用分析[J].网络安全技术与应用，2020（3）：5-6.
[4]熊丽丽，王诺.计算机网络安全技术在网络安全维护中的应用研究[J].电子世界，2020（18）：110-111.
[5]王伟.计算机网络安全技术在网络安全维护中的应用研究[J].网络安全技术与应用，2021（1）：155-157.
[6]魏清刚.计算机网络安全技术在网络安全维护中的应用[J].网络安全技术与应用，2020（12）：3-5.
[7]石红胜.中国通信运营行业网络运维成本与内部控制问题研究[D].北京：首都经济贸易大学，2017：57.

计算机信息管理技术在科研院所网络安全中的运用研究

◆金涛　庄会富[通讯作者]

（中国科学院 昆明植物研究所科技信息中心　云南　650201）

摘要：在现代科学技术快速发展的如今，计算机技术和互联网技术支撑下的网络安全已成为影响科研工作的关键因素之一。在稳定的网络安全环境下构建更为广泛、系统、深入、科学的科研数据信息传输和科研网络系统，为科技发展和社会进步提供更为先进的信息技术支持。但随着网络影响范围持续增加，网络安全问题正在不断出现，如科研数据泄漏、资料损毁、信息丢失等都可能给科研事业造成严重损失，因而有效运用计算机信息管理技术显得至关重要。本文立足于科研院所中计算机信息管理技术和网络安全，研究计算机信息管理技术在园区网络安全中的运用价值，并提出运用策略，进而为计算机信息管理技术在网络安全中发挥应有作用和功能提供参考。

关键词：网络安全；计算机信息管理技术；运用问题；运用策略
基金项目：中国科学院青年创新促进会会员支持项目（2022397）；云南省生物资源数字化开发应用（202002AA100007）

计算机技术和互联网技术与科学研究工作已密不可分，越来越多科技工作者参与网络活动，在网络环境中做科学计算、数据分析、信息传递、文献获取，网络使得科研群体之间的交流研讨、合作钻研等距离持续拉近，真正实现了突破时间和空间的科研合作。伴随网络与科研工作的深度融合，网络赋能科研范式变革的同时，相应的园区网络安全问题也日渐严峻，使得科研网的包容性、开放性、共享性成为违法分子利用非法手段窃取科研用户数据[1]的重要依托，而且网络安全问题的影响范围十分深远，很有可能给科研工作人员乃至国家造成严重的损失。因此，在园区网络安全中充分运用计算机信息管理技术加强网络环境安全建设具有显著现实意义。

1　计算机信息管理技术和网络安全概述

1.1 计算机信息管理技术概述

计算机信息管理技术应用场景十分广泛，此项技术可以利用计算机系统并依托具体网络平台、计算数据库、互联网技术等完成信息管理。计算机信息管理技术是防范和化解园区网络安全问题[2]的关键技术，可以在实时监测计算机系统和数据信息安全的同时，检测、筛查、过滤不良信息、网络病毒、恶意程序，并且针对潜在的网络安全隐患可以及时发出预警，降低计算机系统和数据信息造成网络安全问题威胁和破坏的可能性。

计算机信息管理技术主要用于维护、管理计算机系统及其内部各类信息，具体分类如下：一是防火墙技术，此类计算机信息管理技术是现阶段最为常见的技术，主要作用是隔断外界因素对计算机信息的负面影响，准确监测计算机信息管理状态，且不会受到访问次数、访问目的、访问频道影响，可以有效防止违法分子利用网络病毒、恶意程序等针对计算机系统和数据信息实施攻击。二是授权访问控制技术，此类计算机信息管理技术是以防御为主的管理技术，可以利用检测、筛查、过滤计算机系统传输和接收的数据信息，及时发现潜在的网络安全隐患，在最大程度上保障计算机系统和数据信息安全、完整。授权访问控制技术可以隔断用户参与网络活动时的登录安全风险，利用身份认证和识别等严格管控网络环境安全[3]。三是信息安全评估技术[4]，此类技术主要指各类杀毒软件和计算机操作系统自带的安全防护软件等，这些软件最直接的功能是实时监测计算机系统运行状态评估安全性，若发现系统存在潜在的网络安全风险，针对可能威胁计算机系统和数据信息安全的隐患作出预警，同时提出处理办法，使计算机系统和数据信息安全始终掌握在可控状态。

