# 高校教学专网信息安全防护策略初探①

董征
（闽南师范大学，福建漳州，363000）

摘　要　随着高校教学信息化手段的丰富和日常教学网络使用需求的提升，教学专网逐步成为高校教学信息化的重要支撑。作为校园网络的一个重要组成部分，教学专网的建设有其特殊性，也因为其相对普通校园网络的差异，针对教学专网的信息安全防护策略也应进行重新思考和设计。本文试图从教学专网的信息安全防护软硬件、制度建设方面着手，同时对新兴技术与教学专网安全建设相结合进行研究和思考。

关键词　高校；计算机；网络信息；安全防护

## 1　引言

计算机网络为人们的生产和生活提供了诸多便利，也越来越多地被运用于高校各项教学活动中，同时计算机网络也存在一定的弊端，在一定程度上给高校教学带来很多不安全因素，其中最显著的就是计算机网络信息安全问题。因此，加强高校计算机网络信息安全防护对于高校教学来说具有很重要的意义。

## 2　高校计算机网络信息安全防护的意义

首先，可以为高校教学活动的顺利开展提供必要的基础。随着社会的进步和科技的发展，教育行业越来越多地运用到了互联网技术，我国高校教学中对计算机的运用也越来越广泛，在实际教学活动中，互联网所蕴含的大量新鲜、全面的素材极大地推动了教学活动的有效实施[1]。同时，高校信息化建设也离不开安全的计算机网络信息环境，一旦高校计算机网络出现安全隐患，那么必定会对高校教学的顺利进行产生不利影响。所以说，加强高校计算机网络信息安全防护可以为高校教学的顺利进行提供必要的基础保障。

其次，可以打造洁净的校园网络环境，有利于高素质人才的培养。积极健康的校园环境可以有效地促进学生的综合素质，特别是当前信息技术高度发达的今天，学生的日常学习和生活都和网络息息相关，而互联网中存在的一些不利于学生人格和价值观培养的资源，会对学生的发展产生消极作用。因此，加强高校计算机网络信息安全防护，能够为学生打造洁净、安全的校园网络环境，使学生免受不良网络资源的侵害，更好地促进高校对高素质人才的培养[2]。

①本文系福建省中青年教师教育科研项目“云安全技术在云多媒体教室系统中的整合和运用”（项目编号：JAT191920）的研究成果之一。

# 3 当前计算机网络信息安全现状

## 3.1 硬件缺陷

当前计算机网络硬件存在的不足之处主要有以下几点：首先，硬件在研发之初本身就存在漏洞，比如系统各项数据和参数配置不完善、检测不达标导致运行不稳定等，而往往这些漏洞都会直接威胁到计算机的安全。其次，硬件存在结构缺陷。当前网络产品品种繁多，每个厂家生产的产品结构都不尽相同，容易和其他配件产品出现不适配的情况，给后期高校网络安全防护工作增加了难度。特别是假冒伪劣和不合格产品不断涌入市场，使得网络信息安全存在严重隐患。最后，不法分子扰乱硬件信息植入。在高校网络信息传输过程中，很多不法分子会通过多种途径对用户传递的网络信息进行拦截，之后植入非法信息以获取利润。高校计算机网络中的许多硬件设备，如路由器、交换机、服务器等，随着使用时间的增加，性能和稳定性可能会下降，甚至出现硬件故障。这种硬件老化会直接影响高校网络的稳定性和可靠性，增加网络被攻击或者崩溃的风险。计算机硬件设备更新迭代的速度快，一些旧的设备已经不被支持，也难以获得最新的安全补丁和升级，存在一定的安全隐患。其次，没有部署安全建设专业的堡垒机产品，恶意攻击者能避开系统访问控制机制，对系统设备及资源进行非正常使用，擅自扩大权限，越权访问信息。在网络中具体表现在：破坏信息的完整性、更改信息的内容、形式，删除某个消息或消息的某些部分，在消息中插入一些信息等，让数据产生错误。同时在高校中由于经费与单位体制的限制，往往将专网产生的数据都存储在内部专门的服务器上，一旦内部服务器遭到干扰、破坏，将会影响到整个网络系统的稳定[3]。这几种硬件的缺陷都严重威胁着高校计算机网络信息传输的安全。这几种硬件的缺陷都严重威胁着高校计算机网络信息传输的安全。

