

在高校治理现代化视域下,基于以上构建的成都体育学院智慧校园建设新理念,参照国家相关标准,并结合学校实际,文章搭建了成都体育学院智慧校园建设框架,如图1所示。建设框架包括基础设施层、支撑平台层、应用平台层、应用终端层、智慧校园技术规范与保障体系、智慧校园信息安全体系六块内容。

4.1 基础设施层

基础设施层是智慧校园建设的基础设施保障,是实现学校治理现代化的硬件支撑,此部分体现了学校在智慧校园建设中对信息技术“新基建”的创新应用。包括校园网络、感知平台、机房等海量数据汇集存储。校园网络是指以有线网、无线网、物联网、5G技术的四网融合为基础网络架构;感知平台包括 ZigBee、传感器、SDN、RFID 等物联网新兴技术应用;学校将在新校区打造 450m² 中心机房,为智慧校园的各种应用提供基础支持。

4.2 支撑平台层

支撑平台层是体现智慧校园云计算、大数据服务能力的核心层,为实现学校治理现代化提供驱动中枢,最主要的平台是大数据平台,还包括私有云存储平台和统一身份认证平台等。大数据平台负责处理结构化数据和非结构化数据。数据中心管理平台负责处理结构化数据,可实现全校各业务系统的深度融合。数据资源的有效整合,进行数据处理、数据交换和数据共享,为全校师生提供数据服务,更为学校基于大数据的决策支持提供基础数据;非结构化数据包含来自网页、日志等数据。私有云存储平台包括服务器、虚拟化云平台、云存储、云桌面,提供面向部门和用户的计算、存储及网盘等公共和个性化基础服务;统一身份认证平台,即推动统一用户管理,实现基于实名身份认证的集中授权和单点登录。

4.3 应用平台层

应用平台层是支撑学校治理现代化的应用体现,主要包括学校智慧校园管理和智慧校园服务、智慧教学环境和智慧教学资源两大板块内容。

(1) 智慧校园管理与智慧校园服务

智慧校园管理与智慧校园服务板块直接体现了学校治理现代化信息系统及应用的谋篇布局,按照学校各业务职能归口原则,总共可分为七个区:党政管理、学工管理、计财资产、后勤基建、安全保卫、舆情信息和业务融合区。在构建治理现代化支撑业务系统时,在每一个业务区分别搭建了独自的业务系统,并且充分考虑到“统筹管理、协同治理、业务融合、系统融合”的建设理念,建立了学校综合管理信息系统(实现基础信息服务、教务管理、人事管理、财务管理、财务管理、资产管理六类功能统一管控),及网上办事服务大厅平台、校园一卡通系统、“领导驾驶舱、学科建设分析、教师画像、学业预警”等基于大数据平台的应用场景的融合业务信息系统,充分体现学校各业务系统资源整合、数据共享,大力提升智慧校园管理与服务的运转效率,推动学校治理现代化发展目标。

(2) 智慧教学环境与智慧教学资源

智慧教学环境与智慧教学资源板块主要体现了应用现代教育技术手段,为学校教学、科研、训练活动搭建智慧化的硬件环境和软件平台。智慧教学环境主要包括多媒体教室、智慧教室、创客实训教室等硬件环境搭建,在此充分考虑学校体育人才培养需要,打造适应体育类专业高校学生的教室环境,将现代信息技术融入教学全过程,创新课堂教学范式,推进课堂革命;智慧教学资源包括教学系统、网络学习空间(超星、智慧树、雨课堂)等软件教学平台搭建,整合集平台资源库、互联网资源、学校资源、个人资源为一体教学资源,优化学校教学管理,促进学生自主学习,提高学习质量。

4.4 应用终端

应用终端包括用户和成都体育学院网站和移动端 APP。用户指的是教师、学生、管理者和社会公众,应用终端即成都体育学院网站和成都体育学院移动客户端。

4.5 智慧校园技术规范与保障体系

根据教育部和相关行业信息标准,结合学校现有信息执行标准和信息化建设实际,制订《成都体育学院智慧校园建设标准规范》等制度体系,规范智慧校园建设,建立全校统一的信息化标准规范体系;保障体系是保障智慧校园建设和运行的基本条件,包括组织机构、规章制度、经费保障、运维服务等内容。

