附件1

**中国高校产学研创新基金-人工智能与数字安全专项**

**申报指南说明**

根据 《关于申报2025年中国高校产学研创新基金的通知》（教科发中心函〔2025〕3号)的相关要求，教育部高等学校科学研究发展中心与三六零数字安全科技集团有限公司、北京中诚同宇科技有限公司联合设立“中国高校产学研创新基金-人工智能与数字安全专项”，支持高校在新形势下的人工智能与数字安全领域人才培养研究、信息化人工智能与数字安全新基建、安全大模型新兴业务场景技术、人工智能安全、人工智能赋能教育改革等方向的科学研究和教学实践。

**一、课题说明**

1.“人工智能与数字安全专项”旨在全国范围内遴选合作高校，共同关注新形势下的人工智能与数字安全领域人才培养研究、信息化网络安全新基建、网络安全新兴业务场景技术、人工智能安全、人工智能赋能教育改革等方向的科学研究和教学实践，培养更多掌握人工智能与数字安全技术的复合型高素质人才，助力地方产业升级。

2.“人工智能与数字安全专项”的申请截止时间为2026年1月31日。计划执行时间为2026年5月1日～2027年4月30日，可根据课题复杂程度适度延长执行周期，最长不超过两年。

3.“人工智能与数字安全专项”为每个立项课题提供总经费10万元至50万元的课题研究经费及科研软硬件平台支持，其中课题研究经费5万元至25万元。

4.“人工智能与数字安全专项”基金课题针对人工智能与数字安全领域人才培养、信息化人工智能与数字安全新基建、大数据、AI安全、车联网安全、区块链安全、人工智能赋能教育改革等领域的科学研究及教学实践，以科技变革促进教育变革，创新人才培养机制，推动社会发展为目标。选题方向见表一（新形势下的人工智能与数字安全领域人才培养研究）、表二（信息化人工智能与数字安全新基建）、表三（安全大模型新兴业务场景技术研究方向）、表四（其他方向）。基金课题提供的相关技术、应用和软硬件平台见表五。

