计算机信息管理技术在网络安全中的实践探究

丁允允，李英，宋彦芳 *

郑州大学第三附属医院，河南 郑州 450000

摘　　要： 随着计算机技术的不断发展，计算机信息管理技术在社会中的应用领域也更加广泛，从企业管理到教育、医疗、行政等各个领域都离不开计算机信息管理技术的辅助。计算机信息管理技术的广泛应用在提高了各领域管理效率的同时，也带来了一定的网络安全问题，因此，在计算机信息管理技术的应用过程中，应当加强网络安全建设 [1]。本文将结合当前网络安全建设中的实际情况，探究计算机信息管理技术在网络安全中的具体应用策略，以求为相关工作人员提供一些参考。

关 键 词： 计算机信息管理技术；网络安全；信息安全；实践探究

The Practice Exploration of Computer Information Management Technology in Network Security

Ding Yunyun, Li Ying, Song Yanfang*

Zhengzhou University Third Affiliated Hospital, Zhengzhou, Henan 450000

Abstract: With the continuous development of computer technology, the application of computer information management technology in the society is also more extensive, from enterprise management to education, medical care, administration and other fields are inseparable from the assistance of computer information management technology. The extensive application of computer information management technology not only improves the management efficiency of various fields, but also brings some network security problems. Therefore, in the application process of computer information management technology, we should strengthen the construction of network security [1]. This paper will combine the actual situation of the current network security construction, explore the specific application strategy of computer information management technology in the network security, in order to provide some reference for the relevant staff.

Keywords: computer information management technology; network security; information security; practice inquiry

在互联网高度发达的今天，网络安全问题已然成为人们在生产生活中关注的重点问题。在计算机技术的使用过程中，有可能会产生数据丢失或数据被窃取等情况，严重影响了计算机信息管理工作的有序开展。为了保障计算机信息管理工作的高效运行，相关企业或事业单位应当积极参与网络安全建设，提升计算机信息管理技术的科学性，推动管理方式的信息化。为此，相关工作人员应当积极探索网络安全的威胁来源，并制定出行之有效的应对策略，保障计算机信息管理的良好发展，促进社会信息化水平的整体性提高。

一、网络安全建设的基本目标

在网络安全的建设工作中，需要事先设计好合理的网络安全建设目标，为网络安全建设工作提供更加科学合理的方向引导。目标主要体现在以下几个方面。

首先是要确保计算机信息管理的完整性。在计算机信息管理的生产、处理、保存、应用等全部流程中，都要保证网络信息在传输过程中的完整性。不能够在管理流程中经过程序的增加影响到网络信息的内容完整，要确保相关信息没有被中途修改或删除，保障信息传输的可靠性 [2]。

其次是认证环节方面，需要在进行网络服务的过程中，保障认证环节的实效性。对于网络应用权限做好规范性限制，避免因网络管理系统被其他用户登录所造成的信息泄露。同时也应当保证管理平台账号的当前使用者和账号申请者在身份上的统一性，并在判读出身份不一致时采取账号冻结处理 [3]。

最后是要确保计算机管理活动的保密性。保障计算机信息管理平台的使用者在进行网络管理活动时产生的数据信息无法被其他人获取。该目标是网络安全建设的核心目标，对于商业机密和

通讯作者：宋彦芳

私密信息的保密工作具有重要意义。同时也是网络安全建设工作中最受关注的目标。

二、网络安全的威胁来源

（一）系统漏洞

计算机网络系统是人工搭建的应用系统，在建设过程中难免会存在着一些漏洞，而用户在使用网络系统进行计算机信息管理活动时也很少会针对系统内容采取一定的防御举措，这便为计算机管理工作带来了许多不安全因素。同时，系统的漏洞对于计算机网络系统的稳定运行具有不良影响，极大地影响了管理工作的有序进行。例如在网络系统的运行过程中，不安全服务、配置、初始化等各项内容都会伴生系统漏洞，这些漏洞会使计算机网络安全等级急剧下降，为网络病毒和黑客攻击留下更多的空间，严重时甚至会出现系统的全面瘫痪，对于整体的计算机网络环境造成严重威胁[4]。

（二）网络病毒

在互联网的应用过程中，用户在进行网络活动时，网络端口处于开放状态，病毒也会随之影响用户的网络环境，对其计算机信息造成影响和侵袭。在当前众多的网络安全威胁因素当中，网络病毒是最为频繁、最为普遍的因素。作为一种网络程序，病毒会在网络环境中伪装成正常的程序，依托网络侵入到用户的计算机系统当中，并对计算机系统中的文件信息造成破坏。网络病毒能够直接影响到用户的文件使用情况，被感染的文件往往会出现损坏或没有办法正常打开，也有可能出现文件的不断复制，造成系统内部混乱，污染更多的信息文件。

