胁预警机制	1)安全事件威胁预警机制方法 2)安全事件威胁预警机制编制操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：安全事件威胁预警机制编制操作实例	2
		（2）网络安全事件风险定级、设计响应级别和应急预案	1）风险定级、设计响应级别和应急预案制定方法 2）风险定级、设计响应级别和应急预案制定操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：风险定级、设计响应级别和应急预案制定操作实例	1
	3-2 网络安全事件证据保存	（1）静态数据提取及固定	1)静态数据提取及固定方法 2)静态数据提取及固定操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：静态数据提	2

				取及固定操作实例	
		（2）动态易失数据提取及固定	1)动态易失数据提取及固定方法 2)动态易失数据提取及固定操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：动态易失数据提取及固定操作实例	1
	3-3 网络安全事件应急响应	（1）复杂网络安全事件应急响应	1)网络安全事件应急响应流程 2)响应并处理复杂网络安全事件操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：响应并处理复杂网络安全事件操作实例	2
		（2）恢复网络安全事件造成的网络或系统损坏	1)网络安全事件造成的网络或系统损坏常用恢复方法 2)恢复网络安全事件造成的网络或系统损坏操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：恢复网络安全事件造成的网络或系统损坏操作实例	1
4.培训指导	4-1 培训实施	（1）培训需求分析	培训需求分析的要求和方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：培训需求分析的要求和方法	1
		（2）编制培训规划	1）培训规划编制的要求 2)培训预算与决算的审核方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：培训规划编制的要求	1
		（3）组织编写培训教材、讲义、教案	组织编写培训教材、讲义、教案的方法	（1）方法：讲授法、演示法、实训（练习）法	1

				（2）重点与难点：实例	
		（4）进行培训宣讲	进行培训宣讲的方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：进行培训宣讲的方法	1
	4-2技术指导	（1）技能指导	指导技能操作的知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：指导技能操作的知识	1
		（2）技能水平考核	技能水平考核的方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：技能水平考核的方法	1
		（3）组织开展技术改造、技术革新活动	技术改造与革新的方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：技术改造与革新的方法	1
课堂学时合计					40

2.2.7 一级/高级技师职业技能培训课程规范（信息安全管理员）

模块	课程	学习单元	课程内容	培训建议	课堂学时
1.网络与信息安全防护	1-1信息安全风险评估	（1）组织关键业务系统风险评估	1）风险评估知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：对组织关键业务系统进行	2
			2）风险评估技术实现方法		

			3)对组织关键业务系统进行风险评估操作	风险评估操作实例	
		（2）出具信息安全风险评估报告	1）信息系统渗透测试知识 2)根据信息安全风险评估结果，出具评估报告操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：根据信息安全风险评估结果，出具评估报告操作实例	2
		（3）制定信息安全风险整改措施	1）信息安全风险整改方法 2)信息安全风险整改措施制定操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：信息安全风险整改措施制定操作实例	2
	1-2新技术、新应用安全防护	（1）云计算应用安全防护策略	1）云计算安全防护知识 2)云计算应用安全防护策略 3)云计算应用提出安全防护策略方案设计操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：云计算应用提出安全防护策略方案设计操作实例	1
		（2）物联网应用安全防护策略	1）物联网安全防护知识 2）物联网安全防护策略 3)物联网安全防护策略设计操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：物联网安全防护策略设计操作实例	1
		（3）移动互联应用安全防护策略	1)移动互联网安全防护知识 2)移动互联网安全防护策略	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：移动互联网	1

