2021年第8期（10月）

信息化工作动态

信息化办公室、网络信息技术中心

网络安全宣传周活动全面展开

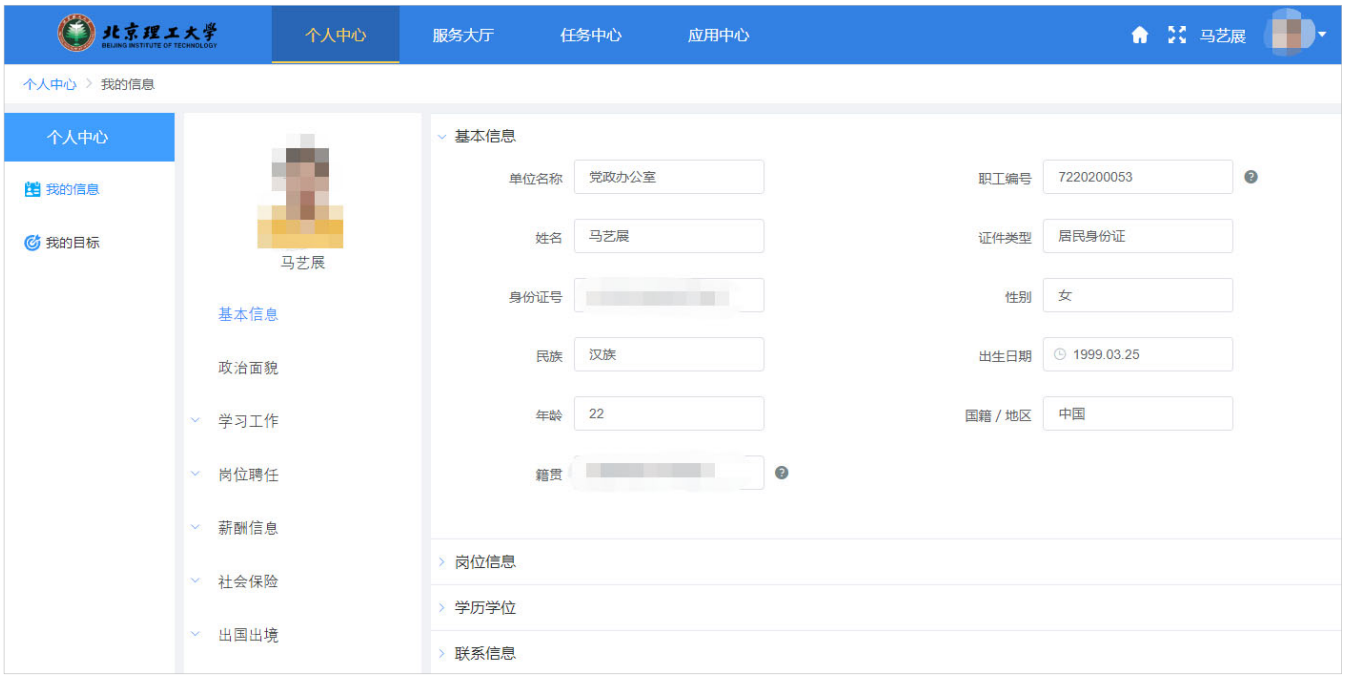
为教育引导广大师生树立正确的网络安全观，普及《网络安全法》《数据安全法》等法律法规，掌握网络安全知识，筑牢校园网络安全屏障，按照上级要求，北京理工大学国家网络安全宣传周活动于10月中旬全面展开，主题为**“网络安全为人民，网络安全靠人民”**，活动由网络信息技术中心主办，网络安全学院、网络开拓者协会、网络安全俱乐部联合承办。

本次网络安全宣传周活动立足师生员工工作生活实际，通过网络安全专题讲座、网络安全知识竞赛、网络直播间、线下网络安全互动展示等多种方式，全面提升参与师生的网络安全意识。在活动周期间，学校从师生校园生活、网络安全技术发展、网络安全形势、网络安全意识等不同角度，邀请北京市公安局刑事侦查总队反诈骗专家高山警官、阿里巴巴集团阿里云安全市场战略负责人王瑜、教育部信息安全专家王永琦、中国软件评测中心网络安全专家白利芳和安恒信息公司专家胡宁等一批高水平专家到校，为师生们举办了**“电信网络诈骗基础知识与防范”“云上云下20年：网络安全20年技术和理念变化”“关注网络安全形势、提升网络安全意识”“网络安全形势分析与监管要求解读”和“网络安全意识漫谈”**等高水平培训讲座。