4.6 智慧校园信息安全体系

制定《成都体育学院网络安全建设规划》,包括网络基础设施安全、信息系统安全、信息终端安全、数据安全、内容安全及安全管理等内容,为智慧校园提供全方位安全保障。

5 结论

智慧校园建设是推动高校治理现代化的重要载体和有力支撑。在建设过程中,需要直面并解决在统筹规划、业务融合、数据治理、技术应用等阻碍发展的多方面问题。智慧校园建设应以顶层设计为智慧校园建设提供明确方向,坚持落实立德树人根本任务的价值旨归,坚持深度融入学校发展规划为行动纲领,坚持突出学校特色为建设亮点,以统筹管理体系为组织保障,以数据治理为驱动力量,以“新基建”为关键支撑,最终实现以信息技术促进高校高质量内涵式发展,以智慧校园建设推动高校治理现代化!

参考文献:

- [1]魏楚元,汪洋海容,孙绪华.以信息化推进高校治理体系和治理能力现代化——北京建筑大学的经验与启示[J].北京教育(高教),2021(4):12-14.
- [2]国家市场监督管理总局中国国家标准化管理委员会.GB/T36342-2018 智慧校园总体框架[S].北京:中国标准出版社,2018:3-5.
- [3][10]谢幼如,黎佳,邱艺,等.教育信息化2.0时代智慧校园建设与研究新发展[J].中国电化教育,2019(5):63-69.
- [4][7]余鹏,李艳.基于教育大数据生态体系的高校智慧校园建设研究[J].中国电化教育,2018(6):8-16.
- [5]刘金扬,杜昀徽,郑剑,等.“双一流”建设背景下智慧校园的规划——以北京航空航天大学为例[J].现代教育技术,2021,31(5):90-96.
- [6]王克平,肖源.高校智慧校园的构建与研究[J].实验室研究与探索,2019,38(7):252-257.
- [8]杨萍,姚宇翔,史贝贝,等.智慧校园建设研究综述[J].现代教育技术,2019,29(1):18-24.
- [9]胡钦太,郑凯,林南晖.教育信息化的发展转型:从“数字校园”到“智慧校园”[J].中国电化教育,2014(1):35-39.
- [11]教育部关于发布《高等学校数字校园建设规范(试行)》的通知[EB/OL].中华人民共和国教育部.http://www.moe.gov.cn/srcsite/A16/s3342/202103/t20210322_521675.html.2021-3-12.
- [12]中共中央关于坚持和完善中国特色社会主义制度 推进国家治理体系和治理能力现代化若干重大问题的决定[EB/OL].新华社.http://www.gov.cn/zhengce/2019-11/05/content_5449023.htm.2019-11-05.

高校网络安全防护中的计算机信息管理技术应用分析

◆时进

(河西学院 甘肃 734000)

摘要:在人们的生产生活越来越依赖计算机与网络的背景下,网络安全成为人们普遍关注的热点问题,也是社会经济快速发展中必须解决的问题。高校也不例外,要想更好地保障网络安全,做好网络安全防护工作,有必要加强对计算机信息管理技术的研究,明确危及高校网络安全的因素,有针对性采取措施进行应对。本文主要从计算机网络安全的内涵出发,分析计算机信息管理技术在网络安全防护中的作用以及危及高校网络安全的因素,讨论计算机信息管理、技术在网络安全防护中的具体应用,探究如何进一步强化高校