## 3.2 软件缺陷与病毒威胁

当前网络市场上，软件的设计者很难完全站在用户的立场去开展软件的研发，这就会导致软件多少都会有一些不完善的地方，而很多不法分子正是抓住了这些不足，对用户的信息传输进行拦截、盗取或篡改等不法行径，以获取非法利润。这些行为会导致一些软件系统的故障甚至瘫痪，严重威胁到了高校计算机网络信息安全的建设。同时因为软件的缺陷也让电脑病毒攻击高校计算机网络有了可乘之机。高校计算机网络面临的很多威胁都是由电脑病毒造成的，特别是对于高校的教学专网的云系统来说，云系统更常遭到病毒的攻击。现阶段比较常见的比如一些黑客或者用户为了获取比特币，非法使用云挖矿病毒对高校的云系统进行入侵，云挖矿病毒是一种利用云服务器计算资源进行挖矿的病毒，会占用服务器资源导致服务器运行缓慢，同时也会增加服务器的运行成本。例如 Crypto 就是一种新型的云挖矿病毒，它能够通过攻击虚拟机镜像文件，从而在云平台上植入挖矿程序。它使用了先进的加密技术，使得检测和删除非常困难。同时在云系统中，云勒索病毒也是一个严重的威胁，云勒索病毒会对云服务器进行加密，使服务器上的文件无法被正常访问和使用，然后勒索受害者支付赎金以解密文件。这种病毒对于高校云系统来说尤为危险，因为高校的教学、研究等重要文件存储在云服务器上，一旦遭受勒索攻击会对高校的正常运转造成巨大影响。

## 3.3 黑客攻击

在计算机网络中，黑客攻击是计算机网络安全无法回避的难题，同时随着大数据与人工

智能时代的到来，使得网络攻击也开始变得多样化 [4]。常见的网络攻击有：利用漏洞进行攻击、分布式拒绝服务攻击、SQL 注入等。黑客利用计算机网络中硬件与软件的缺陷，以及操作系统和应用程序中的漏洞进行攻击。分布式拒绝服务攻击也常被称为 DDOS 攻击，它在短时间内向目标服务器发送大量的假冒请求，使服务器瘫痪。SQL 注入攻击是通过将恶意的 SQL 查询或添加语句插入到应用的输入参数中，再在后台 SQL 服务器上解析执行进行的攻击，是目前黑客对数据库进行攻击的最常用手段之一。

随着技术的革新与发展，现在黑客会采取供应链攻击的新方式，攻击者通过攻击软件供应链中的某个环节，向最终用户分发恶意软件，从而攻击受害者的计算机系统和网络。这种攻击方式的成功之处在于，攻击者可以利用受害者对供应链中某个环节的信任，将恶意代码注入到软件或硬件组件中，从而让受害者自行下载并安装，从而达到攻击的目的。最近，供应链攻击在全球范围内变得越来越普遍，许多著名公司和政府、高校机构都遭受了此类攻击。同时黑客也会利用社会工程学手段进行攻击，例如黑客通过调查高校用户的信息和习惯，采取社会工程学攻击的手段，从而骗取高校用户的个人信息和敏感信息，再假冒高校教职工进行电话诈骗等违法犯罪行为。也有一些网络上的“黑客”可能会采取非法手段，如增加教学专网的节点、使用假冒的系统控制程序来获取或修改使用权限、口令、密钥等信息。通过这些手段，他们可以欺骗系统，获取非法访问权限，并占用合法用户的资源。这些不法分子为了自身利益，不顾法律与道德，非法入侵高校的计算机网络，窃取、篡改高校教学系统中的信息。对于高校来说，在日常的科研教学工作中及高校发展过程中会有许多的机密信息，一旦高校计算机网络遭受黑客攻击，重要信息被窃取，这将给学校和学生造成重大的经济损失和其他严重影响。

