湖北民族大學
HUBEI MINZU UNIVERSITY

# 硕士研究生培养方案

## 适用于人工智能安全与治理

## （2025 版）


智能科学与工程学院

2025 年 6 月

# 编写说明

1. 专业课课程编号为 11 位，编号方式为：

年份代码（后 2 位）学科代码（6 位）+课程类别（B/C/D）+课程序号（2 位）。B 为专业学位课；C 为专业选修课；D 为补修课。

2. 授课方式主要为“面授讲课”、“实践”、“面授、实验”、“讨论”、“面授、讨论”、“自学”等方式。

3. 考核方式为“笔试”（含闭卷、开卷）、“口试”、“提交报告”（含总结、综述、心得体会等）、“课程论文”、“考查”（含检查读书笔记、实验或上机等情况）5 种方式。

4. 封面“适用于 XXX”指的是对应二级学科。

5. 课程类别：公共学位课/专业基础课/专业必修课/选修课/补修课。

6. 教材与参考书目的录入顺序为作者名，书名，出版单位，出版时间。

7. “培养单位名称”为培养方案制定单位名称，应填写全称。

8. 装订要求：A3 纸正反打印，中缝装订。

# 人工智能安全与治理 硕士学术学位研究生培养方案

（专业代码：140504 授　工学　学位）

## 一、培养目标

本学科培养具备良好的政治思想和职业道德素养，掌握坚实的智能科学与技术的基础理论和系统专门知识，具备从事数据安全与隐私保护、可信智能系统等领域人工智能关键方法和技术研究的复合型、应用型的高层次专门人才。

1.政治素养。具备良好的政治思想素养和职业道德素养，深入学习并深刻领会中国特色社会主义理论体系，坚决贯彻执行党的基本路线、方针、政策，严格遵守国家法律法规，具有良好的职业操守和敬业精神，德智体全面发展。

2.知识水平。掌握智能科学与技术基本理论和方法，学习智能科学、优化理论、智能信息感知技术、机器学习、深度学习、人机混合智能等方面的相关理论和知识，具备从事数据安全与隐私保护、可信智能系统等领域人工智能应用研究的能力。

3.科研能力。紧密追踪与把握智能科学与技术发展的前沿理论，能够利用互联网、电子文献数据库获取专业知识和研究方法，具备对获取的人工智能知识进行科学总结和信息提取能力，具备人工智能方法创新、人工智能技术创新能力，能够将获取知识解决实际工程问题。

4.综合素质。具有从事智能科学与技术研究的思维能

力、创新能力、决策能力、执行能力、交流能力、组织协调能力等，具备良好的写作能力和表达能力，能够应用母语和英文以书面和口头方法进行学术交流。

## 二、培养方向

1.数据安全与隐私保护：以信息论、博弈论、控制论和系统论等多学科交叉为基础，构成数据安全的基础理论体系。以网络安全理论与技术为基础，密码学和隐私保护方法为核心，研究数据全生命周期密文处理技术和隐私保护技术，开发数据安全、隐私保护及网络攻防方面的应用示范。

2.可信智能系统：通过密码学、区块链等技术确保系统计算和通信过程的安全性和可信性。在云计算、物联网等环境下，设计安全的加密算法、身份认证机制等，保护系统信息的隐私和完整性，防止信息泄露和篡改，实现系统信息的可信传输和可溯源性。

## 三、学习年限与培养方式

本学科硕士研究生基础学制为 3 年，最长学习年限为 6 年。

培养方式为课程学习、实践活动和学位论文相结合方式。实行导师负责制，采取导师个别指导和导师组集体培养相结合的方式进行，对研究生培养进行全过程指导。

## 四、课程设置及学分要求

应修 32 学分，其中学位课程 19 学分，选修课程 7 学分，

学术活动 3 学分，实践活动 2 学分，“五育”活动 1 学分。

**五、学术成果**

研究生在校期间以第一作者或导师第一、学生第二作者身份，发表 SCI/EI 期刊论文、中文期刊论文或学院认定的高水平期刊论文；或作为第一发明人或第二发明人（导师为第一发明人）获得授权国家/国际发明专利 1 项；或获得中国国际大学生创新大赛、“挑战杯”大学生课外学术科技作品竞赛、中国研究生创新实践系列大赛等学院认定的高水平竞赛。鼓励研究生在中国科协、中国人工智能学会、中国计算机学会推荐的智能科学与技术及相关科学高水平期刊和学术会议上发表学术论文。

