高等学历继续教育
非国控专业增设申请表

学校名称（盖章）：国家开放大学

学校主管部门：北京市教育委员会

专业名称：信息安全与管理

专业代码：310207

所属专业门类或专业大类：电子与信息大类

修业年限：2.5 年

培养层次：本科（专科起点）

学习形式：开放教育

申请时间：2021 年 9 月

专业负责人：王英彬

联系电话：13911106606

中华人民共和国教育部制

目录

填 表 说 明

1. 申请表限用 A4 纸张打印并装订成册（各专业分别装订）；

2.在学校办学基本类型对应的方框中画“√”;

3.所有表格均可另加页;

4.本表内容应真实、准确。

专业增设申请表

专业代码	310207	专业名称	信息安全与管理
培养层次	本科（专科起点）	学习形式	开放教育
修业年限	2.5 年	现有专业(个)	240
学科门类（本科）或专业大类（专科）	电子与信息大类计算机类	本校已设的相近专业及开设年份	信息安全技术应用（专科）(2016 年)
拟首次招生时间及招生数	2022 年秋季，300 人	五年内计划发展规模	4000 人
学校专业设置评议专家组织评议意见	专业设置委员会认为信息安全与管理专业的申报设置，符合国家区域经济社会发展对人才的需要，人才培养符合学校发展定位，专业发展具有较好前景。国家开放大学具备开办该专业的办学条件和师资力量，能够获得相关部门、行业企业的资源支持。专业人才培养方案目标明确，课程体系设置合理。 同意申报设置信息安全与管理专业。 （主任签字） 2022 年 1 月 24 日		
学校意见	（校长签字） 学校（盖章）： 年 月 日		
省级教育行政部门意见	盖章： 年 月 日		

注：专业代码按《办法》规定的专业目录填写。

学校基本情况

<table>
<tr><td>学校名称</td><td>国家开放大学</td><td>学校地址</td><td colspan="2">北京市海淀区复兴路 75 号</td></tr>
<tr><td>邮政编码</td><td>100039</td><td>校园网址</td><td colspan="2">http://www.ouchn.edu.cn/</td></tr>
<tr><td>在校生总数</td><td colspan="2">497.3 万</td><td>专业平均年招生规模</td><td>6725 人</td></tr>
<tr><td>学校类型</td><td colspan="4">☑开放大学　□独立设置成人高校</td></tr>
<tr><td>已有学科门类
或专业大类</td><td colspan="4">本科专业学科：经济学，管理学，法学，教育学，文学，理学，工学，农学，医学、艺术学等 10 个学科
专科专业大类：农林牧副渔、资源环境与安全、能源动力与材料、土木建筑、水利、装备制造、生物与化工、轻工纺织、食品药品与粮食、交通运输、电子信息、医药卫生、财经商贸、旅游、文化艺术、新闻传播、教育与体育、公安与司法、公共管理与服务等 19 个专业大类。</td></tr>
<tr><td>专任教师
总数（人）</td><td>9.1 万</td><td colspan="2">专任教师中副教授及以上职称教师所占比例</td><td>30%</td></tr>
<tr><td>学校简介和
历史沿革
（300 字以内）</td><td colspan="4">国家开放大学是教育部直属的，以促进终身学习为使命、以现代信息技术为支撑、以“互联网+”为特征，面向全国开展开放教育的新型高校，前身是邓小平同志 1978 年亲自倡导并批示创办的中央广播电视大学。2012 年 7 月 31 日，国家开放大学在人民大会堂正式揭牌成立。学校实行注册学习、宽进严出的教育制度，基于网络探索线上线下结合的人才培养模式。
国家开放大学适应国家经济社会发展和人的全面发展需要，强调“开放、责任、质量、多样化、国际化”的办学理念，强调优质教育资源的集聚、整合和共享，强调以现代信息技术为支撑，探索现代信息技术与教育的深度融合，提供教育机会、实现教育公平，建设我国终身教育的主要平台、在线教育的主要平台和灵活教育的平台、对外合作的平台，促进构建服务全民终身学习的教育体系。</td></tr>
</table>

注：专业平均年招生规模=学校年招生数÷学校现有专业总数

增设专业的理由和基础

（包括申请增设专业的主要理由、专业筹建情况、学校专业发展规划及人才需求预测情况等方面的内容）

一、专业设置的必要性

（一）国家有关法律法规及政策的明确要求

网络安全是事关经济社会发展、国家长治久安和人民群众福祉的重大国家战略问题，国际上围绕信息的获取、使用和控制的斗争愈演愈烈，各国都给予极大的关注和投入。习近平总书记在网络安全人才培养方面，明确指出，“没有网络安全，就没有国家安全”、“网络空间的竞争，归根结底是人才竞争”，“加强网络空间安全人才建设，打造素质过硬、战斗力强的人才队伍”。建设网络强国，没有一支优秀的人才队伍，没有人才创造力迸发、活力涌流，是难以成功的。网络安全保障能力是 21 世纪综合国力、经济竞争实力和生存能力的重要组成部分，全方位地影响我国的政治、军事、经济、文化、社会生活的各个方面，建立一支规模宏大、结构优化、素质优良的人才队伍是维护国家网络安全和建设网络强国的核心需求。

由于我国的信息化建设以及信息安全产业起步较晚、起点较低，产业规模和专业人员还处于发展壮大阶段，质素较发达国家仍有很大差距。网络安全人才队伍整体上还存在着人才供需失衡、教育培训缺乏、人才管理和激励机制有限等不足之处，远不能满足信息化快速发展的需要。长期以来网络安全人才市场一直处于供不应求的状态下，预估目前我国网络安全从业人才累计缺口在 **140 万以上**，而每年网络安全相关专业的高校毕业生规模仅 **2 万余**人，严重滞后于社会需求。近年来国家相关部委密集出台了加快信息安全人才建设的多项法规、政策和举措：

1.《中华人民共和国网络安全法》明确提出 “第二十条 国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。”，“第三十四条 除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：……（二）定期对从业人员进行网络安全教育、技术培训和技能考核。”

2.中央网络安全和信息化领导小组办公室、国家发展和改革委员会、教育部、科学技术部、工业和信息化部、人力资源和社会保障部联合发布《关于加强网络安全学

科建设和人才培养的意见》（中网办发文[2016]4 号）中具体提出了八项重要意见：“一、加快网络安全学科专业和院系建设。二、创新网络安全人才培养机制。三、加强网络安全教材建设。四、强化网络安全师资队伍建设。五、推动高等院校与行业企业合作育人、协同创新。六、加强网络安全从业人员在职培训。七、加强全民网络安全意识与技能培养。八、完善网络安全人才培养配套措施。”

3.国务院总理李克强签署中华人民共和国国务院令第 745 号，公布的《关键信息基础设施安全保护条例》中第三十五条明确“ 国家采取措施，鼓励网络安全专门人才从事关键信息基础设施安全保护工作；将运营者安全管理人员、安全技术人员培训纳入国家继续教育体系。”

4. 自主可控是网络安全的必然要求，在此基础上才能构建安全可控的信息技术体系。习近平总书记在中共中央政治局第三十六次集体学习时提出的“加快推进国产自主可控替代计划，构建安全可控的信息技术体系”，“实施网络信息领域核心技术设备攻坚战略”是我国网信领域的一项重大任务。随着《信息技术产品安全可控评价指标》系列国家标准出台、新基建范围和目标的明确，为我国信创这一 自主安全与信息化高度统一的行业创造了巨大的市场机遇，需要培养大批信创行业安全服务实用型人才服务产业应用和可持续发展。

（二）建设网络强国迫切需要全面落实网络安全等级保护制度

伴随信息技术的飞速发展，互联网、通信网、计算机系统、 自动化控制系统、数字设备及其承载的应用、服务和数据等组成的网络空间，正在全面改变人们的生产生活方式，深刻影响人类社会历史发展进程。近年来，随着我国关键信息基础设施和新技术新应用的大规模发展，信息安全风险融合叠加并快速演变。同时，互联网技术应用不断模糊物理世界和虚拟世界界限，对整个经济社会发展的融合、渗透、驱动作用日益明显，带来的风险挑战也不断增大，网络空间威胁和日益增多。比较突出的问题表现在 DDoS 攻击高发频发且攻击组织性与目的性更加凸显；APT 攻击逐步向各重要行业领域渗透，在重大活动和敏感时期更加猖獗；事件型漏洞和高危零日漏洞数量上升，信息系统面临的漏洞威胁形势更加严峻；数据安全防护意识依然薄弱，大规模数据泄露事件更加频发；“灰色”应用程序大量出现，针对重要行业安全威胁更加明显；网络黑产活动专业化、 自动化程度不断提升，技术对抗更加激烈；工业控制系统产品安全问题依然突出，新技术应用带来隐患更加严峻。中国是网络大国，也是面临信息安全

威胁最严重的国家之一，迫切需要建立和完善信息安全的法律制度，提高全社会的信息安全意识和信息安全保障水平。

《中华人民共和国网络安全法》是国家安全法律制度体系中的一部重要法律，是网络安全领域的基本大法，对于确立国家网络安全基本管理制度具有里程碑式的重要意义。“第二十一条 国家实行网络安全等级保护制度。”明确了网络安全等级保护制度是我国网络安全的基本制度，不执行网络安全等级保护制度即为违法。

网络安全等级保护制度是国家网络安全保障工作的基础，通过开展等级保护工作，发现企业网络和信息系统与国家安全标准之间存在的差距，找到目前系统存在的安全隐患和不足，通过安全整改，提高信息系统的安全防护能力，降低系统被各种攻击的风险，是一项事关国家安全、社会稳定的政治任务和迫切需要。

（三）网络安全保障涉及面广泛，人才缺口大，亟需培养高素质技术与管理型人才

当前，我国关键信息基础设施与重要信息系统安全面临的形势十分严峻，既有外部威胁，又有自身的脆弱性和薄弱环节。建立一支规模宏大、结构优化、素质优良的信息安全人才队伍是维护国家网络安全和建设网络强国的核心需求，迫切需要大力培养政府、军队、公安等国家机构，以及电信、电力、能源、IT、银行、税务、金融、证券、学校、电子商务等不同类型关键信息基础设施与各行业重要信息系统的信息安全技术与管理人才队伍建设。

我们需清楚看到我国信息安全专业人才培养严重滞后于社会需求，其直接从业人员缺口高达 140 万以上，人才的培养和储备已成为企业、行业乃至国家亟待解决的问题。特别是《中华人民共和国网络安全法》明确规定“ 国家实行网络安全等级保护制度”，确立了网络安全等级保护制度是维护国家安全、社会秩序和公共利益的根本保障，各行业领域围绕等级保护制度工作的落实已成为首要目标任务，其职责中明确涉及信息安全技术与管理相关内容的岗位更是难以统计，专业人才缺口巨大。

我国对信息安全人才的需求是多层次的，其中就包括大量从事等级保护评估和测评、安全咨询、安全管理、风险评估，安全运维、应急保障等相关工作的高素质技能应用型人才。当前，现代信息技术飞速发展，推动了信息安全产业的蓬勃发展，我国信息安全与管理人才的需求空间快速放大，一方面，需要培养大量技能应用型人才填补产业缺口，全面提升各企事业单位相关岗位人员的安全能力和素养；另一方面，现有从业人员知识、能力和素质参差不齐，亟需与时俱进，学习掌握新知识、新技能，