			3)移动互联网安全防护策略设计操作	安全防护策略设计操作实例	
		（4）工业控制系统安全防护策略	1)工业控制系统安全防护知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：工业控制系统安全防护策略设计操作实例	1
			2)工业控制系统安全防护策略		
			3)工业控制系统安全防护策略设计操作		
		（5）大数据应用安全防护策略	1)大数据应用安全防护知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：大数据应用安全防护策略设计操作实例	1
			2)大数据应用安全防护策略		
			3)大数据应用安全防护策略设计操作		
		（6）区块链等其他新技术新应用安全防护策略	1)区块链等新技术安全防护知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：区块链等新技术安全防护策略设计操作实例	1
			2)区块链等新技术安全防护策略		
			3)区块链等新技术安全防护策略设计操作		
2.网络与信息安全管理	2-1信息安全风险管理	（1）制定信息安全风险管理制度	1)信息安全风险管理基础知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：网络安全风险管理操作实例	2
			2）信息安全风险管理操作		
		（2）制定风险评估方案	1）漏洞评估技术	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：漏洞安全管理措施操作实例	2
			2）漏洞安全管理措施操作		
		（3）业务系统安全风险处置方案编制	1)业务系统安全风险处置方案知识	（1）方法：讲授法、演示法、实训（练习）法	1

			2)业务系统安全风险处置方案编制操作	（2）重点与难点：业务系统安全风险处置方案编制操作	
	2-2网络安全等级保护	（1）网络安全等级保护定级	1)网络安全等级保护定级知识 2)网络和信息系统定级操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：网络和信息系统定级操作实例	2
		（2）网络安全等级保护备案	1)网络安全等级保护备案知识 2)网络安全等级保护备案操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：网络安全等级保护备案操作实例	1
		（3）设计和制定安全管理制度	1）安全管理制度知识 2）安全管理制度编制操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：安全管理制度编制操作	1
	2-3关键信息基础设施保护	（1）关键信息基础设施相关数据安全保护要求	关键信息基础设施相关数据安全保护要求	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：关键信息基础设施相关数据安全保护要求	2
		（2）关键信息基础设施安全检查支持	1)关键信息基础设施安全检查支持要求 2)关键信息基础设施安全检查支持操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：关键信息基础设施安全检查操作	1
3.网络与信息安全处	3-1信息安全事件预警	（1）信息安全事件威胁预警	1)安全事件威胁预警机制方法	（1）方法：讲授法、演示法、实训（练习）法	2

置			2)安全事件威胁预警机制编制操作	（2）重点与难点：安全事件威胁预警机制编制操作实例	
		（2）信息安全事件风险定级	1）风险定级、设计响应级别和应急预案制定方法 2）风险定级、设计响应级别和应急预案制定操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：风险定级、设计响应级别和应急预案制定操作实例	1
	3-2信息安全事件证据保存	（1）静态数据提取及固定	1)静态数据提取及固定方法 2)静态数据提取及固定操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：静态数据提取及固定操作实例	2
		（2）动态易失数据提取及固定	1)动态易失数据提取及固定方法 2)动态易失数据提取及固定操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：动态易失数据提取及固定操作实例	1
	3-3信息安全事件应急响应	（1）响应并处理复杂信息安全事件	1)信息安全事件应急响应流程 2)响应并处理复杂信息安全事件操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：响应并处理复杂信息安全事件操作实例	2
		（2）恢复信息安全事件造成的信息损坏	1)信息安全事件造成的网络或系统损坏常用恢复方法 2)恢复信息安全事件造成的网络或系统损坏操作	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：恢复信息安全事件造成的网络或系统损坏操作实例	1

4. 培 训指导	4-1 培训实施	（1）对培训需求进行分析	培训需求分析的要求和方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：培训需求分析的要求和方法	1
		（2）编制培训规划	1）培训规划编制的要求 2)培训预算与决算的审核方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：培训规划编制的要求	1
		（3）组织编写培训教材、讲义、教案	组织编写培训教材、讲义、教案的方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：实例	1
		（4）进行培训宣讲	进行培训宣讲的方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：进行培训宣讲的方法	1
	4-2 技术指导	（1）技能指导	指导技能操作的知识	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：指导技能操作的知识	1
		（2）技能水平考核	技能水平考核的方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：技能水平考核的方法	1
		（3）组织开展技术改造、技术革新活动	技术改造与革新的方法	（1）方法：讲授法、演示法、实训（练习）法 （2）重点与难点：技术改造与革新的方法	1

课堂学时合计	40

2.2.8 培训建议中培训方法说明

1．讲授法

讲授法指教师主要运用语言讲述，系统地向学员传授知识，传播思想理念。即教师通过叙述、描绘、解释、推论来传递信息、传授知识、阐明概念、论证定律和公式，引导学员获取知识，认识和分析问题。