**六、学位授予**

工学硕士学位。

# 课程设置一览表

| 课程类别 | | 课程编号 | 课程名称 | 学分 | 学时 | 开课学期 | 教学方式 | 考核方式 | 备注 |
|---|---|---|---|---|---|---|---|---|---|
| 学位课程 | 公共学位课 | 000000A09 | 中国特色社会主义理论与实践研究 | 2 | 36 | 1 | 讲授、讨论 | 笔试 | |
| | | 000000A03 | 自然辩证法 | 1 | 18 | 2 | 讲授、讨论 | 笔试 | 理科 |
| | | 000000A16 | 研究生英语（上） | 2 | 36 | 1 | 讲授 | 笔试 | |
| | | 000000A17 | 研究生英语（下） | 2 | 36 | 2 | 讲授 | 笔试 | |
| | 专业学位课 | 25140500B01 | 人工智能理论 | 3 | 54 | 1 | 讲授 | 笔试 | |
| | | 25140500B02 | 最优化理论与方法 | 3 | 54 | 1 | 讲授 | 笔试 | |
| | | 25140500B03 | 随机过程与时序数据分析 | 2 | 36 | 2 | 讲授、讨论 | 笔试 | |
| | | 25140504B01 | 云安全与隐私计算 | 2 | 36 | 1 | 讲授、讨论 | 笔试 | |
| | | 25140504B02 | 物联网安全 | 2 | 36 | 2 | 讲授、讨论 | 笔试 | |
| 非学位课程 | 选修课 | 25140500C01 | 智能科学与技术前沿 | 1 | 18 | 1 | 讲授、讨论 | 提交报告 | |
| | | 25140500C02 | 职业道德与学术伦理 | 1 | 18 | 2 | 讲授、讨论 | 提交报告 | |
| | | 25140500C03 | 科技文献检索 | 1 | 18 | 1 | 讲授、讨论 | 提交报告 | |
| | | 25140504C01 | 混沌密码学 | 2 | 36 | 2 | 讲授、讨论 | 提交报告 | 数据安全与隐私保护 |
| | | 25140504C02 | 现代密码学 | 2 | 36 | 2 | 讲授、讨论 | 提交报告 | |
| | | 25140504C03 | 网络空间安全治理 | 2 | 36 | 2 | 讲授、讨论 | 提交报告 | |
| | | 25140504C04 | 高级图像加密技术 | 2 | 36 | 2 | 讲授、讨论 | 提交报告 | |
| | | 25140504C05 | 人工智能安全与治理导论 | 2 | 36 | 2 | 讲授、讨论 | 提交报告 | |
| | | 25140504C06 | 人工智能应用实践 | 2 | 36 | 2 | 讲授、讨论 | 提交报告 | |
| | | 25140504C07 | 智能检测技术 | 2 | 36 | 2 | 讲授、讨论 | 提交报告 | 可信智能系统 |
| | | 25140504C08 | 工业控制系统安全 | 2 | 36 | 2 | 讲授、讨论 | 提交报告 | |
| | | 25140504C09 | 深度学习应用 | 2 | 36 | 2 | 讲授、讨论 | 提交报告 | |
| | | 25140504C10 | 区块链技术 | 2 | 36 | 2 | 讲授、讨论 | 提交报告 | |
| | | 25140504C11 | 人工智能应用实践 | 2 | 36 | 2 | 讲授、讨论 | 提交报告 | |
| | | 25140504C12 | 人工智能安全与治理导论 | 2 | 36 | 2 | 讲授、讨论 | 提交报告 | |
| | 补修课 | 25140504D01 | 算法设计与分析 | - | 36 | 2 | 讲授、讨论 | 提交报告 | 只记成绩不记学分 |
| | | 25140504D02 | 数字图像处理 | - | 36 | 2 | 讲授、讨论 | 提交报告 | |
| | | 25140504D03 | 现代控制理论 | - | 36 | 2 | 讲授、讨论 | 提交报告 | |
| | | 25140504D04 | 傅里叶分析 | - | 36 | 2 | 讲授、讨论 | 提交报告 | |
| 实践环节 | | 学术活动 | | 3 | | 4 | | 考核合格记学分 | |
| | | 实践活动 | | 2 | | 4 | | | |
| | | “五育”活动（德智体美劳） | | 1 | 1W | 2 | | | |

编写成员：刘嵩　徐建　胡涛
执 笔 人：刘嵩
审 核 人：沈济南