### 3.4 内部用户缺乏网络信息安全意识

管理员和用户缺乏必要的网络安全意识也会使网络信息安全存在巨大隐患，同时也会威胁高校计算机网络信息安全建设 [5]。有一部分网络管理员由于专业素质不足，导致其网络安全意识较差，容易造成操作失误、配置不合理等的情况发生，还会出现随意把密码告知别人或密码设置太简单等行为。而有些用户在利用互联网时只关注自己享受到的网络服务，而忽略了自己的操作会对网络安全造成的威胁。如果学校内部工作人员的计算机与外部网络相连，其计算机遭受黑客的攻击，黑客可以利用被攻击的内部人员的机器作为跳板，进而攻击重要的服务器。此外，来自内部工作人员或内部人员与外部人员勾结的破坏行为对整个系统的影响往往更为严重。因此，教学专网系统同样面临着内部工作人员恶意破坏的威胁。教学专网内部威胁主要体现在两个方面。

其一，内部人员的恶意破坏可能对网络安全造成严重影响。由于内部员工在局域网中可以直接连接到教学专网的核心服务器上，特别是专网的管理员拥有一定的权限，他们可以轻易地对专网内部网络进行渗透、入侵、窃取数据等，进而导致严重后果。

其二，内部人员的误操作或违规操作也可能对网络构成威胁。有时候，内部人员可能因为疏忽或不当操作而引发安全问题。此外，部分工作人员为了方便进而绕过专网的安全系统，违规行事，从而对专网的安全造成潜在的威胁。由此看来，专网内部的安全更需要引起重视。在校学生是用户中最大的一个群体，他

们通过连接校园网接入互联网，他们会在网络上浏览点击网页或者下载某些应用程序等，这样，一些木马程序恶意代码就会夹杂在这些网页、程序中通过学生的点击、下载直接加入到高校计算机网络系统中。如果这些恶意程序代码成功入侵高校计算机网络管理系统中，就会给整个校园计算机网络带来严重的安全威胁。

### 3.5 缺乏健全的校园网络安全管理制度

建立科学的网络安全管理制度是计算机网络信息安全防护建设的保障，是确保高校计算机网络安全运转的有效途径。但是受到多方面因素的影响，当前高校的计算机网络管理存在着一定的缺陷，比如大多高校的计算机网络安全建设都侧重于对硬件设备的管理，一定程度上忽略了对软件的安全建设，具体体现在很多高校的机房都配备有先进的计算机设备，为教师和学生提供了良好的上机环境，但计算机网络信息安全防护的实际运用却不彻底，还有许多高校的相关防护软件本身存在安全漏洞，极易被破解和攻击。随着网络安全事件不断增多，各类信息化单位纷纷加强信息安全建设，广泛采用各类安全技术和产品。但是，现在的许多高校在安全管理方面存在较大薄弱之处。首先在技术上，教学专网缺乏完善的安全管理平台，无法对专网内所有的安全系统进行统一的协调和整合；其次在管理上，教学专网缺乏良好的安全管理体制和策略，包括制度不完善、机构管理混乱和各个分系统的安全策略不统一等问题。这些因素直接导致整个安全体系虚有其表，降低了网络整体安全防御能力，无法真正满足等级保护的安全需求。同时许多高校在制定计算机网络安全管理制度时没有结合自身的实际情况，造成高校网络专业安全管理人员在使用专网时缺乏具体的网络操作管理规范[6]。

## 4 高校计算机网络信息的安全防护策略

### 4.1 建立和完善安全运行管理体系

首先，高校要重视校园网络安全建设，加大资金投入，校园网是一项复杂的计算机系统，需要经过市场调查、参数分析、品牌选择、安装和测试等多个环节方可完成。在选购硬件设备时要考虑加入信息安全设备，例如：网络信息安全隔离网闸、多功能安全网关、IP 协议密码机、安全路由器、线路密码机等[7]。同时，安全建设体系总框架的设计不能忽视国家相关政策要求，所采用的技术手段和安全建设管理，都必须符合相应的国家标准，并且涉及的安全产品需要符合业内安全通用要求和扩展规范。以便于业务系统后期的升级、扩充，以及与行业监管系统、其他第三方平台进行互连、互通。其次，要重整和优化硬件结构设计，加快信息传输速度，使信息传输突破空间的限制，为学生提供更加便利的上网体验。另外，还要加强对计算机网络中心的设施维护，提高计算机设备的安全系数。比如，高校要加强机房的防火和防雷，安排专人对设备进行定期检修，对已损坏的配件或设备及时更新，特别是遇雷雨天气要加强巡逻。还有，要制定明确的容灾备份机制，容灾备份是目前有效规避数据丢失、数据破坏、业务中断等网络系统风险的最有效的手段。