网络安全防护。

关键词：高校；网络安全防护；计算机；信息管理

计算机网络技术的出现打破了人们日常工作生活中存在的时空限制，无论是生活质量还是学习生活效率都得到明显提升，但是由于网络天生所具备的开放性与虚拟性的特点，其为人们带来便利的同时也带来很多的威胁与不安全因素，网络安全是一个迫切需要解决的问题。比如计算机网络环境中常出现病毒问题，不仅会破坏网络质量，还会影响网络系统的安全性，随时可能造成信息丢失，后果非常严重。高校网络信息管理中涉及学生的个人信息与秘密研究信息，更需要做好计算机网络信息安全防护工作。

1 计算机网络安全内涵概述

(1) 基本含义

计算机网络安全指的是为了更好地保障网络信息系统的安全有序运行，对整个系统进行全方位的防护，运用各种安全保护措施，最大限度的保护网络信息数据的安全系数，防止因外部因素的影响被破坏，避免来自外部的恶意攻击而出现数据传输终端，保护网络系统的正常运行，提供更加安全、稳定的网络服务。

(2) 加强网络安全研究的重要性

高校网络对整个社会经济的发展都起着非常重要的推动作用，是实施现代化教育建设的重要场所，在高校网络的快速应用推广过程中，校园网络安全的维护与管理所起到的作用都是非常明显的。如果高校在管理过程中发生计算机网络安全问题，那么无论是高校的科学研究还是教学活动，又或者是学生日常管理等工作，都会受到影响，情况严重时，还会造成巨大的经济损失，在社会造成负面影响，因而需要高度重视高校计算机网络安全防护工作，并进一步研究。一方面，加强高校网络安全工作能够更好地保障正常教学与科研活动的有序开展，并且随着高校教学中计算机网络技术的应用范围不断扩大，能够被应用到教学中的教学资源越来越丰富，已经成为广大教学重要的教学辅助力量，如果网络系统爆出安全问题，必然会破坏正常教学秩序。另一方面，高度重视校园网络安全能够更好地推动高校信息化建设。当前高校开展的信息化工程中依然还存在相当多的恶意节点连接，一旦被人恶意利用，将会破坏网络数据安全。通常高校校园网络中主要采用计算机网络访问控制技术来达到网络安全保护的目的，能够及时发现恶意非法访问，防止出现恶意访问，并且根据用户的身份认证的不同对用户的权限进行划分，并设置相应的安全防火墙，有效提升网络应用安全。

2 计算机信息技术在高校网络安全管理中的作用

在信息社会里，计算机网络管理技术在高校网络安全中得到广泛应用，但是分析当前高校开展的网络安全管理，可以发现，依然普遍存在着对网络安全不够重视的问题，仍然频频出现校园网络安全问题。分析过往校园网络安全相关数据可以发现，在我国有相当一部分高校都曾经遭遇过网络安全，都导致数据信息泄露，对高校正常教学秩序造成了极大的负面影响，因而迫切需要高校进一步加强网络安全管理，将计算机信息技术应用到网络安全管理中去，构建一个更加有效的网络安全系统，营造良好的网络教学环境。

(1) 借助计算机信息技术的应用能够进一步提高校园网络安全

在高校网络系统构建中，借助计算机技术能够完成对重要数据的加密处理，提高信息保密度，通过维护广大师生的数据库、学校教学研究资料库以及图书馆数据库，能够更好地保障高校正常教学秩序。

(2) 借助计算机技术中的网络安全技术应用能够更好地防范来自病毒与黑客的攻击

只要是使用计算机的地方就存在病毒与黑客，而网络通常隐藏在计算机的程序代码与输入文件中。由于高校使用网络的人员比较多，人员成分复杂，相应的浏览的网络内容也千奇百怪，涉及非常大的文件传输量，容易造成病毒入侵，从校园网络安全防护薄弱的区域侵入校园网络。因此要通过计算机网络安全技术来构建一个具有防护性的高校校园网络。借助计算机信息技术中网络安全技术来监控校园网络，隔离不良网络信息，打造一个绿色健康的校园网络环境。

