

网络安全安全一级学科授权点

本硕贯通实验班人才培养方案

Training Program of Integrated Bachelor-Master

（专业代码：080904K 学科代码：083900）

一、培养目标

为深入贯彻落实网络强国战略思想，大力推进我校网络安全学科发展，培养网络安全领域高素质特殊拔尖人才，郑州大学开设本硕贯通拔尖人才“嵩山实验班”（以下简称实验班），旨在培养对党绝对忠诚，政治绝对可靠，综合素质过硬，掌握系统的网络安全学科理论基础和专业知识，在互联网安全和嵌入式安全领域特色突出，具有较强的网络对抗能力和创新实践能力的高素质实战型拔尖人才，具体目标为：

培养目标 1：具有高度的国家安全意识和宽广的国际视野，具备良好的创新精神、人文素养和社会责任感，恪守职业道德，掌握行业相关经济、社会、管理知识和法律法规。

培养目标 2：具备坚实的网络空间安全基础理论和专业知识，能够挖掘本学科最新成果和发展方向，具有较强的工程实践能力、外语理解能力和表达能力。

培养目标 3：能够运用网络安全学科的理论、方法与技术独立从事此领域科研工作，独立解决工程领域的安全技术难题，承担国家及区域安全任务。

培养目标 4：具有自主学习与终身学习的意识和能力，可适应职业发展需求，在科研院所、企事业单位以及行政管理部门从事网络安全领域的科学研究、技术开发与管理工作时，能够展现出强劲的职场竞争力。

二、毕业要求

针对本硕贯通拔尖人才“嵩山实验班”特点，注重学生素质培养，努力使学生具有基础厚、专业强、口径宽和素质高的特点，具有分析问题、解决问题的能力 and 网络对抗创新实践

能力，同时注重提高人文科学、法律法规、职业道德素质等修养，使学生能够成为网络空间安全领域高素质实战型拔尖人才。根据培养目标，实验班本科阶段的基本毕业要求如下：

1. **工程知识：**具备扎实的数学、自然科学、计算、工程基础和信息安全专业知识，并能将其用于解决信息安全领域的复杂工程问题。

1.1 问题表述：系统理解数学、自然科学、计算、工程科学理论及本专业的基础知识，并用于信息安全领域工程问题的表述；

1.2 问题建模：掌握信息安全领域所需的数据分析技术，并用于信息安全领域复杂工程问题中的对象建模和计算求解；

1.3 问题推演与分析：能够将信息安全专业知识和数学分析方法用于推演和分析专业工程问题；

1.4 方案比较与综合：能够利用系统思维能力，将相关工程知识应用于信息安全专业工程问题解决方案的比较与综合，并体现本领域的先进技术。

2. **问题分析：**能够应用数学、自然科学、工程科学和信息安全专业的基本原理，准确识别、表达和分析信息安全领域的复杂工程问题，综合考虑可持续发展的要求，以获得有效结论。

2.1 问题识别与判断：能应用数学、自然科学、工程科学和信息安全专业的基本原理，识别和判断信息安全领域复杂工程问题的关键环节、步骤和特征；

2.2 复杂工程问题表达：能应用相关科学原理和数学模型方法，正确表达信息安全领域复杂工程问题；

2.3 文献研究与分析：能熟练运用文献检索与资料查询方法获取信息安全领域复杂工程问题的可行方案，并认识到解决方案的多样性；

2.4 解决方案表达：能借助文献研究对信息安全领域复杂工程问题的影响因素及可持续发展要求进行分析和推理，正确表达复杂信息安全问题的解决方案和技术路线，并分析方案的合理性。

3. **设计/开发解决方案：**能设计针对信息安全领域复杂工程问题的解决方案，设计满足特定需求的软硬件系统、模块或工作流程，体现创新性，并从健康、安全与环境、全生命周期成本与净零碳要求、法律与伦理、社会与文化等角度考虑可行性。

3.1 系统设计与开发：掌握信息安全设计和系统开发全周期、全流程的设计/开发方法和技术，了解影响设计目标和技术方案的各种因素；

3.2 特定需求保障：能设计满足信息安全项目特定需求的模块、单元或部件；

3.3 创新意识与态度：了解信息安全技术应用前景与最新发展，能够在信息安全的软硬件系统设计与开发中体现创新意识与态度；

3.4 社会与文化因素：在设计中能够综合考虑安全健康、节能环保、法律伦理、文化与社会等因素。

4. **研究：**能基于信息安全领域科学原理并采用科学方法对信息安全领域复杂工程问题进行研究，包括理论分析、设计实验、数据分析与解释、并通过信息综合得到合理有效的结论。

