

河南教育信息化

HENAN EDUCATIONAL
INFORMATIZATION

2020年第03期总第 21 期

本期热点

校园网络安全防护



主管：河南省教育厅科学技术与信息化处
主办：河南省教育科研计算机网络中心

目录 CONTENTS

期刊简介

《河南教育信息化》立足河南，刊载行业动态、热点专题、经验交流及省内资讯等内容，多方位、多层次地探究教育信息化建设的前沿趋势、建设中的经验与问题，为教育信息化领域各级领导及从业人员提供科学、实用的决策依据。

动态

- 人力资源社会保障部上线“高校毕业生就业服务平台” 4
- 2020 全球智慧教育大会线上线下融合召开 免费向公众开放 4
- 5G 新阅读体验中心将落地国家图书馆 4
- 2020 年首场教育金秋系列发布会:高校秋季学期教育教学工作要把握好三点 . 5
- 净化“网课”直播生态! 8 部门依法处置违法违规直播平台 5
- 广东率先实现高校 edu.cn 域名全覆盖 5
- 2020 年全国教育信息化工作视频会议召开 5
- 在线学习服务师等 9 个新职业发布 6
- 国家中小学网络云平台秋季学期课程资源全新上线 6
- 上海将建个人学习电子档案 6

热点

- 河南科技大学校园网络安全体系建设实践 8
- 新形势下的高校数据防护思考 16
- 构建完整的网络安全组织 良好的管理体系是关键 18
- “十四五”期间安全建设要从“攻击者视角、新型技术视角、顶层设计视角”出发 19
- 信息安全管理体的建设是策略、技术与管理的综合运用 20
- 如何在断电后安全关闭服务器 21
- 基于信息安全技术的教育数据安全与隐私保护 25

人物 & 成果

- 智慧校园建设要向数据要“效益”——访南阳理工学院信息化建设与管理中心主任吴绍兴 27

河南教育 信息化

2020 年 / 第 03 期 / 总第 21 期

主管 河南省教育厅科学技术与信息化处
主办 河南省教育科研计算机网络中心

主编 孔繁士 王宗敏
执行主编 汪国安
编辑 吕玉玲
设计 蔡馨庆 吉祥

电话 0371-67763770
传真 0371-67763770
电子邮箱 editor@ha.edu.cn
通信地址 郑州市二七区大学路 75 号郑州大学
南校区逸夫楼西 206 室
邮政编码 450052



扫一扫
关注河南教育信息化
更多精彩内容
为您呈现!

教学信息化

研究导向型理念在线上课程高阶学习中的应用 ·····	30
----------------------------	----

智慧校园

郑州铁路职业技术学院:智慧校园环境下面向服务的校园一卡通系统的建设与实践 ·····	36
郑州升达经贸管理学院:智能门锁 助力智慧校园建设 ·····	40

资讯

2020 年度河南省教育信息化优秀成果奖获奖名单公布 ·····	43
2020 年河南省高校网络安全宣传周“校园日”活动在河南农业大学启动 ·····	43
南阳理工学院与中国移动南阳分公司举行“5G+ 智慧校园战略合作签约仪式” ·····	44
河南理工大学举办 2020 年网络安全等级保护测评培训会 ·····	45
信阳学院:信息化建设与管理处多措并举保障新生顺利报到 ·····	46
郑州铁路职业技术学院与郑州联通签署“5G 智慧校园建设”合作协议 ·····	47
鹤壁职业技术学院与鹤壁联通举行 5G 智慧校园战略合作协议签约仪式 ·····	47
全省网络安全督查组到华北水利水电大学指导工作 ·····	48
安阳工学院:现代教育技术中心组织开展全校新网站群线上技术培训 ·····	49
省教科网暨省互联网协会下一代互联网工委 2020 年信息安全技术研讨会线上召开 ·····	49



征稿简则

·····	51
-------	----

声明:《河南教育信息化》中注明稿件来源为其他媒体的稿件为转载稿,如涉及版权问题,请作者在两周内来电或来函联系。转载或引用《河南教育信息化》稿件,请注明作者及来源《河南教育信息化》。

动态

人力资源社会保障部上线“高校毕业生就业服务平台”

9月1日，人力资源社会保障部上线“高校毕业生就业服务平台”，联通全国服务资源，搭建高校毕业生和用人单位高效对接通道，向高校毕业生提供不间断常态化就业服务。

平台上线当天发布岗位量达27万个，后续将持续动态更新招聘岗位。推出“职业指导公开课”和“职业指导直播课”，发布职业规划、求职技巧、就业手续、创业指导等微视频，职业指导师、人力资源服务专家、创业指导专家等将在线开展就业创业指导交流。发布见习岗位、见习政策、岗位申请入口等，提供多元实践机会。各级公共就业人才服务机构将同步联动上线本地服务平台。

此外，服务平台还加载“未就业高校毕业生求职登记小程序”，支持毕业生自主登记求职意向、就业服务需求，帮助毕业生“一键直达”公共就业服务。同步设大中城市联合招聘高校毕业生生活专区，推出跨区域联合招聘会和服务活动。（新华网）

2020全球智慧教育大会线上线下融合召开 免费向公众开放

8月20日-22日，经教育部批准，由北京师范大学主办，北京师范大学智慧学习研究院、中国教育与社会发展研究院、中国基础教育质量监测协同创新中心、互联网教育智能技术及应用国家工程实验室承办的“2020全球智慧教育大会”通过线上线下融合的方式召开。大会免费向公众开放，公众可通过直播观看。

大会会议主题为“人工智能与未来教育”，核心议题包含人工智能催生未来教育新形态，智能技术促进教育公平与人的发展，智慧乡村、智慧教育发展的成果和趋势，新冠疫情为全球教育带来的机会和挑战。会议邀请了院士、全球知名专家学者、国际组织代表、政府部门、一线教育工作者和企业界人士围绕多个热点和焦点议题展开深入研讨，会议共开启了12个专题论坛，内容丰富前沿，为公众带来了一场全球思想盛宴。（互联网教育国家工程实验室）

5G新阅读体验中心将落地国家图书馆

8月6日，国家图书馆、中国图书进出口（集团）总公司、华为公司在京签署战略合作协议，将共同推进5G时代新阅读。随后，国家图书馆将设立5G新阅读体验中心。

“身临其境、浸在眼前”，在中图集团演示的未来的5G新阅读场景中：使用手机应用就可以全景进入国家典籍博物馆参观“甲骨文记忆展”；可以线上360°全景“走进”红楼公共藏书楼，从书架上点开一本《陆游诗选》即可阅读电子版；置身多面屏环绕的全景空间，刘慈欣的科幻漫画书变成动画，可以读、可以看、可以听。5G+阅读，打破了空间和媒介的界限，延伸了知识获取的途径，更新了人们的阅读体验。

“当前，以5G等新一代信息技术为代表的新一轮科技革命和产业变革正在快速孕育兴起，以数字化知识信息作为关键生产要素的数字经济蓬勃发展，知识信息服务的供需环境急剧变化。”国家图书馆馆长饶权说，无论是公共文化服务机构，或是数字文化产业，在新技术环境下都将面临新的机遇与挑战。打造基于5G、全景视频、全息影像等新技术的沉浸式阅读体验，作为国家级公共文化服务机构，国家图书馆一直积极探索应用现代技术手段创新服务方式、提升服务效能。（《光明日报》）

2020年首场教育金秋系列发布会：高校秋季学期教育教学工作要把握好三点

教育部高等教育司司长吴岩在8月27日教育部召开的2020年首场教育金秋系列发布会上，指出高校秋季学期的教育教学工作要把握好三点。

一是高校的教学模式将从上半年的线上教学为主，转变为线下教学为主、积极推进线上线下教学相结合。

二是课堂理论教学、学校实验教学和校内校外的实习实训等实践教学将全面推开。

三是针对可能出现一个学校突发的个案性疫情或一个地区多校发生疫情，相关高校要根据情况及时将线下教学转为线上线下教学相结合或全面转为线上教学。各地高校要坚持一手抓安全防范，一手抓教育教学，把“战时”在线教学的“新鲜感”转化为中国高等教育的“新常态”。

同时，吴岩指出：举办世界慕课大会、办好中国国际“互联网+”大学生创新创业大赛，是秋季学期教育部要重点推进的工作。（微言教育）

净化“网课”直播生态！8部门依法处置违法违规直播平台

8月3日，国家网信办、全国“扫黄打非”办等8部门联合召开工作部署会，通报网络直播行业专项整治和规范管理工作进展，对深入推进专项整治和规范管理工作进行再部署。国家网信办负责人强调，要强化内容治理。全面清理各类违法违规内容，净化“网课”直播生态，保护青少年健康成长。

国家网信办负责人表示，专项整治开展2个月来，各部门依法处置158款违法违规直播平台，挂牌督办38起涉直播重点案件，督促平台清理有害账号及信息，封禁一批违法违规网络主播，明确直播打赏作为平台和主播履行服务合同的法律性质，规范管理工作稳步推进，行业生态得以明显改善。

但直播行业诸多痼疾顽症并未彻底消除，其中，“网课”直播间推送低俗内容危害青少年健康成长。国家网信办负责人强调，要坚持依法治理、标本兼治、管建并举，强化部门协同，聚焦解决突出问题，压紧压实属地管理责任和平台主体责任。要强化备案准入管理、内容治理、依法治理，扎实推进规范管理。（中国网信网）

广东率先实现高校edu.cn域名全覆盖

为规范教育网站管理，保障广大考生利益，广东省教育厅于2020年4月启动普通高校统一网站标识专项整治行动，明确要求“全省普通高校网站（系统）必须全部使用edu.cn域名”。

3个月的整治工作取得显著成果。据悉，截至2020年7月底，广东154所普通高校和7所省外高校在粤办学机构网站已全部使用edu.cn域名。edu.cn正式成为广东全省正规普通高校统一的网站标识，成为广东正规高校的权威标志。此举有力提升了普通高校网站的权威性和公信力，提高了高校网站辨识度，考生和家长可以通过网站域名有效避免踩到“野鸡大学”这颗雷。

与此同时，统一使用edu.cn，也便于加强高校网站安全规范管理，破解了教育行业网络安全的源头集中管控困境。使用“edu.cn”域名的高校网站（系统）将纳入教育系统网络安全通报预警平台统一监管，由教育网提供一键断网服务，以此实现网络安全源头集中管控。（中国教育在线）

2020年全国教育信息化工作视频会议召开

7月15日，2020年全国教育信息化工作视频会议召开。会议指出，2020年是“十三五”的收官之年，是全面建成小康社会的决战决胜之年，十分关键特殊。决胜全面建成小康社会，必须优先发展教

育，办好人民满意的教育。而夯实基础，加大力度，推动教育信息化引领教育现代化，将是至关重要的一步。

为了实现教育信息化“十三五”圆满收官，会议部署了七项重点工作：一是完成好教育脱贫攻坚政治任务；二是加强教育信息化基础设施建设；三是促进优质教育资源的共建共享；四是持续提升师生信息素养；五是深化网络条件下教学模式改革；六是提高教育治理信息化水平；七是做好教育系统的网络安全保障。

“教育是国之大计、党之大计。”会议强调，坚持党对教育网信事业的全面领导，是做好教育信息化工作的根本保证。加强统筹领导，健全教育信息化管理体制，这是教育信息化全面发展的必由之路。（《中国教育网络》）

在线学习服务师等 9 个新职业发布

7月6日，人力资源社会保障部官网公布了9个新职业，包括“区块链工程技术人员”“城市管理网格员”“互联网营销师”“信息安全测试员”“区块链应用操作员”“在线学习服务师”“社群健康助理员”“老年人能力评估师”“增材制造设备操作员”等。

其中，“在线学习服务师”与教育关系最为密切。该职业的主要工作任务描述为：（1）对学习者的学习情况进行分析，提出针对性的学习规划和学习建议；（2）为学习者提供全方位、全周期的个性化指导、支持和课程管理服务，解决学习者学习过程中的技术、内容、方法等问题；（3）负责在线学习的班级管理，为学习者建立和维护在线交互社群，激发学习者的学习动机，提高学习兴趣；（4）运用分析和评价工具对学习者的学习活动和成果进行综合评价并及时反馈；（5）根据学习者体验，对学习平台、学习工具、学习资源等提出优化建议。

据介绍，此批新职业主要涉及预防和处置突发公共卫生事件领域、适应高校毕业生就业创业需要的新业态领域，以及适应贫困劳动力和农村转移就业劳动者等需要的促进脱贫攻坚领域。新职业响应了互联网技术发展催生的多样化创业就业模式以及信息技术发展对网络信用及安全提出的新要求。（《中国教育报》）

国家中小学网络云平台秋季学期课程资源全新上线

按照教育部的部署要求，为巩固春季学期“停课不停学”取得的成果，进一步推进线上线下教育教学的紧密融合，在深入总结上半年防控新冠肺炎疫情期间大规模在线教育宝贵经验的基础上，国家中小学网络云平台在“课程学习”版块全新上线了秋季学期的课程资源，覆盖小学、初中、高中的所有年级和各门学科。同春季学期资源一样，这些资源全部不用注册、免费使用。

秋季学习课程资源的落实坚持统筹规划。同北京市及其所辖有关区县的课程资源建设工作有机整合，充分发挥中央电教馆的技术优势，调集人民教育出版社、北京市区两级教研部门的专家力量参与课程录制指导和审核把关。课程资源的审查工作由北京教科院负责组织，实行“专家双审、流程双审”，保证课程质量。

课程资源组织上采用“一课一包”的形式。微课视频中学为20-25分钟、小学为15-20分钟，教师资源（教学设计、演示文稿、其他多媒体素材）和学生资源（在线学习任务单、课后练习）等通过“包”的形式供师生自主选择使用。（中央电化教育馆）

上海将建个人学习电子档案

“小到一个学生容易出现的错题，大到一个班级、一所学校大部分学生容易出现的错题、不易掌握的知识，我们都争取能做出一个图谱和画像来。”今年7月初，上海市教委相关负责人在2020世界人

工智能大会教育行业主题论坛新闻发布会上介绍，上海未来将形成覆盖基础教育阶段学生和教师的个人学习电子档案，让每一个孩子都有自己的数字画像，有一个学习情况数据库，它可以帮助教师判断孩子适合学什么、能学到什么程度、从什么角度切入更容易让孩子掌握知识。

根据上海市统计局对上海 70 多万家长、老师、学生的调查，超过 99% 的人对疫情期间的在线网课持肯定态度，“有 70% 左右的学生认为，网课老师的课程比自己原来老师上得好”。（《中国青年报》）



河南科技大学校园网络安全体系建设实践



文 / 周毅 河南科技大学网络信息中心副主任

网络空间事关国家安全，已成为国家安全的战略高地。校园网络安全是学校教育信息化的要求，也是智慧校园建设的基础，更是学校综合实力的体现。维护校园网络安全已成为学校信息化部门一项重中之重的工作，很多学校也成立了专门的网络安全部门来保障校园网的安全。

河南科技大学高度重视网络安全工作，积极探索、勇于创新，建设了校园网络安全体系。学校网络安全体系总体建设思路为“人防+技防+安服”，三方面紧密联系、相互支撑。

一、人防

人防体系建设包括四个方面：组织机构建设、管理制度建设、网络安全宣传、信息资产治理。

1. 组织机构建设

学校设立了以校长为组长的网络安全和信息化领导小组，下设网络安全和信息化办公室（网信办），由担任 CIO 的副校长担任办公室主任，负责学校的网络安全和信息化工作，为网络安全体系建设提供组织保障。

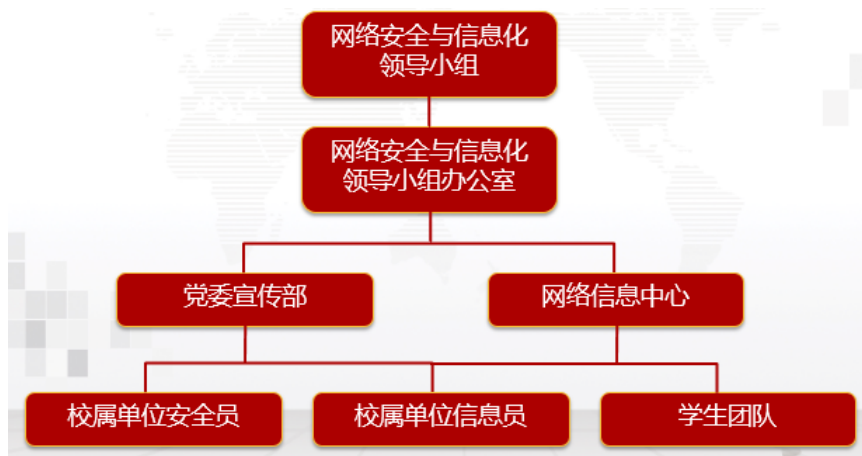


图 1 人防体系中的组织机构

2. 管理制度建设

学校制订了《河南科技大学网络信息安全管理办法》、《河南科技大学信息系统等级保护测评管理办法》、《河南科技大学网络安全事件应急处理预案》、《河南科技大学数据管理暂行办法》、《河南科技大学信息化建设与管理办法》等一系列文件，为网络安全体系建设提供制度保障。

3. 网络安全宣传

通过多种方式对学校师生进行网络安全宣传。

(1) 每年举办“网络安全宣传周”活动，积极响应国家号召，持续推进网络安全工作，全面提升广大师生的网络安全意识和安全防护技能，营造安全健康文明的网络环境。

(2) 利用网络信息中心综合服务大厅为广大师生提供病毒防护、补丁更新、正版软件安装等一站式



扫码分享 ▷

服务，并通过宣传册、书签、明白卡等各种方式普及网络安全知识。

(3) 每季度面向全校发布网络信息安全简报。在简报中会普及网络安全知识，列出近期的网络安全事件以及处置结果等。

4. 信息资产治理

学校成立了网络安全领导和管理机构，制定了一系列网络安全管理制度，怎么把这些管理制度落到实处呢？我们通过信息资产治理来具体落实了各项管理制度。

信息资产治理是落实网络安全管理制度的必要措施，是网络安全建设的必然要求，主要有三方面的原因：

(1) 信息资产增长迅速、管理难度大。以河南科技大学为例，从2013年到2020年，信息系统从9个增加到60个，网站从52个增加到将近160个，线上课程从20门增加到300多门，服务器从30台增加到200多台，数据存储从30TB增加到超过2000TB，虚拟机、容器等应用不计其数。

(2) 信息资产复杂多样、安全漏洞多。学校二级单位的信息资产在学校总信息资产中占有较大比例。二级单位多数没有信息资产管理，对本单位信息资产缺乏有效管控；同时二级单位普遍缺少技术力量，信息资产多依赖系统厂商或学生团队进行运维，安全隐患凸显。2017年3月到2019年3月，我们学校已发现的安全漏洞90%以上在二级单位自建信息系统。在2018年第一次安全服务的渗透测试安全评估中，90%以上被检二级单位信息系统发现安全漏洞。