进一步提升综合安全保障能力。

（四）完善构建终身教育体系、促进学习型社会建设的需要

习近平总书记指出“网络安全为人民，网络安全靠人民，维护网络安全是全社会共同责任，需要政府、企业、社会组织、广大网民共同参与，共筑网络安全防线”。网络安全本质是攻防双方的较量，我国正在落实网络安全等级保护制度，并逐步构建安全可控的信息技术体系，加快推进国产自主可控替代计划和新一代信息基础设施建设。随着我国信息技术创新应用产业蓬勃发展，新技术、新应用快速更新，信息安全从业人员迫切需要接受终身教育，来提高职业技能和业务水平，以适应时代发展，强化综合安全保障能力。

因此，通过高等学历继续教育开设信息安全与管理专业，与公安部主导的国家重要信息系统保护人员执业证书衔接融通，形成高等学历继续教育与非学历的融合机制和模式，快速解决从业人员技术和管理应用能力不足和行业人才缺口的问题。

一方面，信息安全工作覆盖范围广，就业面广泛，人才需求旺盛，缺口日益增大。促使大批没有相关从业背景，但又期望从事相关工作的应届生和转岗人员趋之若鹜，竞相投身从业。近三年来绝大多数的行业求职者来自于计算机、通信工程、电子信息工程及软件工程等专业（图 1），拥有本专业学科教育背景的人数较少，需要进一步加大对各类高校网络安全及相关专业的建设，提升网络安全人才的数量和质量。

专业	2019年	2020年	2021年
计算机科学与技术	8.66%	8.22%	7.15%
通信工程	4.92%	4.75%	4.65%
电子信息工程	4.84%	4.81%	4.43%
工商管理	2.32%	2.33%	2.39%
软件工程	2.46%	2.37%	2.10%
市场营销	1.81%	1.93%	2.05%
自动化	2.06%	1.95%	1.83%
电子信息科学与技术	1.26%	1.28%	1.25%
计算机应用	1.35%	1.28%	0.96%
网络工程	0.87%	0.96%	0.92%

图 1 网络安全行业求职者所学专业 TOP10

另一方面，国内网络安全人才培养的主要途径是大学教育，从近三年的网络安全人才的学历情况统计结果来看，网络安全人才的最高学历分布呈现橄榄型特点，从业人员本科以下层次占比较高超过 80%（图 2）。通过高等学历继续教育开设信息安全与

管理本科专业，有利于较快速弥补网络安全本科层次人才需求缺口，提升个人职业发展空间。

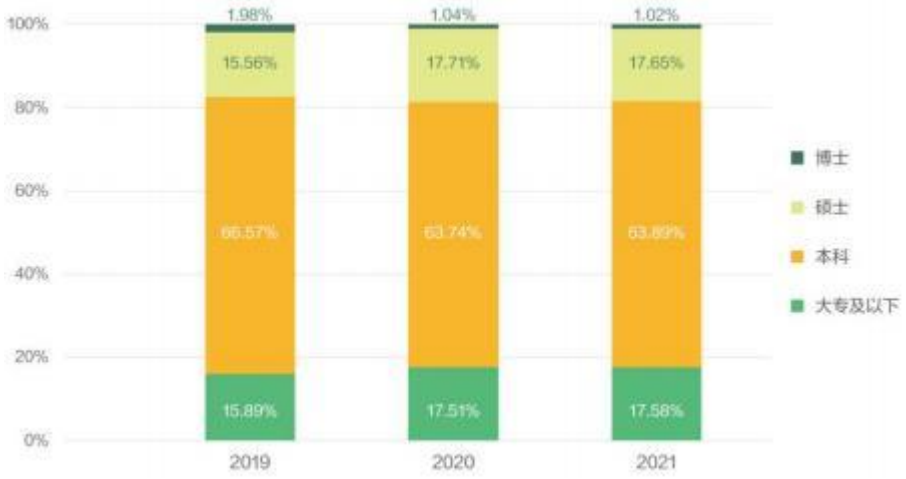

图 2　2019-2021 年网络安全人才最高学历分布

从行业有关单位的职业培训统计看，不具备专业和从业背景的人员知识结构和能力水平参差不齐，且不具备交叉学科的基本知识和技术，仅靠短期职业培训无法达到培养目标，且普遍就职于基础性岗位，需要通过多年的工作积累和自主学习逐步提高专业素质和职业能力。需要通过高等学历继续教育开设专门专业，结合在职岗位实践应用能够快速提高技术和管理应用能力，有利于快速提高从业人员综合专业能力，形成优秀人才梯队建设模式，有效培养并选拔高级人才。

信息安全产业随着国内外形势的发展，我国相关政策的推动，标准和技术的演进，必将蓬勃发展，信息安全高素质人才需求会进一步放大，亟需通过设立高等学历继续教育信息安全与管理专业。逐步形成高等学历和非学历继续教育的融合培养机制和模式，夯实行业产业在职成人的信息安全与管理基础理论知识，不断丰富和更新职业技能，促进信息安全与管理人才梯队的形成，更有利于实用型高端人才的选拔和培养，满足行业产业技术和管理相关岗位的人才需求。同时，借助职业教育国家学分银行，打通行业领域从业人员学历和非学历继续教育的融合通道，进一步发挥国家开放大学体制机制和系统办学优势，促进行业领域学习型社会的建设，更好承担全面“构建服务全民终身学习的教育体系”的新使命。

二、专业设置的可行性及筹建情况

（一）主管部门和行业领域资源支持

2013 年底，国家开放大学与行业主管机构公安部信息安全等级保护评估中心和行

业企业合作，共同成立国家开放大学网络空间安全学院，探索与行业、企业联合开展应用性人才培养的新模式、新机制，发挥国家开放大学在服务学习型行业建设和构建终身教育体系中的重要作用，提高行业、企业从业人员科学和文化素质，提升行业、企业的生产能力和核心竞争力。

公安部信息安全等级保护评估中心是由国家网络安全主管部门为建立网络安全等级保护制度，构建国家网络安全保障体系而专门批准成立的专业技术支撑机构，是全国网络安全等级测评体系技术指导和管理机构，承担着信息技术培训、网络安全测评机构、网络安全测评师能力审验职责，拥有中级网络安全等级保护培训师 30 余名，高级网络安全等级保护培训师 12 名，行业知名专家 10 名，师资力量雄厚。独立制作开发了近 50 门多媒体课件，出版了有关教程教材四套。从 2010 年至今已开展等级保护测评师认证培训近百期，培训网络安全等级保护测评师 7000 余人。为全国各行业贯彻落实网络安全等级保护制度提供了相应的岗位资格认证，是具有国家政策支持的，符合国家有关政策、规范和标准要求的权威教培机构。评估中心还参与国家网络安全等级保护管理规范制定以及网络安全等级保护行政执法体系建设，承担国家网络安全等级保护标准体系设计和重要技术标准的编制及宣贯。也是全国性社会组织中关村信息安全测评联盟的理事长单位。

中关村信息安全测评联盟是在公安部网络安全保卫局指导下、由公安部信息安全等级保护评估中心等 9 家测评机构联合发起成立的全国性社会组织，是一支以国家网络安全等级保护测评体系为基础构建的专业技术力量。 目前联盟成员 200 余家，覆盖了全国各省市自治区。多年来，联盟开展数万个信息系统等级保护测评工作，系统涵盖了电信、广电、能源、交通、水利、金融等各个行业，涉及生产作业、指挥调度、管理控制和公众服务等各个业务类型，为国家基础网络和重要信息系统安全保护工作做出了重要贡献，是我国网络安全事业的一支不可忽视的生力军，为国家关键信息基础设施保护工作发挥不可替代的作用。

以上各级主管部门和行业组织可以提供优质的专家师资团队、成熟的课程课件、丰富的教培经验、实验室实训实践以及广泛的行业资源，在设立信息安全与管理专业中给予了技术研究、人才需求、培养目标、课程体系、实践基地、就业面向等方面的重要支持。通过主管部门和行业领域的优质资源，将为国家开放大学信息安全与管理本科专业的人才培养方案制定、课程资源建设、实训体系建设、师资培训等方面提供

可靠的支撑和保障。

（二）具备数量充足的优质师资队伍

信息安全与管理是培养信息安全技术和管理综合应用能力的专业，对象包括网络资源、信息系统、信息资源，以及云平台、物联网、工控系统、大数据、移动互联等各类新技术应用，涉及工学、理学、管理学等多门学科专业，这些学科已经是教学系统中的一级或者二级学科，都已经比较成熟，各高校都已开设相关专业且均配备了相当强的师资力量，通过师资聘请和引进可满足信息安全与管理专业基础课程的教学需要。

公安部设有专门的网络安全等级保护和国家重要信息系统保护培训机构，自 2008 年起就开始在全国范围开展网络安全等级保护专业师资体系化培养，具备十多位高级网络安全等级保护培训师，具有成熟的教学师资培养课程和课件，全套师资培养系列教材，师资评价标准和执业资格证书，已为全国各行业培养网络安全等级保护和国家重要信息系统保护相关专业师资上千人。同时，还可以将国家重要信息系统保护人员执业资格证书项目引入国家开放大学学分银行互认体系，包括：CIIP-E 信息安全评估师、CIIP-D 信息安全管理师、CIIP-A 信息安全管理员等行业证书。

学院共建方包括专业教培机构，是公安部、中国网络安全审查技术与认证中心、中国信息安全测评中心、工信部考试中心等国家部委网络安全认证培训项目的课程开发和实施机构；国家能源局网络安全重点支撑单位；参与建设运营华北电力大学信息安全工程实验室、电力行业信息安全等级保护测评中心第一测评实验室、信息安全等级保护关键技术国家工程实验室工控安全众测平台等国家和行业重点实验室。可以为信息安全与管理专业提供优秀的专家师资团队、成熟的课程课件和实训实践课程教学支撑及指导。

通过主管部门和行业领域专业机构发挥技术研究、实践应用和行业专家等行业资源优势，能够保障专业教学团队数量充足、结构合理、素质优良，满足专业资源建设和教学工作的需要。

信息安全与管理专业是由国家开放大学网络空间安全学院建设，筹备本专业建设的教师团队由高等院校教师、科研机构研究人员、行业企业知名专家和高级职业培训师共 23 人组成，均长期从事信息安全行业领域的科研和教培工作，也是国家和行业政策法规标准的参与制定者和宣贯落实者，将由信息安全领域的知名教授和行业“双师

型”教师担任本专业的主讲教师。后期学院将根据专业教学工作的具体需要增加课程师资数量，能够保障教学团队数量充足、结构合理、素质优良，满足学院专业资源建设和教学服务工作。

为满足高质量信息安全与管理本科课程建设的需要，学院聘请由国家网络安全等级保护专家委员会、公安部信息安全等级保护评估中心、高等院校、中关村信息安全测评联盟、行业企业的知名信息安全专家组成专业指导委员会，为专业建设和教学质量把关。

（三）产教融合，提供良好的专业实践条件

我国网络安全等级保护实施过程中，已经构建了包括国家行业领域，各省、 自治区、直辖市在内的 200 余家第三方测评机构，均按照等级保护要求建设有等级保护测评实验室，部分机构还承建有信息安全等级保护关键技术国家工程实验室及分实验室。通过有效推进产教融合，信息安全主管部门和行业领域组织机构能够为开设信息安全与管理专业的教学单位，提供良好的专业实践条件和具备丰富实践经验的实训实践教师。