4.1 方案调研与分析：能够运用相关科学原理，通过文献研究和相关方法，调研信息安全领域复杂工程问题的解决方案；

4.2 实验方案设计：能够根据信息安全的对象特征，选择研究路线，设计实验方案；

4.3 实验系统构建与应用：能够根据实验方案构建实验系统，安全的开展实验，正确的采集实验数据；

4.4 获得有效结论：能运用计算机技术和数据分析技术，结合相关原理对实验数据进行分析 and 解释，并通过信息综合得到合理有效的结论。

5. **使用现代工具：**能够根据信息安全领域复杂工程问题的设计、预测、模拟和开发需要，开发、选择与使用适当的技术、软硬件资源、现代工程研发工具和信息技术工具，并能够理解其局限性。

5.1 工具使用方法：了解信息安全专业常用的现代仪器、信息技术工具、工程工具和模拟软件的使用原理和方法，并理解其局限性；

5.2 分析与设计工具：能够选择与使用恰当的设备、信息资源、工程工具和模拟软件，对信息安全领域复杂工程问题进行分析、计算与设计；

5.3 模拟与预测工具：能针对信息安全具体对象，通过组合、选配、改进、二次开发等方式使用现代工具进行模拟和预测，以满足特定需求，并能分析其局限性。

6. **工程与可持续发展：**在解决信息安全领域复杂工程问题时，能够基于信息安全相关背景知识，分析和评价工程实践对健康、安全、环境、法律以及经济和社会可持续发展的影响，并理解应承担信息安全工程师的责任。

6.1 行业标准与法规：了解信息安全领域的技术标准体系、知识产权，以及有关环境保护和可持续发展等方面的方针、政策和法律法规，并理解其理念和内涵；

6.2 正确评价：能站在环境和社会可持续发展的角度，分析与评价信息安全实践对健康、安全、环境、法律以及经济和社会可持续发展的影响，并理解应承担的责任。

7. 工程伦理和职业规范：有工程报国、为民造福的意识，具有良好的人文社会科学素养、社会责任感，能够理解和践行工程伦理，能够在信息安全实践中理解并遵守与本专业有关的政策、法律、法规，自觉遵守工程职业道德和规范。

7.1 科学素养：具有人文社会科学素养，树立和践行社会主义核心价值观，尊重生命、关爱他人、主张正义、诚信守则，恪守工程伦理，理解并遵守工程职业道德和规范，尊重相关国家和国际通行的法律法规，具有思辨能力、处事能力和科学精神；

7.2 社会责任：具有较强的社会责任感，能在信息安全实践中理解和践行工程伦理，自觉履行工程师对公众安全、健康和福祉的社会责任，理解包容性、多元化的社会需求。

8. 个人和团队：具有团队意识和团队协作能力，能够在多样化、多学科背景下的团队中承担个体、团队成员以及负责人的角色。

8.1 团队精神：充分理解信息安全建设中团队的重要性，能在多学科、多元化、多形式的团队中与其他团队成员进行有效地、包容性的沟通与合作，具有合作精神与意识；

8.2 个体责任：正确理解团队成员的个体责任，能在团队中独立承担任务，合作开展工作，完成信息安全实践任务；

8.3 领导能力：具备一定的团队管理能力，能合理分配成员角色与责任，并协调和指挥团队完成工作。

9. 沟通：能够就信息安全领域复杂工程问题与业界同行及社会公众进行有效沟通和交流，包括撰写报告和设计文稿、陈述发言、清晰表达或回应指令，能够在跨文化背景下进行沟通和交流，理解、尊重语言和文化差异。

9.1 沟通能力：具有良好的沟通能力，能就专业问题，以语言表达、文稿、图表等多种形式准确表达自己的观点、回应质疑，理解并包容与业界同行及社会公众交流的差异性；

9.2 国际视野：具有一定的国际视野，了解本专业领域的国际发展趋势、研究热点，理解和尊重世界不同文化的差异性和多元化，并具备跨文化交流的语言和书面表达能力，能就信息安全专业问题，在跨文化背景下进行基本沟通交流。