**表一“新形势下的人工智能与数字安全领域人才培养研究”选题列表**

|  |  |  |
| --- | --- | --- |
| **课题方向编号** | **课题方向** | **课题研究内容** |
| A01 | 人工智能与数字安全课程研究方向 | **研究内容包括但不限于以下方向：****新形势下网络攻击与防护课程研究。**结合前期建设基础，加强课程改革和建设，帮助学生建立起计算机系统安全的整体概念，使学生能够了解和掌握网络攻击与防护的基本原理、技术及最新发展动态。具有网络攻击与防护理论和实战基础。结合授课实践，开发实验资源，以学生为中心，贯彻理论与实践相结合的教育思想提高学生的动手实践能力，并能够灵活运用基本原理及新技术全面地解决实际问题。培养学生逆向思维和学以致用能力。**人工智能与数字安全教学内容和课程体系改革。**面向高校网络安全、信息安全、网络工程、物联网、人工智能等计算机相关专业，融合行业人才培养要求，协助人才培养方案修订，提供网络平台和资源，优化专业课程体系设置，建设适应行业发展需要、符合人才培养规律的可共享可复制的教案、教材、教学案例等资源（包括但不限于《网络安全攻防对抗》《电子数据取证技术》《数据安全》《数据存储与容灾》《人工智能安全》《大模型应用》等信息安全技术应用专业/网络空间安全专业/人工智能专业课程）。 |
| A02 | 人工智能与数字安全赛题研究与红蓝对抗教学实践方向 | **研究内容包括但不限于以下方向：****WEB赛题征集与开发。**征集基于Liunx，Windows等操作系统环境下，满足当代大学生高标准竞技要求，紧随当下时事热点的WEB赛题。CTF赛题运行环境所需软件要求配置好开机自启动；CTF类flag格式：FlagSangFor{16位随机字符数字}。AWD赛题根据实际需要制作成相应格式的环境，需附带相应的check脚本。**人工智能教学实践。**研究通过在人工智能专业/新商科/新农科等专业课程中结合人工智能教学及人工智能赋能教学改革实践，探索建立一套侧重于培养学生生成式人工智能大模型应用知识能力的教学体系，利用校企共建资源等方式，从课程内容设计、课程内容开发、教学计划、教学方法、考核测评、配套平台等方面进行实践研究，为院校未来培养网络安全人才提供一套优质的实践方案。**红蓝对抗教学实践。**研究通过在信息安全技术应用专业/网络空间安全专业课程中结合红蓝对抗教学实践，探索建立一套侧重于培养学生攻防对抗知识能力的教学体系，利用校企共建资源等方式，从课程内容设计、课程内容开发、教学计划、教学方法、考核测评、配套平台等方面进行实践研究，为院校未来培养网络安全人才提供一套优质的实践方案。 |
| A03 | 人工智能与数字安全产教融合师资队伍建设、专业建设、应用型人才培养等方向的研究与实践 | **研究内容包括但不限于以下方向：****人工智能与数字安全产教融合师资队伍建设的研究与实践。**解决信息安全、网络空间安全、生成式人工智能新兴产业师资力量薄弱问题为研究方向，引导院校结合专业建设方向、人才培养计划，开展人才双向流动的制度创新；利用企业在网络安全相关领域的资源优势和平台优势，支持企业技术和管理人才到学校任教，探索产业教师（导师）特设岗位计划；探索符合院校教育特点的专业教师绩效考核标准。**专业建设、应用型人才培养的研究与实践。**解决信息安全技术应用专业/网络空间安全专业/人工智能专业等学科在高校的人才培养体系设计、实践和创新，引导院校结合地方资源和自身办学条件，加速院校在人工智能与数字安全学科的人才培养；利用企业在人工智能与数字安全相关领域的资源优势和平台优势，强化复合型实践教学，完善以应用型人才为主的培养体系；指导院校加强创新创业人才培养，为学生提供多样化成长路径。 |
| A04 | 人工智能与数字安全方向的课程思政示范项目建设工作的探索和实践 | **研究内容包括但不限于以下方向：**探索我国人工智能与数字安全领域人才培养思想政治工作现状和存在的问题，研究出明确可实行的对策建议。再基于课程思政工作的要求和特点，结合360的人工智能与数字安全产品和服务以及学校本身的优势特点，设计出网络安全课程思政示范项目建设方案和具体执行计划。 |

**表二“信息化人工智能与数字安全新基建” 选题列表**

|  |  |  |
| --- | --- | --- |
| **课题方向编号** | **课题方向** | **课题研究内容** |
| B01 | 信息化建设与智能化网络安全运营相结合的实践探索 | **研究内容包括但不限于以下方向：**网络安全建设场景，依托360安全大模型基于网络安全运营平台进行示范应用探索和理论适用性研究，研究内容可以包括但不限于：基于网络安全运营体系的信息化建设进行应用示范性探索；探索和研究各行业各体系的网络安全运营技术（AI、安全威胁情报、流量分析、安全大模型、智能化运营等）的应用和可持续安全运营服务体系的研究与应用。 |
| B02 | 多业务场景安全体系建设实践探索 | **研究内容包括但不限于以下方向：**结合各行业信息化建设，探索各行业多场景网络安全体系建设。研究内容可以包括但不限于：数字安全运营中心建设、IPV6网络安全保障体系建设、等级保护安全建设、关键基础设施安全建设、恶意病毒木马治理等细分场景的典型应用，研究相关核心技术的应用和实践。 |
| B03 | 人工智能+场景下的网络安全保障防护研究 | **研究内容包括但不限于以下方向：**在人工智能与教育、医疗、金融、政府等行业深入结合的背景下，基于网络安全防护技术，建立起互联网安全大平台的安全制度、技术方案、管理办法及服务体系。研究内容包括但不限于个人信息安全保障、数据资产安全保障、新技术新业务安全监测预警、云数据中心的安全防护等 |
| B04 | 人工智能赋能教学改革实践 | **研究内容包括但不限于以下方向：****智能教学助手开发**：基于360安全大模型构建教学智能体研究，实现课程内容自动生成、个性化学习路径推荐、实验环境智能纠错**教学资源知识库构建**：融合360行业威胁情报库（含2000万+恶意样本），开发AI驱动的教学案例自动标注与检索系统研究**教育数据安全合规**：研究教学行为数据隐私计算技术，确保符合《个人信息保护法》要求，输出教育数据分类分级标准研究 |