1.2 网络安全概述

网络安全主要就是指利用现代先进的计算机技术以及配套的管理措施促使网络系统可正常运行，避免网络在实际使用中丧失数据可用性、数据保密性和数据完整性。然而在当今社会，网络安全的定义会随着“角度”而发生改变[5]。例如从具体用户的角度分析。从科研人员角度出发，这类人群在应用网络开展科研工作过程中会更加看重自己的个人信息，包括个人隐私信息、科研实验数据、社交圈子等在进行传播过程中的机密性和真实性，他们也希望隐私和数据得到全面保护[6]。而从单位角度进行探究，在利用网络工作过程中最让其注重的关注点就是单位内部信息的泄漏、网络舆情和数据加密程度。综上所述，现代网络安全具备以下几个方面的特点。第一，就是信息的保密性。在实际应用网络传输各项数据过程中，非授权用户以及其他实体用户无法获取信息，或无法让其使用。第二，数据的完整性。在未经授权的情况下，数据则无法进行特性改变，也就是在实际传输数据或在保存数据的过程中不会出现数据自动篡改或丢失的特征。第三，数据的实际可用性。即已经被授权的实体具备数据访问使用的权限，也就是可以根据实际工作需要使用数据。

2　计算机信息管理技术在科研院所网络安全中的运用价值

计算机信息管理技术是现代信息技术和通信技术高质量发展的重要产物，属于网络安全维护和管理中不可或缺的先进技术，此类技术能够借助计算机系统实现高效化且拥有安全性保障的数据信息传播，对于提高科技人员科研数据信息

传输共享效率起着关键的促进作用。计算机信息管理技术在科研院所网络安全中的运用价值包括但不限于以下内容：第一，计算机信息管理技术可以实现高效化管理科研用户数据，包括存储数据和接入数据，能够保障科研数据始终处于完整、保密的管理状态，这也是计算机信息管理技术被运用于网络安全的重要原因之一，同时此类技术可以便于网络安全维护和管理人员针对计算机信息开展检测和管控。第二，计算机信息管理技术能够在网络安全访问控制中实现统一化、规范化、合理化用户身份认证管理，利用管理技术设置访问控制检测、筛查、过滤内容，有效控制规避潜在网络安全风险[7]。第三，计算机信息管理技术运用价值还体现在科研网建设和信息安全管理良好关系的构建方面，通过管理技术可以在科研人员参与网络活动时提供可靠的网络安全保障，这对于提升信息安全管理成效和促进计算机技术发展具有重要意义。

3 计算机信息管理技术在科研院所网络安全中的运用策略

3.1 加大网络信息访问管控力度

为防止科研数据遭受非授权访问，造成计算机信息被恶意篡改，应运用计算机信息管理技术持续加大科研网信息访问管控力度。选用和设定访问管控技术时需遵循具体问题具体分析原则，明确设置访问权限授权标准，合理划分访问管控身份要求，提升访问管控准确性和可靠性，确保计算机信息和科研数据始终处于完整、安全的管理状态[8]。为此，研究所网络技术支撑人员应对计算机系统及终端设备进行自动化防控设置，整合访问网络地址白名单，设定不同网络地址可直接访问的计算机系统及相关信息，针对网络活动情况和网络流量加强合理化监控，防范不法人员非授权访问内部计算机系统而带入网络病毒。而就身份认证技术来说，该项技术属于网络设备在进行数据传输过程中一种唯一界定的方式。从当代网络信息多元化的传输方式分析，进行身份认证可以在数据传输的环境中和用户实际操控行为之间形成一个具备双方高度信任的渠道。当数据用户使用电脑进行操作时首先就需要进行身份认证，在获取设备信任之后才能获取相关权限。由此也可以认为，身份认证技术可以对计算机网络数据进行最大程度的保护和隔离[9]，这对于有效避免黑客非法攻击设备有着重要作用。

但是，就当前科研院所计算机网络实际运行环境分析，在进行科研数据信息处理时大部分都是以可靠性认知机制对数据信息展开界定。因此，在网络运行环境中也可将其称之为是一种具备通用功能的数据传输架构。为了能够充分保护数据的安全性，身份认证技术可以建立于人类特征的基础之上，比如当代被认为安全系数级别最高的人脸识别技术和指纹技术等，上述技术都是基于人类特征基础上的身份认证。通过对具体用户行为开展程序对接，从而促使整个计算机设备操作活动可以在不使用常规密码设置的方式就可以实现登录账号。也正是因为这一特点，促使黑客即便想采取攻击行为也无法精准找出攻击点，相应也就形成了良好的数据防护体系。

3.2 提高信息管理加密技术水平

加密技术作为计算机信息管理技术的重要组成内容，对于维护和管理网络安全具有十分关键的积极影响。在网络安全实际运用中，数字签名技术是现阶段常见的加密技术之一，该技术属于非对称加密模式，通过签名和验证保障计算机信息和用户数据安全，同时可以检验数据信息真实性。对此，科研人员应对计算机系统及数据信息进行加密，增强密码复杂程度，合理设置复杂密码和账户安全管理策略，利用加密技术阻绝网络安全问题发生[10]。另外，科研人员应对进行传输和共享的计算机信息进行加密，利用节点加密技术提高传输内容安全性，可在正式传输前利用链路加密技术实施再次加密，进一步加强密码破解难度。