2．讨论法

讨论法指在教师的指导下，学员以班级或小组为单位，围绕学习单元的内容，对某一专题进行深入探讨，通过讨论或辩论活动，从而获得知识或巩固知识的一种教学方法，要求教师在讨论结束时对讨论的主题做归纳性总结。

3．实训（练习）法

实训（练习）法指学员在教师的指导下巩固知识、运用知识，形成技能技巧的方法。通过实际操作的练习，形成操作技能。

4．参观法

参观法指教师组织或指导学员进行实地观察、调查、研究和学习，使学员获得新知识或巩固已学知识的教学方法。参观教学法可细分为“准备性参观、并行性参观、总结性参观”等。

5．演示法

演示法指在教学过程中，教师通过示范操作和讲解使学员获得知识、技能的教学方法。教学中，教师对操作内容进行现场演示，边操作边讲解，强调操作的关键步骤和注意事项，使学员边学边做，理论与技能并重，师生互动，提高学生的学习兴趣和学习效率。

6．案例教学法

案例教学法指通过对案例进行分析，提出问题，分析问题，并找到解决问题的途径和手段，培养学员分析问题、处理问题的能力。

7．项目教学法

项目教学法指以实际应用为目的，将理论知识与实际工作相结合，通过师生

共同完成一个完整的项目工作，使学员获得知识和实践操作能力与解决实际问题能力的教学方法。其实施以小组为学习单位，步骤一般分为确定项目任务、计划、决策、实施、检查和评价 6 个步骤。强调学员在学习过程中的主体地位，以学员为中心，以学员学习为主、教师指导为辅，通过完成教学项目，激发学员的学习积极性，使学员既获得相关理论知识，又掌握实践技能和工作方法，提高学员解决实际问题的综合能力。

8．角色扮演法

角色扮演法指学员通过不同角色的扮演，体验自身角色的内涵活动和对方角色的心理，充分展现各种角色的“为”和“位”。

9．情景表演法

情景表演法指教师在实施培训前事先准备和布置培训现场，并设定情景表演的情景、对话内容及评估标准，通过学员现场的情景表演活动以及教师对活动效果的及时评估，从而达到培训的预期效果。

10．实物示教法

实物示教法指教师通过实物的操作演示或对学员实物操作演示的评价，实现对学员技能操作步骤和要领掌握情况的检查、纠错、修正，并演示正确操作方法的一种教学方法。

11．观摩法

观摩法指让学员通过现场观摩、观看视频等形式，学习、获取知识、技能的一种教学方法。

2.3 考核规范

2.3.1 职业基本素质培训考核规范

考核范围	考核比重(%)	考核内容	考核比重（%）	考核单元
1.职业认知与职业道德	10	1-1 职业认知	3	职业认知
		1-2 职业道德基本知识	4	道德与职业道德
		1-3 职业守则	3	职业守则
2.计算机相关知识	20	2-1 计算机硬件基础知识	5	计算机硬件
		2-2 计算机软	5	计算机软件

		件基础知识		
		2-3 操作系统基础知识	5	操作系统
		2-4 数据库基础知识	5	数据库
3. 网络相关知识	20	3-1 网络协议基础知识	6	网络体系结构与协议
		3-2 组网设备基础知识	8	（1）组网设备概述
				（2）路由器基础知识
				（3）交换机基础知识
		3-3 网络配置、故障排查常用命令和工具基础知识	6	网络配置、故障排查常用命令和工具
4.网络安全基础知识	25	4-1 网络安全概述	5	网络安全概述
		4-2 网络安全基础技术	20	网络安全基础技术
5. 相关法律法规、管理规定、标准知识	25	4-1 法律知识	15	法律知识
		4-2 标准知识	10	标准知识

2.3.2 四级/中级职业技能培训理论知识考核规范（网络安全管理员、信息安全管理员）

考核范围	考核比重（%）	考核内容	考核比重（%）	考核单元
1.网络与信息安全防护	40	1-1 网络安全配置与防护	15	（1）配置网络设备接口信息
				（2）配置路由协议
				（3）配置无线网络设备
				（4）配置网络设备基础安全设置
		1-2 系统安全配置与防护	15	（1）配置 Windows 操作系统密码策略与账户策略
				（2）配置 Linux 操作系统密码策略与账户策略
				（3）配置 Windows 操作系统自带的防火墙
				（4）配置 Linux 操作系统自带的防火墙

