

# 高校网络安全防护中的计算机信息管理技术应用分析

刘建文

(广东东软学院, 广东 佛山 528225)

摘要: 伴随社会经济的迅猛发展, 高校课程教学和学生管理逐步朝着信息化、智能化的方向发展, 多样化的网络信息资源为学校教学与管理提供了便利, 与此同时, 也隐藏着各种网络安全问题, 这一问题值得高校领导和教师们特别关注。具体来讲, 校园网络是高校实现信息化教学的重要渠道, 不仅可以为教师开展教学、学生获取知识提供资源, 还可以对行政管理中产生的数据信息进行记录和存储, 进而能够确保高校教学管理能够正常运行。除此之外, 高校推进校园网建设是落实科教兴国的重要举措之一, 同时, 也是推进教育信息化建设的必要方式之一, 在日常教学管理中取得了显著的应用成效, 比如网络教学、办公管理等等。但是结合实际情况可知, 高校在依托网络技术构建信息化教学系统的过程中存在诸多问题, 特别是网络安全问题, 因此, 可以借助计算机信息管理技术来实现网络安全防护。如何充分发挥计算机信息管理技术在网络安全工作中的应用作用是当前领导和技术人员亟待商议的重要问题, 本文将围绕这一问题提出具体的解决思路, 旨在促进高校的信息化长效发展。

关键词: 高校; 网络安全防护; 计算机信息管理技术; 应用分析

近些年, 随着互联网和计算机技术的不断发展, 计算机信息技术包含有网络通信技术、计算机技术、网络安全技术等内容, 其应用更加广泛和显著, 使得人们的生活、工作和学习逐渐离不开互联网技术。为适应现代化教学改革发展所需, 高校在教学管理中大力引入先进技术与设备, 使得网络逐渐成为教育教学的主要方式, 但是由于网络有着较强的互动性、开放性, 也使得高校网络具有巨大的隐藏危险, 因此, 应不断提高对高校网络安全防护工作的重视程度。其中计算机信息管理技术在网络安全防护中起着至关重要的作用, 进而推进社会整体的信息化建设进程。基于各种现实因素的影响, 使得高校的网络系统存在各种危险因素, 不仅会影响网络安全, 还会阻碍学校发展, 为此, 高校应通过应用计算机信息管理技术来维护校园网络安全。鉴于此, 本文结合现有计算机信息管理技术应用经验, 先分析计算机信息技术的内涵、组成、特点以及应用作用, 在剖析危害高校网络安全的因素, 最后来细化计算机信息管理技术应用分类的基础上, 提出具体的应用策略, 旨在为高校正常运行和高效发展提供强大的网络安全保障。

## 一、计算机信息管理技术分析

### (一) 内涵简述

从本质分析可知, 计算机信息管理技术是一种广泛应用的网络安全隔离管理技术, 即会在网络与网络之间建立安全隔离屏障, 进而能够对网络信息提供安全保护的基本网络信息管理技术。该技术是现阶段进行系统保护和安全防护的重要方式之一, 并且该技术的应用能够充分发挥其保护网络信息的功能作用, 进而能够保障网络的访问安全, 提升病毒防御能力, 同时, 还可以了解服务器应用情况和访问现状, 有效保护网络系统安全。

### (二) 计算机信息管理技术组成

第一, 过滤式信息管理技术。这种基于过滤形式的信息管理技术主要通过通过网络参考模型中控制数据传输、网络路由器来实现网络系统保护的。第二, 应用型信息管理技术。这种信息管理技术主要是利用网络 IP 端口的地址转换和地址注册, 在内外网络同时进行访问设计时, 可以借助网络安全网卡来进行自动网络原地址端口处理, 通过与外界网络连接来保证网络管理系统能够发挥其控制效果。计算机信息管理技术具备良好的对网络系统保护功能, 网络入侵者首先要攻破计算机信息管理技术的安全防线才能够对计算机网络系统的目标进行攻击, 其中可以对网络进行多