我为群众办实事

数智驱动，人事系统改造升级

为配合学校推进信息化建设高质量发展，围绕学校智慧校园建设，推动现代信息技术在管理、服务等领域有效应用，人事系统完成新一轮升级改造。

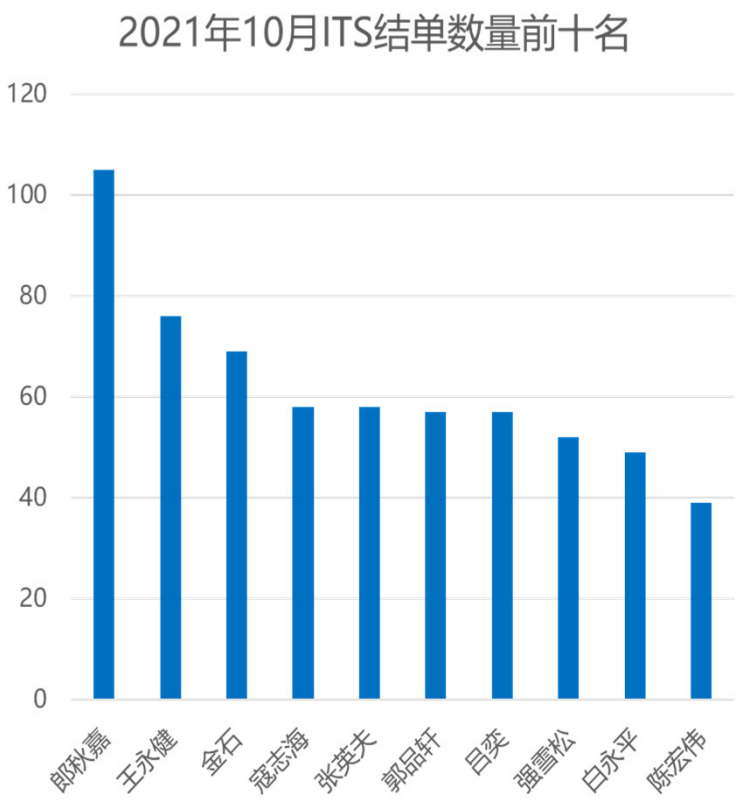


优化体验，上线员工服务中心模块。教职工可在员工服务中心查询个人基本信息，完成相关业务申报。系统自动读取基本信息，无需教师多处填写，利用业务流程促使教师填写的信息准确、真实、规范。申报完成后第一时间通知相关职能部门办理，提高业务审核效率。同时教职工可根据自身需求灵活配置业务模块，深度参与到业务服务平台之中。

简化流程，多业务实现线上申报。在系统建设规划中，多方不断沟通、打磨方案、优化流程，逐步将各项高频人事业务实现线上流程化，最大程度地节省教职工业务办理和信息填报的时间、精力。上线**岗位聘用、内部调动申请、博士后公寓申请**等模块，在响应学校“最多跑一次”理念的同时，向“**一次不用跑**”靠拢。

我为群众办实事

ITS服务和管理流程精细化



服务流程管理系统化。在线报修、在线客服和电话客服接单整合为工单系统。工单系统9月结单量为344件，10月结单量为768件，环比增长超过123%。

运维巡检常态化。良乡校区新安排1名ITS驻场学生工作部，增强文科组团楼服务力量。安排ITS开展全校484个设备间预防性巡检，对1064个可能影响用户网络使用的接电插排和PDU进行排查。

服务考评制度化。从接单响应速度、问题解决效果、结单量、加班量和师生满意度评价等五个维度进行考评，对个人或团队实行月度奖励。

博士毕业生离校流程线上办理

毕业生在离校前，需要线下完成缴费、归还图书、办理退宿等多项业务。10月，信息化办公室牵头，协同网络信息技术中心、计划财务部、图书馆、学生事务中心等多部门，整理博士毕业生**离校7项**核心流程，完成**线上流程再造**。

实现智慧北理统一门户及i北理双入口，提升学生离校体验，**让学生“少跑路”**。各学院可线上查看办理进度，提高工作效率。秋季毕业离校平稳运行，共203名博士完成毕业离校办理。

我为群众办实事

i北理用户粘性持续提升

App使用率持续上升。活跃用户数维持在2.5万/日左右，组织内沟通每日2000人以上，线上视频时长超过2000分钟/日，自建应用访问量超过1.5万次/日，师生协作更便捷。