				（5)安装部署防病毒软件
				（6）配置 Windows 系统高级安全审核
				（7）配置 Linux 系统审核功能
		1-3 应用安全配置及防护	10	（1）配置常见的应用服务
				（2）配置应用服务的基本防护
2.网络与信息安全管理	30	2-1 网络安全管理	10	（1）配置交换机的 VLAN
				（2）配置网络设备的远程管理
				（3）管理网络设备的用户安全级别
		2-2 系统安全管理	10	（1）管理 Windows 系统用户与组的基本配置
				（2）管理 Linux 系统用户与组的基本配置
				（3）管理 Windows 系统文件及文件夹的访问权限
				（4）管理 Linux 系统文件及文件夹的访问权限
				（5）操作系统补丁更新
				（6）防病毒软件安全保护策略配置和定期升级服务
		2-3 应用安全管理	10	（1）企业域名备案
				（2）配置企业应用域名解析
				（3）应用数据备份
3.网络与信息安全处置	30	3-1 网络安全事件处置	15	（1）使用网络诊断工具识别并处理常见网络故障
				（2）识别常见网络层攻击
		3-2 系统及应用安全事件处置	15	（1）识别常见系统安全事件
				（2）恶意代码检测与清除
				（3）应用数据恢复

2.3.3 四级/中级职业技能培训操作技能考核规范（网络安全管理员、信息安全管理员）

考核范围	考核比重（%）	考核内容	考核比重（%）	考核形式	选考方法	考核时间（分钟）	重要程度
1.网络与信息安全防护	40	1-1 网络安全配置与防护	15	操作	必考	15	X
		1-2 系统安全配置与防护	15	操作	必考	15	X
		1-3 应用安全配置与防护	10	操作	必考	15	X
2.网络与信息安全管理	30	2-1 网络安全管理	10	操作	必考	15	X
		2-2 系统安全管理	10	操作	必考	15	X
		2-3 应用安全管理	10	操作	必考	15	X
3.网络与信息安全处置	30	3-1 网络安全事件处置	15	操作	必考	15	X
		3-2 系统及应用安全事件处置	15	操作	必考	15	X
合计	100	-	100	-	-	120	-

2.3.4 三级/高级职业技能培训理论知识考核规范（网络安全管理员、信息安全管理员）

模块	考核比重(%)	考核内容	考核比重（%）	考核单元
1.网络与信息安全防护	40	1-1 网络安全防护	15	（1）安全加固企业级交换机、路由器
				（2）部署配置边界防护设备
				（3）部署配置入侵检测/防御系统
				（4）部署配置无线网络安全

				（5）部署配置网络安全审计设备
		1-2 系统安全防护	15	（1）配置系统安全策略
				（2）配置系统自带防火墙访问控制规则
				（3）防范常见恶意代码
		1-3 应用安全防护	10	（1）配置数据加密传输
				（2）部署配置 Web 应用防火墙
				（3）部署配置应用安全审计
2. 网络与信息安全管理	30	2-1 网络安全管理	10	（1）配置防火墙网络访问控制管理
				（2）管理各类终端接入无线网络
				（3）管理各类边界设备、网络节点远程访问
				（4）留存网络设备安全日志
		2-2 系统安全管理	10	（1）管理安全远程访问
				（2）管理系统漏洞和风险
				（3）管理应用系统备份
				（4）管理系统日志
				（5）应用系统备案
		2-3 应用安全管理	10	（1）安全管理互联网应用
				（2）过滤垃圾邮件等有害数据
				（3）管理审计互联网访问日志
3. 网络与信息安全处置	30	3-1 网络安全事件监控和处置	10	（1）网络数据流量监控
				（2）攻击流量阻断
				（3）网络安全日志留存
		3-2 系统安全事件监控和处置	10	（1）识别、隔离被入侵或感染病毒的计算机
				（2）识别系统异常状态及系统后门清除
				（3）系统异常状态检测及恢复
				（4）病毒样本留存及上报
		3-3 应用安全	10	（1）提取数据库、Web