(3) 网络安全要求高，难以达到管理要求。二级单位信息资产梳理、管理信息更新、等级保护实施等基础管理要求难以达到现阶段网络安全管理要求。单纯依靠责任传递的管理方式加剧了二级单位的管理焦虑，制约了二级单位进行信息化建设的积极性，这不是我们愿意看到的。而通过信息资产治理，我们可以首先摸清家底，然后按照网络安全的要求，对每一类信息资产制定具体的安全策略，以达到规范管理、安全管理的目的。

我们主要开展了网站类、课程类、数据类、流程类等四类信息资产治理工作。

(1) 网站类信息资产治理

通过开展网站及信息系统备案登记工作，理清了各单位网站类信息资产，形成了各单位网站类信息资产表，并制定了相应的治理措施和安全策略。

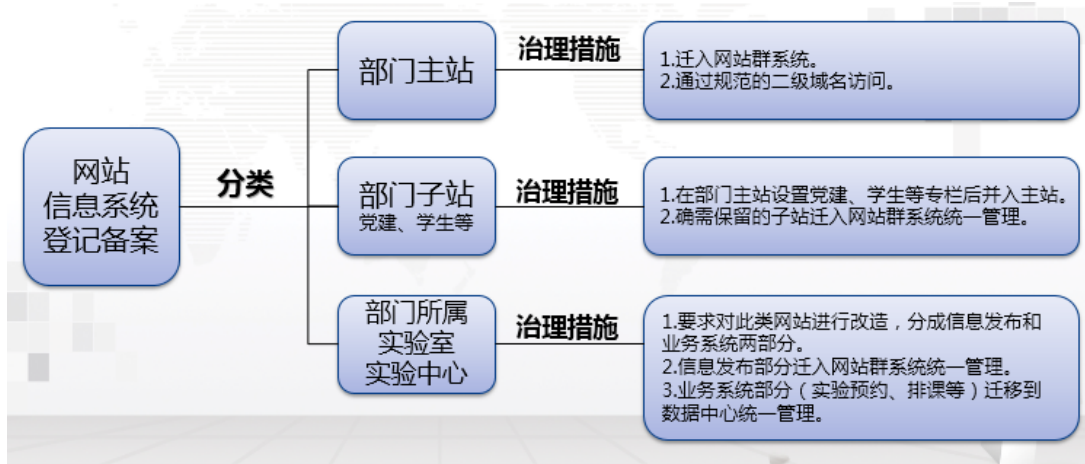


图2 网站类信息资产治理措施

全校所有部门的主站和子站迁入网站群统一管理，并使用规范的二级域名对外提供服务；通过网站群系统，为每个单位设置安全员和信息员，实现了信息发布的分级审核，明确责权。通过治理，关停17个“僵尸”网站，清理3个“双非”网站，消除了网站类，特别是各部门门户网站存在的安全隐患，落实了管理制度。

(2) 课程类信息资产治理

课程类信息资产最为复杂，安全问题也最多。通过与教务处、研究生院密切合作，理清了各单位课程类信息资产，形成了各单位课程类信息资产表，并制定了相应的治理措施和安全策略。

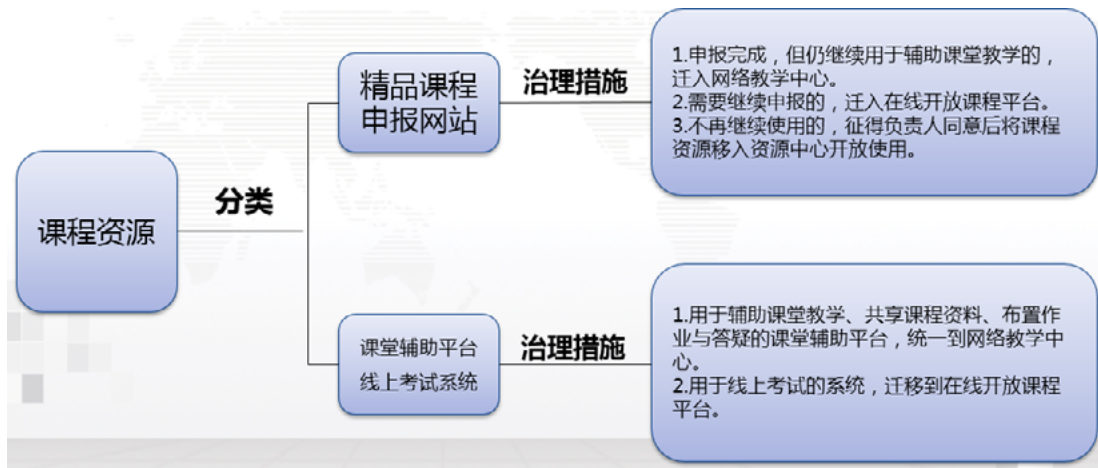


图3 课程类信息资产治理措施

经过治理，全校所有线上课程及资源移入在线开放课程平台、网络教学中心、资源中心三大平台，关停所有课程申报类网站或系统 96 个，消除了安全隐患。

(3) 数据类信息资产治理

数据是所有信息资产的核心，数据安全也是网络安全的核心。数据类信息资产治理就是数据治理。我们通过对各个业务处室、教师代表、学生代表的系统摸底——包括业务处室在使用什么业务系统、每个业务系统具有什么信息资源、需要哪些信息服务等等，做好数据和服务的摸底工作；然后根据摸底情况进行任务分配；建立数据模型，并由业务部门进行确认，最终形成权威数据。

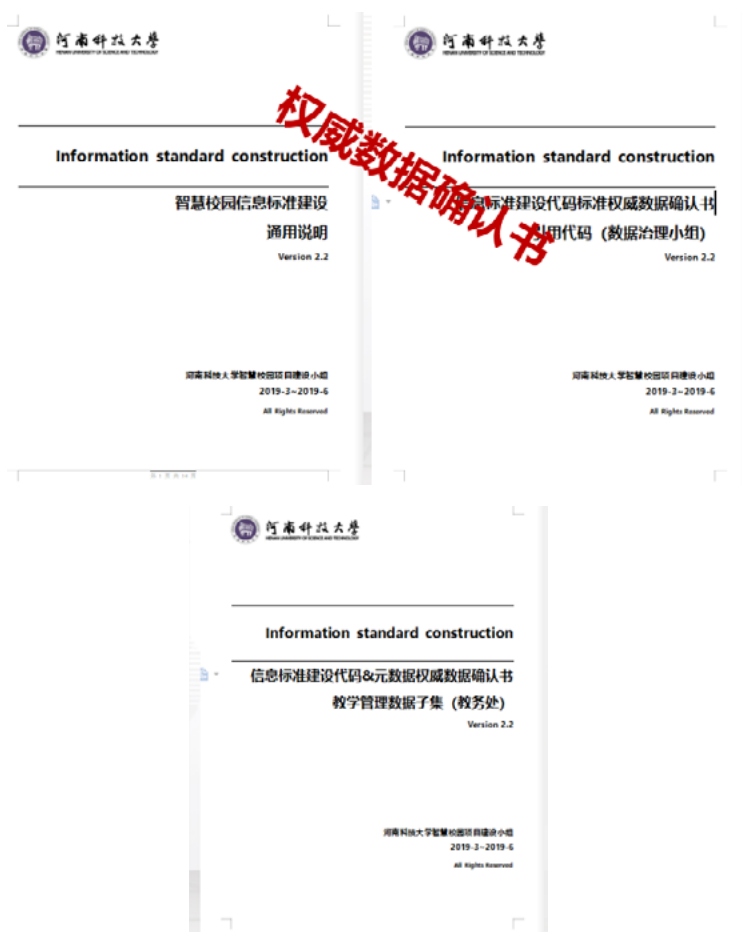


图4 权威数据确认书

(4) 流程类信息资产治理

根据《河南科技大学数据管理暂行办法》规定，我们制定了规范的数据使用流程，避免数据泄露，保证数据安全。业务部门对外提供数据（即便是自己业务系统的数据），也需要使用者签署“数据保密协议”，同时需要数据来源部门、网信办副主任以及网信办主任也就是 CIO 审批同意后，数据中心管理员才可以提供数据。

流水号: 69332 表单 公共附件 会签意见区 流程图

流程已结束

河南科技大学数据使用申请表

申请单位名称	校团委		
申请数据范围	全校2017级、2018、2019级本科生	申请数据项 (请用excel表格列出字段名、样例及说明,以附件形式上传至公共附件区)	学号、姓名、学院、专业、班级、性别
申请数据用途	大学生课外培养成绩单, 河南科技大学课外培养管理服务平台系统使用	是否阅读流程说明及承诺数据保密	<input checked="" type="radio"/> 是 <input type="radio"/> 否
联系人姓名及工号	皇甫毅	联系电话	
河南科技大学数据保密协议 (本流程“流程说明”下载, 签字并扫描后上传附件区)	数据提供给校外单位时需提供 <input checked="" type="radio"/> 是 <input type="radio"/> 否 签署		
申请单位意见	同意。		
数据中心数据管理员意见	数据来源于教务系统, 请教务领导审批。		
数据集成与信息维护工作小组意见	同意, 请数据源单位审批!		
数据来源部门意见	同意。		
校网信办副主任意见			
校网信办主任意见	同意		

公共附件

全选

第1步: 数据申请

附件名称	附件大小	创建人	创建时间
<input type="checkbox"/> 申请数据项.xlsx	8.4K	校团委	2020-06-18 12:36:46
<input type="checkbox"/> 数据保密协议.PDF	2M	校团委	2020-06-18 12:36:46

请选择打印模板:

图 5 数据使用申请表示例 1

疫情期间，教务处要提供教务系统的学生数据给中国大学 MOOC 平台，也需要签保密协议，走流程经 CIO 审批同意后才能提供数据。如下图所示。

流水号: 66725 表单 公共附件 会签意见区 流程图

流程已结束

河南科技大学数据使用申请表

申请单位名称	教务处		
申请数据范围	全体在校本科生	申请数据项 (请用excel表,学生学号、姓名、院系、专业、格列出学段名、样例及说明,以班级、身份证后六位(全部以111111替代)等六项附件形式上传至公共附件区)	
申请数据用途	新冠肺炎疫情期间,我校部分教师申请使用中国大学MOOC平台免费资源开展混合教学、学生进行线上学习,以落实“停课不停学”教学组织工作。	是否阅读流程说明及承诺数据保密	<input checked="" type="radio"/> 是 <input type="radio"/> 否
联系人姓名及工号	赵晓旭	联系电话	
河南科技大学数据保密协议 (本流程“流程说明”下载,签字并扫描后上传附件区)	数据提供给校外单位时需提供 <input checked="" type="radio"/> 是 <input type="radio"/> 否 签署		
申请单位意见	同意数据申请!		
数据中心数据管理员意见			
数据集成与信息维护工作小组意见	同意		
数据来源部门意见			
校网信办副主任意见	同意由教务处通过excel文件格式所列的5项数据按实际课程数量提供给中国大学mooc平台,以保证疫情期间的教学之所需。不得将教务系统和第三方网络产品进行直接对接。教务处作为教务系统的责任单位应按照国家和学校的相关法律法规做好教务数据的管理。		
校网信办主任意见	同意 主任意见,请教务处一定按要求做好相应工作!		

公共附件

全选 批量下载

第1步: 数据申请

附件名称	附件大小	创建人	创建时间
<input type="checkbox"/> 数据保密承诺书-教务处.jpg	2.3M	徐红玉	2020-02-21 22:05:19
<input type="checkbox"/> 中国大学mooc-学生名单模板.xls	20K	徐红玉	2020-02-21 22:05:19
<input type="checkbox"/> 公司授权证明.png	11.2M	徐红玉	2020-02-21 22:05:19
<input type="checkbox"/> 公司承诺-补充协议-信件截图.jpg	241.4K	徐红玉	2020-02-21 22:05:19

请选择打印模板:

图 6 数据使用申请表示例 2

通过人防体系建设,我们落实了各项网络安全规章制度,规范了管理,明确了责任,减轻了各单位的网络信息安全忧虑,为网络安全技防建设和安全服务指明了方向。

二、技防

技防体系建设包括骨干网络安全防护、数据中心安全防护、信息系统等保测评、安全运维四个方面。

1. 骨干网络安全防护

骨干网络安全防护目的是保护校园网络用户免受外部网络攻击威胁,同时记录校园网络用户的各种网络行为,满足上级网络安全要求,并为网络安全策略制定提供数据支持。我们在骨干网络安全防护方面主要进行了以下三方面建设。

(1) 网络出口防火墙

通过网络出口防火墙，可以基于不同的安全策略，对各类校园网络用户提供不同的安全防护，包括阻断来自外部对校园网内用户的网络威胁，以及来自校园网内用户对外部的有意或无意的网络攻击。网络出口防火墙还可以提供 IPS、DDOS、僵尸蠕、重要端口等多方位的安全防护。同时，基于防火墙虚拟化功能，我们可以为不同安全域提供不同安全防护策略。

(2) 内网威胁感知平台

内网威胁感知平台能够基于威胁情报对校园网内的安全数据进行快速、自动化的关联分析，及时发现威胁和异常；有效监控业务系统访问行为和敏感信息传播；准确掌握网络系统的安全状态；及时发现违反安全策略的事件并实时告警、记录；进行安全事件定位分析，事后追查取证，满足合规性审计要求。从而，一方面可基于多维度海量互联网安全数据，进行情报挖掘与云端关联分析，另一方面利用大数据技术进行安全数据分析和威胁溯源。

(3) 全网行为审计平台

全网行为审计平台可以全面记录网络系统中的各种会话和事件，实现对网络信息的智能关联分析、评估及安全事件的准确全程跟踪定位，与防火墙联动阻断外部用户的攻击威胁，满足上级管理部门和网安部门的网络安全要求，为网络安全策略的制定提供权威可靠的支持。

2. 数据中心安全防护

数据中心安全防护是防护体系中的重中之重。我们主要进行了以下六个方面的建设。

(1) 数据中心边界防火墙

进行数据中心安全防护时，我们主张“先把口袋扎住”。首先建立了数据中心边界防火墙，以划分数据中心和校园网络的边界。在此基础上，通过安全策略，首先关闭数据中心服务器的所有对外端口，再按需逐一开放，如提供 Web 服务的，只开放 443 端口，运维默认端口 22、3389 等全部改用其它端口，且只能通过运维审计系统访问。通过安全策略，禁止数据中心服务器访问互联网，再按需开放，如财务票据 CA 服务器就只能访问财政厅的一个 IP 或域名。同时通过调整安全策略，实现紧急情况下一键断网。

(2) 数据库审计系统

通过数据库审计系统，我们对数据中心实现了全方位的实时审计——实时监控来自各个层面的所有数据库活动，以及细粒度的行为检索——一旦发生安全事件，提供基于数据库对象（用户、表、字段及记录内容）的完全自定义审计查询及审计数据展现，摆脱数据库的黑盒状态。

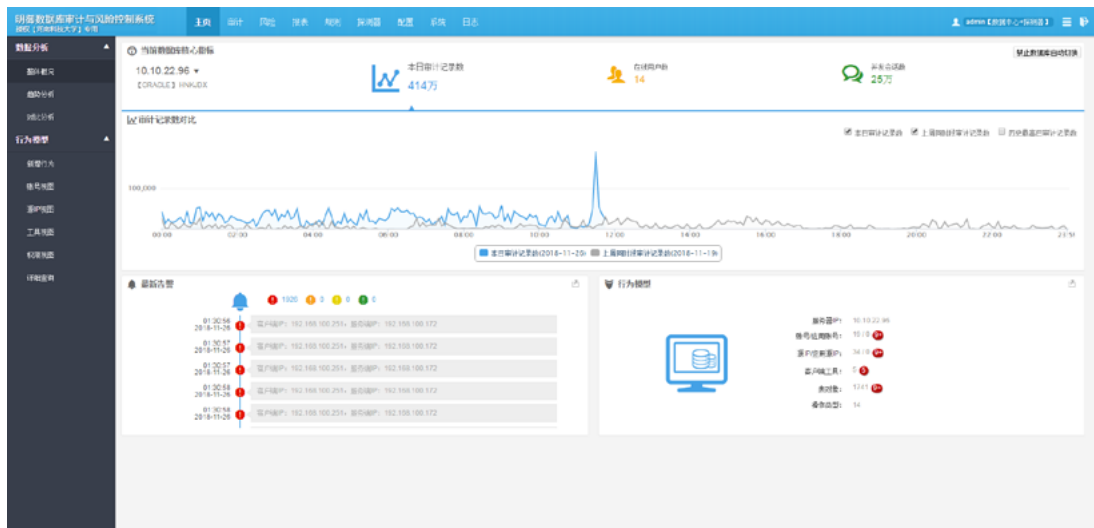


图 7 数据库审计系统

(3) 安全评估及漏洞扫描系统

在数据中心旁路我们部署了安全评估系统，定期对数据中心所有服务器及系统进行细致深入的漏洞检测、分析，主动诊断安全漏洞并提供专业防护建议和预防措施，有效地对资产进行风险管理。

(4) 虚拟化云管理与安全防护系统

数据中心有很大一部分应用为虚拟化应用。我们通过虚拟化云管理与安全防护系统统一管理数据中心的 Windows、Linux 虚拟机和物理机的病毒防护、恶意软件防护。

(5) 安全日志分析平台

学校部署了很多安全设备和服务器系统，它们本身会产生很多日志，如果我们只是孤立地看待这些日志，就很难发现问题。所以我们通过安全日志分析平台来进行日志收集、关联分析，实现多样化的安全预警。目前安全日志分析平台已收集各类日志数据超过 200TB。

(6) 异地数据容灾备份中心

目前全校所有的数据都存在数据中心，数据安全工作显得尤为重要。2019 年我们进行了异地数据容灾备份中心的建设，实现了同城异地备份。

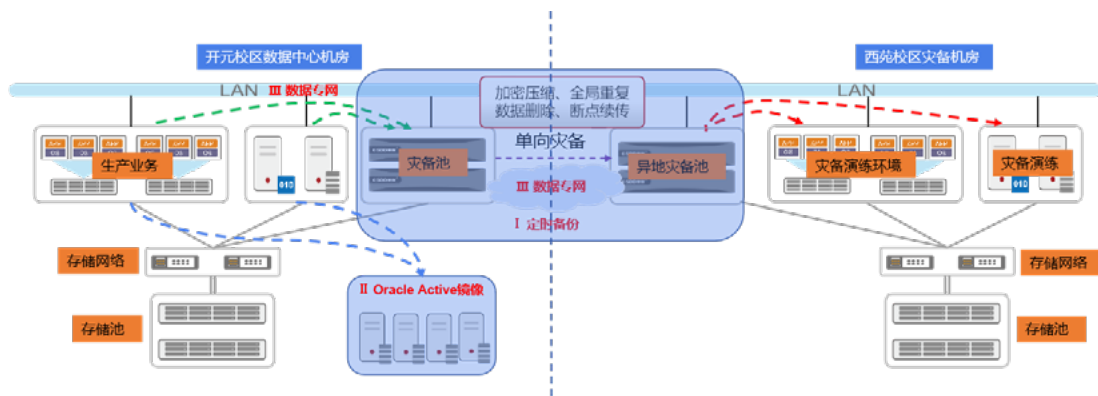


图 8 异地数据容灾备份中心

我们主要建设了三部分内容：一是定时备份，主要是各类虚拟机、文件要传输到异地；二是在本地建立了数据库实时镜像，保证生产业务系统数据库一旦出现问题，可以及时切换到数据库镜像上继续提供服务；三是建立了数据专网，实现到异地和本地数据中心内部的数据备份实时性，同时数据备份时是对网络带宽消耗非常大的时候，数据专网与业务网分开可以保证数据备份时不会影响业务系统的正常运行。