截止目前，接入i北理APP的校内应用共涉及6大板块，47个业务，其中12个应用月度使用超过万次。

线上教学：延河课堂中乐学、直播、录播、精品课等8个应用

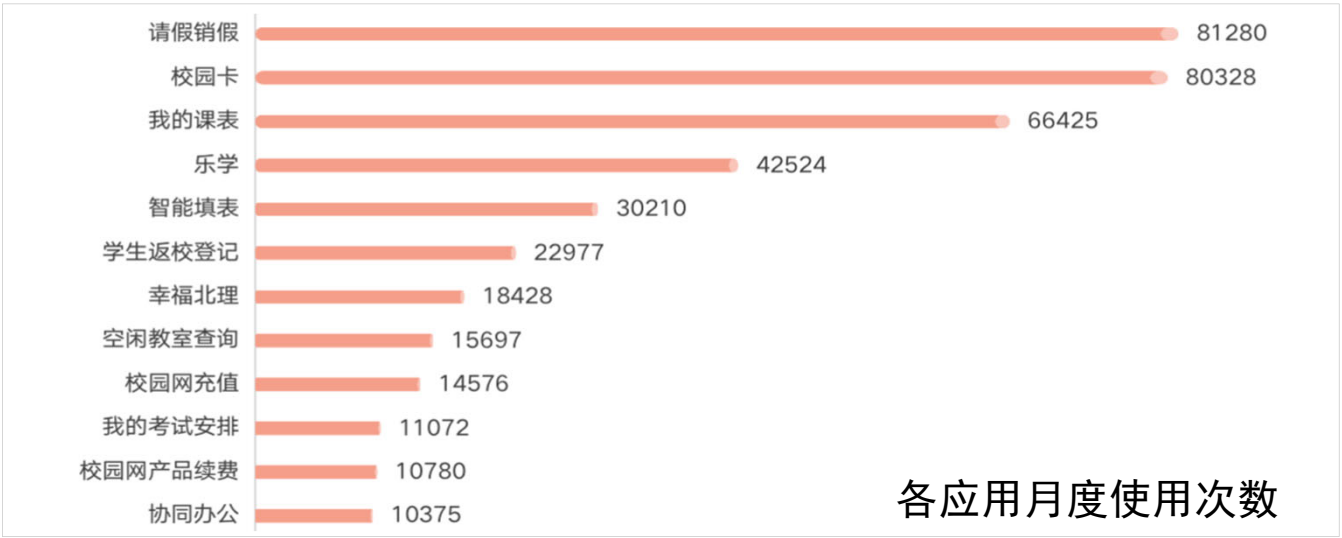
教务管理：课表查询、调停课、空教室查询、考试查询等12个应用

校务管理：访校人员登记、协同办公、每周会议、公文发布等7个应用

学生事务：返校登记、请假销假、场地预约、学生信息等7个应用

校园服务：校园卡、班车查询、党费缴纳、京工飞鸿等9个应用

IT服务：校园网充值、IPTV、电脑义诊、身份切换4个应用



各应用月度使用次数

数据治理

一站式填报启动学院绩效考核

10月27日，信息化办公室在2号楼133会议室召开教师工作量考核平台培训会议，各学院分管教师工作量考核院领导、人事干事及信息化专员共计30余人参会。

会议介绍了标准化教师工作量考核平台与论文认领平台的操作方式，对下一步标准化教师工作量考核平台的推广工作进行了部署，要求各学院继续对照考核办法确认考核指标体系，明确四类考核指标审核人员，通知本学院教师认领论文。

会后一周，共360名教师认领了9250篇论文。10个学院对平均22项指标提出修改意见，网络信息技术中心梳理意见并逐一整理，将标准化教师工作量考核平台的指标体系从18项一级指标28项二级指标扩充至26项一级指标39项二级指标。