3.3 加强传输与存储加密技术的应用

对于计算机加密技术来说，传输加密主要涵盖以下两种方式。第一，就是端与端之间的加密[11]，此种加密方式主要就是指数据发送者在利用设备进行数据传输过程中对数据加密，利用数据包的方式确保除指定数据接收人以外其他人无法获取数据。在对数据进行端——端加密后，当数据顺利到达目的地后就会自行解密，并且总会转化成为接收人能够识别和读取的信息。第二，就是线路加密法[12]。主要是指通过多种形式的加密密钥方式对数据传输的网络进行加密，从而避免了外部不良攻击所带来的干扰。而相比于端端的传统加密方法，线路加密可避免对信源和信宿间数据的保护。而数据加密技术则分为了存取控制和密文管理二类，二者都是对信息的保存进行了安全保护。不过，两者中的数据加密技术存在一定的差别。其中，前者主要是通过审核和控制注册客户的身份来进行数据的维护，并强化了对客户数据真实性的控制和保护；后者主要是通过增加信息、加密方式等各种手段来达到密文安全保护。

3.4 提升网络安全风险应对能力

为有效应对网络安全风险，应首先提升网络风险监测和识别能力，通过日志审计软件和抓包工具持续收集网络病毒信息，分析黑客攻击技术手段及其原理，针对网络风险来源进行整合，依据已有信息资料研判网络风险出现频率与发展方向，提前预判并制定应对预案，建立网络风险识别和应对系统，确保系统可以准确识别网络病毒和黑客攻击行为，除了将网络安全风险和计算机系统内部数据库进行信息比对，还需要分析病毒攻击路径，深层次进行网络安全防控，为网络风险防范和管控提供支持，避免计算机信息和用户数据发生泄漏、损毁，切实保障网络环境安全。将计算机信息管理技术应用到网络安全中，必须采取科学合理的技术手段对网络安全风险进行严格控制，减少网络安全问题的发生，将网络安全风险造成的影响控制在最低程度。在网络安全检测过程中，也可以采取一些适当的措施，一旦出现网络安全风险，则可以对相关的信息进行收集，之后对信息进行分析，并制定出合理的应对策略，及时处理网络安全风险。由于网络安全工作是一个长期且复杂的过程，应安排专业的技术支撑人才，树立良好的工作理念，通过分类管理进行统一归纳，从而提高网络安全管理的工作水平[13]。

3.5 提升防病毒技术应用的质量

处理病毒问题是保护计算机操作系统的关键路径。所以，在实际应用现代计算机技术手段的过程中，科研院所单位都必须着重做好对反病毒技术的运用，以便于更加优化计算机控制系统的工作环境。而由于现代计算机信息科学与技术手段的不断更新，反病毒技术手段也更新迭代，研究所还可按照自己对微机操作系统的安全要求，针对科研设施的不同科学合理地选用反病毒技术体系[14]，以便于有效控制计算机系统病毒的侵入发生概率。也因此，研究所可以在局域网链路的出口处选择病毒程序的检测技术体系，如 WAF 检测技术、IPS 入侵检测等，对与病毒有关或者类似的程序进行重点检查，以防止微机操作系统在实际应用过程中，出现的病毒侵入风险隐患。同时，我们也需要对服务器、计算机、手机等终端的系统数据和文档进行病毒检测，从而确保计算机系统中的病毒风险得以有效管控。另外，还需要着重做好侵入测试体系构建，针对计算机系统外围软件环境和有关侵入信息系统，实施严密的流量使用、硬件资源占用情况、软件可用性、服务可靠性等多角度测试，剖析是否存在病毒危险隐患，并通过具体的分析结果确定是不是可以进入，以此保障计算机网络内部工作环境的安全可靠，并保持系统稳定。

3.6 打造精良的计算机支撑人员团队

在科学研究领域，更需要有专业的计算机信息技术和网络技术支撑人员团队[15]，科研院所必须着力做好不同专业领域的计算机技术人员素质建设，努力培育更多优秀的深入了解计算机技术的运维人员，并在继续教育深造和职称评聘等方面给予支持。科研院所还可以和高科技企业合作，在科研基础设施建设之初便根据专业需求考虑计算机信息系统和网络安全的设计，注重计算机系统安全防护相关培训工作，把与计算机系统安全相关的实际知识和应用技巧，逐步传播给科研人员，从而实现强大的人员储备，助力科研范式变革和科技创新发展。

4　结束语

科研院所是国家科技力量的前沿阵地，科研网络安全关乎国家安全。在网络安全中运用计算机信息管理技术，能够防止网络病毒和黑客攻击，避免科研网络运行发生瘫痪造成严重损失。为此，应当运用访问管控、加密管理、研判网络安全问题、构建安全管理体系等技术措施，建立有效的、智能的网络安全防护和管理体系，保障科研生产网络安全、稳定、高效运行。

参考文献：

[1]艾琼.科研用户访问国外学术数据库的隐私保护与对策[J].图书情报工作，2019，63（10）：12-20.