同时，还需要建立一套完整、规范、科学，结合自身情况的安全运行管理体系，把保障校园网络信息安全当作工作的重中之重。为确保专网的安全运行，需要设计一个完善的管理体系，重点涵盖安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理等方面。制定由全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系，使信

息安全管理覆盖各类安全管理活动，制定专网信息安全的总体方针与安全策略，阐明专网信息安全工作的总体目标、范围、原则和安全框架等。同时对计算机网络安全管理中的每一个环节进行合理规范的安全性评估，及时发现管理中的安全问题。总之，严格监管计算机硬件与建立完善的安全运行管理体系离不开高校内部对网络安全建设的重视，从各方面入手加大对硬件设施的维护，制定科学合理的管理体系，保障校园网络信息安全。

### 4.2 加强网络安全技术建设，提高安全防护技术

高校应引入先进的安全防护软件，持续监管和防护校园网络计算机，保障计算机网络信息安全。安装杀毒软件，定期进行病毒扫描，并要求网络安全管理人员定期进行系统漏洞扫描和更新补丁程序以确保网络系统的安全稳定。在教学活动中，应重视防护软件的重要作用，确保防护软件的正常运行，保障计算机信息传输的安全，有效推动教学活动的开展。同时，高校的计算机网络安全建设需要管理者不断学习并提高网络安全防护技术。随着计算机网络安全问题得到社会的广泛关注，一些实用的网络安全技术逐渐得到推广与普及。例如可以部署动态防御系统，在数据中心真实服务周围虚拟出大量虚假的 IP 地址和端口，诱导并迷惑恶意攻击者，增加恶意攻击者攻击业务系统的难度，只要恶意攻击触碰到虚拟的 IP 或者端口，动态防御系统就能识别和定位出包括 APT 攻击、木马、蠕虫、勒索病毒在内的攻击行为，防止恶意攻击在全网蔓延。

还可以在数据传输上使用数据加密技术，设置专用的加密函数、解密算法及解密钥匙。同时对专网中的用户要进行等级管理，严格控制不同用户的权限，也对数据库中的信息进行加密处理。在加强网络安全建设的同时，也要跟进做好应用安全、数据安全、管理安全等策略。在应用安全上做好专网计算机的授权管理、软件管理等；在数据安全上做好数据传输安全、数据存储安全；在管理安全上制定科学合理的管理制度、同时在一定时间段对安全日志进行保存。现在也有越来越多的网络安全工作者在平台上开源分享计算机网络安全技术与管理经验。高校计算机网络管理者需要不断地学习，与时俱进，提高高校计算机网络安全防护技术，确保教学专网安全、稳定运行。

### 4.3 加大宣传和培训力度，提高安全防护意识

高校日常计算机网络运行和使用中，要注重对教师和学生网络信息安全防护意识的培养，只有用户真正认识到计算机网络信息安全防护的重要性，才能在实际使用的时候减少人为因素造成的信息安全事故，降低安全隐患，从而保障教学活动的顺利开展。因此，高校要下大力度在校园内部开展宣传和相关培训活动，提高教师和学生的网络信息安全理论知识和计算机专业操作能力，使其从自身做起，严谨规范地进行各项网络操作。同时，高校也要注重对教师和学生网络道德的培训，从思想道德层面教导学生自觉抵制网络中的不良信息，树立正确的价值观，共同维护网络环境。在不侵害学生隐私权益的前提下，要切实对部分学生学校网络进行安全强控，对一些学生的上网活动进行实时的远程监控，也对一些危险网站进行隔离、限制访问处理。同时还要加强对高校机房管理员的业务培训，提高其安全防范意识，熟练运用防护软件有效对高校计算机网络进行日常维护和监管，把安全运维过程中产生的丰富经验进行积累和总结，形成有效的知识库，建立共享机制，提供信息共享和交流的平