10. 项目管理：具有一定的信息安全项目管理能力，能理解并掌握工程项目中涉及的管理与经济决策方法，并能在多学科环境中应用。

10.1 管理方法：正确理解信息安全项目中涉及的经济与管理因素，掌握相关工程管理原理与经济决策方法；了解信息安全及产品全周期、全流程的成本构成，理解其中涉及的工程管理及经济决策问题；

10.2 有效管理：能在多学科环境下，综合运用工程管理知识与经济决策方法，有效组

织和管理信息安全建设。

11. **终身学习**：具有自主学习、终身学习和批判性思维的意识 and 能力，能够理解广泛的技术变革对工程和社会的影响，适应新技术变革。

11.1 学习意识与能力：能在最广泛的技术变革背景下，认识到自主和终身学习的必要性；掌握自主学习的基础知识和方法，了解获取知识和能力的有效途径，能理解技术问题、归纳总结并提出问题，具备批判性思维和创造能力；

11.2 个人发展：能针对个人职业发展，采用合适的自主学习方法，不断更新完善知识体系，接受与应对新技术、新事物和新问题带来的挑战。

三、主干学科

网络空间安全（0839）。

四、专业主干课程

人工智能、应用密码学、网络编程技术、编译与反编译、网络对抗技术、逆向分析技术、恶意代码分析与检测、物联网安全、无线网络与移动终端安全。

五、学制、修业年限、（分流学期）及授予学位

学制 6 年，涵盖 4 年本科培养阶段与 2 年研究生培养阶段，大四与研一阶段融合为一年培养。不能按时毕业者，可以将学习时间延长至 7 年。符合郑州大学授予学士学位规定，授予工学学士学位；符合郑州大学授予硕士学位规定，授予工学硕士学位。

六、毕业学分要求

本科阶段，须修满培养方案中规定的 160 学分（其中通识课程 57 学分、专业课程 88 学分、个性化课程 15 学分），方准毕业。

研究生阶段，须修满培养方案中规定的课程学分至少 26 学分（其中公共必修课程 4 学分、公共基础课程 2 学分、专业基础课程 10 学分、学术活动和实践环节各 1 学分、专业选修课程不少于 8 学分）和论文学分 18 学分（其中开题报告、中期考核、预答辩各 2 学分，学位论文 12 学分），方准毕业。

七、主要实践性教学环节

实践性教学环节主要包括：编程能力实训、网络空间安全创新实践（I）、网络空间安

全创新实践（II）、网络空间安全创新实践（III）、安全漏洞分析综合实训（I）、安全漏洞分析综合实训（II）、网络安全前沿技术实训、网络空间安全综合演练和毕业设计。

1、编程能力实训

作为网络空间安全竞赛训练的前置基础，培养学生在网络攻防对抗领域具备的正向编程开发能力。主要包括 C/C++、Python、Java、汇编语言、PE/ELF 文件格式、Web 前后端开发技术、HTML/CSS/JavaScript 基础、网络协议分析等知识。

2、网络空间安全创新实践（I）

培养学生的网络空间安全竞赛基础能力，使学生掌握网络空间安全竞赛的主要解题思路、工具链使用、学习竞赛平台的使用，能够学习和复现国内外社区中低难度题目，提高学生独立完成签到题或低难度题目的能力。

3、网络空间安全创新实践（II）

面向具备网络空间安全竞赛基础的学生，培养特定方向的高阶竞赛能力。使学生能够独立做出国家级赛事的中等难度题目。主要包括复杂漏洞链构造、新型网络协议安全缺陷解析、HTTP/2 协议状态机、WebSocket 安全机制等。

4、网络空间安全创新实践（III）

培养学生复现高难度网络空间安全竞赛题目的能力。主要包括突破现代防护机制、对抗控制流混淆技术、动态脱壳技术、CSP 策略绕过技术、现代框架安全、Django/Flask 安全配置等。