各教学单位也可联合网络空间安全学院共建方及相关行业组织，对已开设计算机类相关专业现有的实验室或实践基地进行改造扩容，培养本单位专业实训教师，推进实验实训设施建设，加快实训标准和实训项目的开发，使其在现有软硬件基础上实现本专业实验室和实践基地的建设，为信息安全与管理专业实训实践提供有利的条件，能够保障本专业的实践教学质量，形成一定程度上的示范效应。另外，可由公安部主管的覆盖全国的第三方测评机构承接本专业学生的毕业实习，在全国范围内提供优良的实践实习条件和专业的实习实践指导。

网络空间安全学院根据多年的远程教育实践和摸索，联合信息安全等级保护关键技术国家工程实验室、华北电力大学信息安全工程实验室、北京市能源电力信息安全工程研究中心、中关村信息安全测评联盟等单位机构，以及信息安全教学实训平台等专业设施，为信息安全与管理专业构建了“网络虚拟实践、校内实践、校外实体实训”三者相结合的“三元一体”实践教学体系，充分利用先进信息技术满足现代开放远程教育线上线下数字化和实训实践教学的需要。

网络虚拟实践。主要是在远程开放教育模式下，构建以信息技术为支撑的网络虚拟实训平台实现线上线下实践教学。

校内实践。以办学单位校内现有的实验室、实训室及实训基地为基础，开展课程实训实践环节的线下教学。

校外实体实训。学院以信息安全等级保护关键技术国家工程实验室、华北电力大学信息安全重点实验室、北京市能源电力信息安全工程研究中心为基础实践基地，并与中关村信息安全测评联盟的独立第三方网络安全测评机构作为学院的实训实践基地。校外实训基地依托于分布在全国各地的等级保护测评机构，在全国三十多个省份配套有完善的实训设施、实训场景、实训教学老师，为开设本专业的学习中心和实践单位提供了覆盖全国的校企合作实训实践条件。

学生结合所学知识就近自主选择开展课程实训实践活动，在教学、科研、人才培养上能够发挥积极作用。推进产教融合、校企合作共同发展，为学院开设信息安全与管理本科专业提供了良好的实践教学环境。

（四）相关专业办学经验

国家开放大学网络空间安全学院于 2013 年成立，充分依托各方优势资源已将自身打造成为特色鲜明、资源优质、开放融通、体系完整、创新务实的行业技术应用型人才培养基地和创新实践教学平台，在学院软硬件保障、专业课程资源建设、创新实践平台、办学服务管理等方面均取得了一定的阶段性成果。

学院完成了信息安全技术应用专科的专业资源建设，在多年来的建设和教学过程中，不断积累了丰富的课程建设和教学管理经验，在学习资源优化，师资队伍培养，实训实践环境，教学服务提升，人才培养模式创新等方面，为信息安全与管理本科的筹备建设和教学实施打下了良好的基础。

（五）满足专业教学的图书资料和资源建设

随着网络安全法的施行，网络安全等级保护制度的广泛实施，不仅仅带动信息安全全产业链迅猛发展，随之用于信息安全与管理的教学和科研图书资料也逐渐增多且完善，比如信息安全管理类、信息安全技术、信息安全测试类，以及云计算、工业控制、物联网、大数据和移动互联网等安全方向的相关图书在各大图书市场和网络商城上种类繁多，均可参考借鉴满足信息安全与管理专业的教学需求。

公安部信息安全等级保护评估中心主编的网络安全等级保护系列教材。教材内容涵盖等级保护工作的全流程和全要素，相关内容可将等级保护测评师培训课程与信息安全与管理专业课程融通，开展学历证书和行业执业职格证书双证培养，实现学生专

业理论知识和实际工程技术应用能力的双提升。

网络空间安全学院已开设了信息安全技术应用专科专业，具有丰富的课程建设和教学管理经验，为信息安全与管理专业的开设奠定了良好的基础。学院将聘请信息安全领域的知名专家和“双师型”教师为本专业的主讲教师，组建包括科研院所、高等院校和行业企事业单位在内的教师团队进行资源建设，一定能够建设出优质的课程资源。

（六）广泛的就业渠道和广阔的就业前景

网络空间作为第五大疆域已纳入国家安全战略。近年来围绕信息安全的法律法规和制度标准密集出台，网络安全等级保护制度更是国家网络安全的基石，是维护国家安全、社会秩序和公共利益的根本保障。其范围覆盖全社会全行业，即各地区、各单位、各部门、各企业、各机构的信息系统；覆盖所有保护对象，包括网络、信息系统、信息，以及云平台、物联网、工控系统、大数据、移动互联等各类新技术应用。可以说，本专业的就业渠道涵盖各行各业的网络运营者，信息技术相关软、硬件产品及服务提供者，信息安全厂商和信息安全服务商等各级政企事业单位。

网络安全作为国家战略，对数字化发展起着至关重要的作用，与信息化项目“同步规划、同步建设、同步运行”，落实网络安全保护措施的“三同步”要求和信息化建设并行。由此可见，信息安全与管理专业人才的就业面向包括上游系统及产品的安全开发，筹建项目的规划设计，在建项目的建设测试整改，运行项目的管理测评运维，信息安全防护产品及服务以及废弃项目的评估销毁等信息化建设的全生命周期，前景非常广阔。

不仅仅是信息安全产业，在国家政策背景驱动下，我国各行各业的信息化建设和运行对信息安全与管理专业人才需求量都很大，特别是在各网络运营单位，信息安全厂商和信息安全服务商中从事信息安全技术和管理岗位的应用型人才缺口巨大。通过分析普通高校信息安全相近专业的人才培养目标，建议本专业主要对接的岗位包括安全测评、风险评估、安全咨询、安全管理、安全集成、安全运维、渗透测试等，行业领域相关岗位缺口可满足信息安全与管理专业学生的就业需求。

三、学院专业发展规划

（一）坚持立德树人根本任务

人是信息安全的根本保障，学院积极落实“立德树人”根本任务。一方面，建成

了学院思想政治课程教学团队，聘请著名高校马克思主义学院教授担任思政课程顾问和责任教师，由学院院长、副院长并聘请党政机关领导和党支部书记担任辅导教师，保障了学院思想政治课程教学方向和质量。另一方面，学院专业课程聘任的师资均是长期从事信息安全行业领域教学和科研的专家学者，并参与国家和行业政策法规标准的制定和宣贯，对国家信息安全战略、安全形势与政策、网络安全等级保护制度等均有深刻的理解，能够通过多种形式将课程思政元素融入教学过程之中，弘扬社会主义核心价值观。

同时，信息安全与管理专业是以国家网络安全等级保护制度为核心，课程涉及等保测评、工控安全、系统运维等相关岗位技能，具有天然的思政属性，能够在课程讲授中潜移默化体现出爱国教育、普法教育、育人教育和职业素质教育等思政元素。

（二）培养信息安全行业领域高素质技术和管理型人才

信息安全覆盖面广泛，行业研究方向众多，具有明显的科技密集型特点。根据信息安全行业产业的发展来看，信息安全人才的需求是多层次的，包括大量从事咨询、评估、管理、运行、维护、应急等高素质技术应用和安全管理人才。从行业从业人员调研来看，信息安全从业人员的岗位分布多集中技术和管理岗位，其中技术岗位占比接近 50%，管理和研究岗位各占比约 20%。学院开设信息安全与管理专业正是以国家网络安全战略为指导，网络安全等级保护制度为核心，以行业产业实际用人需求为导向，以为国家和社会培养从事安全技术服务和安全管理相关工作的高素质技术和管理应用型人才为培养目标。

（三）加强双师型师资队伍建设

师资队伍建设的总体目标为：加大师资培养规模和力度，持续引进行业领域知名专家，建成一支师德高尚、业务精湛、素质优良、结构合理的专业师资团队。师资队伍的教育教学水平、科研能力和职业素质达到本专业国内教育先进水平。力争 3 年内再培养 2 名专业带头人，专业带头人在国内信息安全领域具有较高知名度和影响力，师资团队双师型教师比例达到 80%以上。

（四）探索开放教育特色的人才培养模式

本专业在远程开放网络环境下，采用多种媒体和现代教育手段进行专业教学和人才培养。由高校、科研机构、行业企业的知名专家组成的专业建设指导委员会和专业教学团队，探索并实施“一二四 ”教学模式。即以教学一体化设计为主线，突出以学

生为主体的教学组织形式，突出信息技术与课程整合， 自学、导学、助学、促学，四学相连。强调让学生在教育实践活动中自主探索、小组协作、发展创新为特征的教学模式。学院充分认识到教学模式改革的重要性和必要性，将努力探索通过四个结合创新网上教学：一是学校与行业、企业相结合；二是线上线下相结合；三是学历和非学历相结合；四是教学方法与教学效果相结合。

四、人才需求预测

（一）体系内相关专业专科毕业生专本衔接的必然需求

国家开放大学信息安全技术应用专科专业于 2019 年开展招生和教学工作，现有本专科专业在校生近 2 万人。在网络安全行业领域人才需求明确以及缺口仍较大的背景下，学校与行业在人才政策、专业建设、素质培养等方面紧密合作，在保障办学质量的前提下，招生规模必将逐步提升，预计每年将输送近万名信息安全相关专业的专科毕业生。根据专科生入学情况调研信息来看，绝大多数报读信息安全技术应用专科专业的学生有进一步继续深造的意愿，且优先考虑报读本专业领域内的本科专业，专业衔接需求明显和意愿明确。

另一方面，国家开放大学每年输送各类专业专科毕业生上百万人，其中电子与信息大类相关专科专业毕业生约二十万人。随着网络安全人才培养战略被推上前所未有的高度，各项人才措施全面推进，得到了全社会的热烈响应，也必将为电子信息大类相关专业的专科毕业在就业提升和岗位需求等多方面提供专本衔接的途径，给予有从业志向和岗位提升等意愿的专科学生报读信息安全与管理本科专业的通道。

（二）网络安全等级保护评估/信息安全测评方向人才需求

《中华人民共和国网络安全法》明确国家实行网络安全等级保护制度，2019 年等保 2.0 相关国家标准颁布后，各企事业单位围绕等级保护对象加大安全合规相关的测评和评估工作，使得网络安全等级保护测评和安全评估相关岗位人员的需求增长迅速，并对评估师和测评师的学历标准、职业素质、技能水平、实践能力都提出了更高的要求。

为了更好地推广网络安全等级保护工作，国家在各省市设置了 200 多家网络安全等级保护测评第三方机构，随着设立机构的增加，网络安全等级保护测评机构的工作人员须参加等级保护测评师的培训和认证才能上岗。

同时，各企事业单位也加大了自身网络安全人员的等保评估能力培训，为适应需

求，公安部部署了一批社会培训机构参与对等级保护技术人员的培训，但仍然力量不够，需要高等教育与职业培训体系结合并举，系统性培养从业人员的综合素质和评估能力。

测评师方面： 目前我国经认证具备出具测评报告能力的网络安全等级保护测评机构在全国范围内分布在 31 个直辖市、省市、自治区，共计 200 多家。认证测评机构需要具备足够数量的测评师方可达到要求，每个测评机构需具备至少 8 个初级测评师、2 个中级测评师、1 个高级测评师。随着我国各行各业信息化程度的不断提高，我国等级保护测评机构的数量也在不断增加。

