计算机网络信息通信的安全防范

付海波
武昌职业学院　湖北武汉　430200

摘　要：随着网络的广泛应用，网络安全问题也逐渐成为了关注的焦点。损害网络安全的行为不仅可能造成信息的泄露，还可能导致财务损失和声誉损失。计算机网络信息通信安全是目前面临的一项重要挑战。随着科技的进步和互联网的普及，网络安全风险也在不断增加。本文将介绍计算机网络信息通信安全防范的重要性，以及一些有效的防范措施，其中包括使用强密码、定期更新软件、使用防病毒软件、进行安全培训等，希望能够提高读者对网络安全的重视程度，并采取适当的防范措施来保护自己的网络安全。
关键词：计算机；网络信息；通信安全；安全防范

Computer network information communication security guard

Haibo Fu
Wuchang Vocational College, Wuhan, Hubei , 430200

Abstract: With the widespread use of the internet, network security issues have gradually become a focus of attention. Acts that compromise network security can not only result in information leakage but also lead to financial and reputational losses. Computer network information and communication security is currently facing an important challenge. With the advancement of technology and the popularity of the internet, network security risks are constantly increasing. This article will introduce the importance of computer network information and communication security prevention, as well as some effective prevention measures, including using strong passwords, regularly updating software, using anti-virus software, and providing security training. It is hoped that this article will raise readers' awareness of network security and encourage them to take appropriate measures to protect their own network security.
Keywords: computer; network information; communication security; security prevention

引言

计算机网络信息通信安全是当前面临的一个重要问题。随着互联网的发展和普及，计算机网络信息的交流和存储已经成为人们日常生活中不可缺少的部分。然而，随着网络的普及，网络安全风险也在不断增加。网络攻击、病毒感染、信息泄露等安全问题已经成为了社会的严重隐患。因此，保护网络信息安全显得尤为重要，要从计算机网络信息通信安全的定义、现状、重要性等方面入手，对计算机网络信息通信安全防范进行研究和分析。在实践中，我们可以深入了解计算机网络信息通信安全防范的内容和方法，并制定出一套有效的防范措施来保护我们的网络信息安全[1]。

一、计算机网络信息通信安全发展趋势

随着计算机网络信息通信浪潮的兴起和发展，无论是对于网络信息服务的支持，还是对安全问题的处理都有独特的优势。正是因为计算机网络信息通信与网络传统安全的有效融合，才能够真正为安全评估工作赋予新的动能。由于计算机网络信息通信安全在本质上是一种新技术的安全问题。计算机网络信息通信在技术领域有突出的作用。因此，可以利用其可预测性、可解释性、可处理性等方面的特点，将安全问题转化为操作问题。对信息数据等内容的合理管控与评估，构建完善的网络系统，可以降低安全隐患。计算机网络信息通信在发展的过程中，同样处于通信环境中，自身也需要防御不安全因素的攻击与威胁。这些方面使得计算机网络信息通信可以突破传统评估模式的壁垒，对安全信息评估工作提供更强的赋能。基于计算机技术的发展，现代计算机网络信息通信网络在提高防护能力、自我检测能力等方面也体现出了更强的功能。为了更好的处理网络安全问题，提高监控的效果，要构建多维的分析模型，准确应对网络信息服务安全评估中的各种问题[2]。

二、现代计算机网络信息通信的发展趋势

随着科技的不断发展和人们对网络安全的关注度的提高，计算机网络信息通信安全防范已经成为当今社会的一个重要课题。未来计算机网络信息通信安全防范将会有以下几个方面的发展趋势：第一智能化安全防护。

随着人工智能技术的不断发展，计算机网络信息通信安全防范也将逐渐智能化。未来的安全防护系统将能够自动识别攻击行为，并采取相应的防范措施。第二，云安全。云计算技术的普及和应用将使得计算机网络信息通信安全防范进一步走向云安全。未来的安全防护将不再仅限于本地计算机，而是在云端实现。第三，移动安全。移动设备的普及使得移动安全成为了计算机网络信息通信安全防范的重要方面。未来，移动安全将成为安全防护的重要组成部分，以保护移动设备上的敏感信息。第四，区块链安全。随着区块链技术的不断普及和应用，区块链安全也将成为计算机网络信息通信安全防范的重要组成部分。预计未来越来越多的金融机构和企业将采用区块链技术，因此，区块链安全将成为计算机网络信息通信安全防范领域的热门话题。第五，物联网安全。随着物联网技术的不断发展，物联网安全也将成为计算机网络信息通信安全防范的重要组成部分。预计未来，物联网技术将在生活的方方面面得到广泛应用，因此，物联网安全将成为计算机网络信息通信安全防范领域的重要话题。综上所述，未来几年，计算机网络信息通信安全防范将继续向智能化、云安全、移动安全、区块链安全和物联网安全等方向发展，以更好地保护网络信息和通信安全[3]。