3. 信息系统等保测评

对于信息系统等保测评，国家一直都有明确的要求，且在 2017 年把实施网络安全等级保护制度写入了《网络安全法》，在 2019 年 5 月又提出了等级保护 2.0 标准。根据国家及教育部门提出的对信息系统等级保护的要求，我们采用了统一申报、合理打包、集中测评的方式对信息系统进行等级保护测评，形成等保合规的长效工作机制。具体来讲：

统一申报：由各信息系统主管部门做预算时向网信办统一申报进行等保测评。

合理打包：网信办将各部门申报的等保测评需求合理打包。

集中测评：通过公开招标，选定测评公司进行信息系统集中等保测评。

滚动实施：由于等保测评证书的有效性限制，采用滚动实施测评的方式，使等保测评工作成为每年的常规工作，等保测评经费成为常规支出经费。

4. 安全运维

通过运维审计与风险控制系统，为每一个信息系统设置“三员”：运维员、运维管理员、运维审计员，实现分级运维，保障运维安全。运维员一般由业务系统管理员或厂商运维人员担任。管理员一般由

各单位信息安全员担任。审计员一般由单位主管安全的领导担任。运维实行两级审批管理：运维员在系统中提出运维申请，运维管理员审批通过后，运维员才能进行运维。运维审计员可以对运维过程进行全程审计。

同时，我们也采用了其他一些方法进行安全防护，如：（1）负载均衡和反向代理：增加反向代理和负载均衡设备，用于内网资源的安全对外发布。通过反向代理，可以避免数据中心内部服务器直接暴露于互联网上。同时还可以设置安全规则，保证所发布资源的安全。（2）Web 应用防护：设置详细的 WAF 防护策略，进一步保障 Web 应用安全。（3）全部网站启用 HTTPS 协议：自 2019 年始，通过购买泛域名 SL 证书，实现学校所有网站启用 HTTPS 协议。

三、安服

购买和选择安全服务，我们主要考虑四个方面：实现网络安全评估、系统安全策略加固、特殊时期安保支持、系统上线安全评估。目的是为了弥补学校网络安全维护人员严重不足的问题，实现定期对学校的所有信息系统进行安全评估及渗透测试，找出安全隐患，协助安全加固。

在脆弱性评估方面，安全服务可以实现：（1）开放端口探测：发现数据中心网络中开放的业务端口，形成端口信息表。（2）系统漏洞探测：测试数据中心业务中存在的系统软件漏洞；逐个人工分析，分别从数据中心区域和校园网区域尝试利用已经发行的漏洞，确认漏洞风险可见范围。（3）Web 漏洞探测：结合端口信息表中 HTTP 协议端口和校方网站导航中站点，形成 Web 业务清单；对 Web 业务清单进行弱点探测；手工同时在校园网（经过 WAF）和数据中心网络（不经过 WAF）进行漏洞验证。

通过以上“人防+技防+安服”的网络安全体系建设，校园网络安全实现由“单点独立防护”到“立体协同防御”的转变，完成由“被动安全防护”到“主动智能防御”的升级，最终形成网络安全防护闭环。我们要通过严格落实法定义务，抓好常态化人防、技防以及网络安全应急响应工作，形成规范化的网络安全管理机制，同时通过落实等级保护要求规避法律风险。

四、遇到的问题

目前主要遇到了以下问题：

1. IPv6 安全策略部署不健全。很多安全设备自称支持 IPv6，但在使用过程中发现其对 IPv6 的支持并不完整。如数据中心防火墙，虽然支持针对 IPv6 的安全策略，但对 IPv6 的日志记录不完整。

2. 部分安全设备没有发挥应有的作用。目前数据库审计设备的作用就没有完全发挥出来。因为只是审计设备，无法对发现的不合规操作进行阻断，因此，只能做事后发现、亡羊补牢的事情。

3. 容器等应用日益广泛，现有的虚拟化防护手段不能满足需求。我们遇到过由于权限设置问题导致的 Docker 逃逸问题，现有的安全手段对此无能为力。

五、未来的规划

对于未来，我们有如下几项规划：

1. 以等保 2.0 为标准，继续完善学校的网络安全体系建设。
2. 继续推进专业网络安全服务，扩大安服的覆盖面，同时要求安全服务公司承担更多的责任。
3. 发挥学校及学科优势，建立一支能为校园网络安全提供高水平服务的安全服务团队。

新形势下的所高校数据防护思考



文 / 任小金 河南大学信息化管理办公室副主任

随着《中华人民共和国数据安全法（草案）》的发布，数据安全治理与防护被提升到了法律层面，要求各行业切实履行数据在生成、传输、处理、存储、利用、销毁等方面的安全防护义务，确保数据的安全性。高校的安全建设方向以及思路也应遵循国家的总体指导方针，由传统的以“网络”为中心的安全思路转变为以“数据”为核心的安全防御理念，所有的安全管理制度与技术手段都应以保护数据安全为出发点，以“数据”的可用性、完整性、机密性三项指标为审核条件，做到高校数据安全防护的闭环管理。为此，我们认为需从数据资产梳理、管理与技术、安全运营评估三个方面对数据进行防护。

一、数据资产梳理

在资产梳理阶段需要考虑两件事：一是学校现有哪些数据资产以及资产相关的属性；二是数据资产使用与管理必然涉及开启、关闭，这是一个动态过程，因此需考虑引入管理机制。

从业务层面来讲学校的数据主要分为：组织机构信息，教职工数据，教学数据，科研数据，财务资产数据，数字档案，个人信息数据等。存储这些数据的服务器的物理位置、IP 地址、开放端口、数据核心表字段等应为首要的梳理对象。其次，需关注数据资产直接关联的资产信息，包括中间件、运维审计平台、接入交换机、虚拟化平台等资产的相关信息。资产梳理的完整性直接决定了治理的有效性，是整个数据安全治理工作的核心。此项工作需各业务部门配合，明确分工、职责到人，做到不遗漏。

前期梳理完成后，在学校数据运营过程中会涉及资产的增删改，所以学校内部需要形成数据资产的审批流程，通过人工或自动方式实现数据资产的变动。

二、管理与技术

数据安全管理的核心为“人”，从访问数据的人员组成来区分，主要包括学校师生的安全意识、安全团队管理、三方运维人员管理。

1. 安全防御最行之有效的方式就是提升数据使用人员的安全意识。学校的师生是管理的核心。学校可以通过多种途径加强其安全意识，如：设置公开课加强对学生的网络安全法制教育；对相关专业的学生增加数据安全知识防护相关课程；开设安全知识专题讲座；举办安全技能大赛；紧抓实事热点，在校园内开展数据安全宣传工作等。

2. 加强安全人员的风险意识和知识技能。“看不见风险是最大的风险”，学校的安全团队应先识别风险，继而化解风险。提升风险意识就是把数据安全防护重点放在风险事件发生之前，不应总是疲于奔命的进行应急处置，不应总是担任“救火队员”，而应该将风险前移，将工作重心放在事前预防、事中控制，重点放在对尚未暴露的风险隐患的排查、发现和及时化解，做到未雨绸缪，心中有数，防患于未然。如果风险事件真正发生了，应深入总结分析，查明根本原因，举一反三，落实整改措施，直至彻底解决。要提升安全知识技能储备，提升漏洞的发现和修复能力，根据国家标准如《数据中心设计规范》、《网络安全等级保护基本要求》保障学校内部的数据中心安全。

3. 引入三方外包增加了数据安全的风险点。数据资产作为学校的核心资产，其根本的控制权应该在学校，涉及到数据中心的账户管理、权限控制、审计策略、认证体系等需要自主管理与运营。涉及到业务侧的功能改造或是性能调优层面必须引入外包人员，则需要在受控的情况下开展工作，并对其行为进



扫码分享 ▷

行完整记录。

同时，我们应从“数据”出发，明确访问数据的来源，并做好以下技术控制：

1. 网络访问的访问控制：严格划分网络安全域，分为业务安全域、数据中心安全域、安全管理中心安全域。每个区域之间通过网络防护墙策略进行 IP 以及端口层面的控制，尤其需要注意的是安全域内部的主机主动外发的网络连接行为，如非必须一律禁止，原则上只允许运维审计堡垒机的 IP 和业务的 IP 可以访问数据中心 IP 的指定端口。

2. 应用级别访问控制：通过自学习架构进行学校数据访问准入规则的固化——自动学习到数据访问行为的五元素“访问源地址、访问源主机名称、访问源用户名称、访问工具名称、登录帐号名称”，设置固化安全规则。未被固化的数据接入行为都会被进行应用层的实时预警和阻断会话。

3. 访问行为控制：基于最小化权限原则，对数据库的传输协议进行解析控制。控制数据库的权限，要细化到关键表字段以及操作，如：对学生及教职工关键信息表设计的违规查询，对考试信息修改操作等设置行为基线策略，防止信息非法篡改与泄露，特别是学生成绩、一卡通、教职工职称等关系到个人切身权益的信息，最终提升关键数据的安全防护能力。

4. 业务的漏洞防护：业务系统的漏洞安全问题会引发数据泄漏风险，因为业务系统一般都委托第三方软件提供商开发，因此是学校最不可控的安全风险。在这里提供一些风险的纵深处置思路：事前预防，事中控制。“事前预防”要求软件供应商提供内部的 SDL 安全开发标准流程，例如源代码中对数据访问的模块采用预编译技术控制，上传文件部分、调用系统命令采用白名单的过滤机制；要求采用多因素认证体系规避弱密码风险。“事中控制”，思考这一层的安全需要一个假设，假设业务是不安全的，因此需要构筑第二道数据安全防线，对业务 SQL 语句的关键字、逻辑关系等特征自动采样学习，并结合高性能的 SQL 语义分析计算，构建对应的 SQL 语法树，完成模态数据建模。从而对未知威胁进行高效、及时、精准的预警和阻断，并追踪到攻击源，这样就能彻底解决互联网接入、无线接入等外围接入方式造成的 SQL 注入、APT 攻击等“脱裤”行为。

5. 数据中心运维安全：在运维方面需要避免共享账号问题，需要做到为每个人分配不同权限的账号，并统一通过堡垒机进行数据中心的运维和审计，避免使用数据库特权账号的登录。

三、数据安全运营评估

安全是业务的属性，安全的目标是保障业务里信息资产的保密性、完整性和可用性，简记为 CIA。CIA 是安全的目标，自然也是安全架构要达成的目标。

学校的数据 CIA 是否能被有效保障，可以基于 5A 的安全架构进行评估，即身份认证、授权、访问控制、审计、资产保护。运营评估可以是内部审核也可以是借助第三方进行。

1. 身份认证作为信任基础，最核心的评估手段是检查数据访问账户是否存在弱密码问题。

2. 授权的评估可以基于“网络接入授权”和“数据可访问内容级别的授权”设计规范。

3. 访问控制是授权设计的执行。评估手段主要是依靠基于授权的设计规范，查看网络端口级别的控制措施以及数据访问账号的权限。

4. 运维和业务的数据流审计，主要指审计数据是否符合独立性原则（不可被篡改）和符合法律法规的存储时间要求。

5. 资产保护涉及的内容有：基于数据资产的漏洞探测和修复，重要业务数据共享的安全控制机制，数据传输、存储过程的加密机制。

评估数据安全建设的手段还有很多，在资源有限的情况下可以基于 5A 框架有重点的进行分析评估，查漏补缺，不断地完善学校数据安全治理工作。

高校数据安全防护需要不断感知安全形势，完善组织建设，落实管理责任，优化制度流程，升级技术工具，提升专业技能，推动学校数据安全治理水平不断取得新突破、迈上新台阶。

构建完整的网络安全组织 良好的管理体系是关键



文 / 张喜平 河南师范大学网络中心副主任

网络安全是一个系统、全方位、动态的大工程，三分靠技术，七分拼管理。构建一个完整的网络安全组织，必要的技术设备是基础，良好的管理体系是关键。高校的校园网要实现安全、绿色、高效、可靠。我认为，在网络安全方面需要注意以下几个方面：

1. 组建由学校主要领导担任负责人的网络安全管理组织。领导重视、全员协力才能构建网络安全人员防护网。

2. 加强全校网络安全知识培训，提高全员网络安全防护意识。网络安全是一个全方位的工程，一人的不安全，会造成全网安全防护前功尽弃。

3. 校园网中各项通讯要零信任，采取必要的防护措施。对外提供的服务，做到“最小可用”，不必需即关闭。

4. 校园网中根据用户群体不同、功能不同，尽可能细粒度划分网络区域，不同区域之间访问采取必要的防护措施。

5. 网络是动态变化的，网络安全防护也必须是动态的。要实时监控网络流量、网络日志等，动态感知可能存在的风险。网络安全人员需要不断根据感知的风险调整网络安全防护体系的各项策略，让网络攻击者摸不清网络安全防护体系采取的各项策略，增加攻击者成功的难度。



扫码分享 ▷

“十四五”期间安全建设要从“攻击者视角、新技术视角、顶层设计视角”出发

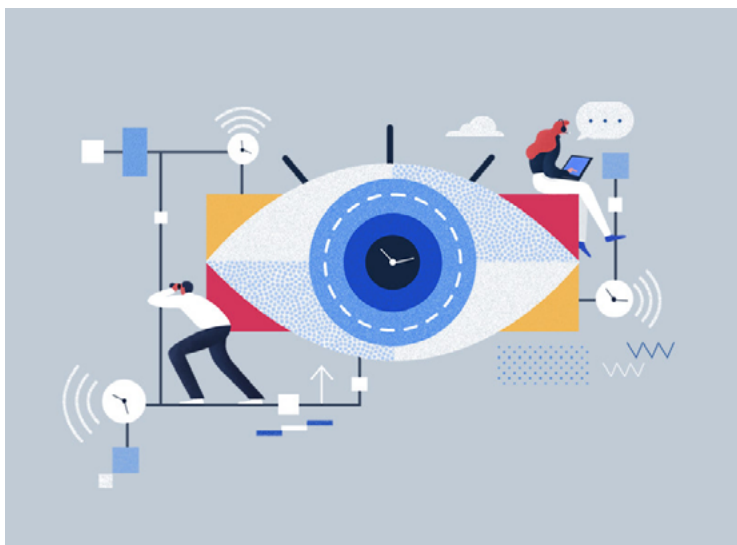
文 / 吉鹏霄 郑州铁路职业技术学院信息化办公室主任

2020年是“十三五”规划的收官之年，教育部办公厅秉承“十八大”报告中关于信息化的“没有网络安全就没有国家安全；没有信息化就没有现代化”的核心理念，印发了《2020年教育信息化和网络安全工作要点》。《要点》中对教育信息化“十四五”规划、推进“互联网+教育”发展提出了明确的指导意见。

即将到来的“十四五”，将是数字化战略的转型建设关键阶段，数字经济将全面深化。尤其是“新基建”作为先行举措，进一步加快了数字化转型步伐。数字化转型将使学校的核心业务越发依托信息系统，数据已成为学校的核心资产。“云大物移智”等新兴技术的不断涌现使得学校自身业务越发依赖于互联网，网络信息安全风险也随之上升，学校也在逐渐加大对网络信息安全的投入力度。

随着网络安全技术的发展，传统的安全防护理念由“被动防御”向“主动防御”，由“单一防护”、“补丁”模式向“系统规划、整体协防”演进。大数据、AI、SDN、IPv6、安全情报等新兴技术推动了网络安全新的建设模式，具备数据分析、安全运营和情报收集等能力的安全产品逐渐被学校所重视。

学校在制定“十四五”期间的安全建设计划时，要从“攻击者视角、新技术视角、顶层设计视角”出发，规划网络安全体系全景，设计出将网络安全与信息化相融合的目标技术体系和目标运行体系。同时，学校需要持续开展网络安全监测预警，提高数据分析和态势感知能力，完善网络安全通报机制建设，落实国家网络安全等级保护 2.0 的相关要求。



扫码分享 ▷

信息安全管理体系的建设是策略、技术与管理的综合运用



文 / 孟先新 华北水利水电大学信息化办公室网络信息部主任

信息安全管理体系 ISMS (Information Security Management Systems) 是组织在整体或特定范围内建立信息安全方针和目标, 以及完成这些目标所用方法的体系。对于高校来说如何建立起适合于自己并且能真正落实的信息安全管理体系至关重要。而信息安全管理体系的建设不是纯粹的技术问题, 也不是产品与技术的堆砌, 它是策略、技术与管理的综合运用。设想尝试通过以下三个方面来建立和落实信息安全管理体系。

1. 可以参照信息安全体系标准 ISO 27001:2013 来进行建设。具体可以引进专门从事 ISO27001 认证的机构, 以 ISO27001 标准指导学校建立信息安全管理体系, 并且制定和完善本校相关信息安全具体规范、标准和制度, 达到建章立制, 做到有据可依。

2. 多数高校的信息化管理部门人员偏少, 特别是网络安全专业人才更少。在这种情况下, 作为过渡, 可以将技术性和部分管理性的工作外包给专业的网络与信息安全技术服务公司, 通过驻厂和远程支持, 进行 7*24 小时的信息安全运营。技术服务重点关注安全培训、访问控制、日常检查、定时评估等。当然, 从长远来看, 高校必须要建立起一支自己的既懂技术又懂管理的专职队伍来从事信息安全管理工

作。

3. 国外一些著名高校建立了专门、独立的信息安全管理部门, 直接向学校最高管理层负责。基于目前我国多数高校的组织架构, 这种模式可能不太现实, 但至少在学校信息化部门下设置相对独立的信息安全管理科室, 并配备专门管理人员还是行得通的。建议用相对稳定的内聘人员进行持续的信息安全管理, 同时在校内各部门设立二级 CIO、信息化专员岗位, 强化信息化队伍建设。信息安全管理部门要重点关注信息安全体系运作情况和信息安全运营情况, 并进行持续的优化和改进。



扫码分享 ▷

如何在断电后安全关闭服务器



文 / 胡耀东 河南工程学院计算机学院副教授

意外断电对服务器、虚拟化平台，特别是运行 UNIX 系统的数据库服务器等简直是灾难性的，轻则数据库回滚、文件系统检查，重则数据信息丢失、崩溃以及系统无法进入等。为防止意外断电，各种类型的数据中心、机房几乎都配备了 UPS 电源，对关键和重要的服务器加以保护，用来保障电力中断时系统能够正常运行，维持服务的持续性。经过多年发展，数据中心逐步采用了模块化 UPS，满足了在线更换、扩容等要求，可靠性进一步提高。