信息安全评估师方面：各企事业单位网络安全等级保护工作的工作流程：定级→备案→安全建设和整改→等级测评→安全监督检查。由工作流程可以看出，除了等级测评环节是需要等级保护测评机构人员直接参与，其他环节大部分是由企业内部人员开展的，所以国家推广等级保护工作的效果又取决于企业内部人员的技术水平和工作能力。保障企业内部网络安全等级保护工作仅仅针对测评单位的人员进行技术培训已经远远不能满足全国等级保护工作开展的需求，企业内部等级保护评估技术人员的教育培训更加重要，且需求数量更加巨大。 目前，企业内部从事网络安全岗位的人员大多数为非专业出身，基础素质和技能水平参差不齐，单一的职业认证培训无法达到既定的效果，需要为企业制定学历与非学历融合的新人才教育培训模式，通过学历素质教育结合职业技能培养，引入通用网络安全实训环境对企业内部工作人员进行场景式教学，在实践中巩固等级保护相关工作的方法和技能。

等保评估/信息安全测评方向主要就业方向：等保测评人员、信息安全评估人员、安全管理咨询、安全运维咨询、安全运维服务人员、安全管理评审人员、安全资质认证人员等。

（三）工业控制系统信息安全方向人才需求分析

随着我国两化融合和工业互联网的深入发展，工控安全已成为实施制造强国和网络强国战略的重要保障。近年来，随着中国制造全面推进，工业数字化、网络化、智能化加快发展，我国工控安全面临安全漏洞不断增多、安全威胁加速渗透、攻击手段复杂多样等新挑战。网络安全法明确落实企业主体责任，确保信息安全与信息化建设同步规划、同步建设、同步运行，在新时期两化深度融合发展的需求背景下，特别是等保 2.0 工业控制系统安全扩展要求发布后，使得各工业企业对工控安全人才需求猛

增，供需矛盾日益激烈。

而工控安全方向是集自动化、计算机、通信工程、电子信息、信息安全等于一体的交叉学科， 目前的现状却是师资匮乏、专业建设基础尚薄，学科体系缺乏标准，教学开展和实训环境没有依据，人才培养处于半真空状态。 目前，大量从事工控安全工作的人员，多为传统信息系统安全人员，对于工业控制系统安全缺乏足够的知识和技能。以信息安全关注程度高，工业控制系统应用比较普及的电力行业为例， 目前全国省级调度以上单位 39 家、地市级调度企业 431 家、大型发电集团 22 家、接入地调以上发电企业 6790 家、接入县调发电企业 29482 家；工控安全人员需求按照省级调度以上单位每家 20 人、地市级调度企业每家 30 人（220kV、110kV 变电站多数由地市调度管理）、大型发电集团每家 10 人、接入地调以上发电企业每家 5 人、接入县调发电企业每家 3 人计算，仅电力行业工控系统安全人员需求大约 13 万人；而目前电力行业十分缺乏专业的工控安全人员，人才缺口非常巨大。至于工业控制系统应用较大的石油化工、轨道运输、冶金、汽车、燃气、 自来水、 自动化生产企业等，工控安全人才需求量较电力行业更大，而人才缺失比例较电力行业更高。随着国家对工业控制安全的重视程度的加大，工控安全技术人员的需求将出现井喷式的增长。

工业控制系统安全主要就业方向：

国计民生关键基础设施（电网、电厂、石油石化、水务等相关行业）及生产制造、工业互联网：信息安全专责、工控安全专责，生产调度部门、科信部门、生产控制系统运维、运检部门、信息中心等相关安全岗位。

（四）信息安全运维方向人才需求分析

在确保信息安全与信息化建设同步规划、同步建设、同步运行的要求下，信息系统建设工作从大规模建设阶段逐步转型到“建设和维护 ”并举的发展阶段，信息系统安全运维工作已覆盖信息系统全生命周期 80%以上，信息安全运维体系的建设已经越来越被广大用户重视。企业开始重视运维安全的建设，需要更多的人才来维护网络安全，运维安全工程师也越来越被看重。与企业对安全运维人才需求相对应的是，我国 188 所高校设立了网络安全相关专业，而在注重培养信息安全运维实用型人才上几乎是空白，绝大多是安全运维从业人员是传统 IT 运维人员通过加强信息安全职业培训来提升技术能力。现今我国对网络安全人才的需求达 140 万，面向信息安全运维岗位的人员占比达 40%，生源数量和岗位能力还远不能满足社会需求。

据业内权威市场调查机构调研显示，目前国内企业对网络安全职位需求相对平均，但安全运维仍为最大的需求之一，特别是等保 2.0 基本要求明确了安全运维管理要求，各行业企事业单位自身和安全服务机构对信息安全运维岗位需求也将持续高速增长。

信息安全运维主要就业方向：网络运维、网络管理、信息安全专员、信息安全管理员、信息安全主管、安全运维主管、网络运维工程师、安全运维项目经理、安全运维驻场、网站安全运维等职位。

增设专业人才培养方案

包括培养目标、基本要求（素质要求、能力要求、知识结构要求）、修业年限、主干学科、主要课程、主要实践性教学环节和主要专业实验、教学计划等内容

一、专业名称、专业层次、专业所属学科门类或专业大类

专业名称：信息安全与管理

专业层次：本科（专科起点）

学科门类：电子与信息大类计算机类

二、入学要求

具有国民教育系列相同或相近专业高等专科（含专科）及以上学历者。

三、培养目标

本专业坚持立德树人的教育思想，培养德智体美劳全面发展的社会主义事业的建设者和接班人。以国家对网络空间安全学科建设及人才培养相关政策为基础，培养适应信息安全行业领域产业发展需要的，具有较高的文化水平、良好的职业道德、扎实的信息安全技能和安全管理能力，能够从事网络安全等级保护测评，风险评估，工控系统及信息系统安全咨询、安全管理、安全集成、运维整改等安全技术服务和管理工作的高素质技术和管理型人才。

四、培养规格

（一）修业年限：最低修业年限 2.5 年，学生学籍自注册入学起八年内有效。

（二）学习形式：开放教育

（三）总学时学分：1296 学时，72 学分

（四）人才培养知识、能力和素质要求

1．素质要求：

1）思想政治素质：：爱党爱国，拥有公序良俗认可的正确世界观、人生观、价值观，能够把爱国情、强国志、报国行自觉融入坚持和发展中国特色社会主义事业、建设社会主义现代化强国、实现中华民族伟大复兴的奋斗之中，争做社会主义合格建设者和可靠接班人。

2）文化素质：崇尚宪法，遵守法纪，诚信友善，尊重生命，乐观向上，珍视劳动，热爱生活与艺术，具有社会参与意识和关怀社会的责任感，具备良好的公民素质。

3）信息素养：具备信息搜集、判断、整合和应用能力，能够在工作、学习、生活中运用现代信息技术获取相关信息。

4）职业素质：具有良好的职业道德，具有创新意识和质量意识，具有团队精神，具有规范化的代码编写习惯，能够在工作中综合考虑环境、法律、安全等制约因素。

5）身心素质：具有良好的身体素质和心理素质。

2. 知识要求：

1）通用基础知识：掌握工作、学习、生活需要的通用的计算机、英语、应用写作、人文社会科学等知识。

2）专业知识：

熟悉从事本专业相关工作所需的计算机信息系统及工业控制系统的基础知识、技术路线和应用场景；

较扎实地掌握本专业的基础知识和基本理论，初步掌握信息安全保护技术的基本方法和技能；

理解并熟悉我国颁布的信息安全法律、法规和标准，具备较扎实地信息安全合规性管理知识；

熟悉我国网络安全等级保护相关的政策法规标准，较扎实地掌握我国网络安全等级保护相关政策法规标准，掌握典型等级保护测评工具的使用方法；

熟悉工业控制系统的基本知识和工作原理，初步掌握工控系统安全防护的基本方法和通用技术；

熟悉信息安全产品的分类、功能、特点和应用场景；

熟悉通用信息系统安全运维体系与实施流程，初步掌握日常安全运维和应急响应各步骤工作的内容和要求。

3. 能力要求：

1）学习能力：具有终身学习意识，能够获取并学习新技术、新知识，持续提高自己的综合能力。

2）分析、解决问题能力：能够综合运用所掌握的理论知识、分析方法和应用技术解决信息安全实际问题的能力。

3）人际协作能力：具有一定的组织协调能力、团队协作能力、沟通能力和人际交往能力。

4）创新能力：具有创新意识，具有一定的创造性思维能力和创新实验能力。2)熟悉从事本专业相关工作所需的计算机信息系统及工业控制系统的基础知识、技术路线和应用场景，有能力将其运用到实际工作中。

5)专业能力：具有较强的安全防护实践和安全管理组织能力；具备遵照网络安全等级保护相关要求开展自评估和测评工作的基本能力，能够合理设计测试用例获取测评和评估数据；基本具备主流信息安全产品在信息系统和工业控制系统中的部署和配置方法；具备开展安全运维和应急响应的基本方法和能力。

五、课程体系

（一）课程模块设置

本专业共设置 5 大模块 9 个子模块，主要包括公共基础课模块（思想政治课、公共英语课、公共基础课程）、专业课模块（专业基础课、专业核心课、专业拓展课）、通识课模块、综合实践模块、补修课模块。

（二）课程设置

1. 公共基础课模块

1）思想政治课

该模块最低毕业学分为 10 学分，模块最低总部考试学分为 8 学分，模块最低设置学分为 10 学分。

必修课：习近平新时代中国特色社会主义思想、马克思主义基本原理、中国近现代史纲要、形势与政策。

2）公共英语课

该模块最低毕业学分为 6 学分，模块最低总部考试学分为 6 学分，模块最低设置学分为 12 学分。

3）公共基础课

该模块最低毕业学分为 5 学分，模块最低总部考试学分为 5 学分，模块最低设置学分为 9 学分。

必修课：国家开放大学学习指南、计算机应用基础。

2. 专业课模块

1）专业基础课

该模块最低毕业学分为 11 学分，模块最低总部考试学分为 11 学分，模块最低设置学分为 26 学分。

必修课：信息安全导论、密码学基础、信息安全技术基础。

2）专业核心课

该模块最低毕业学分为 16 学分，模块最低总部考试学分为 16 学分，模块最低设置学分为 30 学分。

必修课：网络安全法规与管理、网络安全等级保护、信息系统安全运维、工控系统网络安全。

3）专业拓展课

该模块最低毕业学分为 4 学分，模块最低总部考试学分为 0 学分，模块最低设置学分为 10 学分。

3. 通识课模块

该模块最低毕业学分为 2 学分，模块最低总部考试学分为 0 学分。

国家开放大学设置统一的通识课程平台所有专业适用此平台的课程；通识课设置及通识教育是国家开放大学人才培养的特色之一，是实施素质教育的具体措施，通识课模块课程原则上不得免修免考；已取得国家开放大学毕业证书的学生，若再次注册学习国家开放大学相关专业，原修专业已注册过的通识课程，在新修专业中不得再次注册学习（在教务管理系统中此类课程将不能实现注册）和申请办理课程免修免考，此模块的毕业最低学分通过修读本模块的其他通识课程获得。

4. 综合实践

该模块最低毕业学分为 16 学分，模块最低总部考试学分为 0 学分，模块最低设置学分为 16 学分。

综合实践课包括网络安全等级保护测评，毕业设计（信息安全与管理本）共 14 学分，由网络空间安全学院根据国家开放大学制订的实践环节教学大纲组织实施。该环节原则上不得免修。