**表三 “安全大模型新兴业务场景技术研究方向”选题列表**

|  |  |  |
| --- | --- | --- |
| **课题方向编号** | **课题方向** | **课题研究内容** |
| C01 | 基于大数据分析的安全技术研究与应用 | **研究内容包括但不限于以下方向：****移动终端恶意软件检测系统的设计与实现。**研究基于大数据分析的移动端恶意软件检测技术，并设计检测系统，主要研究内容包括但不限于：通过对软件静态特征信息进行模型训练构建预测模型，通过对软件的动态恶意行为进行模型训练构建预测模型。**物联网威胁数据捕获与信息抽取系统的设计与实现。**基于大数据的网络攻击溯源系统实现基于大数据技术对攻击流量和日志进行分析，提取出关键有效的攻击信息，对网络攻击进行溯源追踪。主要研究内容包括但不限于：攻击流量和日志捕获、海量攻击数据的存储、基于大数据技术的攻击流量分析、攻击行为感知、被入侵主机检测和定位、主机侧溯源、网络侧溯源、攻击行为还原及攻击者画像。**网络攻击溯源系统的设计与实现。**基于大数据的网络攻击溯源系统实现基于大数据技术对攻击流量和日志进行分析，提取出关键有效的攻击信息，对网络攻击进行溯源追踪。主要研究内容包括但不限于：攻击流量和日志捕获、海量攻击数据的存储、基于大数据技术的攻击流量分析、攻击行为感知、被入侵主机检测和定位、主机侧溯源、网络侧溯源、攻击行为还原及攻击者画像。 |
| C02 | 基于深度学习、机器学习、人工智能的安全技术研究与应用 | **研究内容包括但不限于以下方向：****基于深度学习的非结构化文本分类算法实现。**研究深度学习在自然语言处理领域中文本表示与分类方法的应用，解决非结构化文档内容识别、高维度稀疏问题、上下文信息缺失问题、高频词汇扰动问题，完成对非结构化数据的自动分类和优化功能，应用场景包括但不限于与：数据防泄漏、语言感知、机器翻译、语义理解、智能问答。研究内容包括但不限于：多维文档内容提取技术；多语言自然语言处理技术；分类特征提取技术；未知样本自动分类技术；基于混合深度信念网络的多类文本表示与分类方法；基于卷积神经网络结合深度玻尔兹曼机的多标签摘要文本表示与分类方法；基于长短时记忆模型的不均衡多标签全文文本表示与分类方法等。**基于机器学习的网络攻击数据挖掘。**结合网络攻击特点，基于机器学习技术，对海量日志、流量抓包、恶意程序样本等原始信息进行分析处理，构造数据驱动安全的方案。主要研究内容包括但不限于，可迁移的攻击特征提取方法、攻击判别模型研究、威胁情报生成、新型攻击的发现和挖掘。**移动端APT检测技术研究。**基于机器学习技术，设计检测模型来针对移动平台APT进行检测。包括但不限于：通过静态检测方法对攻击特征进行检测，通过威胁情报共享来匹配恶意特征。**固件分析工具实现与优化。**研究在人工智能的辅助支持下，对异构物联网设备固件的智能扫描、智能归类、固件威胁信息预警等。主要研究内容包括但不限于：异构物联网设备固件智能扫描平台的实现，基于人工智能的固件智能扫描算法实现与优化，智能扫描涵盖：恶意代码、零日漏洞、敏感信息等。**自动化代码分析。**通过静态代码分析的方法可以有效的检测具有类似模式的大多数漏洞，但是对于不容易区分的代码常常会导致检测精度过低。通过人工智能的方法进行特征提取，根据不同程序语言的特性进行预处理，提高处理效果和效率，通过大量的样本，对预先定义的模型进行训练。由于人工智能算法可以挖掘输入特征之间更深层次的练习，更加充分的利用代码的信息，因此会有更高的准确率。 |
| C03 | 智能网联汽车安全技术研究与应用 | **研究内容包括但不限于以下方向：**针对智能网联汽车的各类攻击面，围绕机器视觉欺骗、GPS欺骗、ECU漏洞、智能汽车代码安全、车载系统安全、远程通信安全等，展开研究。探索智能网联汽车的攻击方式，漏洞利用，渗透测试方案方法，入侵检测方法等。提高智能网联汽车在各种攻击场景下的智能网联汽车的防护方案，切实提高智能网联汽车的信息安全能力。 |
| C04 | 安全大模型行业应用创新研究 | **研究内容包括但不限于以下方向：**多模态威胁分析引擎：研发支持文本、代码、流量、日志的多模态威胁检测模型，实现金融/政务/教育场景自动化风险研判研究（误报率≤5%）行业决策优化系统：基于360安全大脑实时数据，构建行业安全知识图谱，输出攻防策略优化研究（响应效率提升40%+）生成式渗透测试：AI红蓝对抗工具研究，自动生成钓鱼攻击剧本、漏洞利用代码，覆盖10+高危漏洞类型（CVE-TOP20） |
| C05 | 低空智联网安全技术的研究与应用 | **研究内容包括但不限于以下方向：**研究低空智联网安全态势感知与预测技术、ADS-B 等无线入侵智能检测技术、低空智联网多维安全威胁检测等。主要研究内容包括但不限于：低空智联网安全态势感知与预测技术、对低空航空器有线和无线攻击入侵检测能力、空中安全地图测绘能力等。 |