但使用 UPS 也带来了新的问题，比如：断电后空调无法工作，导致温度过高；断电时间较长，电池耗尽后系统断电等。因此，在断电后安全关闭相关的服务器是很必要的。

一、常规解决方案

主流的 UPS 厂商提供了相应的解决方案，常见的有以下两种：

1. 提供 RS232 或 RS485 接口

使用对应的串口线缆和相应的 UPS 管理软件，可以满足关闭服务器和 UPS 自身的需求。这种方案的主要问题是需要额外的串口电缆，服务器需要相应的接口，不加扩展只能关闭一个服务器。

2. 提供 UPS 智能卡接口

除了提供一些 I/O 接口、温湿度等接口外，通常提供有网络接口。通过网络接口可以较为完整地控制 UPS 的行为，也能通过网络接口和相应的软件在发生长时间停电后关闭一定数量的服务器。一般情况下要求服务器和 UPS 管理卡在同一网段，并安装对应的软件，同时关闭的服务器数量有一定的限制等。

以上方式通常能够满足一部分需求，但是部分管理人员抵触安装 UPS 管理软件，且关闭同网段的服务器也有一定的限制等。如何克服以上方式的限制，在不增加硬件成本的情况下获取断电信息、利用系统本身的功能安全关闭服务器是一个值得探讨的有趣问题。

二、新方案探索

1. 在不增加硬件成本的情况下获取断电信息

在不增加硬件成本的情况下，我们分三种情景获取断电信息。

(1) IPMI 获取断电信息

IPMI 是智能型平台管理接口 (Intelligent Platform Management Interface) 的缩写，是管理基于 Intel 结构的企业系统中所使用的外围设备采用的一种工业标准，该标准由英特尔、惠普、NEC、美国戴尔电脑和 SuperMicro 等公司制定。用户可以利用 IPMI 监视服务器的物理健康特征，如温度、电压、风扇工作状态、电源状态等。更为重要的是，IPMI 是一个开放的免费标准，用户无需为使用该标准而支付额外的费用。

IPMI 协议被广泛用于服务器监控中，包括采集 CPU 温度、风扇转速、主板温度以及远程开关机等。IPMI 的硬件设备 BMC (Baseboard Management Controller) 是一个独立的板卡，独立供电。因此 IPMI



扫码分享 ▷

独立于硬件和操作系统，无论是 CPU、BIOS，还是 OS 出现故障，都不会影响它的工作。目前主流的服务端都提供了该接口，只需将该接口接入网络，进行相关配置后即可使用。

在 Linux 环境可以联网的环境下只需要敲入命令 “[root@localhost]# yum install OpenIPMI OpenIPMI-tools OpenIPMI-libs OpenIPMI-devel”，就可以安装相应的软件包。如无法访问外网可以下载相应的软件包安装。

安装完需要启用 IPMI 服务，可以敲入 “service ipmi start”。开机自动启用服务则可以敲入 “chkconfig ipmi on”。

该方式可以在本地和远程环境下使用。

本地使用时，在 shell 环境下直接键入：

```
[root@localhost]# ipmitool sdr elist | grep -E "(Power1|Power2)"
```

显示信息如下：

```
Power1      | 07h | ok | 10.96 | 123 Watts
```

```
Power2      | 08h | ok | 10.97 | 96 Watts
```

其中 Power1 是 UPS 供电，Power2 是市电供电。依据此环境，结合 grep 和 awk 命令写出脚本如下：

```
#!/bin/bash
power_ipmi=`ipmitool sdr elist | grep -E "(Power2)" | awk '{print $9}'`
echo "power is: $power_ipmi"
```

运行该脚本可以直接获得电源 2 的即时功率，并打印出功率信息。

远程环境下使用时，假设远程 IPMI 的 IP 地址是 192.168.1.100，用户名是 root，密码是 password，远程 IPMI 服务器是华为的 2288v2，键入 “ipmitool -H 192.168.1.100 -U root -P password -I lan sdr elist” 即可。

(2) SNMP 获取断电信息

简单网络管理协议 (SNMP, Simple Network Management Protocol) 是基于 C/S 的模型。它实现了这样一种功能：当管理端需要获取被管理端的一个状态信息时，管理端就发送一个获取指令给被管理端，被管理端收到此指令后把管理端要获取的信息封装成报文后返回给管理端；当管理端需要修改被管理端上的一些配置参数时，管理端就发送一个修改指令给被管理端，被管理端收到后修改相应的配置，如果修改成功则返回修改成功的信息给管理端，如果未修改成功则返回相应的错误信息给管理端；如果被管理端自己知道自己发生了故障，那它就主动发送一个消息给管理端，说明自己哪里出现了故障。

根据对应的 mib 串，我们可以获得网络设备的信息。下面我们以 H3C 的三层交换机 5820 为例，获取电源状态信息。该设备有两个电源模块——电源模块 1 为 ups 供电、电源模块 2 为市电供电，交换机的 community 只读共同体名字为 public，IP 地址为 192.168.1.1。

管理机为 Linux 系统安装了 net-snmp 管理包，通过对电源模块 2 的接通电源和断掉电源的状态比较如下：

接通市电：

```
[root@localhost]# snmpwalk -v 2c -c public 192.168.1.1 1.3.6.1.4.1.25506.8.35.9.1.2.1.2
```

```
SNMPv2-SMI::enterprises.25506.8.35.9.1.2.1.2.1 = INTEGER: 1
```

```
SNMPv2-SMI::enterprises.25506.8.35.9.1.2.1.2.2 = INTEGER: 1
```

断掉市电：

```
[root@localhost]# snmpwalk -v 2c -c pubic 192.168.1.1 1.3.6.1.4.1.25506.8.35.9.1.2.1.2
```

```
SNMPv2-SMI::enterprises.25506.8.35.9.1.2.1.2.1 = INTEGER: 1
```

```
SNMPv2-SMI::enterprises.25506.8.35.9.1.2.1.2.2 = INTEGER: 2
```

结合 awk 命令写出可以直接获得市电状态标记的脚本：

```
#!/bin/bash

snmp_state=`snmpwalk -v 2c -c pubic 192.168.1.1 1.3.6.1.4.1.25506.8.35.9.1.2.1.2.2 | awk '{print $4}'`

echo "power state is: $ snmp_state"
```

运行该脚本，市电供电的情况下是 1，断电的情况下输出为 2。

(3) ping 获取断电信息

我们可以在 shell 状态下用 ping 命令，通过简单的 shell 脚本，获取市电状态信息，其中 192.168.1.254 是一个市电供电的网络设备，简单脚本如下：

```
#!/bin/bash

ping -c 1 192.168.1.254 > /dev/null 2>&1

echo "power state is: $?"
```

脚本仅检查了 ping 一个包的情况。对于较稳定的主干设备，ping 一个包的可靠性是没有问题的。如果需要更高的可靠性，则可以多 ping 几个包。

2. 利用系统自身功能安全关闭服务器

获取了市电状态，依赖 UPS 电力供应，结合操作系统的计划任务，我们就可以根据 UPS 的能力及实际需要，在市电中断的情况下自由选择多长时间关闭服务器。下面我们以 Linux 系统为例，编写一个简单的 shell 脚本，添加计划任务，完成安全关闭系统服务器的任务。

利用 IPMI 读取连接市电电源的功率，判断市电状态 shell。此 shell 可以判断电源提供的功率是否为 0。“0”代表市电中断，则需要测试断电后的状态。测试中断电可以先不使用 shutdown 关闭系统，可以采用一些命令来测试状态是否与设想一致。如下：

```
#!/bin/bash

power_ipmi=`ipmitool sdr elist | grep -E "(Power2)" | awk '{print $9}'`

if [ $power_ipmi -eq 0 ];then

echo "power is bad"

shutdown -h now

else

echo "power is ok"

fi
```

利用 SNMP 函数读取双电源供电的交换机状态，以判断市电状态关闭系统的 shell。此 shell 直接读取市电供电的交换机的电源模块状态，也需要验证是否与设想一致。如下：

```
#!/bin/bash

snmp_state=`snmpwalk -v 2c -c pubic 192.168.1.1 1.3.6.1.4.1.25506.8.35.9.1.2.1.2.2 | awk '{print
```

```
$4}'`  
if [ $snmp_state -eq 2 ];then  
echo "power is bad"  
shutdown -h now  
else  
echo "power is ok"  
fi
```

利用 ping 命令获取市电状态关闭系统的 shell。此 shell 可以判断网络中市电供电的设备状态，如果关闭服务器，也需要验证是否和设想的一致。如下：

```
#!/bin/bash  
ping -c 1 192.168.1.254 > /dev/null 2>&1  
if [ $? -eq 0 ];then  
echo "power is ok"  
else  
echo "power is bad"  
shutdown -h now  
fi
```

添加到计划任务中，假设上面断电关机的 shell 名称为 power.sh，在 linux 系统直接可以运行 crontab -e，添加一行 “*/5 * * * * /sbin/power.sh >> null” 即可。

系统会每 5 分钟检测一下市电状态。当检测到市电断电后，即可执行关机 shell，根据 UPS 电池和需求灵活调整该时间间隔。该计划任务在最极端情况下市电断电 5 分钟内关闭系统。

除了 UPS 厂商提供的方案，本文至少探讨了三种方法检测市电状态。这些方法在各类机房、数据中心是比较容易实现的，不增加硬件费用，且不需服务器有相关的 RS232、RS485 等接口，在虚拟机环境下也容易实现，关闭的服务器数量没有限制，没有安装第三方软件，文中大部分是以 Linux 环境为基础的，实际上在各类 Windows 系统上，MacOS 系统上都可以实现。

三、注意事项

1. 利用本地 IPMI，需要服务器自身有双电源——一路为 UPS 供电，一路为市电供电。如果读取远程的 IPMI 信息，在笔者的环境下我们发现，服务器的网段只有和远程的 IPMI 接口网段在同一网段时，才能够读到具体的电源功率。

2. 利用 SNMP 读取市电状态，在笔者的环境下，需要一个双电源的交换机——一路 UPS 供电、一路市电供电，只要服务器和交换机 IP 可达即可实现。

3. 利用 ping 命令获取市电状态，这种方式适用的范围更加广泛。在同一机房有市电供电的可网管设备下方便使用。在整个机房供电全部由 UPS 供电环境下，可以寻找一个在同一变压器供电的比较重要的外围市电供电的网络设备来判断。

基于信息安全技术的教育数据安全与隐私保护

文 / 刘梦君、姜雨薇、曹树真等 湖北大学

信息安全技术保障教育数据安全与隐私保护的模型

典型教育信息系统里面包含着学习者、教师、教学管理人员和系统运维人员 4 方面用户。这 4 方面用户对于教育数据而言既有可能是合法用户，也有可能是安全威胁。

教育数据安全与隐私保护的目的是通过接入控制、攻击防护、数据加密、隐私保护等信息安全技术：在学习者合法使用教育信息平台的同时，保护学习记录和个人信息等数据安全的隐私，同时阻止和检测出对他人数据的非法访问；为教师提供合法的信息化教学辅助的同时，防止其教学资源 and 成果被人非法窃取，并尽可能减小其对学生数据有意无意的非法获取；为管理人员提供合法的信息化管理辅助同时，阻止并检测出其有意无意间泄露用户数据及隐私；为系统运维人员提供维护系统接口同时，阻止并能检测出对教育业务数据的访问记录。

简而言之，让上述 4 方用户在保障教育数据安全同时，依然能够开展正常的教、学、管、维活动，形成一个教育数据安全共同体。

信息安全技术保障教育数据安全与隐私保护的框架

信息系统安全遵循木桶理论，即系统的安全程度高低由最薄弱环节决定。因此，理论安全的教育信息系统任一环节上的安全都需要得到最大化的加强。一个安全的教育信息系统需要解决三个环节上的安全问题，即：安全地“采和传”、安全地“存”、安全地“用”。即系统内的数据生成及流动过程中不被泄露或非法篡改，存放在系统期间不被泄露或非法修改，使用时候不被泄露或非法篡改。具体保护流程如图所示。

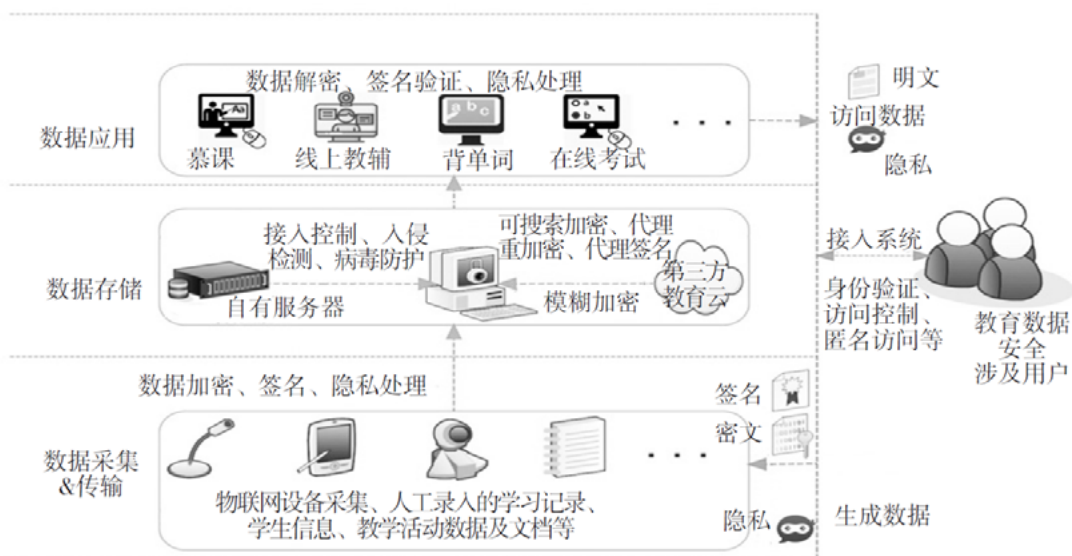


图 1 教育数据安全与隐私保护框架

在教育数据采集和传输过程中，需要根据所面临的安全威胁，来决定使用一种或者几种信息安全技术的组合，构建安全的数据采集与传输方案。

1. 当想阻止可靠的设备传输数据内容被泄露时（如音视频设备录制数据，固定点采集活动数据），通



扫码分享 ▷

常由交互发起方使用对称密钥，对交互数据进行加密后发送给另一方。

2. 当想阻止篡改通信数据或者抵赖数据来源时（如学习者准备提交给系统的学习行为数据），则由交互发起方，使用基于哈希函数和非对称加密技术的数字签名技术，对交互数据生成签名，另一方则使用交互发起方公开密钥，验证签名来判断原始数据有无被篡改。

3. 如想同时防止数据泄漏和数据被篡改（如学习者的个人资料数据），则由交互发起方先对原始数据使用对称密码加密，然后使用哈希函数生成摘要，再使用非对称的私密密钥生成签名，然后将密文和签名一同发送给交互另一方，另一方验证签名后再解密数据。

以上数据泄漏都是针对有权限接触到用户数据的管理者外的人员，如果还想防止个人敏感数据（如教学评价数据，投票调查数据）被管理者知晓，则需要使用个人隐私保护技术对个人敏感数据进行隐私消除处理，再传输给平台。

在教育数据存储安全保障中，需要根据系统自身所拥有的资源来决定使用一种或者几种信息安全技术的组合，构建安全的数据存储方案。

1. 当教育信息系统主管单位有充足资源时（如大型高校和大型在线教育平台），一般自建硬件平台和防火墙、入侵检测、病毒查杀维护等子系统，此时教育数据存储在系统运营方自有平台上，因此存储时，数据一般不会加密。

2. 当教育信息系统没有充足资源时（如广大中小学校和小型的在线学习平台），一般使用大型第三方的云存储服务，云服务提供商会提供防火墙、入侵检测、病毒查杀等服务。此时，由于数据脱离了教育信息系统主管方控制，数据内容有泄露和被篡改风险，需要对数据进行对称加密，并生成哈希摘要后签名。系统主管方只需要用一台小型的安全设备做好加解密密钥、签名数据的存储及管理，而这台设备只对系统运维人员开放。

在教育数据使用安全保障中，需要根据业务的类型和运行机制，来决定使用一种或者几种信息安全技术的组合，构建安全的数据使用方案。数据的使用有两种类型，一种是用户去信息系统查询，如学生查询自己课程考试成绩。另一种是系统主动对外公开，如学生考试成绩的及格人数、最高分、最低分、平均分等统计信息。

1. 对于前一种数据的使用，在系统宏观层面设置身份认证机制，用户在进入业务系统时，需要输入密码、权限卡片、手机验证码、脸纹、指纹等验证手段中的一种或几种，进行身份验证，通过后方能进入系统。而后对具体的数据，使用访问控制技术，划定细分的访问权限。只有授权的用户拿到数据才能够解密，未授权用户，即使拿到数据，也无法获悉内容。

2. 对于后一种数据，系统在向外公开时，需要先去除身份标识符，而后添加差分隐私噪声值，再对外发布。数据的使用还需要和数据的存储方式关联。对于存储在第三方云服务平台上的数据，需要使用可搜索加密技术、代理重加密、代理签名技术对数据进行处理后存储，使得数据加密存储后，还可被用户检索及云平台协助验证有无被外界篡改。（《中国电化教育》）

智慧校园建设要向数据要“效益”——访南阳理工学院信息化建设与管理中心主任吴绍兴



吴绍兴：副教授，南阳理工学院信息化建设与管理中心主任，河南省教育科研计算机网（HERNET）专家委员会委员。长期从事高校教育信息化建设与管理工 作，尤其是在 IPv6 部署与应用、网络安全建设、数据治理方面有深入的研究。

南阳理工学院校园网从 1997 年开始建设，目前已覆盖校园各个角落，为全校的管理、教学、科研提供了优质的网络资源，对学校的人才培养、学科建设、科学研究、行政管理和师生生活等产生了明显的效益。南阳理工学院高度重视信息化建设，以信息化引领学校教育教学高质量发展。2020 年，学校启动了新型智慧校园建设；建设了以数据资产为底座的校园网安全管理模式；与中国移动南阳分公司举行 5G+ 智慧校园战略合作签约仪式，成为南阳市首个 5G+ 智慧校园落地项目；新版官方网站在全球 IPv6 测试中心顺利通过 IPv6 Enabled Phase-2 认证，成为全省首个通过该认证的高校网站。南阳理工学院在推进智慧校园建设方面又迈出了重大步伐。近日，我们就相关问题采访了吴主任。