5. 补修课模块

补修课是对于在注册试点本科（专科起点）专业学习中，部分不具备该专业专科学历或不具备学习该专业相关基础知识的学生的必须补修的课程。补修课程学分是按

规定需要补修的学生必修的学分和毕业审核的必要条件。补修课程统一使用国家开放大学确定的课程名称，执行统一的教学大纲或教学要求，并由国家开放大学推荐教材、提供相关教学支持服务，并计入毕业总学分。本专业需补修的课程是：计算机导论#、工控系统概论#，共 8 学分。

（三）课程说明（部分）

1. 形势与政策

本课程 2 学分，共 36 学时，在校学习期间开课不断线。

《形势与政策》是国家开放大学面向本专科各专业学生开设的一门思想政治理论必修课程。通过本课程的学习，学生学会运用马克思主义的形势观和政策理论，科学地分析国内外形势，正确地理解党的现行政策， 自觉地拥护党的基本路线，维护社会主义制度，学习世界政治经济与国际关系基本知识，增强实现改革开放和社会主义现代化建设宏伟目标的信心和社会责任感。

本课程的主要内容包括：党和国家重大的理论政策、社会主义现代化建设的形势、国际形势与国际关系、各省经济社会发展形势与特点、安全教育等内容。

思想政治理论课实践教学的标准要求，由总部征求各方意见后制定，各分部和学院按照总部要求组织开展。

2. 国家开放大学学习指南

本课程 1 学分，课内 18 学时，开设时长为一学期。

课程性质及主要内容：本课程是国家开放大学各专业开设的一门必修课。课程内容包括国家开放大学历史、办学模式、学习方式的简介；专业内容和学习过程的说明；课程学习资源、课程考试、学习网和学生空间的介绍；网上学习操作技能和上网工具的简要培训以及对学生事务服务、学生活动及奖励的说明。

学习目标：学生通过本课程的学习，能够了解国家开放大学的概况、历史，熟悉专业、课程设置情况和学习环境，熟悉与远程学习模式相适应的学习方法，学会运用现代信息技术进行网络学习和交流，如收发邮件、使用国家开放大学学习网和学生空间等，知道学校学生相关事务的管理规定、参与学生活动的方式以及获得奖励的相关要求。

3.计算机应用基础

本课程 4 学分，课内 72 学时，开设时长为一学期。

本课程是国家开放大学本科各专业必修的基础课。通过本课程的学习，学生应能够掌握计算机的基础知识、基本概念、基本操作技能，学会使用微机进行日常办公事物处理，掌握网络基本使用方法，了解现代信息技术，为使用计算机和进一步学习计算机有关知识打下基础。

课程的主要内容：计算机基础知识（含计算机系统组成、信息编码、微机硬件及配置和多媒体技术与应用）；微机操作系统及其应用；计算机网络基础；文字处理系统；电子表格系统；电子演示文稿系统；信息安全与网络道德等。

4.信息安全导论

本课程 4 学分，课内 72 学时，开设时长为一学期。

本课程是信息安全与管理本科专业的专业基础课。本课程将“立德树人”贯穿于课程教学全过程，注重加强爱国教育、普法教育和育人教育，内容设计全面。通过本课程的学习，学生应能够掌握信息安全的发展历程和重要意义，及相关基础知识和基本概念，熟悉系统安全、网络安全、内容安全和安全管理等不同层面的安全内容及方法，学会从信息安全角度理解和分析信息系统面临的安全风险和防护策略，重点做到理论与实际相结合为进一步后续专业课程知识打下基础。

课程的主要内容：信息安全概述、物理安全、身份认证、访问控制、可信计算、网络威胁、网络防御、网络安全协议、内容安全、信息安全管理等。

5.密码学基础

本课程 3 学分，课内 54 学时，开设时长为一学期。

本课程是信息安全与管理本科专业的专业基础课。本课程充分融入普法教育和育人教育等元素，强调国产密码的标准和应用，通过本课程的学习，学生应能够熟悉密码学的基本原理、基础知识和密码体制分类，了解主流密码算法和国产密码算法，掌握加解密、数字签名和密钥管理方面的应用技能，学会从实际出发初步掌握证书管理、认证技术和防伪识别中的基本应用。

课程的主要内容：密码学概述、对称密码体制、公钥密码体制、哈希函数及消息认证、密钥管理、国产密码算法体系及标准、密码工程应用等。

6.信息安全技术基础

本课程 4 学分，课内 72 学时，开设时长为一学期。

本课程是信息安全与管理本科专业的专业基础必修课。本课程充分融入育人教育

和职业素质教育等元素，通过本课程的学习，学生应能够熟悉计算机网络基础理论知识、体系结构和 OSI 与 TCP/IP 参考模型，掌握计算机网络的应用方法和技能。熟悉信息安全相关理论知识，理解信息安全保障体系中有关防御保障、安全工程和技术对策的内容，初步掌握常用网络服务的安全问题以及安全协议和攻防手段。通过了解数据库的基本概念和体系结构熟悉数据库的安全措施和管理方法，初步掌握防火墙和入侵检测的技术原理、设计机制和基本使用方法。

课程的主要内容：计算机网络基础、体系结构、OSI 与 TCP/IP 参考模型、信息安全保障体系，安全体系机构、常用网络服务安全问题和攻击手段，数据库系统与安全，网络安全协议，防火墙及入侵检测、安全通信等。

7.C 语言程序设计

本课程 4 学分，课内 72 学时，开设时长为一学期。

本课程是信息安全与管理本科专业的专业基础选修课。通过此课程的学习，培养学生的程序设计能力、初步的算法设计能力和代码实现能力。

本课程的主要内容：程序设计的基本概念、基本数据类型的应用、程序设计的基本控制结构、函数模块的编写、构造类型数据的应用、地址的应用、算法设计及其实现、文件的应用等。

8. 网络安全法规与管理

本课程 4 学分，课内 72 学时，开设时长为一学期。

本课程是信息安全与管理本科专业的专业必修课。本课程将“立德树人”贯穿于课程教学全过程，着力培养学生的爱国爱党精神、奋斗精神和奉献精神，对我国在网络安全领域出台的重要法规和制度给予特别关注，强化普法教育和育人教育。通过本课程的学习，学生应能够熟悉我国颁布的信息安全有关法律，关键信息基础设施安全保护条例，网络安全等级保护制度有关标准，以及信息安全管理体系等法规和管理内容。

课程的主要内容：网络安全法、数据安全法，关键信息基础设施安全保护条例，网络安全等级保护主要标准、信息安全管理体系等。

9.网络安全等级保护

本课程 4 学分，课内 72 学时，开设时长为一学期。

本课程是信息安全与管理本科专业的专业必修课。本课程以网络安全等级保护制

度为基础，强调网络安全保障的重要性，体现爱国教育、育人教育和职业素质教育，将“立德树人”贯穿于课程教学全过程。通过本课程的学习，学生应能够对我国网络安全等级保护制度相关标准中基本要求有较系统性的理解，初步掌握安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心五个分类的安全范畴和控制点指标；初步掌握安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理五个分类的安全范畴和控制点指标，能够按照基本要求中的常用控制点实施初步测评，获取测评数据并判断合规性。

课程的主要内容：网络安全等级保护基本要求解读，安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心相关控制点及基本要求；安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理相关控制点及基本要求等。

10.信息系统安全运维

本课程 4 学分，课内 72 学时，开设时长为一学期。

本课程是信息安全与管理本科专业的专业必修课。本课程将思政和创新职业素养、人文素养融入课程教学，通过本课程的学习，学生应能够对信息系统安全运维服务有系统性的认识，熟悉安全运维的特点、模型、对象和合规性要求，对建立安全运维体系有初步了解，掌握分析运维安全需求和制定策略的方法，能够制定基本的运维实施方案并进行过程有效性评估。

课程的主要内容：安全运维概述，安全运维模型和模式，安全运维体系，合规要求，安全策略，运维准备，运维实施，运维安全评估和监控，评审和改进等。

11.工控系统网络安全

本课程 4 学分，课内 72 学时，开设时长为一学期。

本课程是信息安全与管理本科专业的专业必修课。本课程以国际、国内工业控制系统网络安全事件为切入点，强调工控系统安全防护的重要性，体现爱国教育、育人教育和职业素质教育。通过本课程的学习，学生应能够熟悉工控系统网络安全防护的基础理论知识，熟悉网络安全等级保护制度相关标准基本要求中针对工业控制系统的扩展要求，初步掌握工控系统安全防护技术，了解工控安全防护体系和产品，为形成工控系统安全系统思维和工程能力打下坚实基础。

课程主要内容：工控安全概述，工控安全威胁与风险，工控安全风险评估，工控

安全防护技术与方法，工控安全产品及应用，工业互联网安全。

12.信创技术与应用

本课程 4 学分，课内 72 学时，开设时长为一学期。

本课程是信息安全与管理本科专业的专业拓展课。强调爱国教育、育人教育和职业素质教育，重点介绍我国安全可控信创产业的发展和应用。通过本课程的学习，学生应能够理解自主可信计算原理、技术体系及规范，熟悉自主可信计算的典型应用；了解安全可控信息系统的重要意义、技术体系及应用；熟悉新型信息基础设施的建设及运行；初步掌握典型信创产品的安全机制和应用场景。

课程的主要内容： 自主可信计算、安全可控信息系统、新型信息基础设施、典型信创产品应用等。

13.网络安全等级保护实践

本课程 6 学分，课内学时 108 学时，开设时长为一学期。

本课程是信息安全与管理本科专业的综合实践课。通过网络安全等级保护实训实践着重强调爱国教育、育人教育和职业素质教育。通过本课程的学习，学生应能够熟悉网络安全等级保护制度相关标准中的测评要求和测评过程指南，掌握网络安全等级保护的安全测评通用要求和新技术新应用扩展要求，能够按照等保测评工作要求和流程对第二、三级等保对象开展并实施初步测评活动。

课程主要内容：等级测评概述，安全测评通用要求，安全测评扩展要求，测评准备活动，测评方案编制，现场测评活动，测评报告编制，测评活动实践。

14.计算机导论#

本课程 4 学分，课内 72 学时，开设时长为一学期。

本课程是学习计算机专业知识的入门课程。

通过本课程的学习，引导学生认识以计算机为核心的信息技术在现代社会和现代文化中的地位和作用，提高学生的信息素养。课程主要围绕计算机的基本概念和知识展开，通过学习使学生掌握计算机系统的基本软硬件知识，具备软件与硬件的基本安装、使用能力，具备基本的信息采集和运用组织能力，为专业的深入学习奠定必要的信息素养基础。

本课程主要内容：计算机系统基础；操作系统与应用软件；多媒体技术及其应用基础； 计算机网络技术及其应用；数据管理技术基础；软件开发技术；信息的收集、

处理、表现的基本方法等内容。在课程的实训中则针对微机系统的组成与安装；操作系统使用；网络与多媒体技术以及网络资源的获取和组织处理进行一定的实验和演示，加强理论与实践的结合。

15.工控系统概论#

本课程 4 学分，课内 72 学时，开设时长为一学期。

本课程是学习工业控制系统的入门课程。本课程以我国工控系统发展历史和现状为实例，强调工控系统国产化对我国网络安全的重要性，以爱国教育、育人教育和职业素质教育着力点贯穿教学全过程。课程要求熟练掌握工业控制技术的原理和基本概念，了解工业控制系统的发展历程，了解工业控制系统的应用情况，掌握工业控制系统的架构及工作原理，熟练掌握主流工业控制系统的应用案例，熟练掌握工业控制系统的基本操作。