三、计算机网络信息通信体系的安全问题分析

第一，存在信息安全问题。计算机网络信息通信系统平台在面对数据安全管理过程中，需要明确信息数据安全所面临的风险类型，这样才能够加快信息处理和分析的能力，得出准确的结果。首先我们考虑的是信息数据的安全问题。信息数据如果在传输中被违规处理，或是篡改，就会导致信息数据判断出现问题。这在极大程度上会导致恶意样本或是伪造数据的出现。面对这种信息数据不安全的情况，应该强化计算机算法模型的完善性，提高运算判断的准确性。而导致这一问题出现的原因有以下几个方面。对于信息数据的管理要从信息数据的稳定性和安全性入手明确，外部因素对网络数据的危害形式最为常见的就是我们所说的中毒。这是一种对于数据安全的攻击方式。通过修改相应的数据模块，调整范围值，对原始数据进行修改等。这种方法会使得数据分析方向出现偏离，导致分析结果不准确的情况出现[4]。

第二，数据不准确问题。数据是网络信息服务系统的组成部分，同时也是运算的承载者。识别和判断数据处理中存在的偏差和错误，才能阻碍外部的恶意攻击。所以，在数据框架的构建上要考虑如何降低安全风险。出现数据异常需要在相应的系统中找到数据泄露的原因，并且借助相应的技术手段，调整评估和管理方式，避免数据遭到进一步的破坏。计算机网络信息通信技术已经被应用到很多领域，对于信息数据的处理同样发挥着重要的作用。有些时候，导致数据信息泄漏或错误，是由于数据信息收集过剩。在这种情况下，现有的设备或是系统，无法对这些数据进行有效的收集和识别，这就会导致个人信息或是数据遭到泄露的情况[5]。

第三，存在外部安全威胁。信息技术的应用使得人们在交流和实践更加顺畅，同时，人们也会更加重视网络信息服务的安全性和有效性。要想做好具体工作，就必须要在安全评估中应用新的技术手段，抵御外部系统或是环境的恶意攻击。人工智能技术的提升必然会面对黑客等不法分子对于网络数据的窃取和盗用。通过人工智能系统可以自动锁定目标，并对相关的数据进行分析，扫描系统漏洞，提高攻击效率。但是，在应用这一技术的时候，我们还要明确人工智能对于自动编辑和虚假威胁信息等迷惑行为的处理效能。在进行安全评估时，就必须要考虑到如何应对这些虚假错误且具有威胁性的攻击行为，如果无法判断信息的真实性，就会导致评估失利的行为[6]。

四、提升计算机网络信息通信安全防范水平策略

面对这些风险，如果想要处理数据，避免数据丢失，既要确保信息传递的准确性，明确计算机网络信息通信系统和信息服务系统没有安全隐患，同时还要对于一些错误的信息做出及时的判断和纠正，这样才能够真正保障信息服务安全评估工作的有效性[7]。

（一）构建科学的安全防范体系

计算机网络信息通信安全防范的技术策略包括多项措施，以确保网络和通信的安全。计算机网络信息通信安全防范的技术策略是一种多重措施的综合方案，它们在保障网络和通信安全方面发挥着重要作用。首先，防火墙技术是必不可少的。防火墙可以阻止黑客的攻击，并保护网络数据和系统。它们可以通过限制不安全的流量进入网络，并通过进行数据包过滤等方式保护网络的安全。其次，加密技术对网络和通信安全也非常重要。加密技术可以保证数据的保密性和完整性，防止数据被窃取或篡改。加密技术通常包括对称加密和非对称加密等多种方式。身份验证和授权技术也是防范网络信息通信安全的重要措施。它们可以确保只有授权的用户才能访问敏感的网络资源和信息，从而避免未经授权的访问。智能监测和响应技术是有助于快速发现和解决安全问题的技术。它们可以通过实时监测网络的活动，并在发现异常情况时快速响应，从而保护网络的安全。另外，数据备份和恢复技术也是防范网络信息通信安全的重要措施。它们可以帮助组织在灾难发生时快速恢复数据，并最大限度地保护网络的安全。同时，网络安全审计技术也是防范网络信息通信安全的有力工具。它们可以帮助组织识别和解决安全问题，并不断改进网络安全策略。在网络信息通信安全防范中，采用多重安全技术和策略是非常重要的。它们可以通过利用各种安全技术和策略的优势，有效地保护网络和通信安全，确保组织的业务正常运行[8]。