向数据要“效益” 构建新型智慧校园

《河南教育信息化》：今年，南阳理工学院启动了新型智慧校园建设工程。具体能跟我们介绍一下吗？

吴绍兴：南阳理工学院新型智慧校园建设工程，提出了打造数据融合底座、构建“数据治理+应用生态”的新型智慧校园建设理念。因为大数据时代，数据已经成为一种新型生产要素。学校的发展，教育质量的提升，怎么才能管得更好、教得更好、学得更好，也都需要利用好数据这个生产要素，向数据要“效益”。所以，我们提出了“数据治理+应用生态”的新型智慧校园建设工程。

目前，学校通过新型智慧校园建设项目，制定了校园标准信息模型，实现了全校层面在数据沟通语言上的统一。通过建设数据治理平台，实现了校园数据的全域融合、全量融合、实时融合能力，全面打



扫码分享 ▷

通教务、人事、财务、学工、科研、设备、国资、一卡通、图书馆、后勤等十大业务系统，创新设计教职工、本科生、师资科研、一卡通、资产、院系、驾驶舱等 7 大类、30 个子类、上百个数据融合应用场景。在数据治理的基础上，通过建设数据服务开放中心，学校实现了校园数据服务的自主化开发、服务化共享，形成全校师生既是使用者、又是开发者的生动局面。通过繁荣的“数据治理 + 服务接口体系”，以及规范化的校园业务系统建设要求，最终形成了以数据融合为底座的“数据治理 + 应用生态”新型智慧校园环境。



图 “数据治理 + 应用生态” 架构

基于“新一代数据治理体系”建设的新型智慧校园，将是我校贯穿“十四五”的一项系统性创新工程，我们希望与兄弟院校一起探索，共同进步。

打造以数据资产为底座的校园网络安全管理模式

《河南教育信息化》：作为学校信息化建设的重要基础设施，校园网的安全管理成为信息化建设工作的重要内容。如何理解南阳理工学院以数据资产为底座的校园网络安全管理模式？

吴绍兴：学校非常重视校园网络安全建设，该项目是智慧校园建设与应用的安全保障。首先说下建设的背景，学校各部门原自建的业务系统，因为种种因素，产生了维护困难、管理无序、存在大量信息安全隐患等“痛点”，为了规范信息安全管理，降低信息安全风险，全面落实和提高系统安全的防护能力，所以今年，我们依据《网络安全法》、《网络安全等级保护基本要求》和《教育信息化 2.0 行动计划》等相关法律法规、重要文件，结合学校的实际情况，通过调研分析，打破我校传统网络安全建设模式，提出了以数据资产为底座的校园网络安全管理模式。截至目前，该项目已经基本建设完成。

这种管理模式主要分三个部分：

首先，通过全日志采集、全流量分析、人工录入的方式对所有 IT 资产进行全面数据采集，最终实现摸清学校信息化的“家底”，建立安全运营基础。

其次，在摸清学校信息化“家底”的基础上，融合多源数据建立基础数据资源池。然后基于场景化安全模型对数据进行挖掘分析，从而在校园海量数据的使用过程中实现透视数据安全，设置合理的数据使用策略，建设数据使用风险分析模型和场景，建设整个数据资产“采集、传输、存储、处理”的安全生命周期，以及建立起数据安全策略、安全事件管理、安全事件溯源的监管体系，从而把所有资产在各个环节面临的信息安全问题展示出来。

通过本次建设，学校的校园网络安全管理实现由“被动防护”向“主动防御”的进阶，基于数据做到安全威胁可视化、可量化、自动化，实现安全风险可视化管理，形成整体安全联动机制的“安全大

脑”，提升学校的风险感知能力和预警能力，以及应对高级安全威胁、隐蔽安全事件的发现和处置能力，并结合管理制度为学校打造了一个以数据为底座的智能信息安全运营体系。

最后，打造安全运营协同防护机制，确保智能信息安全运营体系的有效运行。包括建立共享情报与处置平台，优化事件预警、指标监测、应急处置等流程，形成联动效应。同时加强网络和信息安全领域的安全交流合作，建立威胁情报共享机制和技术平台，实现威胁情报协同处置。

大力促进5G技术的转化应用 推动5G+智慧校园建设

《河南教育信息化》：7月21日，南阳理工学院与中国移动南阳分公司举行5G+智慧校园战略合作签约仪式，成为南阳市首个5G+智慧校园落地项目。请问学校是在什么样的背景下提出并开启了“5G+智慧校园”项目建设？

吴绍兴：2019年1月教育部办公厅发布关于“智慧教育示范区”建设的通知，提出全面加强各级各类学校数字校园建设，促进数字校园应用全面深入普及。政策加持为5G在远程教育、智慧课堂/教室、校园安全等场景的发展提供了新的发展方向，助力促进教育公平、提高教育质量。2019年9月19日，教育部联合十部委发布《关于促进在线教育健康发展的指导意见》要求“抓住第五代移动通信技术(5G)商用契机，加快推动物联网、云计算、虚拟现实等技术在教育领域的规模化应用”。2020年3月6日，国家发改委与工信部下发组织实施2020年新型基础设施建设工程（宽带网络和5G领域）通知，主要包括支持基础网络完善和5G创新应用提升两大工程，其中5G+智慧教育示范应用工程属于5G创新应用提升工程的其中一项。受以上政策的驱动，以及线上教学的需求，南阳理工学院决定把5G+智慧校园建设提上了日程。

《河南教育信息化》：校园建设如何与5G接轨？学校是否有相关的行动计划？

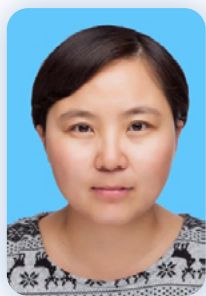
吴绍兴：南阳理工学院与中国移动南阳分公司将积极探索5G+智慧校园建设的新模式，大力促进5G技术的转化应用，围绕南阳理工学院智慧校园发展需要，打造“5G校园专网”、“5G创新研发中心”、“5G+VR教学”、“5G校园一卡通”、“5G展示演示平台”、“5G智慧安防”等一批5G应用项目，按先局部试点，再全面铺开的原则，不断创新运营模式，共同探讨拓展相关新兴应用和智慧校园业务建设。

《河南教育信息化》：您认为，“5G+智慧校园”会给学校的教育信息化工作，以及教育、教学及管理带来哪些影响和变化？

吴绍兴：以5G为代表的新兴技术为智慧教育创新性变革提供了保障。我们知道，5G技术具有高速率、低时延、大带宽等优势，能够为AI、VR、云计算、大数据等信息技术与教育教学的深度融合提供强大的网络支持。

5G与AI、大数据、云计算等为代表的新兴技术的融合，必将引发学习资源、学习环境等教育场景要素的深刻变革，也将对教师的教育理念、教学方式等产生重大影响。与此同时，也将带来教学内容和学习方式的重大转变，以满足“人人互联”时代学生各种的学习需求，为学生提供“无限”、舒服的网络学习空间，为学生的个性化、自适应、精准化学习提供有力的技术支持。目前项目刚刚启动，我们也非常期待“5G+智慧校园”给学校教育带来积极的变化和无限的可能。

研究导向型理念在线上课程高阶学习中的应用



文 / 孟俊贞 华北水利水电大学讲师

在严峻的新冠肺炎疫情形势下，为确保学生的安全与健康，全国高校和中小学响应教育部“停课不停学”的工作部署，实施了覆盖全国的在线教学，这是新型网络课程与学习观在特殊时期的一次实战演练。随着在线教学的陆续开展，逐渐暴露出一些问题，反映出教师与学校定位和理解在线教学方面的偏差，同时也给教育机构的优化策略部署反馈了思路，更是郑重地对教师的教学理念和能力提出了挑战——如何组织教学？如何保证质量？如何保证效果？如何保证教学目标达成？

一、线上学习的优势与劣势

与线下教学相比，线上教学的优点非常突出，充分体现了个性化学习的特点——只要拥有网络、电脑及智能手机，就可以自己调整学习计划，随时随地学、反复听、反复学、接触优质的教学资源、交流互动范围扩大、相关信息共享与及时反馈等。线上教学突破了时间、地点的种种限制，使学生真正掌握了学习的自主权。

但线上学习也存在问题与不足，其中最大的挑战是对学生自主学习能力的挑战。因此，面对敢做、敢想、有思想、会创造的年轻人，教师应思考：如何点燃学生心中自学的火焰，提高其进行课外自主学习的能力，激发其课内讨论知识点的兴趣，锻炼学生真知实干的实践能力，同时发挥学生的创造力？

鉴于上述分析，在保证基础知识及基本体系的前提下，教学的体系、内容、方式等都需要改变，需要教师、学生共同参与，共同努力。采用研究导向型教学的理念进行在线教学的设计与开展是可行性方案之一，不但可以有效解决上述问题，而且可以培养学生的创新思维和养成终身学习的能力。

二、研究导向型教学的理念

建构主义教育哲学认为，学习是学习者基于原有的知识经验，通过启发性的活动，在与社会文化探究互动中生成意义、内化并建构理解的过程。在信息高速发展的时代，尤其处于人工智能、互联网快速行进的高速列车上，学习不止是对知识的掌握，更重要的是对未来人才竞争中的各种能力、精神和素养的培养与提升。因此，学习不仅仅体现在课堂上，更体现在从生活的真实问题中学习和解决问题的能力上。

研究导向型教学理念则是通过问题导向或者实际案例研究等方式来启发学生思考，旨在引导学生主动综合运用所学知识去分析、解决问题，促进学生在不断反思的过程中积累经验，养成科学思维的习惯，并在“研究—学习—再研究—再学习……”的过程中逐步建立正确的认知模式，培养学生的创新思维、批判精神、团队合作能力，进而提升学生走入社会后应对挑战的能力及终身学习的能力。

研究导向型教学理念注重学生在课堂上的讨论与展示、课下的材料搜集与整理、方案的确定与验证。因此，课程的考核实行多个阶段进行，采用过程性评价与总结性评价相结合的多元化考核评价模式，采用多形式、多阶段、多类型的考核方式，重点考核学生的综合素质与能力，并坚持公平、公正和公开的原则让学生参与评价过程。



扫码分享 ▷

三、研究导向型教学过程

作者所在教学团队教授的《地籍与房产测量》课程，是实践性很强的一门课程，来源于生活也服务

于生活，对技术人员不但有测绘技术知识的要求，还要求有对最新的土地和不动产法规知识的掌握。这里以该课程为例，讲述研究导向型教学过程。

1. 教学设计与策略

研究导向型教学设计紧紧围绕“变”与“不变”这一主线来进行：教学目标不变、教学任务不变、教学质量不变；教学理念要变、教学方式要变、组织形式要变。研究导向型教学以学生素质能力的提升为主要归依点，是一种集“教、研、学、做”于一体的教学方式，不仅培养学生的学术研究能力，同时还培养学生对理论知识的实际应用能力。

在教学设计主轴线的引领下，在知识目标的培养上，通过思维导图和主题讨论，让学生畅所欲言，给出自己的想法；在技术目标的培养上，主要结合当前疫情这个案例，注重培养学生学以致用意识与能力；在能力目标的培养上，通过团队合作和头脑风暴培养学生的沟通、协作能力、创新思维和养成终身学习的能力；在情感目标的培养上，注重对学生正确的学习态度及价值观的培养，让思政、社会责任感、全民素养走进课堂，加深学生对国土与房产的认识，让学生珍视国土、珍爱家园，增强学生的责任感和使命感。

基于教学理念和教学目标，教学设计以逆向设计思维制定了“七步式”教学策略。首先，利用精心设计的教学软件，让学生明确学习目的，引入研究导向型学习理念；其次，创造学习情境，结合鲜活生动的实践案例（新冠肺炎疫情和自己所居住的现实环境）设计互帮互助的小组学习活动；第三，考虑学生的个体和发展差异，创设团队意识和归属感；第四，开展头脑风暴（主题讨论），激发学生多向思维，产生多种可能创意点；第五，创设目标导向的务实氛围，细分复杂任务和主题，标出逻辑顺序，确定高效的教学方式方法（引入思维导图的讲解和使用）；第六，加强团队意识，注重锻炼学生的自我管理，引导辨别是非，并适时给出信号和提醒，鼓励富有成效的行为和成果（引入论文写作讲解和大学生创新创业项目申报）；第七，利用技术手段加强沟通与合作，为学生提供帮助，确保有价值学习任务的顺利完成。

2. 课程开展形式

结合新冠肺炎疫情以真实问题切入，因事而化，在情境中学习，形成固定的、有特色的教学板块（课堂交流区、主题讨论区、思维导图展示区、研究导向型学习成果展示区），每个板块对应相关学习内容和学习目标，在潜移默化中引导学生成为善于自我规划的学习者，培养学生的自主性、自律性。

引导学生从社会责任感、数字敏感度及其重要性、社会可持续发展、创新思维四个方面探讨重大事件和问题的解决方案。学生们基于各自不同的兴趣结合专业方向，从不同的角度对疫情进行聚焦、凝练出丰富观点从而确定研究方向，让学生从基础知识的积累过渡到具体问题的研究，实现从知识积累逐渐迭代为发现问题、提出方案、验证观点到最后的解决问题这样一个过程。整个过程为学生提供了丰富多元立体的学习方式，包括视频观看、问卷调查、课后测评、线上主题讨论、思维导图展示与讨论、海报设计与展示、结合真实场景的实验、师生互动、生生互动以及评估反馈等方式。



图 1 问卷调查



图 2 学生思维导图展示区

3. 探索与实践

研究导向型教学通过精心的教学组织和设计，努力构建班级之间、小组之间、学生之间、师生之间的学习共同体，课堂的重心由灌输式转为自主学习式。课程团队老师以入驻小组的方式带学生走进实战课程，引导学生自主地搜索文献和资料，通过团队合作、共同探讨与实践提供问题解决方法。

首先，团队建设。如图3所示，参与学生以小组为单位。基于共同的研究兴趣每5-6人自发组成一个学习小组，通过组内讨论或投票选出一名组长，负责组内学习活动的组织与实施。

学习小组的组成，有利于集思广益，培养团队协作意识。同时多种正确、创新的思维碰撞在一起，组内分工、分块进行课题研究，课程总结等，可以产生更加高效的解决方案。分组研究还有利于帮助、提升组内个别组员对知识点的理解力、自主学习能力。



图3 团队建设案例

其次，过程保障。课程建设团队中的9名教师根据分组情况分别加入各学习小组（如图4），以课程内容学习为主体，以社会真实问题“新冠肺炎疫情所触发的一系列社会问题”为引线引导学生去学习，通过对现实问题进行解析、凝练、实践、探索，最后透过现象去分析和把握问题背后的本质。

言传身教地鼓励学生充分利用网络资源、多媒体工具及相关软件，引导他们通过探究，在与外界互动、甄别的过程中构建对问题的认知。鼓励学习者在学习过程中运用研究导向型思维，把更多有效互动时间投入在认知维度的高级阶段，即对“知识”的“理解、应用、分析、综合、评价、创新”等。



图4 课程团队老师入驻小组建设

在目前营造的学习环境中，必须打破校内与校外的界限、课堂和课外的界限、教育与年龄的界限，鼓励学生充分利用线上网络资源与途径，在实践中真正提高甄别、整合及使用相关信息的能力。

第三，确定主题。将学习内容和社会热点结合在一起，既增加了学生对于学习课程内容的兴趣，又对社会的一些问题有所了解。不再是死读书的模式，而是增加了学习内容的宽度和广度。当脑海中有了疑问之后，就会带着这些疑问去寻找答案，带着疑问去学习和思考，更有利于培养学生的学习能力。

基于此模式，一方面，在课堂中引入主题讨论。小组讨论当中可以各抒己见，思维的碰撞可以产生更多的想法，能够充分调动学生学习的主观能动性，彼此之间可以互补、完善和进一步升华。每天所发生和经历的无数事情，有哪些是具备研究和解决的价值又和专业内容相关，是考虑成为研究主题的关键。另一方面，在各小组确定了大方向之后，以大方向为关键词采用思维导图的形式开始头脑风暴，不断把处于雏形化的问题概念化、形象化、具体化，并经过不断思索，一步步为其找到落地基石。网上和课堂是输入，小组学习是输出。学生分组及分工安排如图5所示。

地籍与房产测量课程分组名单

院别: 测绘与地理信息学院 专业班级: 测绘工程 人数: 30

组别	组长		组 员	项目名称
1	姓名	马文静	王正阳 刘龙辉 张梦琦	疫情影响下房地产行业破局之路
	电话			
2	姓名	师琼	刘宇航 孙露露 吴豪	无人机在武汉灾难型事件中的应用和影响
	电话			
3	姓名	魏怡婷	杨真真 郝梦琳 张强燕	网络资源课程在灾难性事件中的应用与影响
	电话			
4	姓名	韩凯旋	唐明旭 黄廷 韩凯旋 董建涛 王鹏举 王香涵 朱梦源	大数据在灾难性事件中的应用
	电话			

每组具体分工安排

第一组:

张梦琦:历史、上疫情对房地产的影响及当时采取的措施采取的措施。
马文静:当下疫情对房地产行业的影响及现阶段所知采取的措施。
王正阳:分析当前局势,有什么有效措施可以降低疫情对房地产行业的影响?
刘龙辉:根据现在的疫情分析未来房地产行业的走势以及预估疫情结束后房价的增长趋势。

第二组:

孙露露:收集此次疫情中无人机测量应用的相关资料。
师琼:分析疫情中无人机测量与往常的异同与优缺点。
吴豪,刘宇航:分析无人机测量在此次疫情中的影响。

第三组:

张强燕:本次事件中不同年龄阶段学生所用的不同软件及应用感受。
杨真真:本次事件中网络课程的应用与影响。
魏怡婷:历中上同由内从灾难性事件中的处理方式

图 5 学生分组及分工安排

第四, 找出落地基石。按“概念解读—材料甄别—案例分析—制定评价标准—辩证讨论—落地”的流程执行。针对落地的基石, 提出各种解决方案, 对每一种方案进行验证, 最终得出可行性方案。

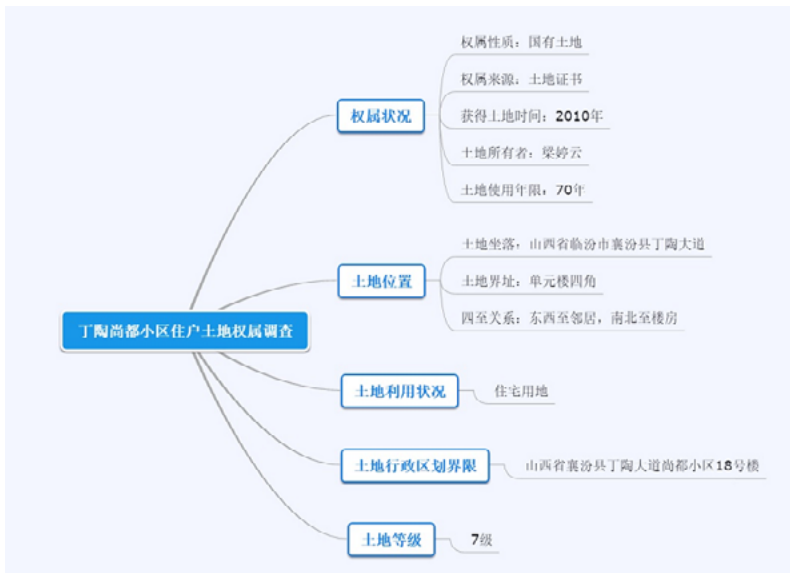


图 6 思维导图形式实验报告

第五, 有效引入思政元素。

当前教育强调“思政进课堂”, 习近平总书记在全国高校思想政治工作会议中强调要用好课堂教学这个主渠道, 各类课程都要与思想政治理论同向同行, 形成协同效果。结合当前疫情, 引导学生从实际案例中深深体会我国政府和人民的高度责任感以及“命运共同体”正确价值观, 使思政元素水到渠成融入教学过程中, “润物细无声”地使学生在畅游知识海洋的同时慢慢树立起正确的价值观。