通过学习，使学生了解工业控制系统的基本设计流程和要点，并熟悉掌握 PLC、上位机软件的选择和使用。该课程使学生学会阅读并理解现场总线协议/规范，能够设计一般设备的现场总线通信接口，掌握典型现场总线系统的基本应用技术，并为学生进行现场总线系统设计和现场总线分析奠定一定的基础。了解工控系统面临的安全威胁和存在的安全风险。

（四）课程考核方式

本专业课程考核一般包括形成性考核和终结性考试。课程考核的内容必须符合教学大纲，以基本理论、基本知识和基本技能考核为主，同时注意考核学生综合运用所学理论、知识和技能，分析解决问题的能力。本专业总部考试课程的考核形式为形成性考核和终结性考试，形成性考核占课程综合成绩的 50%，终结性考试占课程综合成绩的 50%。课程考核成绩统一采用百分制，即形成性考核、终结性考试、课程综合成绩均采用百分制。课程综合成绩达到 60 分及以上（及格），可获得本课程相应学分。

本专业课程的考核方式以每门课程的考核说明为主要依据。

六、毕业规则与学位规则

（一）毕业规则

本专业最低毕业总学分为 72 学分，各模块最低毕业学分为：思想政治课 10 学分；公共英语课 6 学分；公共基础课 5 学分；专业基础课 11 学分；专业核心课 16 学分；通识课 2 学分；专业拓展课 4 学分；综合实践 16 学分；补修课 8 学分。

各模块最低总部考试学分之和为 46 学分。

（二）学位规则

按照学校学位授予相关规定执行。

七、教学计划进程表

电子与信息大类计算机类
信息安全与管理（专升本）专业教学计划进程表

专业名称				信息安全与管理					规则号			
学生类型				开放					专业层次		本科（专科起点）	
毕业学分				72					总部考试学分		46	
主模块名	模块名	模块毕业最低学分	模块最低总部考试学分	模块最低设置学分	序号	课程代码	课程名称	学分	课程类型	课程性质	建议开设学期	考试单位
公共基础课模块	思想政治课	10	8	10	1	5014	马克思主义基本原理	3	统设	必修	2	总部
					2	4391	习近平新时代中国特色社会主义思想	2	统设	必修	1	总部
					3	4681	中国近现代史纲要	3	统设	必修	1	总部
					4	4392	形势与政策	2	统设	必修	1-5	分部
	公共英语课	6	6	12	5	4007	理工英语 3	3	统设	选修	1	总部
					6	4008	理工英语 4	3	统设	选修	1	总部
					7	4019	管理英语 3	3	统设	选修	1	总部
					8	4020	管理英语 4	3	统设	选修	1	总部
	公共基础课	5	5	9	9	2970	国家开放大学学习指南	1	统设	必修	1	总部
					10	815	计算机应用基础	4	统设	必修	1	总部
					11	4848	人工智能专题	2	统设	选修	2	总

												部
					12	2155	大学语文	2	统设	选修	2	分部
					13	1803	应用写作（汉语）	4	统设	选修	2	分部
	专业课模块	专业基础课	11	11	26	14	新建	信息安全导论	4	统设	必修	2	总部
						15	新建	密码学基础	3	统设	必修	2	总部
						16	新建	信息安全技术基础	4	统设	必修	3	总部
						17	3595	C 语言程序设计	4	统设	选修	2	分部
						18	1692	管理信息系统	4	统设	选修	3	分部
						19	3164	JavaScript 程序设计	4	统设	选修	3	分部
						20	新建	信息安全产品应用	4	非统设	选修	3	分部
		专业核心课	16	16	30	21	新建	网络安全法规与管理	4	统设	必修	3	总部
						22	新建	网络安全等级保护	4	统设	必修	3	总部
						23	新建	信息系统安全运维	4	统设	必修	3	总部
						24	新建	工控系统网络安全	4	统设	必修	4	总部
						25	1250	软件工程	4	统设	选修	3	分部
						26	4406	Web 开发基础	4	统设	选修	2	分部
						27	4691	Python 程序设计	4	统设	选修	4	分部
						28	2154	数据库应用技术	4	统设	选修	4	分部
						29	4410	移动开发导论	4	统设	选修	2	分部
						30	4399	大数据分析与挖掘技术	4	统设	选修	4	分部
						31	52709	云计算及应用	3	非统设	选修	4	分部
						32	新建	能源行业网络安全应用	4	非统设	选修	4	分部

					33	新建	金融行业网络安全应用	4	非统设	选修	4	分部
					34	新建	交通行业网络安全应用	4	非统设	选修	4	分部
					35	52860	操作系统运维管理	5	非统设	选修	4	分部
					36	52293	网络工程与组网技术	4	非统设	选修	4	分部
	专业拓展课	4	0	10	37	新建	信创技术与应用	4	统设	选修	4	分部
					38	51203	计算机网络安全技术	3	非统设	选修	3	分部
					39	53157	分布式系统	4	非统设	选修	3	分部
					40	51386	网络规划与设计	4	非统设	选修	4	分部
					41	51383	网络通信技术	4	非统设	选修	5	分部
	通识课	2	0	14	42	具体详见国家开放大学通识课列表及要求						
	综合实践	16	0	16	43	新建	网络安全等级保护实践	6	统设	必修	4	分部
					44	新建	毕业设计（信息安全与管理本）	10	统设	必修	5	分部

信息安全与管理专业（专升本）补修课程

序号	模块名	课程 ID	课程名称	学分
1	补修	768	计算机导论#	4
2	补修	4553	工控系统概论#	4

八、支持服务能力

（一）师资队伍

本专业建设团队共有 23 人，其中高级以上职称 22 人，硕士以上学位 18 人，均具有丰富的教学经验和专业技术资格，是本行业领域的双师型教师队伍，现有 22 名高级及以上职称的教师正在从事网络安全行业领域专业相关教学和学科研究。国家开放大学经过多年的发展，办学体系计算机相关专业专兼职教师总数千余人，在教学改革、教学研究与学科研究上取得了丰硕的成果，能够满足教学需要。

本专业必修课程都组建了课程教学团队,负责课程建设、课程教学与课程学习支持服务。按照学校规定，必修课程在课程建设过程中的教学大纲、多种媒体资源、课程考核等重要环节均需经过学科专家严格审定才可使用。开设本专业的分部、学院需每门课程配置一名责任教师，各学习中心按照学生选课数量配置一定数量的辅导教师和实践教师，为学生提供学习支持服务。

（二）教学资源

本专业为学生提供较为丰富的专业学习资源。为适应远程开放教育学习，本专业的思想政治课、公共基础课、公共英语课模块中的统设必修课程都有网络课程，专业基础课、专业核心课、综合实践课模块中的统设必修课程在课程开设学期前完成网络课程等教学资源。教学资源主要有网络课程、文字教材、视频教材、试题库、实验指导等。为适应移动学习需要，还配有课程讲义和辅助学习资料等数字教材。通过引入或开发网络安全行业领优质证书资源，借助职业教育国家学分银行，进一步加强本专业学历教育课程与网络安全专业认证的衔接性。

（三）设施设备

设施设备主要包括与培养规模和培养形式相适应的本专业日常教学所需的网络学习平台、标准教室、校内实训室、校外实习实训基地、图书资料等。

1．网络学习平台：具备支撑国家开放大学“一路一网一平台”顺利运行的软硬件条件。网络学习平台能够支持网上学习、作业、测试、考试、辅导答疑、毕业设计等功能，满足教学互动、协作学习等需要。网络学习平台还可以记录学生网上学习过程和学习行为，提供教学管理数据。

2．标准教室：专业教室配备黑（白）板、多媒体计算机、投影设备、音响设备、互联网，并实施信息安全防护措施；安装有应急照明装置并保持良好状态，符合紧急疏散要求，标志明显，保持逃生通道无阻。

3．校内实训室：配置有网上虚拟实训平台、计算机实训室、工控实训室等，用于信息安全类和工控安全类课程的教学与实训。

4．校外实习实训室：具有与学生规模相适应的稳定校外实训基地，能够提供本专业的相关实习岗位并定期接纳学生实习，配备有相应数量的指导教师对学生进行指导。

5. 图书资料：国家开放大学总部、分部、学院和有条件的学习中心都建有图书馆和数字图书馆，可以实现馆际借阅。专业建设单位提供了专业拓展学习平台数字资源、

包括视频课程、案例库、文献资料库等适合开放远程教学和多终端学习需要的数字化教学图书资料。

九、主要教学环节

1.入学教育

新生入学认真组织好入学教育，切实上好“国家开放大学学习指南”课，使学习者对远程教育的教学特点和学习要求与方式、本专业的课程设置和课程的实施与组织、综合实践教学的要求、学习支持服务等有基本的了解，同时应培养学习者应用计算机的能力，利用网络获得信息和学习支持服务的能力。

2.制定学习计划

本专业的课程有一定先后接续性，据此指导学生按教学计划中的课程进度表选课。编制学生学习计划手册，列出本专业开设的所有课程的名称、学分等信息。

3.网络教学

国家开放大学统设必修课的网络课程中包含教学要求、教学内容、 自测练习、作业提交、交流互动等课程资源，每学期开学前会统一部署到国开网络学习平台上，为广大师生提供一个在线交流、自主学习与个性化学习的环境，引导学生利用网络学习，积极参加网上教学活动。新开课程、滚动课程每学期网上有相应的教学和教研活动，期末时有相应的辅导。

4.面授辅导

各学习中心的专职或兼职辅导教师，选择学员方便的时间安排线上和线下集中讲解、答疑。集中面授辅导除针对课程的重点、难点进行适量讲解和答疑以外，也为学员提供实际操作技能训练的机会和指导。提倡辅导教师采用案例、任务驱动教学方式进行辅导以及实验，引导学生发现问题，培养学生分析和解决问题的能力，面授辅导不提倡系统讲授，应指导学生使用录像教材，共享优质教育资源。

5.实践教学

信息安全与管理专业实践教学是培养本专业毕业生具备实践能力的基础性环节，切实通过实践教学课程体系来培养提高学生的实践能力。本专业实践教学从学习者职业背景出发，按照学习者从业实际工作、校内实训室设施和校外实践基地等条件设置不同的实践教学环节，按照专业培养目标和规格制定实训实践评估标准，通过实验室实践、网络实践和工作实践等方式，丰富实践评估的方式和手段。

本专业实践教学由课程实践和综合实践组成。

（1）课程实践

课程实践与知识体系对应，按照专业教学的要求，每门信息安全与管理专业的主干课程都设置一定学时的课程实践内容，这些课程都要求学生提交实践成果作为课程形成性考核的组成部分。

（2）综合实践

学生均需参加教学计划中规定的综合实践模块。本专业综合实践模块设置有具体实践方式方法及实践考核标准，由各办学单位结合开放教育办学特点和实际实训实践条件组织实施。完成综合实践模块的成绩合格者可取得相应学分。未取得实践环节的学分者不得毕业。