（二）做好专业人才的培养

网络信息通信安全人员的职业技能和专业素养决定着人工智能应用的效果。在实践中，要强化对专业人才的培养。专业人才既要在技术和能力上符合评估工作的要求，同时还应积极开展专业化的培养工程，制定并实施相关的管理政策。只有在加大培养力度上做足功夫，才能真正实现人才推动的价值。众所周知，人才是驱动行业发展的关键。人工智能技术的应用离不开专业人才的加持，所以为了提高互联网信息服务安全评估工作的有效性，就必然要在人才培养上进行深入的探究[9]。在系统应用中，专业人才应了解网络信息通信技术的应用方式和手段，同时还要及时发现智能技术中存在的问题，避免造成不良影响。了解网络信息通信的内涵、优势和工作方法，才能从理论和实践角度提高对网络信息通信技术的应用水平。除了人才培养方面，还要鼓励人才进行自我发展和自我学习。对网络信息通信技术的应用是专业技能的体现，对网络信息通信技术的研究和发展才能真正促进研究成果的出现。在信息安全评估工作中，专业人才对网络信息通信的深入探究是促进工作升级的有效手段。因此，专业人才不仅是在开展工作，更多的也是对网络信息通信技术的积极探索。只要掌握网络信息通信的核心技术，就能在互联网信息服务安全评估工作中找到新的落脚点和出发点，最大限度的提高系统运行的有效性，避免风险的发生。

（三）合理优化安全评估方法

得益于网络信息通信技术的独特优势，需要结合网络信息通信的基本特点，对于信息服务安全评估进行有效的革新，并且利用恰当的评估方法开展工作。常见的分析方法有层次分析法，综合评定法等。这些方法的应用，要结合信息安全评估工作的具体需求予以选择。层次分析法是在数据内容分析时构建不同的层次结构，并且利用网络信息通信给不同层次的数据确定原始变量，然后在网络信息通信的作用下做好网络风险评估工作。这种分析方法的特点在于可以在实践中运用技术，依据以往的经验和资料，合理得出结果。值得我们注意的是，层次分析法只适用于计算量较小的信息服务，安全评估过程。除此之外，综合评定法也是网络信息通信技术应用的途径。综合评定法能够实现信息系统的有效应用，避免在运行中出现一些安全性的问题。所以，模糊评定法在信息风险评估过程中的作用更加显著，能够给出客观专业的评价。将层次分析与综合评定结合在一起，也是风险评估中的常见方法。这种多层次的综合评定办法能够弥补定性指标及定量指标评估方面的不足，让安全风险级别能够变得更加明确。同时，当互联网信息服务安全评估遇到阻碍时，这种方法还可以降低信息系统运算中所存在的风险。所以，这种评估方法也能够凸显人工智能技术的优势，让安全评估工作变得更加合理有效。

五、结语

综上所述，通过对计算机网络信息通信安全防范的研究，表明了保护网络信息安全的重要性。网络安全风险日益增加，因此，我们必须采取有效的防范措施来保护我们的网络信息安全。总的来说，计算机网络信息通信安全防范是一个复杂且持续发展的问题。必须不断加强对网络安全的关注，并采取有效的防范措施来保护我们的网络信息安全。

参考文献：

[1] 李鹏 . 计算机网络信息通信的安全防范 [J]. 集成电路应用 ,2020,37(10):36-37.

[2] 邱景怡 . 计算机网络信息通信的安全防范 [J]. 信息系统工程 ,2018(6):101.

[3] 章菊广 . 局域网环境背景下的计算机网络安全技术应用策略 [J]. 网络安全技术与应用 ,2022(1):2-3.

[4] 李洪亮 . 基于大数据的计算机网络安全防范对策 [J]. 网络安全技术与应用 ,2022(6):161-163.

[5] 李浩铭 , 乔桂林 . 大数据时代计算机网络安全技术应用分析 [J]. 网络安全技术与应用 ,2022(3):70-71.

[6] 魏彬 . 计算机网络安全技术中防火墙的应用分析 [J]. 网络安全技术与应用 ,2022(1):14-15.

[7] 郝晓康 . 基于网络安全维护的计算机网络安全技术应用 [J]. 网络安全技术与应用 ,2022(2):174-175.

[8] 王根 . 计算机网络安全技术发展与防火墙技术探讨 [J]. 网络安全技术与应用 ,2022(3):6-7.

[9] 陈辉 . 网络计算机安全隐患及漏洞挖掘技术研究 [J]. 网络安全技术与应用 ,2022(4):13-14.

作者简介：付海波（1987.05 - ），男，汉，湖北房县，大学本科，讲师，研究方向：计算机网络技术 。