第六, 学习评价与反馈。

成绩评定时将文献的查阅与平时材料的收集整理 (5%)、线上视频学习与单元测试 (20%)、高阶思维成果的头脑风暴 (20%)、思维导图展示 (10%)、思维创新的课堂讨论与展示 (30%)、结合居住地环境的实验 (15%) 都纳入其中, 用学生自评、师生互评和同行评价的模式构成形成性和过程性评价。这样的考核方式才能对研究导向型的教学模式提供保障。考核方式是检验教师教、学生学效果的重要方式, 也是学生学习方向的“指挥棒”。我们应该让考核方式这个“指挥棒”发挥应有的作用。

四、实施效果分析

通过录制小视频进行课堂展示, 学生明显呈现梯度性进步, 变得敢表达、会表达, 表达沟通能力得到了提升; 通过交叉混合组队, 确定各小组以课程为依托的研究主题, 学生逐渐学会自我定位以及处理合作中出现的各种问题, 变得懂合作、善协作, 团队协作能力得到了提升; 确定研究主题后, 需要学生自主学习, 投入巨大精力去查阅大量文献、搜集相关资料, 在经历过“磨难”后, 学生学会了自主学习方法, 获得了自主解决难题的自信; 获取信息后, 甄别和处理信息这一过程的训练, 使学生的逻辑批判能力得到提升; 提取有用信息后需要验证思路、进行试验、测试软件等找到落地基石, 从而提出解决办法, 这就需要大家讨论、展开头脑风暴, 这一过程使学生的思维能力、分析能力、解决问题的能力都体

现得淋漓尽致；通过观察社会热点，将现实问题融入课程，学生不但提升了发现问题、分析问题和提出自己观点的能力，而且润物细无声地将思政、社会责任感、全民素养带进课堂；学生根据自己的研究主题，结合研究的成果进行了大学生创新创业项目的申报和科技论文的撰写，进一步拓展了思维，提升了创新能力，并为毕业论文选题拓展了思路，对毕业论文质量的提升打下了基础。

研究导向型学习理念在实施过程中受到了督导专家及学生的认可与好评，图7是其评语。此理念下的成果之一是部分学生进行了论文撰写，图8是撰写的部分论文。

华北水利水电大学本科教学在线课程教学质量评价表（督导用）

基本信息	在线课程教学质量评价标准	在线课程教学质量评价表 (60%)					教学效果与学生学习效果 (25%)	综合评价
		教学设计与方法	教学组织	教学团队情况	教学特色	教学效果与学生学习效果		
教师姓名	孟俊贞	15	20	20	10	10	25	100
学院	地理	得分	14	10	10	9	9	92
课程名称	地理与房地产测量	<p>在中国大学MOOC平台建有地理与房地产测量省级精品在线开放课程，学生自主学习课程，每周上课时间在课程讨论区在线讨论和答疑。本环节在督导团展示区提交督导意见，各小组在研究导向型课程截止3月16日的工作进展总结（同时要求每个小组都要截止3月16日的成果发送到指定邮箱）。视频制作良好，讲解清晰，利用思维导图引导学生学习，方式比较新颖，总体效果较好。</p>						
本节授课内容	地理控制测量	<p>说明：针对在线教学方式、听课时间可以灵活掌握，既可以听1节课，也可以对若干在线课程进行巡视。请听课程相关情况记录，并对课堂教学存在的问题提出建议，页面不足可加页。对申请教学质量评价的老师听课后可另附课堂教学质量评价表。</p>						
学生专业	测绘2017014-016	<p>听课人（签字） 康克东 2020年 3月 17</p>						
学生人数	65	<p>建议后续重点跟踪的课程：（学院、课程名称、教师信息及存在的主要问题）</p>						
听课时间	3.17-14:30	<p>将学习内容和热点结合在一起，既增加了我们对于学习课程的内容，又对社会的一些问题有所了解。不再是死读书的模式，而是增加了学习内容的广度和深度。就好比，当我看到老师提供的观点时，就是那个医疗垃圾在土地资源红线线下不当的处理如何改善时，我的脑海中就蹦出来了几个问题。医疗垃圾和土地资源红线有什么关系？医疗垃圾是如何处理的？垃圾处理所占用的土地的面积又是谁？是国家，还是相关的企业？当脑海中有了疑问之后，就会带着这些疑问去寻找答案，带着疑问去学习和思考，更有利于学生的学习。这样的学习模式能够充分调动我们学习的主观能动性，毕竟兴趣是最好的老师，所以这种学习方式能够帮助我们的学习。而在这个模式之上再加上小组讨论就更好了，在小组讨论中可以各抒己见，思维的碰撞可以产生更多的想法，你的想法我没有，当我思考你的想法之后又会产生更多的想法和问题，自然有助于学习。总之小组讨论下的社会热点与课程结合的模式我很喜欢，希望快速落实。</p>						



图7 督导及学生评语

为了进一步验证相对教学改革的其他方法，研究导向型教学模式对学习者的知识体系和价值体系的形成建设带来的影响，我们在学期初（课程开始前）对学生学情进行过调查、分析和记录，图9是参加该方法学习的学生（2017级）最终成绩与往届（2014、2015、2016级）学生的学习成绩横向比较，图示清晰地呈现出该方法的优秀结果。我们计划在课程结束半年到一年后对参加该种模式学习的学生学情进行再次分析和记录，通过数据的纵向比较，分析其产生的影响和效果。

无人机在武汉灾难事件中的应用和影响

摘要：针对传统的救援抗灾模式探讨无人机在此次武汉灾难性事件中发挥的重要作用。通过此次武汉疫情爆发中无人机在报道、宣传、运输物资、测量等方面表现与积极作用来推论无人机在类似灾难事件中实施快速有效管理与支援。

关键词：无人机 报道 宣传

疫情下房地产企业的破局之路

自新冠肺炎疫情爆发以来，我国经济受到了巨大的冲击，房地产也自然成为这次疫情中最“受伤”的行业之一。延长假期、推迟复工、关闭售楼处等举措令销售、新开工、施工、竣工等的房地产行业受到全方位影响。本文以当前受新冠疫情影响的房地产企业为对象，结合2019年房产累计销售额的数据，从楼市、资金链等方面分析房地产企业面临的困境，主要通过研究当前房企与房地产采取的不同应对措施，帮助房地产企业寻找继续经营的方法，进而预估房地产企业未来的发展趋势。

关键字：疫情影响 房地产 措施 趋势

1.背景

新冠肺炎疫情突如其来，牵动举国人心。一场没有硝烟的“疫”

孟俊贞 去掉
孟俊贞 改为
孟俊贞 得分分析的很不错

图8 研究导向型学习成果之一

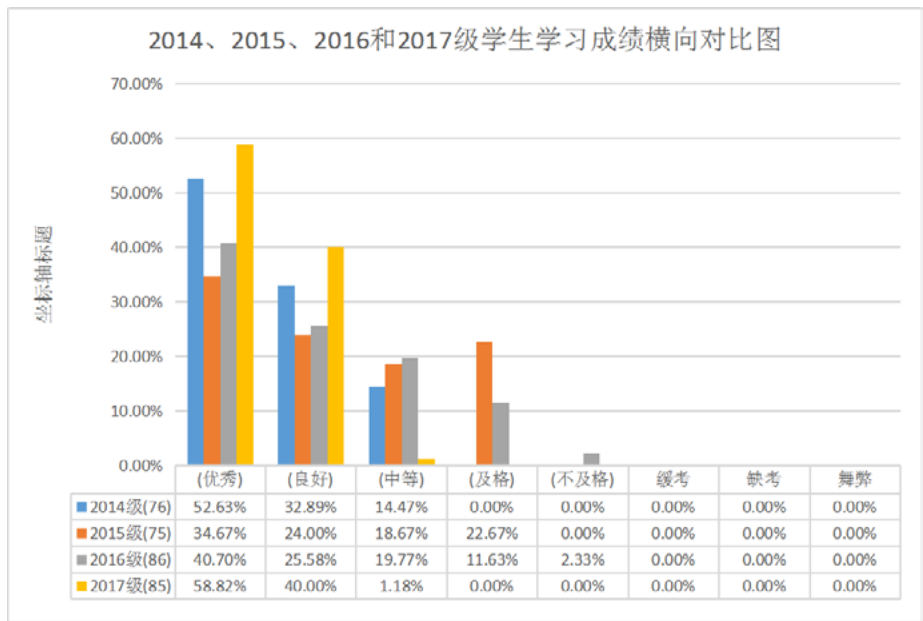


图9 各届学习学习成绩横向对比图（其中2017级学生采用的是研究导向型教学法、2016级采用的是线上线下混合教学法、2014和2015级采用的是传统课堂授课法）

五、总结

研究导向型教学，围绕提升“学习体验”这一核心，建立在“以学习者为中心”基础上，通过“引导”，将每一位学生内心的“火焰”点燃。因此课程本身就是对我们正在经历的一次疫情挑战的研究，而研究导向型教学使学生通过学习，一步步自主地找到属于自己小组的研究主题，这不仅体现了学生对传统学习模式与框架的突破，同时也是老师对自身的教育过程得以完成的最好体现。在疫情期间，研究导向型教学取得了良好的教学效果。同时在整个教学过程中，也获得了一些感受与建议供参考。

1. 研究主题的确立

对研究主题寻找和确定是很多小组无法逾越的障碍，但经过历练最终取得了突破性进展。学生的研究主题不仅涵盖了课程主体模块中各重点的探讨，而且涉及到医药、健康、经济、民生、动物保护、道德素养、法律完善等方面。例如：探究经济可持续性发展与土地生态保护的关联；土地资源红线下如何改善医疗垃圾的不当处理；“火神山”医院建设背景下的土地社会经济特性分析；大数据在新型冠状病毒事件中的应用与影响；网络资源课程在灾难性事件（新型冠状病毒）中的作用；无人机测量在武汉疫情事件中的应用等。

2. 团队老师要积极与学生沟通互动

老师在此过程中担任的是信息传播者、学习支持者和成果观点分享者的角色，通过引导让学生自主地完成学习，不直接干预学生的学习和讨论，而是带给学生一些和学习方向相关的发现，不是直接告知学生该怎么做，而是协助学生对问题进行细化、抽丝剥茧从而理出可能的解决方案，从而验证各方案的可行性以达到解决问题的终点。

大部分学生非常喜欢并享受这种学习模式。然而，也有少部分学生（即被动学习者）并不适应这种学习方式，由于不再有所谓的“标准答案”，他们在应试教育下培养起来的死记硬背技能使他们在在这个过程中显得无所适从。这需要老师多加引导，团队成员多给与帮助，让其慢慢适应并逐渐转变学习观念。

郑州铁路职业技术学院：智慧校园环境下面向服务的校园一卡通系统的建设与实践

文 / 吉鹏霄、梅茜、陈静远等 郑州铁路职业技术学院信息化办公室

一、一卡通的发展趋势

随着“智慧校园”建设理念的深入人心、各类新技术的逐步成熟和信息化应用需求的不断发展，一卡通系统产品和应用方式也正在不断创新。



图 1 高校一卡通发展路径

校园卡不再是唯一的人机交互方式，使用手机和生物特征作为支付和认证的验证方式逐步成为可能；一卡通支付将覆盖校园内多样化的支付场景，各类费用的缴纳都将可以使用一卡通体系；线上支付、移动支付将和刷卡支付方式混合并存，但逐步向全面的移动支付过渡；线上支付和手机支付可以聚合多样化的支付通道，如借记卡圈存签约、网银、第三方支付等；一卡通系统将扩展至高校内的教学、安保、管理等业务领域，配合第三方信息化建设，充分发挥“物联网”的应用价值；一卡通业务办理将逐步整合至移动终端，同时，由于一卡通系统和校园信息化建设的不断融合，各类应用整合也将使用移动终端进行人机交互，如图书借阅、场馆预约、课表查询等。

二、郑州铁路职业技术学院一卡通体系介绍

“面向服务的校园新型一卡通”使得一卡通系统不再是后勤管理的工具，它能服务于校园内的财务收支、信息化资源整合、信息化运维、能源监管、安防防范、后勤服务、业务联动、流程优化。

一卡通系统的各种产品（各种功能）应构成一个应用体系，使之成为客户面向用户提供的一种服务，在满足管理需求的同时，尽量以自动化的智慧方式简化管理过程、提高管理效率、降低管理成本，也充分考量用户的使用体验，尽量以便捷的操作方式、多方位的服务渠道提高用户黏性、降低使用功能所要付出的时空成本。



扫码分享 ▷

1. 软件体系设计

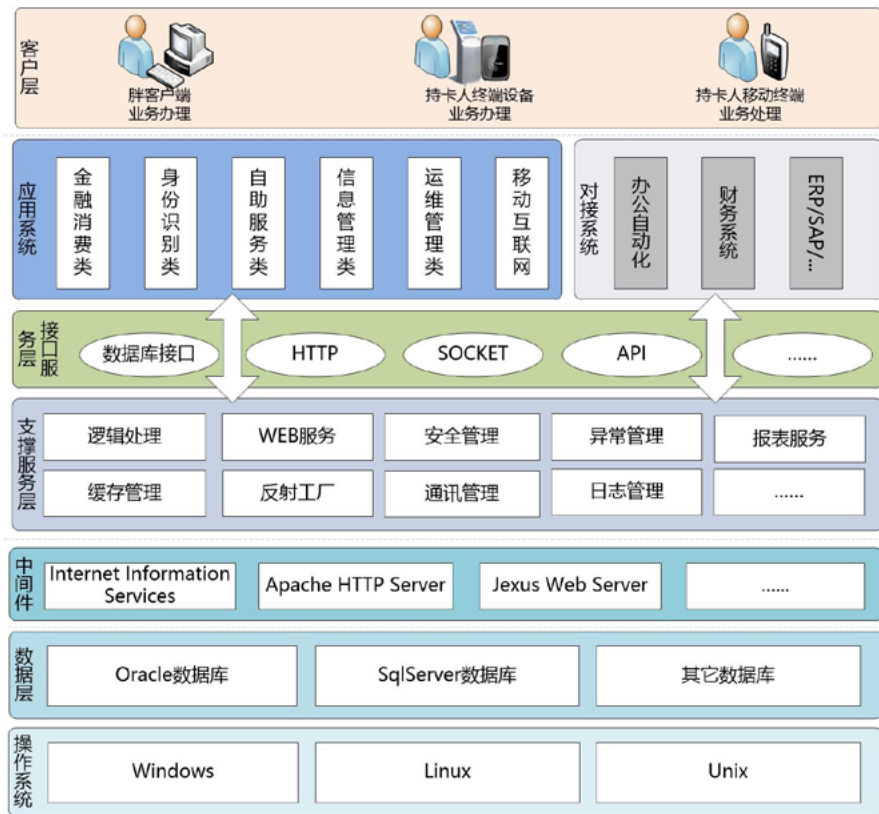


图 2 一卡通系统软件体系

一卡通软件体系具有以下特点：

(1) 维护和升级方式简单。一卡通软件体系部署方便，软件维护只需要管理服务器，所有的客户端都是浏览器，不需要做任何的维护。无论用户的规模有多大都不会增加任何维护升级的工作量，所有的操作只需要针对服务器进行。如果是异地，只需要把服务器连接专网，即可实现远程维护、升级和共享。

(2) 跨平台，选择更多。软件体系采用 B/S 架构，实现了一卡通软件体系与操作系统的无关性，支持使用各种浏览器访问。一卡通系统基础平台服务层，采用 SOA/SCA 架构模式，实现服务组件的灵活装配和快速实现多种协议模式的服务发布，快速满足不同应用系统的调用需求。

SOA (Service-Oriented Architecture) 是一种面向服务架构模型，它可以根据需求通过网络对松散耦合的粗粒度应用组件进行分布式部署、组合和使用。服务层是 SOA 的基础，可以直接被应用调用，从而有效控制系统中与软件代理交互的人为依赖性。

SCA (Service Component Architecture) 是一种组件化的面向服务架构模型，是 SOA 的进一步延伸，SCA 组件与传统业务组件最大区别在于 SCA 实现了“组件和传输协议的分离”、“接口和实现语言的分离”，并提供更完善的组件装配模型和装配策略。并且使用 Web Service、XML 技术、缓存管理等技术进行建设，面向系统整体需求，分析系统内部的各要素如用户、数据、表现、权限等，针对各要素开发可自我管理、自我扩展的管理构件平台，并最终形成可集成、可搭建、可维护、可扩展、高安全、高性能、高质量的信息化系统。

2. 硬件组网设计

承载一卡通系统的网络一般是学校的自有局域网，多机构互联互通和移动互联网应用模式下，也涉及到利用互联网承载部分数据通信的情况，加之项目规模的大小和应用子系统的多少，这些客观需求决定了网络拓扑结构的复杂程度。郑州铁路职业技术学院一卡通系统的网络拓扑是一种“金字塔”结构（如图 3）。数据中心位于“金字塔”的顶端，是整个网络的中心（核心层网络）；中间层是连通分支

机构、第三方系统、移动设备和一卡通终端设备的汇聚层网络；最下层是分布于楼宇内的接入层网络。

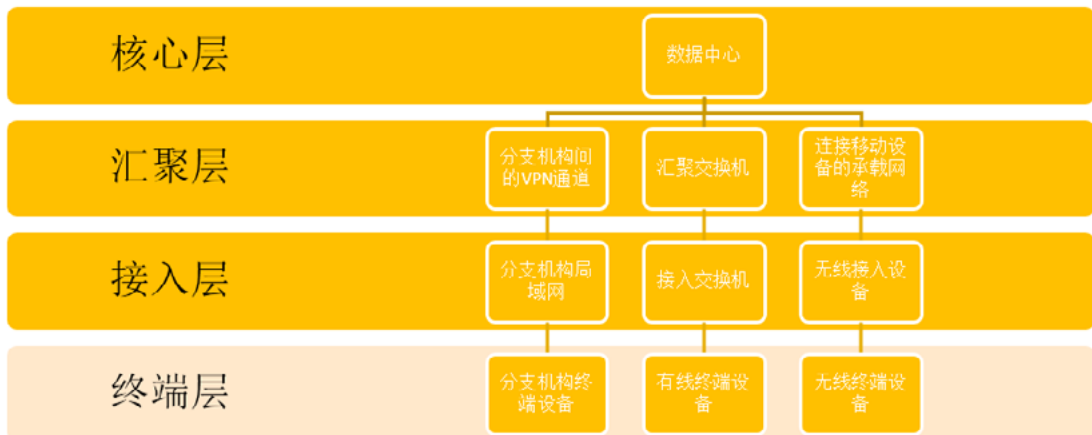


图3 一卡通系统网络拓扑

数据中心的各类设备通常接入机房内的核心交换机，为星型结构。服务器机组支持分布式部署、虚拟化部署，支持 VLAN（虚拟局域网）划分，以保障与其他服务器之间的数据隔离。若选择采用两台数据库服务器进行双机热备模式部署并使用磁盘阵列进行数据存储，则使用 FC-SAN（光纤存储局域网）模式。