6.学习支持服务

每门课程建立由主编主讲、主持教师、责任教师、辅导教师和班主任等组成的教学支持服务团队，为学生提供全程学习支持服务。主持教师、责任教师、辅导教师在开课前、开课中、课程结束时通过网上教学平台、电子邮箱、电话、QQ、微信等远程交互工具跟踪学生学习的全过程，辅导教师担任课程学习辅导、解答学习中遇到的问题，班主任组织学生上网学习、检查学习情况。每门课程提供课程教学大纲、课程教学设计方案、课程教学实施细则等教学文件；提供多种媒体教材（印刷教材、录像教材、多媒体课件和网络课程等）；通过面授或网络，指导学生掌握课程学习方法，介绍课程教学安排、学习方式、学习要求、考核方式等。通过网上教学、面授教学，组织学生进行个别学习、协作学习、集中学习，对学生学习过程进行指导；通过面授课考勤、网上学习行为监控、形成性考核等方式监督和促进学生学习。提供课程期末辅导的学习资源和专项辅导，指导学生顺利通过期末考试。

7.考核

（1）形成性考核

本专业每门课程均安排形成性考核，主要组成形式有自测、实验实训、小论文、小组活动等，成绩可占总成绩的 50%，具体参考各门课程考核说明的具体要求。未完成形成性考核者，不能参加终结性考试。

统设必修课的形成性考核由国家开放大学统一安排，其他课程的作业由学院责任教师安排，可以通过网络或辅导教师等渠道加以布置。由各学习中心落实本地区的形

成性考核工作，并组织作业批改。

（2）终结性考试

终结性考试针对课程特点有纸质考试、网络考试等形式，具体安排请参考各门课程的考核说明。根据成人学习的学习特点，积极探索过程性评价、表现性评价、社会性评价等课程多元评价模式与机制。

学院负责考试管理、巡考、阅卷、登分等考试组织与实施工作，并向国家开放大学报送有关考试数据及每学期的考试情况和成绩分析。

十、质量保障

（一）保证专业教学的组织与运行要求

1.课程建设

1）课程体系建设思路清晰，规划合理，措施得力，成效显著。课程设置科学合理，与专业培养目标一致。

2）课程教学基本文件齐全，符合远程教育教学特点，并方便师生查阅。

3）根据课程教学需要开发教材和多种媒体课程教学资源，专业课程均有适合开放远程教学和多终端学习需要的多种数字化教学资源（网络课程、课件、案例库、题库、教材、文献资料库等），满足学生多样化学习需求，并在一定程度向社会共享开放。

4）重视与行业企业共同建设与技能提升紧密衔接的专业课程，优化知识结构，不断更新课程内容，促进本科人才培养。

2.课程教学

1）学习资源于开课前两周到位，开课前完成各项教学准备工作。

2）入学教育、专业教育、课程教学、毕业教育组织有序，教学过程落实到位，注重信息技术与教育教学相结合，满足混合式教学要求，教学效果较好。

3）实现多种教学环境下的师生互动、生生互动、倡导讨论式、案例式、参与式教学，创新多样化、交互式、翻转式、全程式在线学习模式。

3.实践教学

1）实践教学管理规范，有明确的目标和内容，环节设置合理，时间有保证，实验开出率不低于 90%，能够达到培养方案的要求。

2）按规定配备实践教学指导教师，学生实践报告齐全，教师对实践教学有总结。

3）毕业设计：指导及管理文件和规章制度完备，有较为完备的工作方案，选题符

合专业对学生综合训练的要求。

4）指导教师具有相应的任职资格，指导教师与学生比例适当，每名专任教师指导学生人数为不超过 15 人，每名兼职教师指导学生人数不超过 10 人。答辩主持人具有高等学校教师资格，经培训合格后持证上岗。

5）毕业设计的选题、指导、答辩和评价等过程管理严格、规范。

4.学习支持服务

1）专业和课程有完整的开展学生学习支持服务的设计方案，符合专业与课程特点。

2）必修课程均配有网络教学团队，团队能够积极开展导学、助学、促学、督学，提供各类学习过程的支持服务。

3）每门课程均能够通过网络、电话、邮件、移动终端等多种形式为学生提供辅导答疑。

4）每门课程都能通过文本、双向视频或单项视频的形式组织在线实时教学活动。

（二）专业建设与持续改进机制要求

建立毕业生跟踪反馈机制，及时掌握毕业生满意度和用人单位对毕业生的满意度，以及毕业生和用人单位对培养目标、课程体系、课程教学的意见和建议。采用科学的方法对毕业生跟踪反馈信息进行统计分析，并形成分析报告，作为质量改进的主要依据。

建立有信息安全行业企业专家有效参与的人才培养方案定期修订制度，从国家经济社会发展需求出发，适时更新专业人才培养目标、课程体系、教学要求，保证培养的人才对社会需求的适应性。

（三）教学质量监控机制要求

建立质量监控机制，使主要教学环节（包括培养方案制定、课程建设、课程教学、实践教学、学习支持服务）的实施过程处于有效监控状态。

建立对主要教学环节的定期评价制度，采用大数据分析与预警、教学检查、教学督导、年报年检、专项调查等形式落地实施。

增设专业专任教师情况

序号	姓名	性别	年龄	专业技术职务	最后学历毕业学校、专业、学位	现从事专业	拟任课程	是否“双师型”	专职/兼职
1	王英彬	男	67	教授	华北电力大学、计算机、学士	信息安全	信息安全导论	是	专职
2	周庆根	男	60	高工	华北电力大学、计算机、学士	工控安全	工控系统网络安全	是	专职
3	吴秋新	男	54	教授	北京邮电大学、信号与信息处理、博士	密码学	密码学基础	是	兼职
4	闫怀志	男	46	副教授	北京理工大学、机械电子工程、博士	信息安全	信息安全技术基础	是	兼职
5	秦宇	男	42	高工	中国科学院研究生院、信息安全、博士	信息安全	工控系统网络安全	是	兼职
6	吕春利	男	43	副教授	中国科学院研究生院、信息安全、博士	信息安全	信息系统安全运维	是	兼职
7	李涵	女	44	副教授	济南大学、控制理论与控制工程、硕士	信息安全	操作系统及安全	是	兼职
8	马力	男	58	副研究员	北京航空航天大学、系统工程与管理、硕士	信息安全	网络安全等级保护	是	兼职

9	任卫红	女	58	研究员	北京师范大学、固体物理专业、硕士	信息安全	网络安全法规与管理	是	兼职
10	李升	男	46	副研究员	中国矿业大学、电力系统及其自动化、硕士	信息安全	网络安全等级保护实践	是	兼职
11	曲洁	女	43	副研究员	内蒙古工业大学、材料加工工程、硕士	信息安全	网络安全等级保护	是	兼职
12	袁静	女	44	副研究员	中国地质大学、计算机应用技术、硕士	信息安全	网络安全法规与管理	是	兼职
13	于东升	男	46	副研究员	北京理工大学、计算机技术与应用、硕士	信息安全	信创技术与应用	是	兼职
14	张振峰	男	39	副研究员	哈尔滨工业大学、计算机科学与技术、本科	信息安全	操作系统及安全	是	兼职
15	陈广勇	男	40	副研究员	北京大学软件学院、计算机技术与应用、硕士	信息安全	信息安全导论	是	兼职
16	陶源	男	40	副研究员	北京科技大学、控制理论与控制工程 、博士	信息安全	网络安全等级保护	是	兼职

17	李明	男	46	研究员	上海交通大学、计算机应用技术、博士	信息安全	网络安全法规与管理	是	兼职
18	李强	男	46	高工	中国科学院光电技术研究所、物理电子学、硕士	信息安全	信息系统安全运维	是	专职
19	苏畅	女	36	讲师	华北电力大学、信号与信息处理、硕士	工控安全	工控系统网络安全	是	兼职
20	焦健	男	43	副教授	北京航空航天大学、信息安全、博士	信息安全	密码学基础	是	兼职
21	皮志贤	男	39	高工	华北电力大学、计算机科学与技术、硕士	数据安全	网络安全等级保护实践	是	专职
22	王会涛	男	39	高工	北京航空航天大学、计算机科学与技术、学士	信息安全	信息系统安全运维	是	兼职
23	刘警	男	36	高工	华北科技学院、网络工程、学士	工控安全	信息安全技术基础	是	专职

增设专业计划开设的主要课程

序号	课程名称	课程 总学时	课程 周学时	授课教师	授课 学期
1	信息安全导论	72	4	王英彬	2
2	密码学基础	54	3	吴秋新	2
3	信息安全技术基础	72	4	闫怀志	3
4	网络安全法规与管理	72	4	任卫红	3
5	网络安全等级保护	72	4	曲洁	3
6	信息系统安全运维	72	4	王会涛	3
7	工控系统网络安全	72	4	秦宇	4
8	信创技术与应用	72	4	于东升	4
9	网络安全等级保护实践	108	6	李升	4

增设专业基本办学条件

专业名称	信息安全与管理			开办经费	500 万		
申报专业副高及以上职称（在岗）人数	22	其中该专业专职在岗人数	5	其中校内兼职人数	0	其中校外兼职人数	17
可用于新专业的教学图书（万册）	9	可用于该专业的教学实验设备（千元以上）	54（台/件）	总价值（万元）	2300		

序号	主要教学设备名称（限 20 项）	型号规格	台(件)	购入时间
1	安全运维实训平台	SECYW-Y200	30	2019
2	信息安全测评实验平台	SECCP-C100	6	2018
3	西门子 PLC	S7-200 Smart	17	2017
4	火电厂电力监控仿真系统	NADD-S100	套1套	2018
5	燃气仿真系统	NADD-S200	1 套	2016
6	水务仿真系统	NADD-S300	1 套	2016
7	变电站仿真系统	NADD-S300	1 套	2018
8	电力调度自动化平台	IES AMP200	1 套	2015
9	和利时 DCS 系统	HOLLiAS MACS	1 套	2015
10	工控安全便携式实验箱	EBPB-R100	12	2019
11	信号发生器	AWG5200	20	2018
12	网络安全管理平台	V1.0.0	1台台	2020
13	主机安全卫士	V1.0.0	1 套	2020
14	可信安全免疫系统	V1.0.0	1 套	2020
15	网闸	EBGW-V100	1 台	2016
16	信息安全攻防实训平台	EBEDU-V100	1 套	2019
17	新能源电力物联网仿真平台	NEE1000	1 套	2018
18	工控渗透测试	E-Blue-R100	1 套	2019
19	工控软件协议	E-NS-P200	1 套	2019
20	工控入侵检测系统	NIDSNX3-H13	1 套	2019