**表四 其他方向选题列表**

|  |  |  |
| --- | --- | --- |
| **课题方向编号** | **课题方向** | **课题研究内容** |
| D01 | 其他 | 根据自身的条件和区域的特点，结合项目提供的平台（相关平台介绍见表五），融合网络安全、人工智能、大数据、云计算、区块链、虚拟仿真等新一代信息技术，申请院校自主选择研究方向进行申报。 |

**二、申报条件和要求**

1. 团队成员在选定的项目研究方向有较好的技术储备，包括与申报课题研究内容相关的研究成果、教材、论文、专利、获奖等；

2. 团队组成合理，分工明确，数量不少于3人；

3. 优先支持已经设立信息安全、网络空间安全、人工智能相关专业或已经成立相关研究中心的院校；

4. 优先支持研究内容有创造性、前瞻性和实用性，有可转化前景的课题；

5. 优先支持有明确研究成果，成果有应用价值，可复制、可推广的课题，不支持纯理论研究；

6. 优先支持研究方向明确，研究内容详实，研究方案完整可行的课题；

7. 申请人应客观、真实地填写申报书，没有知识产权争议，遵守国家有关知识产权法规。在课题申报书中引用他人研究成果时，必须以脚注或其他方式注明出处，引用目的应是介绍、评论与自己的研究相关的成果或说明与自己的研究相关的技术问题。对于伪造、篡改科学数据，抄袭他人著作、论文或者剽窃他人科研成果等科研不端行为，一经查实，将取消申请资格；