分支机构之间的组网一般采用 VPN（虚拟专用网络）技术利用互联网连接分支机构的局域网，其技术实现是使用虚拟隧道通信技术在互联网上构建虚拟专用通道，以保障通信速率和数据安全。机构内的局域网作为一卡通系统的承载网，一般采用 VLAN 技术将一卡通系统内数据通信和其它数据通信（如 OA、网页浏览等常规的网络访问数据）进行隔离。

大部分一卡通终端直接以 TCP/IP 方式接入局域网；部分特殊设备以 CAN-BUS 或 485 方式接入数据采集器，采集器以 TCP/IP 方式接入局域网；一卡通无线终端设备利用 WiFi、zigbee 等技术接入局域网；手机等使用 GPRS、CDMA 技术的无线终端设备经由运营商网络从互联网接入数据中心，一般使用防火墙等设备进行安全防护。

三、建设成效

1. 无现金支付环境

依托系统的支付体系，通过多样化的应用子系统，打造无现金流通的校园支付环境。目前已实现食堂商超、综合缴费、淋浴开水、公寓水电、校车、医疗、借书上机等方面的无现金支付以及虚拟卡支付，达到“完善金融收支渠道，优化财务清结算实现过程”的目的。

充值：支持人工现金充值、圈存机自助充值、现金充值机自助充值、PC 端自助充值和手机端自助充值；支持各类补助金发放，支持 Excel 表格导入和批量规则发放；充值和补助资金，持卡至任意消费终端、领款机、圈存机、自助机等设备，均可刷卡领款，支持手机 NFC 领款（手机须支持 NFC 技术）。

消费：支持多个校区内一卡通行；食堂商超消费支持刷卡支付和虚拟卡支付；支持通过圈存机、自助机、PC 端和手机端进行自助购水购电，购买量自动网络下发，无需人工干预；通过对接使一卡通成为第三方系统的支付手段，包括校医院、图书馆借阅、市内乘坐公交地铁等；支持刷卡控制热水淋浴和开水直饮水，按时长或流量计费，以经济杠杆调节能源利用率。

校外人员食堂就餐：可以通过综合缴费系统的管理端生成代表商户的二维码，校外人员使用微信 / 支付宝扫码支付（须自己输入缴费金额）；也可以通过连接在管理工作站上的扫码枪，扫描校外人员使用微信 / 支付宝生成的付款码进行收款操作（须管理人员在 PC 上输入金额）。

2. 智慧公寓—能耗管理

一卡通系统为宿舍水电提供的解决方案，有效辅助后勤管理，打造绿色节能智慧校园。宿舍电控

(或水控) 不仅仅是计量和收费, 通过补助水电量和阶梯水电价的设置, 可有效缓解浪费严重的现象, 使用经济因素培养学生的节能意识。

宿舍用电的管理需求多种多样。系统支持分路分时段送 / 断电、分路恶载识别功能, 一旦发现违规电器的使用, 自动断电; 并且支持识别规则学习功能, 可根据实际放行或阻止特定电器的使用。

3. 维护安保秩序

系统将校内人员车牌号与人员信息绑定, 出入自动放行。校外车辆可根据需要选择放行 (计费) 或者不放行。

4. 移动端服务整合

一卡通完美校园 APP 主要整合了以下几方面的应用和服务常规卡务操作, 如充值、挂失、查询等; 虚拟卡的载体; 移动支付, 包括一卡通体系内支付 (购水购电、充值等); 校园信息化整合, 包括完美就业、学校介绍、账单查询、通知公告、在线课堂等。

5. 一卡通运维保障

自助现金充值、自助补卡: 卡务中心大部分的工作量都是人工充值和人工补卡, 借助自助设备, 可以有效减少人工成本, 并提升用户体验。

批量智能发卡: 每年暑期过后的迎新发卡压力巨大, 使用批量智能发卡机一次性完成卡片的信息写入和卡面打印, 支持 140 张 / 分钟, 基本实现无人值守, 可大大减轻卡务运维工作的压力。同时, 它还可以用于日常的卡务工作, 如补卡、发放临时卡等场景, 比常规人工发卡方式更高效。

运维 (风险) 稽核: 一卡通系统中终端设备数量众多、体系庞大复杂、业务链条较长, 其运维工作比较复杂, 以往都是“事后处理”。学校运维 (风险) 稽核系统针对一卡通系统正常运转涉及的多个层面 (包括但不限于设备、服务器、数据库、接口、性能、拓扑等) 和一卡通系统的业务链条 (包括但不限于卡状态、缓存交易流水、数据库表空间、坏账等) 进行全面监控, 支持自动体检, 并可以自动发送体检报告。系统旨在收集系统运行数据, 注重运维和业务风险预测, 进而“事前预防”, 并分析系统状态规律, 形成故障的自处理模式。

四、后续发展思考

郑州铁路职业技术学院一卡通系统解决了以往的一卡通系统存在的多校区信息无法互通, 各校区财务独立结算, 无法统一管理、应用孤岛现象严重, 业务流程和应用相互脱节, 人工办理服务效率低下, 运维管理和运营成本高昂, 用户体验较差, 稳定性和可靠性低, 无法满足新的应用需求等问题, 为师生学习、工作和生活提供了高效便利的服务。但是, 一卡通系统仍然存在数据无法跨部门、跨系统共享流转, 各类数据不能形成有价值的信息等问题, 阻碍了学校信息化建设的整体进程。

一卡通系统不能仅仅停留于后勤管理和保障, 下一步更应该借助于一卡通系统真实记录用户的金融数据和行为数据, 侧面收集第三方信息化系统的过程数据, 推动信息的集中与共享, 通过数据建模分析数据意义, 体现数据背后的价值, 实现数据分析辅助决策。(本项目获河南省“2019 年度教育信息化优秀成果 (创新应用类)”二等奖。)

郑州升达经贸管理学院：智能门锁助力智慧校园建设

文 / 杨静、万鹏 郑州升达经贸管理学院现代教育技术中心

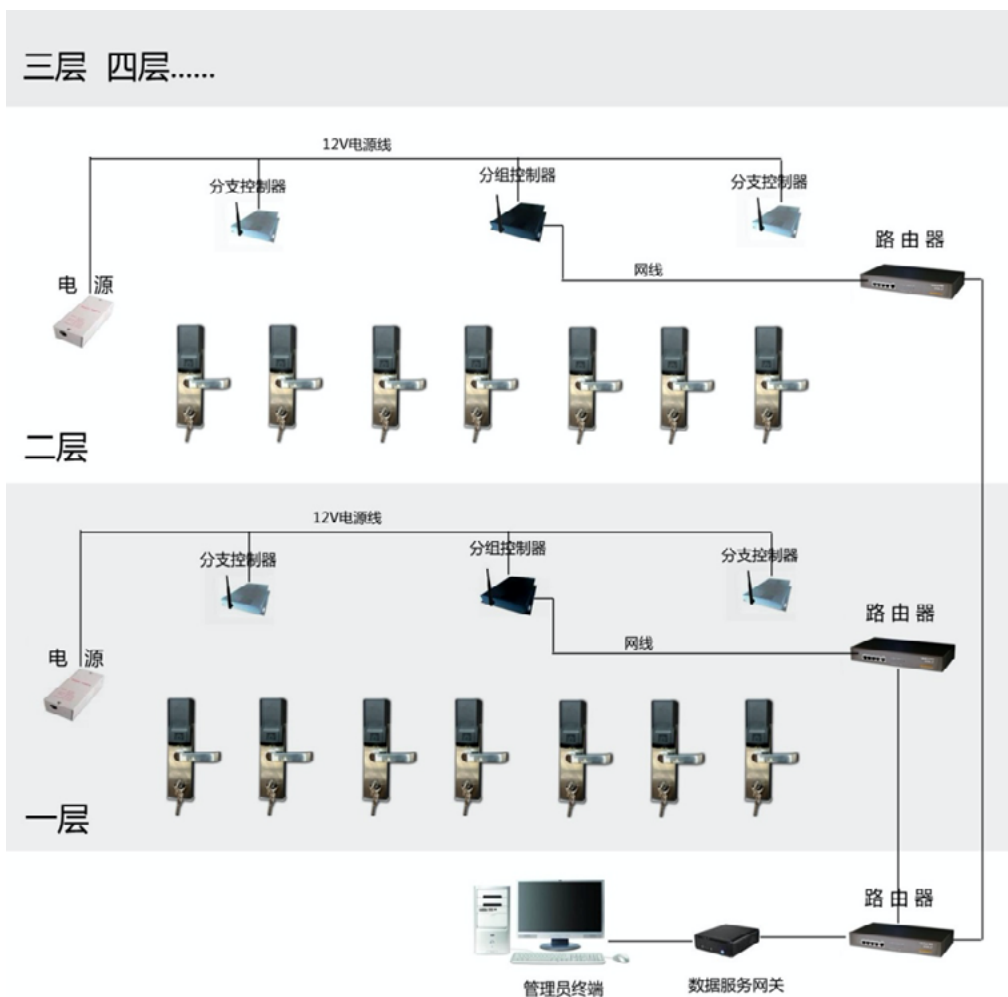
2019年2月，中共中央、国务院印发《中国教育现代化2035》，要求各地区、各部门结合实际认真贯彻落实构建未来校园环境，提升校园智能化水平。郑州升达经贸管理学院也开始加速推进智慧校园建设。智能门锁项目的启动及实施，拉开了学校智慧校园建设的序幕，同时提高了机房管理的效率。

传统门锁，采用机械门锁，使用、维护繁琐且无法记录信息。智能门锁将一卡通技术、物联网技术与门锁有机结合，使用校园一卡通代替钥匙，配合管理软件实现门锁智能化控制和管理，利用无线控制器采集的数据实现安防监控和智能化管理。

一、智能门锁方案

学校通过调研考察，结合实际，对项目实施分期建设。目前，一期已经完成并投入使用，二期已经启动。

为了使设备能有稳定的工作环境，在布线之前需要对现场实际情况调查，包括每栋楼楼内布线情况、线槽走向、竖井位置和常用电源（220V）配电箱位置，以及楼内其他无线信号源对公寓锁安装的影响等。我们通过对这些数据的详细了解和他分析，确定最终的施工布线图如下：



扫码分享 ▷

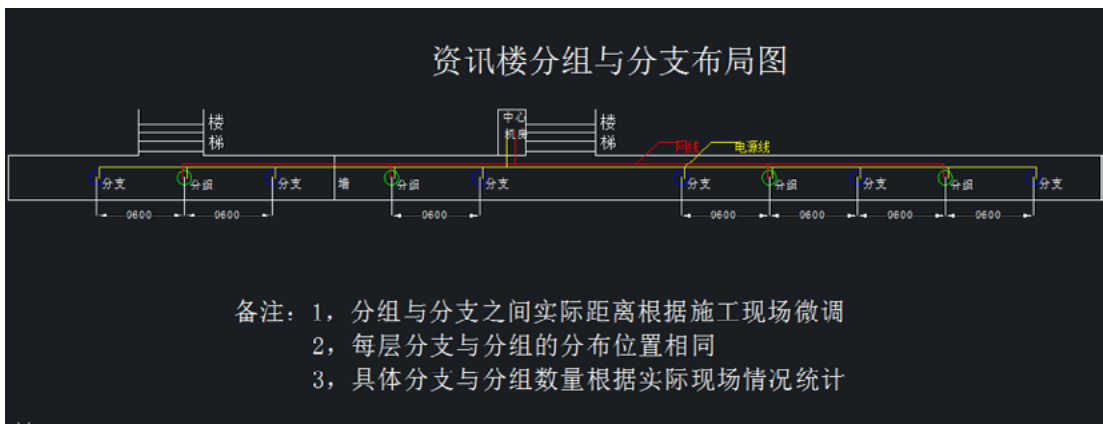


图 1 施工布线图

二、实施效果

1. 对接校园一卡通，权限管理更智能

智能门锁系统中可分区域设置管理员及其权限。后台系统全天 24 小时不间断安全监控，出现异常情况则自动告警，防范于未然。



图 2 门锁管理系统

同时，智能门锁系统与校园一卡通对接，学生可通过一卡通打开对应教室，后台管理软件可实时记录刷卡信息，为之后的校园信息化建设提供数据支持。

2. 与自主研发实时课表系统对接，实现教室管理智能化

宿舍管理与智能门锁对接，每学期只需分配一次权限用户即可。而智能门锁运用到教室管理中，除与一卡通对接外，还需与教务处实时课表对接。门锁管理系统通过读取课表信息，判断在该教室上课的学生，然后把该班级学生一卡通信息下发到门锁，学生可在上课前 10-20 分钟凭自己一卡通刷卡开门锁，进入教室。

资讯大楼 实时课表				
节次	教室名称	课程名称	任课教师	上课班级
01,02	资-206	Access		18级电商专3班(57人)
01,02	资-207	统计学		17营销本2班(53人)
01,02	资-211	计算机应用基础		2019英语本科4班(52人)
01,02	资-212	广告招贴设计		2019视觉传达设计专升本2班(28人)
01,02	资-214 (营销沙...)	市场调研与预测大赛赛...		17营本与电本学生(8人)
01,02	资-215	计算机应用基础		2019翻译本科1班(39人)
01,02	资-216	面向对象程序设计实验		17物联网本1班(59人)
01,02	资-304	C语言程序设计		2019电子信息工程本科2班(58人)
01,02	资-306	计算机应用基础		2019国际经济与贸易专科2班(52人)
01,02	资-309	电脑美术设计 (一)		18级广告本科班(60人)
01,02	资-312	UI设计综合实验		17软件本1班(59人)
01,02	资-313	网页策划与编辑		17汉语言本2班(57人)
01,02	资-314	计算机应用基础		2019社会体育指导与管理本科2...(25人)
01,02	资-316	WEB前端综合实验		2019计算机科学与技术专升本1...(59人)
01,02	资-318	数据分析综合实验		17金本3班(55人)
01,02	资-404	计辅CDR		18级视传本3班(34人)
01,02	资-405	Photoshop平...		18级电商专5班(58人)

图3 门锁管理系统读取课表信息

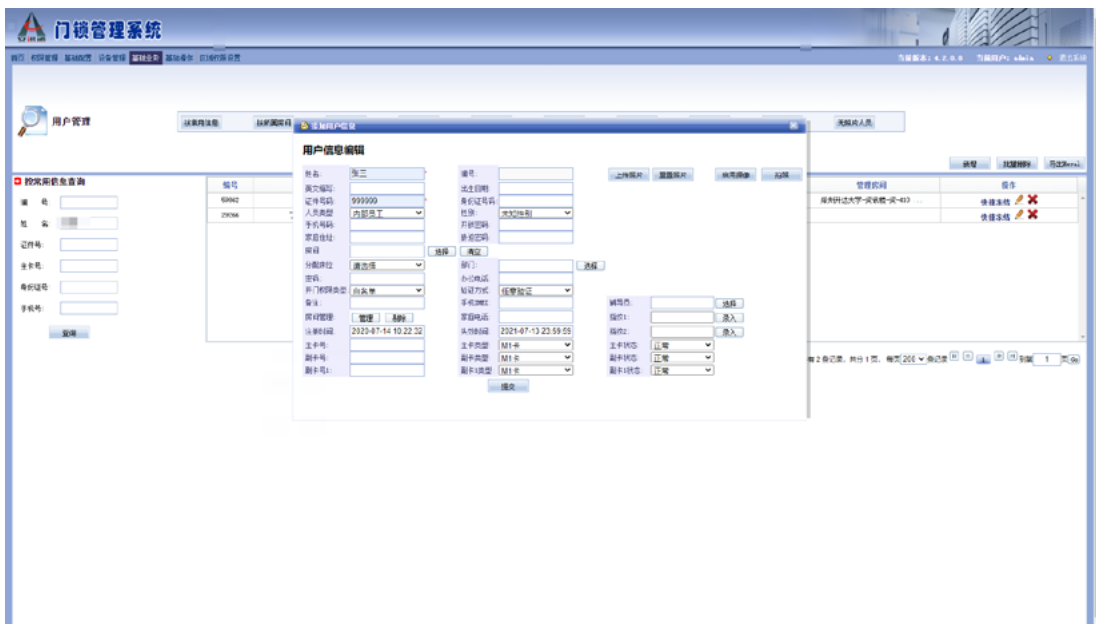


图4 门锁管理系统 - 用户管理

打造智慧校园不是一蹴而就的，智能门锁是打造智慧校园的重要一步。未来，智能门锁将会在功能性和稳定性上持续优化、升级，为广大师生提供更多便利。

资讯

2020 年度河南省教育信息化优秀成果奖获奖名单公布

按照河南省教育厅办公室《关于开展 2020 年度河南省教育信息化优秀成果奖申报工作的通知》（教办科技〔2020〕69 号）要求，经单位申报、专家评审、授奖公示，9 月 1 日，河南省教育厅公布 2020 年度河南省教育信息化优秀成果奖获奖名单，包括理论研究类成果获奖名单、创新应用类成果获奖名单、信息技术与课程融合优质课获奖名单、优秀教育电视节目获奖名单。多所学校硕果累累。

查看链接：<http://www.haedu.gov.cn/2020/09/01/1598944225982.html>

2020 年河南省高校网络安全宣传周“校园日”活动在河南农业大学启动



面对复杂多变的网络安全形势，提高学生网络安全意识、增强学生网络安全自我保护能力尤为重要。9 月 15 日上午，由河南省教育厅主办、河南农业大学承办的 2020 年河南省高校网络安全宣传周“校园日”活动在河南农业大学龙子湖校区开启，来自周边 11 所高校的师生代表参加启动仪式，共同表示要捍卫网络安全，清朗网络空间。

9:00，启动仪式在河南农业大学举行，中共河南省委高校工委专职委员何秀敏，河南农业大学党委书记魏蒙关等领导出席并为 11 所高校大学生网络安全宣传队授旗。

仪式现场进行了网络安全政策法规咨询、电脑“120”服务热线、网络安全宣传推广站、网络协同采摘机器人、智能云端苗圃管理机器人、手机信息安全常识宣传、高校网络安全攻略与典型案例展等 7 个特色项目展示，向大家介绍了网络智能化技术的进步和网络安全存在的漏洞、危害以及应对措施。