3 在“大数据”的背景下危害网络安全的因素

(1) 互联网本身所具有的特性

互联网络之所以能够得到广泛应用的一个根本原因就在于其与生俱来的开放性，虽然互联网的应用为社会创造了巨大的经济价值，但是也要看到其中存在的问题。网络的开放性是我们所重视的，但是也会被不法分子所利用。当前计算机信息技术中应用的IP协议对网

络信息所起到的保护作用并不强，容易出现信息传输时被篡改等问题，破坏网络安全。

(2) 网络病毒的入侵

计算机网络中存在的病毒能够借助网络数据的传播快速传递，有着很强的传播特性，并且病毒还表现出很强的隐蔽性，常常隐匿在网络数据与外来设备的数据中，在平常很难被发现。当前新兴的大数据，虽然便捷了人们的日常生产生活，但同时也意味着病毒传播更加方便。在庞大的计算机用户中，通过网络浏览传输的信息非常多，覆盖了非常多的内容，很难对每一条信息做到实时监测。网络病毒的入侵会破坏用户设备，带来利益损失，甚至还会在社会广泛传播，造成恶劣的社会影响。

(3) 黑客的非法攻击

黑客攻击也是高校网络常常遇到的一大威胁。部分黑客为了个人利益恶意攻击网络，对高校数据进行窃取或者篡改，在这个过程中，由于黑客有着很高的技术水平，在操作时也表现出很高的技术含量，网络的防护系统并不能完全发挥作用。而高校计算机网络中存在有庞大的信息资源，潜在价值巨大，很容易吸引黑客通过攻击网络来获取教学资源，窃取师生个人信息，无论对社会还是对学校都有着巨大的危害。还有部分黑客是出于个人报复心理来攻击高校网络，以获取精神上的愉悦。这些来自黑客的攻击都影响了高校计算机信息安全。

(4) 计算机用户使用不当

计算机网络的作用要想得到充分发挥离不开使用者的正确使用，但是在实际中由于每一个使用者都具有个人的特性，对计算机的操作习惯都是不一样的，部分用户如果操作习惯不规范，那么对计算机安全都是一个隐患。高校中虽然学生计算机水平比较高，但是依然有部分师生安全意识不高，低估了虚拟网络的损害，甚至完全没有意识到计算机网络安全带来的负面影响。

(5) 网络漏洞带来的隐患

由于在计算机网络刚发展时没有重视网络安全问题造成的，加上计算机网络系统庞大，涉及非常多的程序，计算机网络中或多或少都存在漏洞，这些漏洞的存在对网络安全来说始终是隐患。除此之外，计算机用户网络使用方法的欠缺以及系统的配置过低都会造成计算机网络漏洞。

(6) 计算机网络管理艰难

计算机世界变化万千，就拿病毒来说，其表现形式与种类就是千变万化，并且随着计算机网络技术的发展也在不断精华，已经从过去的单一病毒变成了多种形式的病毒，隐蔽性更强，很难被发现，这些都会对计算机网络带来挑战。而计算机网络的管理系统更新速度不高，难以赶上病毒的发展速度，也就意味着难以去维护计算机网络安全。如果采用的计算机管理方式一直不变，无法跟上计算机网络的发展速度，那么计算机网络安全也难以得到保障。

4 计算机信息技术在高校网络安全中的应用

(1) 防火墙技术的应用

防火墙在高校网络安全管理系统中扮演着非常重要的角色，在有效防范外来病毒入侵的同时，还能对日常文件的传输与下载起到实时监测作用，防止有问题的数据进入到系统中去。一般防火墙被安装在内网与外网的连接部分，能够对网络数据进行分析监控。

(2) 数据加密技术的应用

数据加密指的是借助加密钥匙以及加密函数来转换数据，最大限度保障数据安全。通常数据加密技术被应用在高校网络安全管理系统，能够有效防止信息数据的泄露。当前我国高校网络数据加密信息主要漏洞扫描技术、加密钥匙技术和数字签名认证技术。