种类型配置, 并设计不同网络系统层级, 其中层次越高的计算机信息管理技术应用则有着较高的应用选择。

### (三) 计算机信息管理技术特点

一般来说, 计算机信息管理技术的一个主要特征便是作为关键控制点, 能够极大改善整个系统的内部网络安全性, 与此同时, 还可以通过过滤危险网络因子来降低网络服务风险, 此外, 只有依托网络选择和网络安全协议才能够有效应用计算机信息管理技术, 为此, 有必要时刻关注和检测网络系统环境是否安全。计算机信息管理技术是目前世界上最重要的一种网络安全控制防护手段, 从专业安全性角度分析, 不难看出, 该技术包括多个网络系统, 并且可以通过网络系统之间的控制转换来实现网络系统组件拼接。计算机信息管理技术实现了本地区网络与外界网络系统之间的系统防御, 并且能够在企业的系统内部网络安全和外部网络系统安全之间实现良好隔离, 并通过限制性访问来保护部分区域网络的应用稳定性。

### (四) 计算机信息管理技术应用作用

随着社会经济的快速发展, 高校依托互联网朝着信息化的方向持续发展, 其中校园网在学校的课程教学, 课程研究, 行政服务、后勤管理以及师生交流等方面发挥着重要的应用价值, 是高校教育教学信息化建设的重要方面。随着时间的推移, 高校校园网办理规模更加广泛, 使用功能更加多样, 深受师生的关注和重视, 并逐渐成为衡量高校办学质量、综合实力的重要指标。在高校建立校园网之初, 并未得到广泛应用, 其安全问题也并不突出, 但是伴随网络规模的扩大和应用范围的扩展, 产生了大量的数据信息, 与此同时, 网站破坏和病毒入侵导致校园网面临着严峻的网络安全问题。此外, 伴随校园网功能的不断完善, 其应用效果也更加显著, 为此, 学生对校园网的设置和功能有着更高诉求和要求, 而网络安全问题逐渐成为校园网建设的重要内容, 并且对高校健康发展起着重要影响, 因此, 高校管理者和教师都应该高度关注校园网的信息安全问题。

针对这一情况, 高校必须对校园网的使用情况及存在的问题进行全面剖析和深入分析, 并在此基础上制定相应的防范措施, 为各项工作的是顺利开展创设安全的环境。高校构建的多功能网络平台, 应具备防病毒、身份认证、信息保存、数据恢复等安全功能, 以此来避免不安全因素出现, 提升网络使用的安全性, 使得网络平台平稳运行, 信息数据畅通, 为高校的领导、教师进行

日常教学管理工作提供了技术保障,同时,还可以推进教育教学信息化发展,最终提高高校的社会核心竞争能力。

## 二、危害高校网络安全的因素

### (一) 网络安全漏洞

高校建立计算机互联网平台的目的在于实现资源共享,提高数据分析效率,但同时,也使得互联网中存在着各种各样的安全隐患,这便是网络信息安全问题的根源所在。网络安全漏洞指的是软件系统在设计 and 编码时存在的缺陷和不足,而这一错误或是缺陷可能会被不法分子利用,进而植入病毒或是恶意攻击计算机系统,最终使得信息数据被破坏或是网络系统无法运行。高校师生在日常操作计算机平台的过程中,也可能会因为操作失误导致产生软件漏洞或者系统漏洞,这些漏洞会对师生的正常使用带来影响,若是影响了网络正常运行,则很可能会对学校的网络安全造成潜在威胁,一旦被黑客或者病毒入侵,则可能会造成无法弥补的损失。

### (二) 网络电磁辐射泄漏

计算机所产生的电磁辐射主要来源于电脑在运转状态下的主机、线路或外部设备等,透过它所产生的电磁辐射及传导辐射,很可能导致信息泄露问题的发生。信息不但可以通过电磁辐射来进行传输,而且还可以通过信号线、电源线等来进行导电发射,这对高校计算机网络系统的信息安全性造成了极大的影响和威胁。