[2]马福春.园区网网络安全问题及防护[J].电脑知识与技术，2014，10（24）：5607-5608+5610.

[3]黄逊.网络安全中计算机信息管理技术的应用[J].网络安全技术与应用，2022，2022（8）：159-161.

[4]卫星君.信息安全风险评估关键技术研究[J].科技传播，2017，9（04）：25-26.

[5]本刊编辑部.华为：定义网络安全新模式[J].网络安全和信息化，2022，2022（08）：48.

[6]王朔.桓高校科研数据服务能力评价指标体系构建[D].黑龙江省：黑龙江大学，2020.

[7]董文心.计算机信息管理技术在维护网络安全中的应用[J].市场周刊：商务营销，2020，2020（17）：68-70.

[8]任红.计算机信息管理技术与计算机网络安全应用[J].网络安全技术与应用，2021，2021（6）：156-157.

[9]余幸杰.云计算中的身份认证技术研究[J].信息网络安全，2012，2012（08）：71-74.

[10]路松.论网络安全中计算机信息管理技术的应用[J].信息记录材料，2021，22（03）：40-41.

[11]樊春.南基于RSA的AIS数据传输加密系统仿真[J].通信技术，2018，51（09）：2228-2233.

[12]闫辉.基于 5G 建设的传输端到端光缆建设方案[J].通信与信息技术，2021，2021（01）.

[13]张蒙蒙.计算机网络安全技术在网络安全维护中的应用探析[J].信息与电脑，2019，420（2）：216-217.

[14]胡越乔.论计算机反病毒技术的发展现状与展望[J].科技经济市场，2017，2017（12）：184-185.

[15]金涛.试析大数据云计算下网络安全技术实现的路径[J].电子元器件与信息技术，2023，7（02）：183-186+190.

人工智能对网络安全的威胁与应对

◆王明　孙志文　杨海燕

（河北科技师范学院　河北　066001）

摘要：随着人工智能技术的迅猛发展，网络安全防御面临前所未有的挑战与机遇。利用人工智能技术进行网络攻击的手段层出不穷，而传统网络安全防御措施在技术滞后、应对手段单一以及缺乏智能化等方面存在不足。本文着重关注人工智能技术在网络安全领域的应用与影响，分析其中的挑战与机遇。首先概述新时代人工智能技术的特点与发展趋势，然后深入分析基于人工智能技术对网络安全防御的威胁，并针对这些威胁提出具有可操作性的综合性应对策略。最后，探讨人工智能等新技术在提高网络安全水平中的重要性，为网络安全防御工作提供应对建议。

关键词：网络安全；威胁与应对；人工智能

在当今信息技术高速发展的背景下，网络安全问题愈发凸显，成为各个领域都不容忽视的关键议题。特别是在人工智能技术广泛应用的今天，网络安全所面临的挑战也随之发生了质的变化。为了应对这些新挑战，我们需要重新审视现有的网络安全防御策略并进行改进。本文将从一个全新的角度来探讨人工智能技术对网络安全领域所带来的网络安全威胁，并针对这些威胁提出综合性的应对策略。以及如何利用这些技术来加强网络安全防御。同时，本文还将讨论新技术在提升网络安全水平方面的潜力，以期对未来网络安全防御的相关工作提供一些有益的思考与建议。

1　相关概念综述

1.1 人工智能

人工智能[1]（Artificial Intelligence，AI）是一门致力于研究、开发、应用能够执行特定任务的计算机系统的科学领域。其目标是通过模拟人类智能，实现对信息的处理、学习和推理。人工智能技术近年来得到了广泛关注，逐渐渗透到众多领域，如自动驾驶、医疗诊断、智能家居等。人工智能在网络安全领域的应用具有巨大潜力。例如，通过使用机器学习算法，可以实时分析海量网络数据，快速识别潜在的威胁和异常行为，从而提高网络防御的效率。然而，人工智能技术的发展也给网络安全带来了挑战。恶意攻击者可能利用人工智能技术制定更复杂、更难以预测的攻击手段，以规避传统的防御机制。同时，人工智能系统本身可能存在安全漏洞，成为攻击者的潜在目标。人工智能等新技术在网络安全领域的应用和影响是双面性的。一方面，它可以提高网络安全防御的效率和效果；另一方面，它也给网络安全带来了新的挑战和隐患。因此，在发挥人工智能技术优势的同时，也应关注其在网络安全方面的潜在风险，并采取相应的防范措施。

1.2 网络安全防御概述