(3) 病毒入侵检测技术的应用

可以借助病毒入侵检测技术来弥补防火墙技术的不足之处，其能够对网络系统中存在的危险信息进行自主检测，并将检测报告发送给计算机用户后自行修补漏洞。高校网络常常选择将网络入侵检测技术应用到网络核心交换机中，对网络信息进行全方位检测。

(4) 杀毒软件技术的应用

杀毒软件是计算机网络安全防护中常常使用的一种外在防护技术，通过在计算机系统中安装杀毒软件能够在对计算机内部配置进行优化的同时，防止病毒入侵。高校计算机体系主要分为服务器与工作站，一般来说，杀毒软件安装在工作站内，对工作站的数据进行监测。

还可以在服务器中安装可装载的防病毒软件,对计算机系统进行全面扫毒与清毒,从源头上保护好计算机系统,确保网络正常运转。

(5) 访问控制技术的应用

校园网络属于问答式访问控制,在构建网络过程中,需要从信息上对访问控制程度进行把控,从策略上对其进行规划,在这个基础上制定访问控制决策。教务系统登录是校园网最中间的访问控制体系,学生凭借正确的账号密码登录,这种控制技术能够在一定程度上防范非法入侵。

(6) 虚拟局域网技术的应用

校园网络会借助 VLAN 对网络进行分段处理,根据实际使用需求的不同将网络分成不同的段,构建局域网,依托 VLAN 技术实现对不同网络端的监控,以此防范非法入侵。通常在网络分段时会给局域网网络站点授权,确保不同站点数据的正常交换,实现校园网络的正常运行。

5 信息化时代高校计算机网络安全防护技术研究

(1) 在高校大力宣传计算机网络安全防护工作

在高校管理过程中,计算机网络安全防护工作也是非常重要的一个部分,为了提高计算机网络安全水平,要广泛发动师生参与到高校计算机网络安全工作中去,大力宣传计算机网络安全防护工作,可以借助校园广播、校园网络等渠道面向师生宣传计算机网络安全防护小知识,让其了解计算机使用中可能存在的各种安全问题,提高安全防范意识,更好地规范自身的网络使用行为,培养良好的计算机使用习惯,最大限度减少计算机网络安全问题的出现。

(2) 培养专业的计算机网络安全管理人才

要想确保计算机网络得到安全使用,就要培养一支高素质的计算机网络安全管理人才。高校要重视计算机网络安全管理人才的培养与教育,通过专题培训有针对性地提高网络安全管员的业务素质,从技术上为计算机网络安全提供保证。与此同时,高校要从计算机专业筛选专业的计算机网络安全管理人才充实到管理队伍中去,定期组织专业技能考核,只有通过考核的人员才能上岗,以此激励管理队伍不断学习,提高自身水平。

(3) 加强计算机网络安全防护技术的推广应用

随着高校教学过程中越来越多的使用计算机网络技术,网络安全问题也越来越多地暴露出来,需要高校正确认识计算机网络安全防护技术,加强对网络安全防护技术的研究力量,在广大师生中大力推广应用,从技术上来保障高校计算机网络安全。在构建高校计算机网络安全信息系统过程中,先借助先进的网络信息安全防护技术来打造一个高安全系数的防护网络,防止信息数据被盗取,对计算机应用过程中涉及的信息做好加密处理,利用先进的计算机技术对信息进行加密传送,避免信息在传送过程中被攻击。

正是由于计算机信息技术的快速发展与更新换代,才造就了今天的大数据时代。高校要紧跟跟上时代发展的步伐,借助计算机网络助力高校教学工作的开展,创造更大的经济价值。大数据意味着有更多的资源能够用来分享,更多的人能够来使用大数据,通过数据资源共享来推动社会前行。但是在这个过程中高校也要更加重视计算机网络安全,通过计算机信息管理技术来加强网络安全防范工作,进一步提升网络安全管理专业的专业素养,让高校网络安全防护工作更上一层楼。

参考文献:

- [1] 赵彦成. 计算机网络信息管理及安全防护策略[J]. 数字化用, 2019, 025 (030): 50.
- [2] 李晶晶, 杨红森. 计算机网络信息技术在高校中的应用及其安全防护[J]. 数字技术与应用, 2020, v.38; No.357 (03): 206-207.
- [3] 聂玉成. 关于计算机网络信息管理及其安全防护策略探析[J]. 电子世界, 2019, 561 (03): 111-111.
- [4] 武军. 计算机网络信息管理的防护策略[J]. 信息与电脑(理论版), 2019, 422 (04): 220-221.
- [5] 罗繁. 计算机信息技术在高校网络安全中的应用[J]. 电子技术与软件工程, 2019 (3): 199.