### (三) 网络病毒传播攻击

在计算机使用过程中出现的病毒基本都是由人工编程并借助各种方式、途径传输到计算机介质或是程序中的。当计算机运行过程中达到一定条件时便会激活病毒,进而破坏信息资源或是指令代码。计算机网络病毒具有传播速度快的特点,若高校校园网用户没有安装防火墙,甚至没有安装杀毒软件,则就会造成计算机网络病毒迅速传播,不仅对用户电脑安全构成带来严重威胁,还会造成网络资源的严重浪费,最终影响了整个校园网。具体地说,病毒在广泛传播之后会对数据库造成破坏,进而给高校网络信息安全带来威胁,部分用户会选择使用U盘或者电子邮件进行传播,这种方法比较隐秘,一是防不胜防,二是难以追踪,容易导致数据库被破坏,使得高校网络无法正常运行,其中可以通过拦截重要信息或是破坏数据来影响网络信息安全。

### (四) 网络非法入侵攻击

部分非法用户会通过窃取合法用户口令来获取访问身份,从而能够入侵网络,破坏数据或是篡改信息,这样,不仅会破坏信息资源,还会影响合法用户的正当访问,从而出现拒绝服务的现象发生,以上非法入侵行为均对高校网络信息安全提出了巨大挑战。伴随互联网技术的进一步优化,网络攻击手段也更加先进,导致用户很难防察觉和防控,进而导致网络上出现各种木马、病毒等攻击性软件,进而能够轻易地攻击计算机软件,最终导致系统崩溃或是运行瘫痪,严重威胁了高校网络信息安全,不利于学校的长效发展。

### (五) 网络管理不足

网络世界千变万化,以病毒为例,其表现形式和种类都是多种多样的,而且还会随着计算机网络技术发展而不断进化,逐渐从以前的单个病毒发展到现在的多个病毒形态,变得更加隐蔽和难以检测,无形中为计算机网络安全维护带来了新的挑战。而计算机网络管理系统更新速度较慢,无法跟上病毒发展速度,这就意味着计算机网络的安全很难得到维护。如果仍采用传统的计算机管理方式,是无法适应网络的发展,就很难保证计算机网络

安全。

## 三、高校网络安全防护中的计算机信息管理技术的应用分类

### (一) 加密技术应用

信息发送方会对消息内容进行加密处理,在现实生活中,系统安全密码主要方式是由接收方进行控制,并通过建立安全网络系统壁垒来实现在系统内部网络和外部网络之间的信息与数据的及时传输,这样能够有效保证在网络系统中的信息内容不会被第三方盗取。一般来讲,校园网络用户会将计算机网络系统安全归类为网络形式的隐私和信息保护,并且能够确保高校网络不受到外部因素的干扰,而网络系统供应商则认为,网络信息系统的安全维护要对各种类型的网络系统软件和整体网络环境的影响进行全面的分析,应该起到主动的网络系统保护的作用,能够在网络系统发生异常时提高网络通信维护的效率和合理性。

### (二) 网络连接技术应用

网络连接的前提是系统路由和系统互联条件下实现的。校园网络IP是固定的,这种类型的网络应该在第一时间确保进入主干网络系统,利用对主干校园网络的系统访问和系统控制来避免产生服务器管理漏洞,并及时地记录并了解各类型的校园网络数据信息。网络系统的实际操作流程主要包括对控制位置的预设和对防火墙系统IP的设置,在这个过程中,防火墙技术会自动实现网络路由中断,这样就能确保对控制表的访问方便性,还能有效地过滤出非法IP数据网络,进而会阻断外界数据和信息的访问。

### (三) 加密存储技术应用

计算机信息管理数据加密和存储技术的应用能够实现对校园网络系统的安全保护,数据加密方式的网络安全维护主要是利用网络连接和网络端口的加密处理来完成的,因此,只需要网络安全维护程序信息来源与协议类型与实际的网络信息筛选条件相匹配之后,便可以执行传送过程中的数据信息内容。与此同时,这一类型的计算机信息管理技术的工作过程和具有较高的透明性,从而可以有效保证实际的安全处理工作效率和工作质量,但是这种技术既不能对应用层的网络协议提供有效的支撑,又不能有效地保护网络的安全,同时,还不能避免网络黑客攻击和新型病毒威胁。