数据门户确认本科教学可视化原型

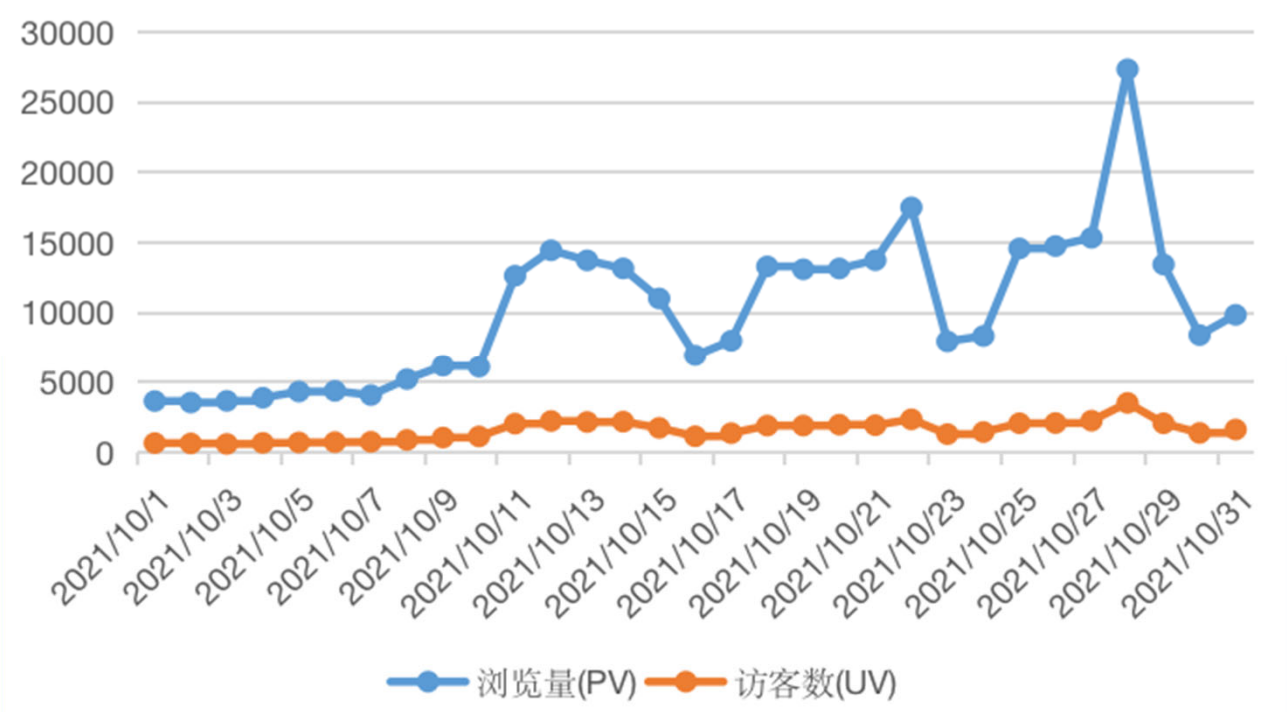
10月，网络信息技术中心联系教务部对北京理工大学数据门户中本科教学部分进行原型确认与数据抓取工作。

本科教学可视化原型将采用饼图、柱状图、堆叠图等多种形式，从本科生总体概况、本科生招生情况、本科生教学等5大类15小类描述本科教学相关业务。根据使用人员的不同，划分不同的权限，如干事、辅导员、管理人员等，并可以自定筛选项进行灵活查询。

延河课堂

延河课堂用户访问量持续增长

延河课堂用户日均访问量超1.2万，日均用户数超1200人，共计观看直播9.2万次、观看录播23万次，总用户数超1万人。其中观看最多的课程为《近代数学基础》，累计观看次数超4000次。



延河课堂联盟共享课正式开课。10月，延河课堂上线联盟共享课程16门，共计447人选课，站内资源观看3.5万次，同时将校内生命科学基础、大学物理A(II)两门课程的录播视频开放至联盟高校学生，推动优质课程内容共享，提升教学效果。

联盟共享课（部分）	观看人数	选课人数
Python语言程序设计	1139	68
基础免疫学	957	15
大数据技术导论	913	22
创新工程与实践	909	29
创新创业管理	808	27
现代文学名家短章精读	592	23
沟通与人生	517	13
C语言程序设计（上）	427	11
公司财务管理	404	20
微积分（一）	386	184
礼仪文化与有效沟通	377	15