台，提高管理员的工作效率。保障信息传输安全，助力高校各项教学活动的实施。

### 4.4 利用人工智能与大数据驱动的新思路

随着人工智能技术的不断发展和应用范围的不断扩大，越来越多的行业开始将其应用到信息安全领域，高校也不例外。大数据技术也为高校计算机网络信息安全防护提供了新的思路与解决方案。它们可以为高校教学专网提供更加智能化和高效化的安全保护。

（1）网络攻击的检测与防御智能化

高校网络安全日益受到黑客、病毒、木马、恶意代码等各种攻击的威胁，攻击手段越来越复杂。人工智能技术可以通过机器学习算法、深度学习算法等技术来学习大量的网络攻击数据[7]，建立起网络信息安全入侵检测模型，同时利用自动化的技术与检测模型结合的方式进行网络入侵检测，对高校教学专网进行监控与防范。这样不仅提高了检测效率和准确性，也能对网络攻击进行实时检测和防御。

（2）数据安全与网络流量分析智能化

高校计算机网络每天都产生大量的数据信息以及存在大量的网络流量，需要对数据信息与网络流量进行有效的管理与分析。通过机器学习和大数据技术结合可以对高校计算机网络中的数据信息进行智能分析和预测，自动识别数据异常，降低数据丢失和泄漏的风险。同时通过建立安全数据模型，加强对数据的分类、分析和处理，提高教学专网中数据的安全性和可靠性。通过数据采集与数据预处理等技术对网络流量数据进行处理与分析，利用机器学习算法对网络流量数据中的网络攻击进行特征提取，进行快速的分析与识别。一旦识别到网络攻击，即可通过智能化策略对攻击进行实时响应，进行针对性的防御，最大程度地减少攻击对系统的影响。

（3）行为分析和安全日志分析智能化

高校计算机网络中存在着各种各样的异常行为和恶意行为，同时高校计算机网络中拥有着大量的学生群体与教师用户，每天会有大量的安全日志产生，因此对用户的行为与安全日志进行分析至关重要。人工智能技术可以通过异常检测和行为分析技术，对网络异常行为和恶意行为进行实时检测和分析。可以使用基于深度学习的异常检测算法来检测网络异常行为，并采取相应的防御与控制措施。可以利用自然语言处理和深度学习算法对安全日志进行深度智能分析，可以帮助管理员发现网络中存在的潜在威胁，并采取相应的安全措施。同时通过安全事件的大数据仓库，结合网络安全设备的攻击信息，综合安全事件的相关特征，将攻击信息通过大数据技术进行分析，完整还原网络攻击事件。

### 4.5 基于零信任模型的新策略

随着信息化程度的不断提高，高校教学专网已成为高校师生学习、教学、科研和管理的重要平台。传统的网络安全模型通常将内部网络视为安全的，并假设内部用户和设备都是可信任的。然而，随着网络环境变得更加复杂和动态，这种模型已经不再适用。内部网络面临着来自恶意软件、内部威胁和数据泄露，防护不够全面等风险。因此，零信任模型作为一种新的安全防护模式，引起了人们的广泛关注[8]。零信任模型是一种以“不信任”为前提的安全模型，即在网络交互过程中，始终不信任任何一方，需要对所有的访问请求进行验证和授权。其核心原则是“验证、授权、限制、监控”，即对访问请求的身份、设备、时间、地点等进行全面验证，根据验证结果进行授权，并限制和监控访问的行为。零信任模型将访问控制从网络边缘向应用内部推进，从而实现了对所有

访问请求的精细控制。

（1）访问控制

在零信任安全模型中，所有用户、设备和应用程序都需要进行身份验证和授权，只有通过验证的用户才能访问网络资源。高校可以通过实施访问控制策略，采用防火墙、行为管理、负载均衡、入侵防系统、堡垒机、或其他具有相应访问控制能力的安全产品实现基于用户级的访问控制，限制访问网络资源的用户范围，从而有效地防止未经授权的访问。