5、安全漏洞分析综合实训（I）

培养学生在真实场景中系统掌握软硬件或漏洞分析的能力，为安全研究、渗透测试及漏洞防御工作奠定坚实基础。主要包括漏洞复现、动态调试、流量分析、逆向分析、漏洞定位等。

6、安全漏洞分析综合实训（II）

培养学生漏洞发现和分析的高阶能力，从软件安全开发缺陷和 Web 漏洞原理出发，结合源码审计技术、混合调试技巧，使学生能够深度剖析真实目标漏洞。通过独立或团队项目挑战真实场景的漏洞挖掘，使学生掌握攻防对抗、安全研究及产品防御体系构建的核心技术。

7、网络安全前沿技术实训

培养学生在真实场景中探索、复现及验证学术前沿成果的能力。引导学生深入剖析前沿高水平论文的创新思路和技术实现，培养学生的批判性思维与技术创新能力，为其参与高水平科研、应对新兴威胁及开发原创安全工具奠定基础。

8、网络空间安全综合演练

培养学生攻防兼备的战术思维能力、工具链集成能力及自动化防御策略设计能力，提升学生在真实网络对抗场景下的攻防实战能力与协作意识。课程构建高仿真网络攻防演练环境，结合实战化复盘，涵盖“信息收集-漏洞挖掘-攻防对抗-溯源反制”全链条。

9、毕业设计

培养学生综合运用所学的专业知识，形成对专业方向的清晰思路，结合领域技术发展，完成具有一定难度和创新性的项目设计、开发和测试，或者网络空间安全技术的实践与创新，并撰写格式规范的毕业论文。

八、学分、学时汇总表

表 8.1 本科阶段学分、学时汇总表

			通识 通修 课程	通识 分类 课程	核心 通识 课程	专业 基础 课程	专业 核心 课程	个性化 课程	其中实践 学分/学时	备注
学期 学分 与学 时	一	学分	11	8	——	4		——	3	23
		学时	208	128	——	72		——	56	408
	二	学分	6.5	11		3	1		6	21.5
		学时	120	176		56	24		88	376
	三	学分	9			11			5	20
		学时	160			192			152	352
	四	学分	9			17	2		8	28
		学时	160			288	32		120	480
	五	学分	0.5			3	13		3.5	16.5
		学时	8			56	228		156	292
	六	学分	2			2	13.5		6	17.5
		学时	32			32	240		96	304
	七	学分					5.5	15	4	20.5
		学时					120	216	96	336
	八	学分			——		13		19	13
		学时			——		456		456	456
合计		学分	38	19	——	40	48	15	54.5	160
		学时	688	304	——	696	1100	280	1220	3068
占总学分比例			23.75%	11.88%	0.00%	25.00%	30.00%	9.38%	34.06%	100.00%
占总学时比例			22.43%	9.91%	0.00%	22.69%	35.85%	9.13%	39.77%	100.00%

注：实践总学分包含综合实践 25 学分、课内实践合计 29.5 学分，共计 54.5 学分，占总学分比例 34.06%。

表 8.2 研究生阶段学分汇总表

项目	子项目	学分	备注
课程学分	公共必修课	4	≥26 学分
	公共基础课	2	
	专业基础课	10	
	学术活动	1	
	实践环节	1	
	专业选修课	≥8	
	公共选修课		
	补修课程		
论文学分	开题报告	2	18 学分
	中期考核	2	
	预答辩	2	
	学位论文	12	

注:

①研究生必须根据培养计划通过课程考试或考查。学位课考试成绩大于或等于 75 分（百分制）方可取得学分，其他课程大于或等于 60 分可取得学分。

②课程学习 16 学时计作 1 学分，培养环节中研究生参加学术论坛或听学术报告 1 学分，进行实践训练 1 学分，其他不计入学分。

九、本硕贯通实验班教学计划及修习要求

（一）通识课程

通识课程要求修满 57 学分，占总学分比例 35.63%。课程设置详见下表。

课程类型	课程编号	课程名称（英文名）	学分	学时		各学期计划学分								备注
				理论	实验	1	2	3	4	5	6	7	8	
通识课程	通识通修课程	392053 思想道德与法制 Morality & Fundamentals of Law	3	32	16	3								
		331002 国家安全教育 National Security Education	1	8	8		1							
		397005 “四史”教育专题 Special Topics on the Education of the “Four Histories”	1	8	8		1							
		391026 毛泽东思想和中国特色社会主义理论体系概论 Introduction to Maoism and Chinese Characteristic Socialism Theory System	3	32	16			3						