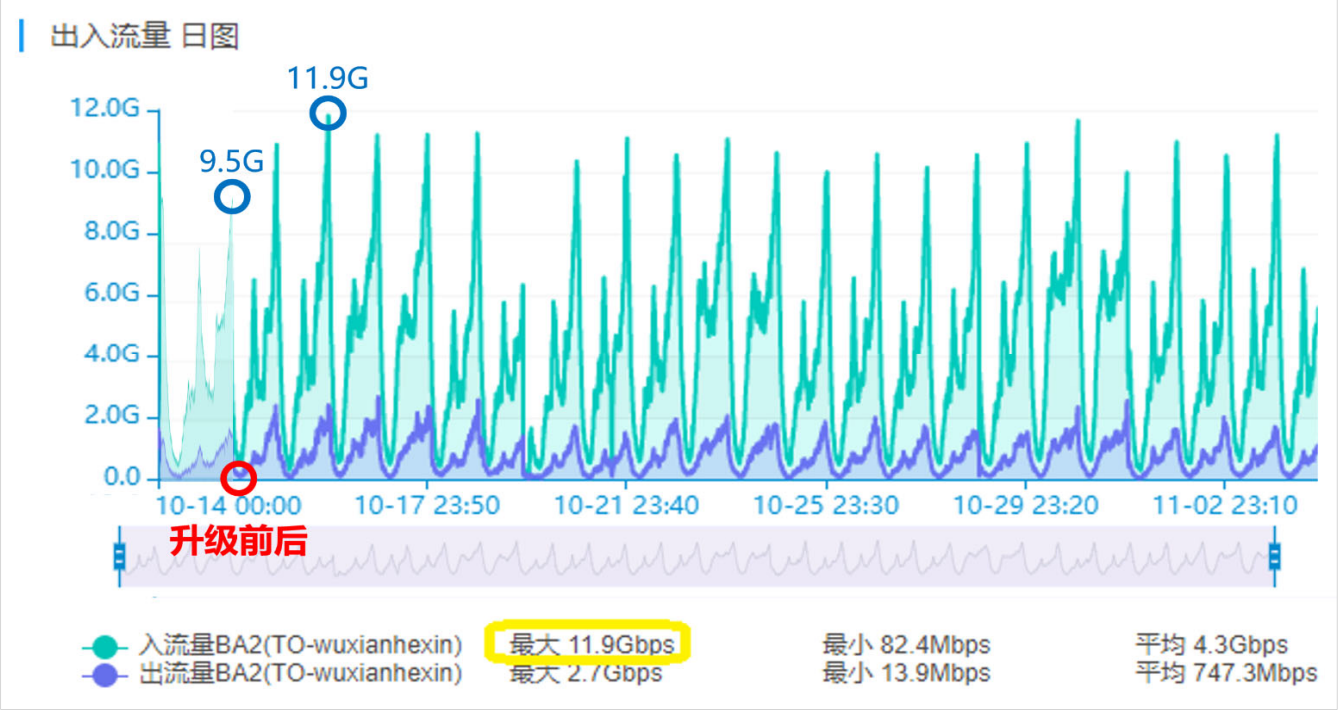
站内观看次数Top7课程	观看次数	观看人数
近代数学基础	4155	226
研究生导师岗前培训	3976	349
安全概论	2205	862
大学计算机	2197	300
工程制图C	2022	241
计算机仿真与Matlab	1719	120
概率与数理统计	1594	425

信息化“新基建”

中关村宿舍区无线网络带宽扩容

宿舍区骨干互联带宽倍增。主动巡检过程中发现中关村宿舍区无线网存在用网瓶颈，升级后宿舍区骨干互联带宽由10G倍增为20G。

峰值用户流量提升20%。升级之前，中关村宿舍区无线网峰值为9.5G，接近原有10G互联带宽的瓶颈点；升级之后，峰值流量提升为11.9G，整体流量提升近20%，消除拥塞瓶颈的同时有力提升终端用户的无线网访问体验。



良乡校区核心机房UPS升级

全面消除核心机房供电安全隐患。原有UPS设备从2007年良乡校区建成至今已运行近14年，严重超期服役，主机及后备电池均存在极大安全隐患。

UPS满载供电时间倍增。升级后UPS容量由20kVA增加到30kVA，电池节数由32节倍增至64节。市电中断时，UPS电池的供电时间由2小时倍增提升至4小时，有力保证了良乡校区整体核心网络设备的平稳有序运行。

校园网出口防火墙软件优化升级

主控芯片软件升级，优化主控设备检测机制。单次检测提升为双次检测，160微秒超时提升为10000微秒超时，充分保障通道检测信号的可用性。**优化DMA通道处理机制，降低故障修复时间。**支持板卡热插拔方式恢复DMA通道数据读取。**防火墙配置查漏补缺。**防火墙配置定期备份，增加核心互联设备探测次数，针对挖矿域名实施精准阻断。