（2）多因素身份验证

在零信任安全模型中，多因素身份验证是一项重要的措施，可以有效地增强安全性。高校可以通过引入多因素身份验证技术，采用身份认证网关、堡垒机、终端准入或对应用系统进行改造，对应用系统用户进行基于口令、令牌、数字证书等方式的两种或两种以上的组合身份鉴别，来增强用户身份验证的可靠性和安全性，防止身份冒充。

（3）网络分段

在零信任安全模型中，网络分段可以实现不同安全级别的网络资源之间的隔离。高校可以通过网络分段来划分不同的安全区域，将敏感数据和资源隔离出来，限制攻击者在网络内部的活动，使攻击者无法轻易地访问和攻击到这些资源，从而使网络安全性增强。同时进行安全域的划分，制定信息系统资产划分的规则，将信息资产划分为不同层次和级别安全域后进行合理安全防护设计，以体现层层递进、逐级深入的安全防护理念。

### 4.6 区块链技术在高校网络中的应用

随着互联网技术的发展，网络信息安全问题越来越受到关注，其中涉及的数据存储、传输和处理等方面，都需要采取相应的安全措施。区块链技术因其去中心化、不可篡改和高安全性的特点，被广泛应用于金融、物流和公共服务等领域。那么，区块链技术同样也可以运用到高校计算机网络信息安全建设中。区块链技术是一种去中心化的分布式数据库技术，其基本原理是将多个节点上的数据分散存储在网络中，形成一个链式的数据结构[9]。每个数据块都有自己的唯一标识符，而且数据块之间的关系是通过加密算法实现的，保证了数据的不可篡改性和安全性。

（1）区块链技术在高校数据存储与敏感信息管理的应用

高校在教学、科研、管理等方面都需要大量的数据存储与共享，而传统的数据存储方式容易被黑客攻击。因此，高校可以将区块链技术应用于数据存储与共享方面。利用区块链的去中心化特点，可以将数据分布在多个节点上，确保数据的安全性和可靠性。此外，区块链技术还可以实现数据的跨组织共享，提高高校间数据的交流和合作。同时高校教学、科研和行政管理中会存在大量的敏感信息，需要进行有效的管理和保护。区块链技术可以提供不可篡改的信息存储和加密技术，保障敏感信息的安全性和可追溯性。

（2）区块链技术在高校身份认证方面的应用

高校计算机网络需要对学生、教职工等人员进行身份认证，传统的身份认证方式存在着被伪造和篡改的风险。高校可以利用区块链技术来进行身份认证。区块链技术可以实现身份信息的去中心化存储，确保身份信息的真实性和安全性，避免了中心化认证机构的单点故障问题。此外，区块链技术还可以实现匿名身份认证，保护用户的隐私。同时每个用户的身份信息都存储在区块链上，只有经过认证的人员才能访问到高校内部的系统和数据，严格管控

接入教学专网的用户和设备。同时区块链技术在零信任安全模型中可以用于实现分布式认证和授权，以及实现网络流量的可信审计。

（3）区块链技术在网络攻击溯源方面的应用

高校计算机网络中存在着各种各样的网络攻击，需要进行有效精确溯源和追踪。区块链技术可以提供不可篡改的交易记录和时间戳技术，可以帮助高校进行网络攻击溯源和追踪。在区块链技术的应用中，每个区块都记录着上一个区块的哈希值，因此整个区块链是一个不可篡改的数据结构。基于这种特点，可以利用区块链技术建立一种去中心化的溯源机制，让攻击者无法隐蔽其行踪，同时也使得溯源更加高效和精准。具体来说，在应用区块链技术进行攻击溯源时，可以将所有网络攻击相关的数据存储在区块链上，包括攻击者的 IP 地址、攻击时间、攻击方式等信息。当出现网络攻击时，区块链技术可以帮助管理员及时发现和记录攻击信息，实现快速追踪攻击源头。