### (四) 防火墙技术应用

在高校的网络安全管理系统中,防火墙起到了很大的作用,它可以有效地防御外部病毒的入侵,并对日常的文件传输和下载进行实时监控,避免有问题的数据进入系统。通常,在内网和外部网的连接处,设置了一道防火墙,可以对网络中的数据进行分析和监测。

### (五) 杀毒软件技术应用

杀毒软件是一种常用的外部保护手段,其可以在保护计算机系统的同时,对计算机的内部配置进行优化,从而达到预防病毒入侵的目的。在高校计算机系统中主要包括服务器和 workstation 两部分,一般情况下,杀毒软件都是安装在 workstation 中用于监控 workstation 中数据的,或者可以在服务器上安装可加载的防病毒软件,对计算机系统进行全面扫描和清除,最终可以从根源上保护计算机系统,保证网络正常运行。

### (六) 数字签名认证技术应用

数字签名认证技术也是计算机信息技术在高校网络安全中的一种重要的应用形式,有口令认证、数字认证两种,口令认证的操作流程和方法相对简单。数字认证指的是在高校信息传递过程中,利用密码技术来对信息传递者的身份进行验证,如果信息传

递者的身份不能得到验证,那么高校网络就会拒绝接受信息,从而防止高校网络受到威胁。

#### 四、高校网络安全防护中的计算机信息管理技术应用策略

##### (一) 宣传网络安全防护

在高校管理措施落实过程中,计算机网络信息安全防护工作占据重要地位,为了让计算机网络安全水平得到进一步提升,有必要组织教师和学生积极参与到学校的计算机网络信息安全防护工作中。其中可以通过加强对网络安全防护工作的宣传力度来调动师生积极性,比如可以通过校园广播、校园网等多种途径来为学生和教师宣传与计算机网络安全防护相关的知识,使得他们正确认识到所使用的计算机中可能存在各种各样的安全问题,进而能增强他们的网络安全意识,培养他们的良好使用习惯,更加规范地使用网络,最大程度上避免安全问题的出现。除此之外,高校还应加大对计算机信息管理技术的普及和运用,在高校教育教学工作过程中,计算机网络技术的应用日益广泛,同时,网络安全问题也日益凸显,这就要求学生能够对网络安全防护技术有个准确认知,并且在此基础上增加对网络安全保护技术的研究力度。其中高校师生能够通过广泛使用计算机信息管理技术来提高网络安全性能。在建设高校计算机网络信息系统时,要利用网络信息安全保护技术建立高安全系数的保护网络,避免信息资料被窃取,并对电脑应用程序中所涉及到的信息进行加密处理,最后借助现代计算机技术来加密传输数据,防止信息在传输过程中受到攻击。

##### (二) 建立网络安全机制

为了让计算机信息管理技术在网络安全方面的作用得到最大程度的发挥,需要建立网络信息安全体系和网络安全机制,不断加强计算机信息网络安全标准化管理,建立信息管理技术模型,最终能够有效保障网络系统的安全性。目前,常见的安全机制有物理安全、入侵检测、防火墙、数据包过滤、金钥加密与数位签章、资料加密、认证技术和认证等等。因此,高校有必要广泛宣传和普及这种网络安全措施,此外,政府有关部门也应从长远角度出发,强化对此类网络安全机制的宣传力度。作为重要的计算机技术网络安全的内容,网络安全是计算机技术网络安全的重要组成部分,也是最关键最核心的技术控制环节,因此,高校需要不断地完善和研究网络安全机制,从而全面提高突发事件应对能力。