网络安全保障

升级邮件网关系统 加强邮件安全巡检

学校邮件系统长期遭受高频次暴力破解用户账号的攻击，10月，学校邮件网关系统升级完成，加强发信管理，及时发现和处理被盗账号，拦截滥发垃圾邮件，保护学校邮箱安全的同时，提升学校邮箱声誉。

邮件启动双向检测。学校用户发送的邮件，除原有的涉密关键字检查外，实施与域外邮件相同的检查策略，阻断学校邮箱发垃圾邮件的行为，日均拦截90封。

拦截被盗账号滥发的垃圾邮件

tls	日期	集群节点	ID	IP地址	发件人	收件人	邮件主题	拦截原因	大小
	10-28 00:36:35	10.0.0.85	61798012.001	117.64.224.182	@bit.edu.cn	1913315606@....	JND→1913315606輕浪....	内容滥发	87.6K
	10-28 00:32:44	10.0.0.85	61797F2A.002	117.68.194.47	@bit.edu.cn	1826927495@....	JND→高大喬ホ18269274....	内容滥发	84.4K
	10-28 00:32:39	10.0.0.85	61797F25.003	117.68.194.47	@bit.edu.cn	3607024226@....	JND→3607024226夾帶....		83.7K
	10-28 00:32:04	10.0.0.85	61797F03.000	60.168.81.129	@bit.edu.cn	1655751555@....	JND→劉勇liuyong海洋资....	内容滥发	85.1K
	10-28 00:27:12	10.0.0.85	61797DDF.000	117.64.225.196	@bit.edu.cn	2331351335@....	JND→汤芹光趙霞zhaoxia....	内容滥发	84.9K
	10-28 00:24:47	10.0.0.85	61797D4E.001	114.97.184.64	@bit.edu.cn	517518967@q....	JND→徐斗邓雨維dengyuw....		85.7K
	10-28 00:19:00	10.0.0.83	61797BF3.000	117.64.224.250	bit.edu.cn	2293082715@....	JND→适喉寬松舊ㅂ堂前燕戰略s....	内容滥发	85.7K
	10-28 00:18:47	10.0.0.83	61797BE6.001	117.64.224.250	@bit.edu.cn	2870704617@....	JND→2870704617炏ф....	内容滥发	84.7K
	10-28 00:17:45	10.0.0.85	61797BA8.001	114.97.185.151	@bit.edu.cn	897738500@q....	897738500-蠶蛋 f9....	内容滥发	84.8K
	10-28 00:16:16	10.0.0.83	61797B4F.000	60.168.81.186	bit.edu.cn	756676892@q....	756676892-菏南 45....	内容滥发	85.2K
	10-28 00:15:50	10.0.0.83	61797B35.002	117.64.234.222	@bit.edu.cn	2430507277@....	2430507277-炮手 9....	内容滥发	85.1K

被盗邮箱随查随封。增加对被盗邮箱的检测、报警策略，对疑似被盗邮箱及时联系用户核实，对确认被盗邮箱立刻查封，截至10月底，已查封被盗邮箱44个。

封禁邮箱发送提醒。对可疑和封禁邮箱发送提醒邮件，确保邮箱密码更新后功能才能开放。截至10月底，已发送可疑账号提醒邮件212封，封禁账号提醒邮件44封。

向封禁账号发送提醒邮件

邮箱安全提醒

发件人 "网络信息技术中心" <antispam@bit.edu.cn>

日　期 2021年11月01日 星期一 15:26

收件人

发送状态：邮件投递成功。 [查看详情]

校邮箱用户：

您好！在我中心10月的邮箱安全监控巡检中，发现您所使用的邮箱有被盗号和盗用发垃圾邮件的情况，系统已自动启动禁止外发信件的功能。为保障您邮箱安全，请您尽快登录学校的邮箱系统，https://mail.bit.edu.cn，修改密码，并请联系68914829解封邮箱发信功能。