		事件监控和处置		服务应用访问日志
				（2）日志分析、识别及定位事件
				（3）违法有害信息识别及处置
				（4）互联网安全事件记录、证据留存及上报

2.3.5 三级/高级职业技能培训操作技能考核规范（网络安全管理员、信息安全管理员）

考核范围	考核比重（%）	考核内容	考核比重（%）	考核形式	选考方法	考核时间（分钟）	重要程度
1.网络与信息安全防护	40	1-1 网络安全防护	15	操作	必考	15	X
		1-2 系统安全防护	15	操作	必考	15	X
		1-3 应用安全防护	10	操作	必考	15	X
2.网络与信息安全管理	30	2-1 网络安全管理	10	操作	必考	15	X
		2-2 系统安全管理	10	操作	必考	15	X
		2-3 应用安全管理	10	操作	必考	15	X
3.网络与信息安全处置	30	3-1 网络安全事件监控和处置	10	操作	必考	10	X
		3-2 系统安全事件监控和处置	10	操作	必考	10	X
		3-3 应用安全事件监控和处置	10	操作	必考	10	X
合计	100	-	100	-	-	120	-

2.3.6 二级/技师职业技能培训理论知识考核规范（网络安全管理员）

模块	考核比重(%)	考核内容	考核比重（%）	考核单元
1.网络与信息安全防护	30	1-1 网络安全防护	10	（1）网络漏洞扫描、分析及安全加固
				（2）安全域配置及安全策略配置
				（3）配置重要设备硬件冗余
				（4）配置虚拟专用网络（VPN）
		1-2 系统安全防护	10	（1） 系统安全扫描及、风险分析
				（2）启用数据加密策略对应用数据进行保护
		1-3 应用安全防护	10	（1）互联网应用漏洞扫描及风险分析
				（2） 漏洞测试及验证
				（3）配置 Web 应用防火墙
				（4）规划反垃圾邮件网关实施方案
2.网络与信息安全管理	30	2-1 网络安全等级保护	15	（1）网络安全等级保护基础
				（2）网络安全基线配置检查及加固整改
		2-2 应用安全评估	15	（1）互联网服务自评估
				（2）信息网络安全技术方案制定
				（3）渗透测试工作配合
				（4）根据渗透测试报告进行加固
3.网络与信息安全处置	30	3-1 网络安全事件监测	10	（1）网络链路运行状况监测
				（2）网络设备运行状况监测
				（3）安全设备运行状况监测
				（4）系统运行状况监测
		3-2 网络安全事件分析	10	（1） 设备监测数据清洗、汇总

				（2）设备监测数据分析
		3-3 网络安全事件响应	10	（1）常见网络安全事件响应
				（2）常见网络攻击溯源和上报
				（3）留存网络安全事件相关证据记录
4.培训指导	10	4-1 培训实施	5	（1）制订培训工作计划
				（2）编制和实施培训方案
				（3）编写培训教材、讲义、课件
				（4）培训宣讲
		4-2 技术指导	5	（1）技能指导
				（2）技能水平考核

2.3.7 二级/技师职业技能培训操作技能考核规范（网络安全管理员）

考核范围	考核比重（%）	考核内容	考核比重（%）	考核形式	选考方法	考核时间（分钟）	重要程度
1.网络与信息安全防护	40	1-1 网络安全防护	15	操作	必考	15	X
		1-2 系统安全防护	15	操作	必考	15	X
		1-3 应用安全防护	10	操作	必考	15	X
2.网络与信息安全管理	30	2-1 网络安全等级保护	15	操作	必考	15	X
		2-2 应用安全评估	15	操作	必考	15	X
3.网络与信息安全处置	30	3-1 网络安全事件监测	10	操作	必考	15	X
		3-2 网络安全事件分析	10	操作	必考	15	X
		3-3 网络安全事件	10	操作	必考	15	X