专业主要带头人简介

<table>
<tr><td rowspan="2">姓名</td><td rowspan="2">王英彬</td><td>性别</td><td>男</td><td>出生年月</td><td>1954.12</td><td>学历</td><td>本科</td></tr>
<tr><td colspan="2">专业技术职务</td><td>教授</td><td>行政职务</td><td colspan="2">常务副院长</td></tr>
<tr><td colspan="2">毕业时间、学校、专业</td><td colspan="6">华北电力大学计算机专业本科，1980 年 1 月毕业</td></tr>
<tr><td colspan="2">主要从事工作与研究方向</td><td colspan="6">1. 担任华北电力大学教授，长期从事计算机网络、高等语言、数据通信、信息安全、网络安全和工业控制系统安全等课程及方向理论和教学研究工作；
2. 创立“ 电力行业信息安全等级保护中心第一测评实验室 ”，从事网络安全等级保护测评的研究工作；
3. 共建“华北电力大学信息安全工程实验室 ”，从事信息安全技术标准规范的研究，以及成果转化工作；
4. 共建“ 国家开放大学网络空间安全学院 ”，从事网络安全相关专业教学的研究工作；
5. 创办“全国工控系统信息安全攻防竞赛 ”从事工业控制系统信息安全攻防场景和技术的研究工作。</td></tr>
<tr><td colspan="2">行业企业兼职</td><td colspan="6">华北电力大学信息安全工程实验室常务副主任；
北京卓识网安技术股份有限公司董事长；
北京华电卓越国际技术培训有限责任公司董事长。</td></tr>
<tr><td colspan="2">工作简历</td><td colspan="6">（一）、从事专业教学工作 40 多年
自 1980 年 1 月华北电力大学毕业留校任教，到 1987 年 5 月调离学校期间，曾主讲了计算机原理、高等语言和计算机网络等课程，并独立地完成了诸课程的全部教学环节。先后讲授计算机原理、高级语言、计算机网络和程序设计等专业课及公共课共约 1200 学时，培养学生 1700 余人次。
自 1987 年至今，一直从事计算机和网络安全相关课程的从业人员教培工作，累计不同层次、不同内容的授课时数总计约 3700 学时，参培人员 4000 多人次。部分教培工作有：
☞ 两次中国工商银行全国科技处长学习班邀请讲授计算机网络课程，课程视频录像在中国教育电视台向全国播放；
☞ 三届保定市电大学员的计算机原理与程序设计课程；</td></tr>
</table>

- 华北石油研究院和保定航空学校教员班讲授计算机网络；
- 九次中国科学院培训中心邀请的计算机网络课程；
- 两次机电部培训中心邀请的计算机网络和数据通信课程；
- 三次北京市公安局举办的信息安全课程；
- 十余次电力行业网络与信息安全课程；
- 二十余次国家重要信息系统保护人员认证课程；
- 五十余次信息安全保障人员系统认证课程；
- 十余次注册信息安全专业认证课程等。

（二）长期从事教学理论研究与实践

自 1981 年任教以来，长期从事理论探索、网络技术及教学方法的研究与实践，有多部著作、论文、译文出版。包括：

1、《计算机网络原理、结构及协议》1984 年编著教材，华北电力学院教材处出版，约 51 万字；

2、《办公室自动化的探讨与实践》 1985 年发表论文，香港《Communications Technologies》杂志刊登，约 1.5 万字；

3、《开放系统用户的程序设计接口》1985 年翻译学术文章，「英」Alongsford 著，华北电力通讯第二期发表，约 2 万字；

4、《ISO/OSI 及 LAN 标准化初探》1985 年发表论文，华北电力学院第四届学术研讨会发表，约 1.2 万字；

5、《计算机网络体系结构与协议》1986 年译著书籍，「美」Pall E. Green. Jr 著，中国水利电力出版社出版；参译约 20 万字（全书 60 万字）；

6、《微型机数据通信的实际应用和实验》1986 年译著书籍，「美」Elizabeth. A. Nichols 等著，中科院科海培训中心出版，约 23 万字；

7、《计算机局部网络》1987 年编著教材，清华大学出版社出版，编写约 40 万字（全书约 45 万字）；

8、《微型计算机集散控制系统》1987 年编著教材，北京科海总公司出版，编写约 11 万字（全书约 23 万字）；

9、《英汉信息技术辞典》1988 年编委成员，电子工业出版社出版，参编约 10 万字（全书约 50 万字）；

10、《计算机网络基础及应用》1988 年编审教材，中国对外贸易教育出版社出版，约 25 万字；

11、《英汉现代通信与计算机字典》1988 年编委成员，电子工业出版社出版，参编约 10 万字（全书约 45 万字）；

12、《IBM Tokon Ring 网络技术剖析》、《多机系统，计算机网络，分布处理》1989 年编译论文，金融电脑二期，共 8500 字；

13、《开放系统指南》1991 年译著教材，地震出版社出版，参译约 8 万字（全书约 40 万字）；

14、《OSI 计算机通信标准模型》1991 年编审教材，地震出版社出版，编审约 10 万字（全书约 30 万字）；

15、《NOVELL 网络操作系统》1991 年审校教材，地震出版社出版，共约 38 万字；

16、《电子货币综述》1993 年发表论文，《计算机世界》刊登，约 3 千字；

17、国家发改委信息安全专项《电力行业信息安全等级保护测评咨询能力建设》 2010 年科研项目获批，承担项目主要负责人。

18、《电力行业信息安全等级保护基本要求》、《电力二次系统安全防护和等级保护评估规范》2012 年参编权威标准，全行业发布。

19、《电力行业信息系统安全等级保护基本要求》释义（管理类信息系统分册、生产控制类信息系统分册）2014 年参编、审核，电子工业出版社出版。

其中，所编写的教科书被多所学校选为计算机网络课教材。后由中国科学院培训中心多次翻印，1987 年受清华大学出版社邀请改编后，被选定为全国计算机培训网的统编教材，深受业界好评。

（三）科研成果、工程应用和产教融合

1、创新“城市电子货币”工程

1991 年 10 月，主抓“鞍山电子货币”工程（中国工商银行总行项目）和“佳木斯城市电子消费系统”工程（科技部项目），该项工程是促进全社会良性消费，提高工商银行竞争力，加速电子化实施步伐的一个重要项目，从现场需求调研、总体方案论证入手，始终跟踪着这两项工程的实施，为国家自 1993 年开始的“三金”工程启动奠定了实践的基础。

2、央企信息化集成项目研发和实施

1992 年以来，组织、参与研发的应用项目有：公文运转自动化处理系统、工商银行储蓄综合分析处理系统、纪检监察统计报表系统、固定资产管理系统、柜员监控多媒体网络系统、存折打印机的设计与

	评价、中国工商银行 OA 系统、IC 卡应用系统、自动银行系统、电力 MIS 系统、SNA Server 的推广与应用、Internet Banking 的开发、推广与应用、工商银行固定资产管理系统等。 **3、部委系统集成项目研发** 2006 年受国家电力监管委员会委托，组织研发电工进网作业许可考试系统平台，一直沿用至 2018 年 10 月该许可项目移交； **4、创立电力行业信息安全等级保护中心第一测评实验室，承担电力行业信息安全测评研究和实施** 多年来一直深入能源电力信息安全领域的研究和技术发展，所执掌的北京卓识网安技术股份有限公司作为独立第三方专业测评机构，长期致力于能源电力行业的工控信息安全测评服务和咨询服务：能源监控系统安全防护评估、信息安全等级保护测评、信息系统风险评估和性能检测、工控安全保障体系规划和工控系统建设整改咨询服务，被公安部、国家能源局（原国家电监会）授权为电力行业信息安全等级保护中心第一测评实验室。多次参与公安部、能源行业组织的各级安全检查、整改加固试点、测评试点工作，以及国家、能源电力行业多个信息安全标准规范的制定，获得十多项软件著作权，是中国可信计算工作组、中国信息协会信息安全专业委员会能源工作组核心成员单位。 公司作为国家高新技术企业、中关村创新企业，拥有完善的自主知识产权体系和研发实力，依托强大的研发实力、领先的技术、专业的服务等综合竞争力，为行业提供等保测评、二次安防评估、安全规划、安全加固、应急服务、安全监理、安全培训等安全服务。主要客户涉及政府部委、事业单位、央企国企、高校、IT 和互联网企业等 1000 多家单位。 **5、承担国家能源局能源电力行业信息安全标准和规范的制定** 2010 年，参与《电力行业信息安全等级保护基本要求》和《电力二次系统安全防护和等级保护评估规范》的起草工作，于 2012 正式发布，为全面提升电力系统的信息安全奠定了基础； 2010 年，参与申报了国家发改委信息安全专项《电力行业信息安全等级保护测评咨询能力建设》，并成功获批，该项目的实施有助于构建电力行业等级保护管理体系，全面提升电力行业信息安全等级保护能力； 2012 年，参与国家能源局组织的《电力行业信息系统安全等级保护基本要求》释义（管理类信息系统分册、生产控制类信息系统分册）的编撰，2014 年由电子工业出版社出版。

6、共建信息安全工程实验室，深入能源领域信息安全的研发与应用

2013 年，与华北电力大学联合成立“信息安全工程实验室”，资源共享、优势互补，加强产、学、研、用一体化共同发展，深入开展能源领域信息安全的研发。

2014 年，信息安全工程实验室通过北京市发改委认证，被授予“北京市能源电力工程技术研究中心”，开展能源行业信息安全工程技术研发和项目申请。

2014 年，受国家能源局委托，开展 PLC 检测研究，为电力设备安全护航，促进电力设备国产化的研究和应用。

7、共建成立国家开放大学网络空间安全学院，推进产教融合

2013 年，与国家开放大学、公安部信息安全等级保护评估中心三方合作共建网络空间安全学院，服务行业产业发展和人力资源开发，探索完善产教融合人才培养的新模式。充分利用现代信息技术，整合利用各方的优质教育资源，通过“学分银行”机理，促进非学历继续教育与学历继续教育的学习成果融通，推动行业从业人员终身教育体系建设，推进行业学习型社会的建立，搭建行业从业人员终身教育“立交桥”。

8、研发工控系统信息安全攻防演练平台，创办“全国工控系统信息安全攻防竞赛”

2014 年，在实验室科研项目成果的基础上，针对工业控制系统信息安全，采用半实物模拟仿真技术，组织研发工控系统信息安全攻防演练平台，应用于工业领域关键信息基础设施的防护研究和演练，着力培养工控系统信息安全保障人才。

2015 年，联合公安部信息安全等级保护评估中心，创办了首届“全国工控系统信息安全攻防竞赛”，赛事关注能源、电力、通信、交通、燃气、水务等城市公用事业领域的关键信息基础设施，通过对仿真环境下的不同等级防护策略中的关键信息基础设施生产控制系统实施攻击，检验工控系统的防护策略与脆弱性，以赛促建，引起了政府主管部门、工业生产控制系统企业、安全设备厂商、科研院所的高度关注。

至 2020 年已连续举办六届全国性赛事，获得网信办、公安部、工信部、能源局等多个主管部委和诸多院士的支持和肯定，参赛单位涵盖科研院所、央企国企、高等院校和行业厂商，已打造成为全国性权威工控安全攻防赛事。

最具代表性的教学科研成果	序号	成果名称	等级及签发单位、时间	本人署名位次
	1	电力行业信息安全等级保护测评咨询能力建设	科研专项，国家发改委、2010 年	第一参与人
	2	《电力行业信息安全等级保护基本要求》	行业标准，国家电力监管委员会，2012 年	共同起草人
	3	《电力二次系统安全防护和等级保护评估规范》	行业标准，国家电力监管委员会，2012 年	共同起草人
	4	电厂电力监控系统信息安全攻防测试与仿真演练平台	一等奖，中国电力企业联合会，2018 年	第一参与人

目前承担的主要教学工作（5 项以内）	序号	课程名称	授课对象	人数	学时	课程性质	授课时间
	1	计算机原理	学生	700	450	专业课 公共课	1980 年 -1987 年
	2	高等语言	学生	600	450	专业课	1981 年 -1987 年
	3	计算机网络	学生	400	300	专业课	1982 年 -1987 年
	4	工控安全	在职人员	900	1600	职业培训	2005 年 -2018 年
	5	信息安全运维	在职人员	1600	900	职业培训	2013 年 -2021 年