网络信息技术中心

2021年11月1日

网络安全保障

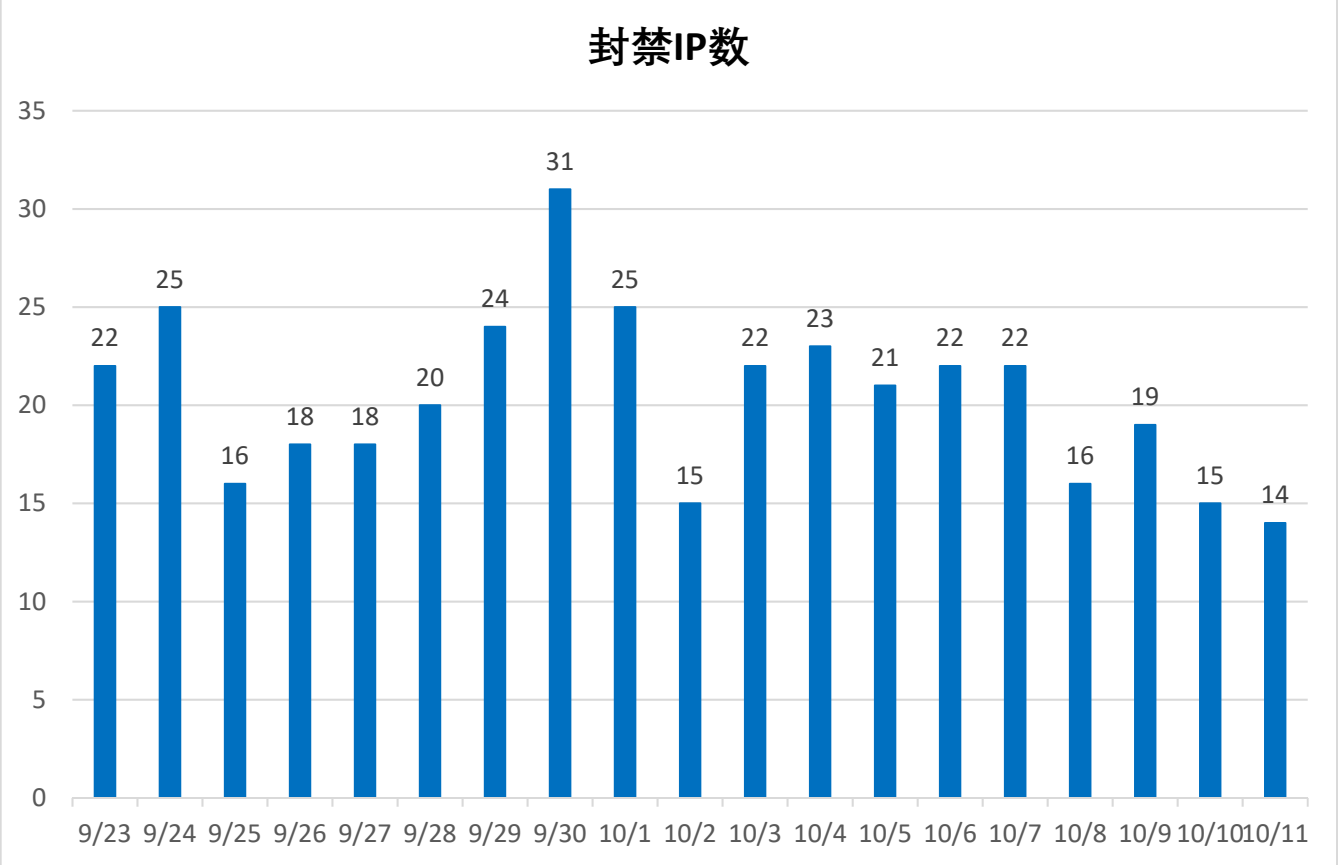
保障国庆期间网络安全

国庆期间重点保障核心信息基础设施。关停问题主机8台次，处置数据中心内部安全事件13起，封禁恶意攻击源388个，处置病毒13起，全面提升安全防御水平。

外连事件类型	外连次数	百分比
僵尸网络事件	11201	32.78%
特洛伊木马事件	10982	32.14%
挖矿事件	4884	14.29%
其它有害程序事件	3665	10.73%
后门攻击事件	1345	3.94%
蠕虫事件	744	2.18%
计算机病毒事件	641	1.88%
勒索事件	528	1.55%
信息窃取事件	155	0.45%
混合攻击程序事件	27	0.08%