391024	中国近现代史纲要 Outline of Chinese Modern History	3	3 2	1 6			3						
392052	马克思主义基本原理 Basic Principle of Marxism	3	3 2	1 6			3						
391027	习近平新时代中国特色社会主义思想概论 Outline of Xi Jinping's New China's Socialist Ideology	3	3 2	1 6			3						
491001	体育（I） Physical Education（I）	1	3 2	0	1								
491002	体育（II） Physical Education（II）	1	3 2	0		1							
491003	体育（III） Physical Education（III）	1	3 2	0			1						
491004	体育（IV） Physical Education（IV）	1	3 2	0				1					
371047	大学英语（I） College English（I）	2	3 2	0	2								
371070	大学英语（II） College English（II）	2	3 2	0		2							
371060	大学英语（III） College English（III）	2	3 2	0			2						
371061	大学英语（IV） College English（IV）	2	3 2	0				2					
371075	大学俄语（I） College Russian（I）	2	3 2	0	2								
371048	大学俄语（II） College Russian（II）	2	3 2	0		2							
371030	大学俄语（III） College Russian（III）	2	3 2	0			2						
371031	大学俄语（IV） College Russian（IV）	2	3 2	0				2					
371071	大学日语（I） College Japanese（I）	2	3 2	0	2								
371072	大学日语（II） College Japanese（II）	2	3 2	0		2							
371036	大学日语（III） College Japanese（III）	2	3 2	0			2						
371037	大学日语（IV） College Japanese（IV）	2	3 2	0				2					
371073	大学德语（I） College German（I）	2	3 2	0	2								
371074	大学德语（II） College German（II）	2	3 2	0		2							
371042	大学德语（III） College German（III）	2	3 2	0			2						
371045	大学德语（IV）	2	3	0				2					

任选完成
其中一种
外语类课
程修习

课 程	基 础	772061	程序设计（II） Advanced Programming	3	3 2	2 4		3						劳动教育 4 学时
		772068	数字电路与数字系统 Digital Circuit and Digital Systems	3	3 2	2 4		3						劳动教育 2 学时
		772019	计算机组成原理 Computer Architecture	4	6 4	0		4						劳动教育 4 学时
		772067	数据结构 Data Structures	4	4 8	2 4		4						劳动教育 4 学时
		772164	计算机网络 Computer Network	3	3 2	2 4			3					
		772017	操作系统原理 Operating System Principle	4	6 4	0			4					
		772065	汇编语言与嵌入式技术 Assembly Language and Embedded Technology	3	3 2	2 4			3					
		772066	网络科学导论 Introduction to Network Science	3	3 2	1 6			3					劳动教育 4 学时
		773302	信息安全数学基础 Mathematical Basis of Information Security	4	6 4	0			4					
		772159	数据库原理及应用 Principles and Applications of Database	3	3 2	2 4				3				
		773351	网络安全法规与标准 Cybersecurity-related Laws and Technical Specifications	2	3 2	0					2			
	专 业 核 心	774005	人工智能 Artificial Intelligence	2	3 2	0			2					
		773378	应用密码学 Applied Cryptography	4	4 8	2 4				4				劳动教育 2 学时
		773363	网络编程技术 Network Programming	2	2 4	1 2				2				劳动教育 4 学时
		773338	编译与反编译 Compiling and Decompiling	3	4 8	0				3				
		773364	网络对抗技术 Network Countermeasure Technology	4	4 8	2 4				4				劳动教育 2 学时
		773366	逆向分析技术 Reverse Analysis Technology	2	2 4	1 2					2			劳动教育 2 学时
		773367	恶意代码分析与检测 Malicious Code Analysis and Detection	2. 5	3 2	1 2					2 . 5			
		773368	物联网安全	2.	3	1					2			