基于数据的大学生网络安全意识现状分析

◆侯小红¹ 郝杰骏²

(1.上海旅游高等专科学校 上海 2014002; 2.上海电子信息职业技术学院 上海 201400)

摘要: 本文采用网络在线调查方式,面向一定范围的大学生采集相关数据,通过 SPSS 软件分析,得出大学生网络安全意识现状,并从社会发展、学校教育、自我教育三方面阐述提高大学生网络安全意识和实践能力的举措,正面引导大学生树立维护网络信息安全的意识,供相关读者参考。

关键词: 大学生网络安全; 学校安全教育; 网络安全防范

1 研究意义

2019年,习近平总书记在国家网络安全宣传周作出重要指示:“国家网络安全工作要坚持网络安全为人民、网络安全靠人民,保障个人信息安全,维护公民在网络空间的合法权益。”据第47次《中国互联网络发展状况统计报告》,截至2020年年底,我国网民人数已达9.89亿,学生网民成为网络用户的最大群体,在校大学生尤为显著^[1]。

网络成为当前人们交往、工作、学习、娱乐的重要空间,互联网迅猛发展的中国,也成为名副其实的网络大国。根据中国互联网络信息中心2021年2月3日发布的第47次《中国互联网络发展状况统计报告》显示,截至2020年12月,我国网民规模达9.89亿,较2020年3月增长8540万,互联网普及率达70.4%^[2]。网络在提供便捷的同时,也滋生了众多安全问题。近年来,欢乐购诈骗、贫困助学诈骗、电信诈骗、钓鱼 Wi-Fi 诈骗等网络诈骗典型案例频发,西方网络意识形态渗透、暗网犯罪、国家级别的网络间谍战等各种各样的网络安全事件频繁出现。从现实社会的传统犯罪到各种新型的网络犯罪,网络空间安全形势日益严峻,应对网络空间安全事件面临严峻挑战。由于网络空间的巨变,与相应的网络技术的更新滞后,相关信息基础设施不够完善,人才队伍不够健全,使得当前网络空间受到巨大威胁,

强化网络安全保障体系与能力建设形势紧迫。

对大学生而言,互联网是一把“双刃剑”。一个安全的网络环境有利于大学生开拓视野,积累课外知识;但一个糟糕的网络环境则容易使得大学生落入网络陷阱,不仅有可能泄露自己的个人信息,背负上沉重的债务,还有可能摧毁一个人的理想信念和坚定意志,耽误国家和民族的复兴大业。基于这一现状,高校应及时做好网络安全教育工作,能在很大程度上保护好大学生的人身及财产安全,同时有利于维护社会的稳定与发展^[3]。

2 大学生网络安全现状分析

2.1 调查对象及方法

为研究大学生日常防护意识和网络安全防范意识的现状,本研究设计出《大学生网络安全调查研究》问卷,采用网络在线调查方式,面向一定样本范围的大学生群体采集相关数据,展开调查。

问卷内容主要是三类,首先,基本信息状况,围绕“性别”、“答题来源地域”、“所在年级”等了解参与问卷的大学生基本情况。其次,设置多选题,通过风险认知、风险警觉、风险防范等具体测量项目,以测定个体网络安全意识各个维度的具体表现和成熟程度。最后,为更全面地了解高校学生对国家网络安全的了解程度,问卷增加了国家网络安全意识相关题目,完善问卷。共设计23题,收到有效调查问卷