		响应					
合计	100	-	100	-	-	120	-

2.3.8 二级/技师职业技能培训理论知识考核规范（信息安全管理员）

模块	考核比重(%)	考核内容	考核比重（%）	考核单元
1.网络与信息安全防护	30	1-1 信息资产安全防护	10	（1)信息资产分类分级
				（2)安全域资源防护策略制定
		1-2 数据安全防护	10	（1）数据安全存储策略、数据加密策略配置
				（2)制定数据容灾策略
		1-3 互联网信息安全防护	10	（1)重要信息脆弱性评估及防护
				（2)员工个人信息安全策略配置
2.网络与信息安全管理	30	2-1 数据安全管理	15	（1）数据在存储、通信中的公私钥和证书管理
				（2）数据高可用管理
				（3）重要数据保护
		2-2 互联网信息安全管理	15	（1)履行信息安全管理义务
				（2)编制个人敏感信息安全保护技术方案
				（3)个人敏感信息脆弱性评估及防护
3.网络与信息安全处置	30	3-1 信息安全事件监测	10	（1)监测信息破坏事件
				（2)监测信息内容安全事件
				（3)监测其他信息安全事件
		3-2 信息安全事件分析	10	（1)信息安全监测数据清洗、汇总
				（2)信息安全监测数据分析
		3-3 信息安全事件响应	10	（1)常见信息安全事件响应
				（2)常见信息安全事件溯源和上报
				（3)留存信息安全事件相关证据记录

4.培训指导	10	4-1 培训实施	5	（1)制订培训工作计划
				（2)编制和实施培训方案
				（3）编写培训教材、讲义、课件
				（4）培训宣讲
		4-2 技术指导	5	（1）技能指导
				（2）技能水平考核

2.3.9 二级/技师职业技能培训操作技能考核规范（信息安全管理员）

考核范围	考核比重（%）	考核内容	考核比重（%）	考核形式	选考方法	考核时间（分钟）	重要程度
1.网络与信息安全防护	40	1-1 信息资产安全防护	15	操作	必考	15	X
		1-2 数据安全防护	15	操作	必考	15	X
		1-3 互联网信息安全防护	10	操作	必考	15	X
2.网络与信息安全管理	30	2-1 数据安全管理	15	操作	必考	15	X
		2-2 互联网信息安全管理	15	操作	必考	15	X
3.网络与信息安全处置	30	3-1 信息安全事件监测	10	操作	必考	15	X
		3-2 信息安全事件分析	10	操作	必考	15	X
		3-3 信息安全事件响应	10	操作	必考	15	X
合计	100	-	100	-	-	120	-

2.3.10 一级/高级技师职业技能培训理论知识考核规范（网络安全管理员）

模块	考核比重(%)	考核内容	考核比重（%）	考核单元
1.网络与信息安全防护	30	1-1 网络安全风险评估	15	（1）组织整体业务系统安全风险评估
				（2）网络和应用系统渗透测试及漏洞验证和修补
		1-2 新技术、新应用安全防护	15	（1）云计算应用安全防护策略
				（2）物联网应用安全防护策略
				（3）移动互联应用安全防护策略
				（4）工业控制系统安全防护策略
				（5）大数据应用安全防护策略
				（6）区块链等其他新技术新应用安全防护策略
2.网络与信息安全管理	30	2-1 网络安全风险管理	10	（1）网络安全风险管理
				（2）漏洞评估及制定安全管理措施
		2-2 网络安全等级保护	10	（1）网络安全等级保护定级
				（2）网络安全等级保护备案
				（3）网络安全等级保护建设整改
				（4）网络安全自我监督检查
		2-3 关键信息基础设施保护	10	（1）关键信息基础设施安全检查
				（2）制定关键信息基础设施安全加固方案
				（3）网络安全事件应急方案编制
3.网络与信息安全处置	30	3-1 网络安全事件预警	10	（1）建立安全事件威胁预警机制
				（2）网络安全事件风险定级、设计响应级别和