何秀敏代表省委高校工委、省教育厅对全省高校提出要求，要求各高校党委要大力营造重视网络安全和信息化工作的浓厚氛围，激励和引导广大师生既要做网络安全的宣传员，更要做网络安全的引领者、倡导者，为落实立德树人根本任务营造清朗的网络空间，为促进国家安全贡献智慧和力量。

“希望大学生们积极主动当好宣传员、监督员，在全社会树立新时代高校师生知网、懂网、用网、爱网、护网的良好形象，在我们建设网络强国的征程中敢担当、勇作为，走在前、做表率。”魏蒙关介绍了河南农业大学开展网络安全的情况，并向广大青年学生发出号召。

在河南农业大学龙子湖校区主干道两侧，两条百米宣传墙形成了网络安全知识长廊。展板上，有关于网络安全的重要内容，还有河南农业大学近年来相关活动开展情况，更多的是各种网络安全注意事项和预防网络诈骗等防范提醒知识。（大河网）

南阳理工学院与中国移动南阳分公司举行“5G+ 智慧校园战略合作签约仪式”



7月21日，南阳理工学院与中国移动南阳分公司“5G+ 智慧校园战略合作签约仪式”举行。校领导刘荣英、肖泽昌、葛晨光，中国移动南阳分公司党委书记、总经理魏际洲等出席签约仪式。会议由校长安士伟主持。

校党委书记刘荣英致辞。她指出，南阳理工学院高度重视信息化建设，2020年学校按照“统一规划、硬件集群、数据集中、应用驱动、重点突破、开放融合”的思路对全校信息化建设进行系统规划和整合，重点开展校园网络、网络安全、智慧校园三大项目建设，其中5G+智慧校园列入特色目标开展建设，5G网络建设作为“新基建”重要领域之一，也是新型智慧校园建设的基础，将会促进人工智能与物联网深度融合发展，万物趋向智能，万物皆可互联，整个社会将因此发生深刻的变革！

她表示，希望双方深入合作，把5G网络与学校智慧校园建设结合起来，使5G新技术赋能智慧校园建设，进一步开拓5G在高校的应用领域，扩大应用范围，打造全方位、多层次的“5G+智慧校园”建设。双方发挥各自优势，砥砺奋进，持续推进信息技术与教育教学深度融合，创建未来教育智慧新场景。

中国移动南阳分公司副总经理曹飞，南阳理工学院副校长葛晨光，分别代表双方签约。签约仪式结束后，中国移动通信集团设计院有限公司河南分公司副总经理郭晓鹏作《创新引领，抢抓数字经济机遇 5G赋能，助推中原经济崛起》经验交流。

据了解，本次双方签约，将联合推进5G+智慧校园建设，积极探索5G+智慧校园建设的新模式，大力促进5G技术的转化应用。（南阳理工学院）

河南理工大学举办 2020 年网络安全等级保护测评培训会



为统筹学校网络安全和信息化发展，查补网络安全漏洞，提升安全防护水平，巩固智慧校园建设成果，7月1日下午，河南理工大学信息化建设与管理中心组织开展了2020年网络安全等级保护测评培训会。会议由信管中心副主任冯文峰主持，学校各职能部门、学院信息安全员和信管中心部分人员参加会议。

冯文峰向与会人员介绍了会议召开的背景和意义。网络安全等级保护是国家网络安全保障的基本制度、基本策略、基本方法，根据国家《网络安全法》和教育部相关工作指南，学校的各类信息系统必须进行等级保护测评。网络安全等级保护测评是今年学校重点工作之一，等级保护测评工作具有较强的专业性，本次培训会议的主题就是向大家普及等级保护的相关知识，对备案和测评工作相关事宜进行解释和指导。

信管中心网络安全科科长刘本仓进行了网络安全等级保护测评培训，详细阐释了等级保护的定义、意义，等级划分及依据，相关条例和指南，等级保护工作流程等内容。就全校网站和系统划分为5个系统（门户网站，校务管理，教学科研，综合服务和一卡通、财务、后勤、监控等）及依据进行了介绍，对信管中心前期的定级和备案准备工作情况进行说明，并结合学校实际情况，就即将开展的等级保护测评的要求、计分点、问题整改等细节，以及对信息系统备案登记表的填写进行了逐条解释和说明，对2020年新增的数据备份一体机和网站代理系统服务向大家做了推广。

会议最后，信管中心综合科科长张俊就近期学校智慧校园推进工作中信息系统统一身份认证和数据集成工作的相关安排向与会人员做了简单介绍。（河南理工大学）

信阳学院：信息化建设与管理处多措并举保障新生顺利报到



9月入学季，信阳学院迎来了六千多名2020级新生入学。受新冠疫情影响，2020年秋季学期的迎新工作时间紧、任务重。面临疫情防控带来的种种不便，信息化建设与管理处开展多项措施服务新生入校，保障迎新工作高效便捷开展。

“智慧迎新”全面升级。信息化建设与管理处依托迎新报到系统，整合了学工、教务、招生、财务缴费、公寓管理、一卡通等多个业务系统，并打通了银行支付、微信支付平台。学生收到录取通知书后，通过电脑或手机登陆迎新系统就可以完成平安入校通行证、上传照片、信息核对、生源地贷款、征兵入伍、在线缴费、自选宿舍、抵校信息登记等事项，入校后学生直接到人脸验证区，1-2秒即可通过身份验证，完成报到。智慧迎新有效避免人员大量集聚，在特殊时期体现出了更大价值。智能、便捷、高效的报到方式令众多新生和家长纷纷点赞。

大数据汇报迎新进度。通过迎新现场智慧大屏或电脑、手机均可实时查看当前入校人数，实时报到率、正在报到人数、各院各专业及各省份报到情况等数据。

做好技术保障。9月10日，信息化建设与管理处提前在学校理工楼广场设置多台人脸识别设备并进行调试，做好迎新准备工作。11日至13日，工作人员全天候坚守现场，保证设备正常运行。为保障迎新期间迎新现场手机信号稳定，信息化建设与管理处协调移动手机信号保障车到达迎新现场。

提前制卡发卡，打有准备之仗。一卡通是每位信阳学院学子在校期间必备的生活、学习小帮手，信息化建设与管理处工作人员提前完成卡片初始化和配卡工作，在新生入校之前将卡片发放至学院，确保每位新生在入校的第一时间拿到一卡通。（信阳学院）

郑州铁路职业技术学院与郑州联通签署“5G 智慧校园建设”合作协议



7月10日，郑州铁路职业技术学院与郑州联通“5G智慧校园建设”合作签约仪式在中牟联通公司举行。郑州铁路职业技术学院校长孔凡士、郑州联通副总经理马成分别代表双方签署协议。

本次5G建设合作协议的签订标志着双方的合作进入一个新的阶段。双方将本着“优势互补、互惠互利、合作共赢”的原则，不断深化校企合作伙伴关系，携手推动“互联网+教育”创新发展新生态。

郑州铁路职业技术学院孔凡士校长表示，希望通过建立合作伙伴关系，整合双方优质资源，在信息化建设等方面进行深度合作，为铁职和联通的发展带来新机遇。

双方将以本次“5G智慧校园建设”为契机，在“5G+”创新领域、教育信息化研发建设方面进行更加紧密的合作，共同助力5G技术创新的发展，为教育现代化建设做出新的贡献。（郑州铁路职业技术学院）

鹤壁职业技术学院与鹤壁联通举行5G智慧校园战略合作协议签约仪式



9月11日上午，鹤壁职业技术学院与中国联通鹤壁市分公司战略合作协议签约仪式在学院举行。院长蔡太生、副院长李希科，中国联通鹤壁市分公司总经理张宏伟、副总经理张红星出席了签约仪式，签约仪式由学院网络安全与信息化处副处长李玉清主持。

院长蔡太生代表学院致辞，介绍了学院的基本情况和近年的发展情况，并对鹤壁联通公司长期以来对学院发展建设的大力支持表示感谢。他希望双方能够秉承合作共赢的理念，以此次合作为契机，围绕智慧校园建设、5G业务应用、专业建设等重点领域开展进一步合作，助力高质量富美鹤城建设和鹤壁市高等教育事业发展，并预祝双方合作圆满成功。

学院副院长李希科、鹤壁联通公司副总经理张红星签署了5G智慧校园战略合作协议。签约仪式结束后，院长蔡太生陪同鹤壁联通公司一行参观了学院图书馆和护理学院。（鹤壁职业技术学院）

全省网络安全督查组到华北水利水电大学指导工作



7月15日下午，由河南省公安厅网安总队和郑州市公安局网安支队组成的督查组一行7人莅临华北水利水电大学检查指导网络安全工作。校党委副书记、工会主席马书臣在龙子湖校区第一会议室主持召开座谈会，党委宣传部部长费昕、党委保卫部部长李尚可、信息化办公室主任周俊胜及信息化办公室相关科室负责人参加座谈。与会人员一起观看了《护网2019》网络攻防演练专题视频。

督查组介绍了此次督察的基本要求，按照“谁执法、谁普法”的原则进行网络安全法的普及宣传，按照省公安厅发出的66号通知书对华北水利水电大学网络安全工作例行检查，根据近期网络安全形势对部分高校进行专题督查和经验交流。马书臣代表学校对学校网络安全工作的领导机制、工作体制和运行状况进行了总体介绍。

周俊胜具体汇报了学校网络安全建设的总体思路、体系框架、主要特色，从组织保障、技术保障、相关法律法规落地执行等方面，详细介绍了学校在网络安全和信息化建设结合方面的具体举措，并就下一步工作规划做了说明。信息安全管理科负责人就学校网络架构、安全等保水平、网络安全软硬件配置等情况向督查组做了现场演示。

听取汇报后，河南省公安厅网安总队等保支队长李恒对华北水利水电大学的网络安全工作给予了充分肯定，他强调华水之所以在全省高校中网络安全工作做得好，得益于学校领导的高度重视和精准指挥，离不开学校在政策和人物方面的全力支持。同时指出，网络安全工作不容小觑，开展等级保护2.0的测评只是手段，目的是通过技术上的日志留存、数据备份可应急处理，为网络安全建设和高水平发展

做好保障。希望学校进一步加强对网络安全工作的领导和关注，在信息安全、网络安全和数据安全方面抓紧抓实、抓细抓小，继续在网络安全工作方面保持稳定、走在前列。

郑州市公安局网安支队等保大队队长洪剑涛谈到，希望学校进一步加强信息化办公室作为责任部门的统筹协调作用，明确全校各部门的共同责任，形成体系化、实战化、常态化的网络安全工作体系。

据悉，督察组还将开展网络安全有关专题测试和检查，针对学校网络安全硬件设备与软件系统进行全面体检和问题排查，提出进一步加强网络安全建设的具体建议。（华北水利水电大学）

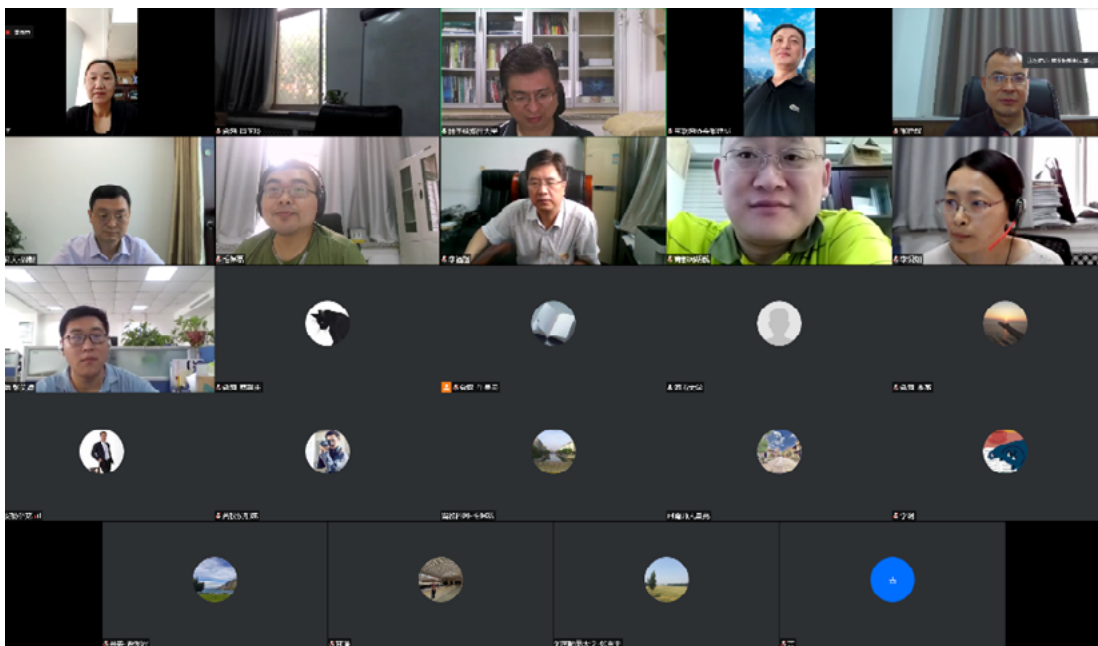
安阳工学院：现代教育技术中心组织开展全校新网站群线上技术培训

2020年7月，安阳工学院网站群系统由VSB9.0版本升级至VSB11版本，共迁移原有网站63个。为了使全校各部门网站管理员尽快熟悉新系统的操作，更好的通过网站开展各项工作，7月8日，现代教育技术中心邀请网站群技术工程师通过钉钉直播对学校教师进行了网站维护及管理的相关技术培训。全校各部门网站管理员、教师代表四十余人参加了培训。

培训中，工程师以图文并茂的方式，从文章编辑、表格编辑、图片编辑、文章发布、文章管理、资料库管理、栏目调整等方面详细讲解了新网站群内容维护的流程和注意事项；从备份与恢复、用户与权限、审核流设定、网站统计等方面详细讲解了网站管理的方法与注意事项，与参加培训的老师们进行了在线交流，详细解答了网站日常管理的有关问题。

此次网站群升级后，实现了电脑端和移动端访问门户网站时的动态适应效果；满足了各部门个性化网页制作需求；实现了对发布文章进行在线审稿核定；提升了网站群的安全性和防篡改能力，达到了计算机等级保护三级的要求，将为学校各项事业发展提供更加便捷、高效、安全的信息技术支撑。（安阳工学院）

省教科网暨省互联网协会下一代互联网工委 2020 年信息安全技术研讨会线上召开



8月19日上午，由河南省教科网网络中心与河南省互联网协会下一代互联网工作委员会联合举办的

2020年“园区网信息安全技术研讨会”在线上召开。河南大学、郑州轻工业大学、河南师范大学、河南农业大学等河南省教科网入网高校，省互联网协会、下一代互联网工作委员会相关人员参加了此次研讨。会议由河南省教科网网络中心常务副主任、下一代互联网工作委员会秘书长林予松教授主持。

会议邀请了战略支援部队信息工程大学国家数字交换系统工程技术研究中心副研究员张建辉、河南科技大学网络信息中心副主任周毅、河南省教育信息安全监测中心副主任李润知分别作主题报告。

张建辉副研究员在其报告《网络信息安全技术发展新趋势》中，从信息安全与网络攻击的主要趋势切入，分析了新形势下网络安全新态势，介绍了网络安全的新技术，为园区网信息安全防护提供了宝贵意见以及更加开阔的思路。

周毅副主任在其报告《校园网络安全体系建设实践》中，分享了河南科技大学“人防+技防+安服”的总体建设思路以及具体实践。对于未来规划，周主任指出：将以等保2.0为标准，继续完善学校的网络安全体系建设；继续推进专业网络安全服务；发挥学校及学科优势，建立一支高水平的安全服务团队。

李润知副主任结合热点事件，阐述了数据安全防护正在面临的各种挑战，分享了如何开展业务梳理、分级分类、策略制定、技术管控、优化改进等五个阶段的数据安全治理工作，以及园区网数据安全的防护思路。

在讨论环节，参会人员围绕会议主题，就校园网络安全监测、企业信息安全防护等问题进行了交流讨论。此次会议搭建了一个专业的交流与学习平台，将进一步助力园区网的信息安全防护体系建设。（河南省教育科研网网络中心）



《河南教育信息化》 征稿简则

《河南教育信息化》由河南省教育厅科学技术与信息化处主管，河南省教育科研计算机网络中心主办。刊载行业动态、热点专题、经验交流及省内资讯等内容，多方位、多层次地探究教育信息化及教育网络建设的前沿趋势、经验与问题，为教育信息化领域各级领导及从业人员提供科学、实用的决策依据。自2020年，河南省教育厅将《河南教育信息化》刊发文章列入“河南省教育信息化优秀成果”评奖依据。[\(点击进入：河南省教育厅办公室关于开展2020年度河南省教育信息化优秀成果奖申报工作的通知\)](#)

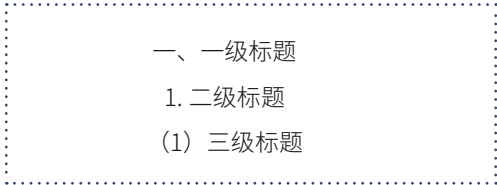
来稿要求如下：

- 1、文章具有创新性，主题明确，数据可靠，论据充分，逻辑严密，语言简洁，图表清晰。
- 2、来稿附作者简介（工作单位及职务，联系电话及E-mail）。
- 3、来稿请以“文章标题+作者姓名”为邮件标题发送电子邮件，文稿（Word格式、宋体）及图表原图添加至附件。

4、文章结构包括：中文标题，摘要（或者核心观点），正文，参考文献（适用于学术性论文）。

文章标题应简明、具体、确切，概括论文要旨，不使用非公知的缩写词、代码等（一般不超过20字）。

文中标题标示格式：

- 
- 一、一级标题
 - 1. 二级标题
 - (1) 三级标题

- 5、论文中图、表和公式应通篇分别编号，图、表必须有图题、表题。
- 6、基金项目：若来稿有资助背景，应标明基金项目名称及编号。
- 7、文责自负，作者对因稿件内容所引起的纠纷或其他问题承担相应的责任。
- 8、依据《著作权法》的有关规定，本刊可对来稿作文字性修改。作者若不同意修改，请在来稿时注明。
- 9、稿件录用后，我们将支付作者适当稿酬。

附：征稿栏目

1、热点

多角度、深入探讨教育信息化热点问题。每篇稿件1500—4000字之间。

2、成果

分享各地各校在教育信息化工作方面的成果，有可供借鉴的思想与方法，促进交流及学习，共同提高。每篇稿件2000—4000字之间。

3、资讯

分享各地各校教育信息化工作相关新闻，稿件中需呈现新闻事件对实际工作的价值和意义。每篇稿件800字左右。

电子邮箱：editor@ha.edu.cn



河南教育 信息化

回目录