课程类别		课程编号	课程名称 (英文名)	学分	学时		各学期计划学分								备注
					理论授课	实验实践	1	2	3	4	5	6	7	8	标明所含 劳动教育 /国际教育 学时
进阶模块A (软件安全)	进阶限选课程	775208	网络空间安全创新实践（I） Innovative Practice of Cyberspace Security （I）	1		24		1							
		773361	网络空间安全创新实践（II） Innovative Practice of Cyberspace Security （II）	3		72			3						
		773362	网络空间安全创新实践（III） Innovative Practice of Cyberspace Security （III）	1		24				1					
		773365	安全漏洞分析综合实训（I） Vulnerability Analysis Comprehensive Practical Training （I）	3		72					3				
		773372	安全漏洞分析综合实训（II） Vulnerability Analysis Comprehensive Practical Training （II）	1		24						1			
	进阶任选课程 (须修满4学分)	774052	数理逻辑与图论 Mathematical Logic and Graph Theory	4	64	0			4						
		774287	软件工程与软件安全 Software Engineering and Software Security	3	32	24						3			
		774294	移动应用系统设计与开发 Mobile Application System Design and Development	3	32	24						3			
		774242	嵌入式系统安全 Embedded System Security	3	32	24						3			
		774277	对抗机器学习 Adversarial Machine Learning	3	32	24						3			
		774274	大模型安全 Large Model Security	3	32	24							3		
		774279	鸿蒙操作系统与应用开发 Harmony Operating System and Application Development	3	32	24							3		

	模块须修满学分数		13		开设课程总学分数					31		
进阶模块 B (密码工程)	进阶限选课程	775208	网络空间安全创新实践 (I) Innovative Practice of Cyberspace Security (I)	1		24		1				
		773361	网络空间安全创新实践 (II) Innovative Practice of Cyberspace Security (II)	3		72		3				
		773362	网络空间安全创新实践 (III) Innovative Practice of Cyberspace Security (III)	1		24			1			
		773365	安全漏洞分析综合实训 (I) Vulnerability Analysis Comprehensive Practical Training (I)	3		72				3		
		773372	安全漏洞分析综合实训 (II) Vulnerability Analysis Comprehensive Practical Training (II)	1		24				1		
	进阶任选课程 (须修满 4 学分)	774052	数理逻辑与图论 Mathematical Logic and Graph Theory	4	64	0			4			
		774316	密码前沿技术 Frontier Cryptography	1	16	0					2	
		774302	密码嵌入式设计与实现 Design and Implementation of Embedded Cryptographic System	2	32	0				2		
		774304	商用密码算法应用 Application of Commercial Cryptography Algorithms	2	32	0				2		
		774305	密码芯片设计 Cryptographic Chip Design	2	32	0					2	
		774306	密码应用创新实验 Innovation Experiments of Cryptographic Application	1	0	24				1		
		774081	密钥管理与 PKI 技术 Key Management and PKI Technology	2	32	0					2	
		774307	密码测评 Cryptographic Compliance Assessment	3	32	24					3	
	模块须修满学分数		13		开设课程总学分数					26		

2. 跨学科模块

无。

3. 创新创业模块

学生可选择创新创业模块课程，作为个性化课程学分，所有个性化修习路径须修习创新创业类课程至少 2 学分。课程模块以教务部每年发布内容为准。

（四）暑期小学期

实验班结合专业特色，利用暑期小学期开展学科综合创新实践和实训，以相关合作企业项目作为实网实战实践案例，同时开设体现科学前沿、知识交叉的学术讲座和研讨等。

其他活动类别/ 课程类别	其他活动编号/ 课程编号	教学活动名称 /课程名称	学 分	学时		各学期计划学分				备注 标明所含 劳动教育 /国际教育 学时
				理论 授课	实验 实践	2 学 期末	4 学 期末	6 学 期末	8 学 期末	
课程	773361	网络空间安全创新实践 (II) Innovative Practice of Cyberspace Security (II)	3		72	3				
课程	773365	安全漏洞分析综合实训 (I) Vulnerability Analysis Comprehensive Practical Training (I)	3		72		3			
课程	773373	网络安全前沿技术实训 Advanced Cybersecurity Technologies Practical Training	3		72			3		

（五）研究生阶段教学计划

课程类型		课程代码	课程名称	学时	学分	开课学期	备注
必修 课	公共必修课	995100202	中国特色社会主义理论与实践研究★ Research on the Theory and Practice of Socialism with Chinese Characteristics	32	2	1	必修
		995100102	英语★ English	32	2	1	
	公共基础课	995300302	数理统计与随机过程★ Mathematical Statistics and Random Processes	32	2	2	必修
	专业基础课	335511802	计算系统安全★	32	2	1	必修