				应急预案
		3-2 网络安全事件证据保存	10	（1）静态数据提取及固定
				（2）动态易失数据提取及固定
		3-3 网络安全事件应急响应	10	（1）复杂网络安全事件应急响应
				（2）恢复网络安全事件造成的网络或系统损坏
4.培训指导	10	4-1 培训实施	5	（1）培训需求分析
				（2）编制培训规划
				（3）组织编写培训教材、讲义、教案
				（4）进行培训宣讲
		4-2 技术指导	5	（1）技能指导
				（2）技能水平考核
				（3）组织开展技术改造、技术革新活动

2.3.11 一级/高级技师职业技能培训操作技能考核规范（网络安全管理员）

考核范围	考核比重（%）	考核内容	考核比重（%）	考核形式	选考方法	考核时间（分钟）	重要程度
1.网络与信息安全防护	40	1-1 网络安全风险评估	20	操作	必考	15	X
		1-2 新技术、新应用安全防护	20	操作	必考	15	X
2.网络与信息安全管理	30	2-1 网络安全风险管理	10	操作	必考	15	X
		2-2 网络安全等级保护	10	操作	必考	15	X
		2-3 关键信息基础设施保护	10	操作	必考	15	X

3.网络与信息安全处置	30	3-1 网络安全事件预警	10	操作	必考	15	X
		3-2 网络安全事件证据保存	10	操作	必考	15	X
		3-3 网络安全事件应急响应	10	操作	必考	15	X
合计	100	-	100	-	-	120	-

2.3.12 一级/高级技师职业技能培训理论知识考核规范（信息安全管理员）

模块	考核比重(%)	考核内容	考核比重（%）	考核单元
1.网络与信息安全防护	30	1-1 信息安全风险评估	15	（1）组织关键业务系统风险评估
				（2）出具信息安全风险评估报告
				（3）制定信息安全风险整改措施
		1-2 新技术、新应用安全防护	15	（1）云计算应用安全防护策略
				（2）物联网应用安全防护策略
				（3）移动互联应用安全防护策略
				（4）工业控制系统安全防护策略
				（5）大数据应用安全防护策略
				（6）区块链等其他新技术新应用安全防护策略
2.网络与信息安全管理	30	2-1 信息安全风险管理	10	（1）制定信息安全风险管理制度
				（2）制定风险评估方案
				（3）业务系统安全风险处置方案编制
		2-2 网络安全等级保护	10	（1）网络安全等级保护定级
				（2）网络安全等级保护备案

				（3）设计和制定安全管理制度
		2-3 关键信息基础设施保护	10	（1）关键信息基础设施相关数据安全保护要求
				（2）关键信息基础设施安全检查支持
3. 网络与信息安全处置	30	3-1 信息安全事件预警	10	（1）信息安全事件威胁预警
				（2）信息安全事件风险定级
		3-2 信息安全事件证据保存	10	（1）静态数据提取及固定
				（2）动态易失数据提取及固定
		3-3 信息安全事件应急响应	10	（1）响应并处理复杂信息安全事件
				（2）恢复信息安全事件造成的信息损坏
4. 培训指导	10	4-1 培训实施	5	（1）对培训需求进行分析
				（2）编制培训规划
				（3）组织编写培训教材、讲义、教案
				（4）进行培训宣讲
		4-2 技术指导	5	（1）技能指导
				（2）技能水平考核
				（3）组织开展技术改造、技术革新活动

2.3.13 一级/高级技师职业技能培训操作技能考核规范（信息安全管理员）

考核范围	考核比重（%）	考核内容	考核比重（%）	考核形式	选考方法	考核时间（分钟）	重要程度
1. 网络与信息安全防护	40	1-1 信息安全风险评估	20	操作	必考	15	X
		1-2 新技术、新应用安全防护	20	操作	必考	15	X
2. 网络与	30	2-1 信息	10	操作	必考	15	X

信息安全管理		安全风险管理					
		2-2 网络安全等级保护	10	操作	必考	15	X
		2-3 关键信息基础设施保护	10	操作	必考	15	X
3.网络与信息安全处置	30	3-1 信息安全事件预警	10	操作	必考	15	X
		3-2 信息安全事件证据保存	10	操作	必考	15	X
		3-3 信息安全事件应急响应	10	操作	必考	15	X
合计	100	-	100	-	-	120	-