##### (三) 完善信息管理系统

伴随高校校园网系统的建设和完善,管理与教育区域信息化发展,而现代化信息管理则是高校管理中的重要基础工作内容,为后续保障教学质量和优化管理成效起着重要的基础作用。现阶段,高校信息管理系统不断完善和持续更新,其中主要包含有OA办公系统、人事管理系统、专业课程系统、学生教学系统、选修课系统、课程管理系统、教师管理系统、事假系统、线上交流系统、科研系统、后勤管理系统等等。高校可以通过构建功能完善的信息管理系统,能够有效对学校事务进行整合,从而能够简化工作流程、明晰工作情况、把握最新动态,最终能够提高学校教学管理工作的针对性和高效性,同时,使得工作质量和效率得到稳步提高。

##### (四) 强化网络技术队伍

高校需要构建专业网络技术队伍,以此来解决学校遇到的各种网络信息安全问题。结合实际情况可知,学校培养专业技术人员,旨在为校园网络安全维修和管理提供技术队伍,旨在提高整体工作效率和质量,最终维护学校安全与稳定。学校建立专业网

络技术队伍之后,应定期检测学校网络安全问题,在找到安全隐患之后尽快解决,能够有效避免安全问题,提高校园信息安全性。基于此,高校应提高对网络技术人员培养力度,通过组织他们参与专业培训来锻炼他们的网络操作技术和维修技术。或者,使学校还可以拓展招聘渠道来引入专业技术人才,参与到学校网络信息管理中,竟然能够在保证整体效率的同时,促进学校信息化建设。学校在采取各种措施之后,应不断提高网络技术人员的工作效率,最终保障其他教育管理工作顺利开展。

##### (五) 做好网络数据备份

数据备份是高校开展校园网络安全防护工作的重要内容,其中网络平台操作人员做好数据备份能够切实避免信息数据丢失和破坏等问题的发生。基于此,高校应不断提高对数据备份工作的重视程度,并且能够根据学校教学情况、管理现状来完成信息和数据的记录和备份,进而可以确保教育管理工作顺利开展。高校网络环境具有显著的开放性、互动性特征,教师与学生需要通过登录网站来获取咨询和资料,但是学校并未针对这一过程来制定监管价值,从而则容易出现信息篡改的情况,这样,不仅会影响用户使用感受,还会影响学校网络安全。为了有效避免以上问题的出现,高校应着重强调校园网使用者应具有数据备份意识,通过定期备份来解决以上问题,进而能够提高工作效率,保障数据安全。高校管理人员在完成数据备份之后,还应检测数据的稳定性和准确性,既然能够保证数据可以利用。其中在日常管理过程,管理人员应具备一定的安全意识,并在网络技术操作中不断提升自身的信息安全防范意识,为后续解决问题提供经验支持。

#### 五、结语

综上所述,随着高校网络体系的持续完善和发展,不仅能够更好地提升系统的便利性,同时也不可避免地会带来一系列的高校网络安全控制与管理方面的问题。应该加强对高校网络的实际应用以及高校网络的维护工作的重视。尽管有很多技术可以对网络系统的维护有很大的影响,其中最重要的就是计算机信息管理技术,然而,单独的计算机信息管理技术并不能完全地处理各种不同的网络系统的安全问题,因此,必须要具有各种更高安全性和更高效率的网络服务。既要校园网的数据进行科学的检测,又要对校园网的整体进行科学的监测。通过对高校网络安全问题的研究,能够起到一定的理论支撑和引导作用,从而推动今后高校网络安全水平的提升。

#### 参考文献:

- [1] 周岩,杜健持.高校网络安全防护中计算机信息管理技术的应用[J].电子技术与软件工程,2021(008).
- [2] 王旭,李昌松,张海青,等.计算机信息管理技术在网络安全防护中的应用[J].百科论坛电子杂志,2018.
- [3] 韩爽.高校计算机网络信息管理及其安全防护策略[J].数码世界,2020, No.181(11): 267-268.
- [4] 刑铁燕.浅析计算机信息管理技术在网络安全防护中的应用[J].工程技术(文摘版)·建筑,2023.
- [5] 原蕾.信息时代发展下高校计算机网络安全防护技术研究[J].网络安全技术与应用,2022(005).
- [6] 时进.高校网络安全防护中的计算机信息管理技术应用分析[J].网络安全技术与应用,2022(008).