			Secure Computer Systems				
		335511902	网络安全★ Network Security	32	2	1	
		335510202	高级计算机网络★ Advanced Computer Network	32	2	1	
		335510102	现代密码学 Modern Cryptography	32	2	1	
		335511502	高级网络安全技术 Advanced Network Security Technology	32	2	2	
	学术活动	995400201	学术活动 Academic Report		1	3,4	必修
	实践环节	995400101	实践环节 Teaching Practice		1	3,4	必修
	专业选修课	335511102	高级人工智能 Advanced Artificial Intelligence	32	2	2	至少 选两 门
		335616902	软件安全 Software Security	32	2	1	
		335510502	算法设计与复杂性理论 Design of Algorithm and Theory of Complexity	32	2	1	
		335617002	安全协议设计与分析 Analysis and Design of Security Protocols	32	2	2	
		335616402	新技术安全 New Technology Security	32	2	1	
		335508402	自然语言处理 Natural Language Processing	32	2	2	至少 选三 门
		335611401	研究生论文写作指导 Postgraduate Research Article Writing	16	1	1	
		335611001	计算机科学与技术（全英） Computer Science and Technology	16	1	2	
		335611101	数据挖掘 Data Mining	16	1	1	
		335611501	云计算安全 Cloud Computing Security	16	1	2	
		335611701	代码安全与漏洞分析 Code Security and Vulnerability Analysis	16	1	2	
		335611801	算法安全 Security of Algorithm	16	1	2	
		335611901	硬件安全技术 Hardware Security	16	1	2	
		335607901	Petri 网理论 Petri network Theory	16	1	2	
		335616501	密码算法分析 Analysis of Cryptographic Algorithm	16	1	2	
		335616601	隐私保护 Privacy Preserving	16	1	2	
		335616701	信息隐藏 Information Hiding	16	1	2	
		335616801	信息内容安全原理 Principles of Information Content Security	16	1	1	

		335615701	密码工程数学基础 Mathematical foundation of Cryptographic Engineering	16	1	1	
		335616301	区块链原理 Principles of Blockchain	16	1	1	
	公共选修课	可在全校博士、硕士课程中选修					
	补修课	需在网络安全相关专业本科主干课程中选修					

注：标★课程为学位课

十、科研要求

研究生阶段，科研成果要求按照《郑州大学硕士研究生科研成果基本要求》和《网络安全学院硕士研究生科研成果基本要求》执行。

十一、学位论文

研究生阶段，学位论文是研究生培养的重要环节，研究生在修完学位课程并完成规定学分后，可以开展学位论文工作。研究生在导师或导师组指导下完成学位论文，导师为第一责任人，对论文质量全程把关。论文工作包括论文选题、开题报告、中期检查、论文撰写、论文预答辩、论文答辩等环节。硕士研究生必须在第三学期末之前进行学位论文开题报告；论文中期考核应在完成学位论文开题报告后的半年内进行；论文预答辩一般安排在学位论文专家通讯评审前，距正式答辩时间至少 2 个月。

学术学位硕士研究生修满培养计划内所有学分，并通过论文答辩，则准予毕业；经培养单位学位评定分委员会和本学部学位评定委员会审核，报校学位评定委员会讨论通过后授予学位。学位授予按照《郑州大学学位授予基本标准》执行。

十二、培养方式与方法

研究生阶段，采用全日制研究生管理模式集中在校学习，实行导师个人负责和导师团队联合指导相结合的培养模式。研究生的思想政治、科研指导和质量把关由其导师负责。导师团队参与科研方向的把握、科研课题选定、中期检查、预答辩和答辩等全过程的指导工作。

注重发挥研究生的主动性和自觉性，更多地采用启发式、研讨式的互动教学方式。研究生必须参加学术讲座、学术报告、讨论班、暑期课程、社会实践和社会调查，并获得相应的学分。鼓励硕士研究生参加省级以上网络安全竞赛，获得省级二等奖以上、国家级三等奖以上者可以直接取得学术/实践活动学分。鼓励硕士研究生出国访学、开展科研合作、参加国

际会议，开阔视野并提高专业外语交流能力。采取课程学习和科学研究相结合，讲授与讨论相结合，课内教学与课外实践相结合等多种形式进行培养。

加强学位论文全过程管理，严格考核程序，严控学术道德与学术规范。对不适合继续攻读硕士学位者进行分流淘汰处理，确保研究生的培养质量。