8. 立项课题项目获得的知识产权由合作方和课题项目承担单位共同所有；

10.项目组在项目开展过程中，需具备可独立支配的研究基础软硬件条件，如需外部资源支持，须在项目申报书中明确指出。

**三、资源及服务**

针对入选合作院校，将提供完善的资源和服务体系，以保证院校顺利开展合作项目，并为院校在人工智能与数字安全领域人才培养、信息化人工智能与数字安全新基建、大数据、AI、车联网安全、人工智能安全等方向的科研及人才培养提供长期有效的支持。

1．“人工智能与数字安全产专项”为每个立项课题提供对应的经费支持和实验设施与服务支持，为申报团队提供创新项目选题指导，协助团队完成科研项目或创新项目基础平台搭建和教师培训工作，并根据需求开展服务校方等工作。

2．项目发起单位将辅助、联合申报院校申报新的科研课题，提供项目咨询服务和技术支持，辅助科研成果的快速产品化及解决方案的包装。

**表五 提供给课题研究的软硬件平台说明**

|  |  |  |
| --- | --- | --- |
| **平台编号** | **软硬件服务名称** | **详细介绍** |
| E01 | 网络安全实训平台 | 网络安全实训平台是基于高度仿真的虚拟网络，模拟物理世界组网，提供网络安全攻防知识培训及实操解题练习，支持在线夺旗考试，并形成完整的人才能力评价体系。在此平台之上，我们还提供了一套完整的培训课程知识体系，覆盖全行业安全方向，可以针对不同的客户提供高度定制化的培训内容。提供SAAS账号和云服务环境 |
| E02 | 网络安全竞赛平台 | 网络安全竞赛平台基于高度仿真的虚拟网络，模拟物理世界组网，是集合各种类型竞赛的网络安全实战竞赛平台。通过高度仿真现实世界中的安全威胁、安全攻击以及网络形态，构建符合对抗需求的攻防目标网络环境；模拟构建各种形式的攻击手段，锻炼学员的安全响应能力。提供SAAS账号和云服务环境 |
| E03 | 数字安全运营平台 | 提供独立门户的智能安全运营协作平台、智能安全大数据分析平台、即时通讯协同门户平台、QPaaS业务流程管理平台各1套，通过安全运营流程标准化工单的打通，引产入校，实现学生快速上手、顶岗实习。提供云服务环境下的独立门户和SAAS账号 |

**四、课题申报说明**

1. 申请人须仔细阅读申请指南，按照指南详细填写申请书，填写不合要求的课题会按照格式不符合要求处理。

2. 请各课题申请人按要求填写申请书（申请书中手机和邮箱必须填写），加盖公章及签字后扫描上传至：https://cxjj.cutech.edu.cn；为方便评审，申请书扫描件请按以下命名规则命名：学校名称+申请人姓名。。

3. 申请书书面材料一份，邮寄至：北京市海淀区中关村大街35号803室，教育部高等学校科学研究发展中心信息化研究发展处。

4. 申请截止时间为2026年1月31日。

5. 课题的计划执行时间为2026年5月1日～2027年4月30日，可根据课题复杂程度适度延长执行周期，根据课题实际情况协商，最长不超过两年。

6. 每位申报人限报一项课题。

7. 课题选题列表上的选题方向都不限定课题数量，但是如果存在内容重复的相似课题，专家组将根据课题组技术积累、课题方案、课题支撑条件等要素择优选择资助课题。

8. 如果以联合课题组的形式申请课题，需要列明不同学校单位的课题任务。

**9. 课题申请人无需向资助企业额外购买配套设备或软件。**

**五、联系人及联系方式**

**教育部高等学校科学研究发展中心联系人：**

张 杰 电话：010-62514689

**企业业务支持联系人：**

迟老师 电话：18601992920

张老师 电话：18600818078

**企业技术支持联系人：**

秦老师 电话：18601194839

冯老师 电话：13716792890