### 4.7 物联网环境下的高校网络安全建设

随着物联网技术的迅速发展和普及，越来越多的设备和应用开始与互联网相连接。物联网技术是指将传感器、嵌入式设备、网络通信等技术与实体物品相结合，实现物品之间的互联互通和智能化控制的一种技术。高校计算机网络拥有庞大的用户群体，每天接入到高校计算机网络中的设备不计其数。对这些设备的监管与维护在高校网络安全建设中是非常重要的。

（1）监测和管理设备安全性

高校中存在着大量的计算机设备和物理设备，这些设备与网络的安全性紧密相连。通过部署物联网传感器和设备，可以实现对设备的实时监测，包括设备的安全性、漏洞和网络连接状况等。同时采用物联网技术实现集中式管理设备的方式，可以建立一个集中的告警分析及展现平台，为系统运维提供更灵活和自动化的事件处理能力。当故障产生时，集中式管理平台能够迅速捕捉到故障事件，并通过实时监测和分析数据，快速定位故障的发生位置和原因。这样运维人员可以迅速针对故障进行响应和处理，节省了故障排查的时间，降低了维护成本，提高了系统整体的可用性。

（2）实现基于行为的认证和访问控制

在高校网络环境中，访问控制是非常关键的一环。传统的基于身份的认证方式可能存在安全漏洞，而基于行为的认证方式可以通过分析用户的行为模式，对用户进行身份验证和访问控制。在用户接入专网系统时，可基于可信根对用户计算机节点的 BIOS、操作系统内核、引导程序的进行可信度验证。当用户在专网系统中进行敏感访问时，对用户所使用的应用程序的关键执行环节对系统所调用的客体、主体及操作进行可信验证，同时也对中断、关键内存区域等执行的资源进行可信验证，在检测到其可信性受到破坏时采取恢复措施，同时将验证结果形成审计记录备份。物联网技术可以通过收集和分析用户的行为数据，同时与零信任安全模式结合，对用户进行严格的风险评估与权限控制，确保高校计算机网络的安全运行。

（3）加强数据安全保护

高校中存在着大量的敏感数据，如学生个人信息、科研成果等。物联网技术可以通过部署物联网传感器和设备，实现对数据的实时监测和分析，及时发现和防范数据泄露和攻击事件。同时，物联网技术还可以通过加密算法和区块链技术等手段 [10]，对数据进行保护，确保数据的安全性和完整性。

## 5 结语

计算机在高校教学中有着非常高的利用率，加上高校计算机用户数量庞大，一旦发生安全事故，则会对高校各项教学活动产生非常大的影响。因此，高校要制定相关管理制度，注重对校园网络硬件和软件的维护和监管，加强师生的网络安全意识，从根源上避免网络信息安全事故的发生。同时高校要做到与时俱进，信息安全技术在不断发展，新技术可以为高校网络信息安全建设提供更多的解决方案和保障。高校应该根据自身实际情况，选择合适的新型技术手段，提高教学专网的安全性和可靠性。

## 参考文献

[1] 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（11）：261-262.

[2] 盛权为. 大数据背景下高校计算机信息安全防护策略[C]. 教育理论研究（第六辑），2019：208.

[3] 郑刚. 计算机网络信息和网络安全及其防护策略[J]. 消费电子，2012（6X）:1.

[4] 彭珺，高珺. 计算机网络信息安全及防护策略研究[J]. 计算机与数字工程，2011，28（1）：121-124.

[5] 杨海利. 对于当前计算机网络信息安全及防护策略的思考[J]. 网络安全技术与应用，2020（6）：2-3.

[6] 王菊霞. 计算机网络病毒防治技术与黑客攻击防范策略[J]. 内江科技，2011.

[7] 张旭辉. 某民办高校网络信息安全方案的设计与实现[D]. 西安：西安电子科技大学，2015.

[8] 姚刚，齐玉东，崔嘉，等. 某内部专网信息安全问题分析与对策研究[J]. 现代计算机，2019（19）：6.

[9] 刘敖迪，杜学绘，王娜，等. 区块链技术及其在信息安全领域的研究进展[J]. 软件学报，2018，29（7）：24.

[10] 于仁飞. 基于区块链的物联网信息安全技术研究[D]. 成都：电子科技大学，2019.