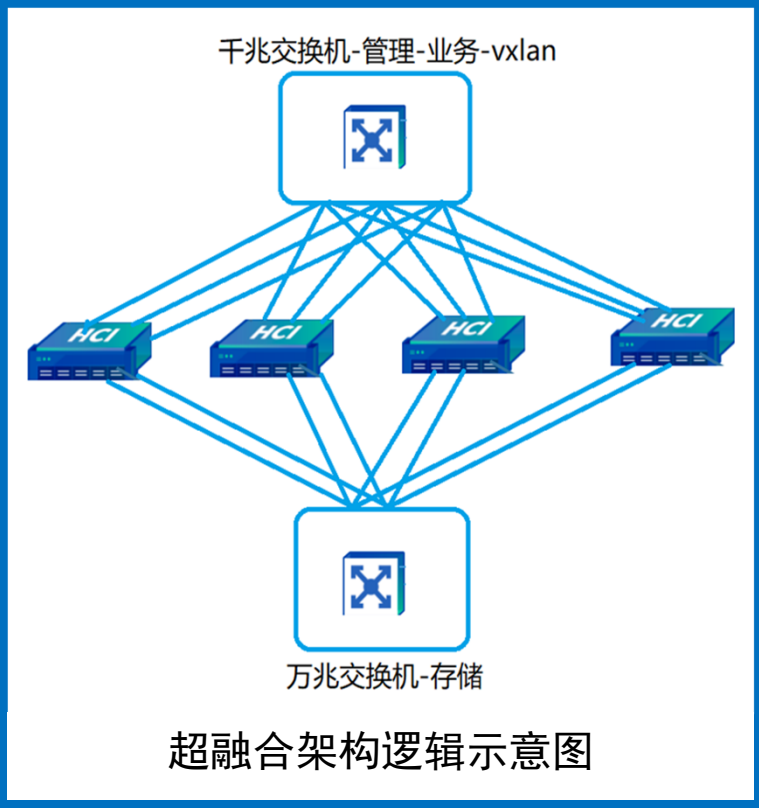
夯实安全基线管理。处置两部门的顽固网络安全问题2台次，升级版本，修补漏洞，事件闭环处理，做到本质安全。

地毯式清理弱口令。处理涉及10个部处学院的12个应用系统的弱口令，处理涉及200台网络设备的弱口令，及时消除安全隐患。



网络安全保障

校园私有云国产化超融合架构初步部署



超融合架构逻辑示意图

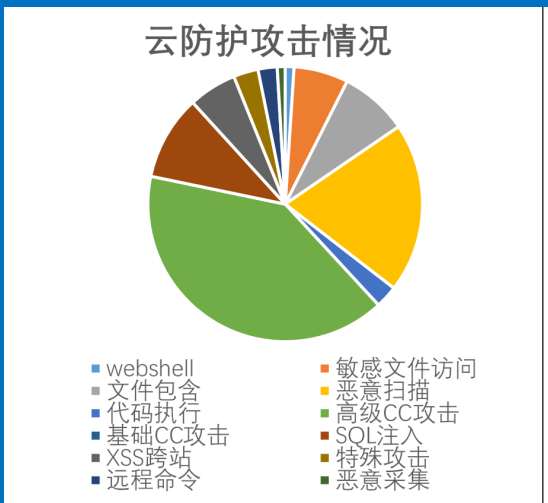
实施国产化私有云平台，破解供应链封锁。建成国产私有云平台计算资源池，CPU96核，内存2T ，可用存储96T，备份池10T。按最佳配置提供一卡通专用计算资源池，逻辑配置专属CPU、内存和硬盘。

精细化私有云网络存储规划。采用专用千兆万兆接入交换机，分隔管理、业务、vxlan及存储网段，确保底层网络平稳顺畅。与项目实施方进行5轮次的讨论制定周密升级方案，保障17台业务系统开机迁移，做到用户无感知，确保不影响师生正常工作生活。

内外双重防护机制保障校园网络安全秩序

外网攻击数量仍在高位。通过云防护平台对学校网站的总请求数53566444次，总流量3218.59GB，平台清洗9.56GB恶意流量。本月遭受黑客攻击总次数4522697次，黑客攻击占总请求数比率8.44%，比9月的3.3%有较大增长。

内网攻击数较上月更加严峻。动态优化防御策略，精确定位，发现攻击行为3371464起，环比增加275.7%。处理可疑事件3652起，环比增加19.6%。



攻击类型	攻击数
webshell	46789
敏感文件访问	290246
文件包含	362933
恶意扫描	904314
代码执行	119577
高级 CC 攻击	1815106
基础 CC 攻击	95
SQL 注入	451394
XSS 跨站	256557
特殊攻击	131541
远程命令	101747
恶意采集	42243
其它	155