（三）黑客攻击

黑客攻击也是当前网络安全的重要威胁，同时对计算机管理工作造成的影响和破坏更为明显。黑客是一种互联网信息技术发展过程中伴生出的非法群体，通过自身高超的计算机技术寻找计算机系统中的漏洞对网络系统展开攻击。黑客攻击带有明确的目的性，以获取非法利益为主，对计算机信息管理工作造成较大的破坏。黑客攻击主要有以下几种手段：一是通过制造大量的网络信息垃圾大量占用用户的网络系统资源，造成用户的网络拥堵，使主机在运行时无法得到网络响应，造成用户系统的瘫痪。二是通过破解用户的账户密码窃取重要信息，在认证环节对用户进行攻击，盗取用户的密码信息，通过账号密码假冒用户的身份完成登录认证，从而获取相应的信息内容，实现信息的窃取。三是直接攻击用户的网络环境，对用户的计算机信息功能造成破坏，并利用系统漏洞直接控制用户系统，直接进行窃取、篡改非法活动，对用户造成重大损失[5]。

三、网络安全管理中过程中的技术分析

（一）防火墙技术

防火墙技术的本质是借助硬件或软件系统，为内外网络环境搭建出一个防护屏障，保障内部网络环境下的用户无法直接受到外部网络环境的攻击。通过防火墙技术可以形成对数据访问行为的实时监管，并对网络环境下数据交互进行安全性筛选，保障计算机信息管理活动的环境安全。防火墙从原理上可以分为标准模式和双网关模式两种类型。标准模式的构建核心是 Unix 工作站，以 Unix 工作站为基础，通过两侧端口实现联通和交互活动[6]。标准模式下在激活特殊的软件程序时，可以主动调高管理级别，实现较好地防护效果。标准模式下的防火墙在面对数据传输时，可能会存在一定的滞后性。而双网关防火墙模式也可以进行系统的单独利用，以实现防火墙的不同功能，同时在面对复杂程序时的防控效率也可以得到保障。通过防火墙技术能够有效避免非授权用户的访问，过滤掉一些不良信息和风险内容。

（二）访问控制技术

访问控制技术和防火墙技术有一定的相似性，其主要目的是对网络信息进行及时的监测和筛选，对危险信息进行隔离，避免未授权访问的影响。通过较为严格的访问限制增强网络身份认证技术，实现对网络安全内容的总体管控。在访问控制技术下，可以通过网络追踪精确获取攻击者的 IP 地址，并为非授权入侵者布置安全陷阱，从源头上增强系统的安全性能。访问控制技术的技术性能总体较高，能够进一步完善网络运行环节和相关控制功能，进一步推动网络数据安全工作的建设，为网络安全的有效落实提供重要支撑。

（三）信息安全评估技术

提前预防是网络安全管理工作的重要环节，也是实现网络安全建设的前提条件。通过网络安全的评估工作可以提前了解网络环境的实际情况，并将网络环境中存在风险隐患的内容进行过滤和筛选，为信息化管理提供更加可靠的网络运行环境，保障信息管理的安全性。网络信息安全评估技术所应用的软件种类十分丰富，因此也较为复杂，通过提前的预判和评估能够以更具针对性的方式增强网络安全的防护工作，对于病毒进行提早评定，减少不明来源的程序对于系统的攻击，以最大限度规避网络信息中存在的安全隐患。

（四）信息加密技术

网络信息的加密技术在当前已经被广泛地应用于计算机信息管理的各个领域当中，对于网络信息的安全防护工作起到了重要作用。网络信息加密技术可以将需要读取的文件转入到秘密文件当中，并通过加密算法实现文件的加密工作，让文件无法被直接读取，以加密的形式实现对于文件信息的保护。在网络信息加密技术的加持下，黑客攻击将面临更加复杂的流程，可以有效降低黑客窃取信息的概率，实现重要网络信息的保密化处理，确保网络信息的安全[7]。

四、计算机信息管理技术在网络安全中的具体应用策略

（一）加强网络风险评估，做好网络安全建设的监管和预测

为应对网络监测管理技术缺失的问题，需要做好网络风险的提前评估活动，以增强计算机信息管理活动中的网络安全性[8]。为

实现这一目标，可以采用以下几点举措：首先是要结合各种网络安全问题的特点，做好针对性识别，通过网络安全事故的基本特性进行提前预判，并对事故的危害情况进行实时评估。其次是要对潜在的网络风险进行合理评估，以科学的评估和理性的分析应对潜在的网络安全风险，以求在风险发生之前提前制定好应对及反制措施，确保网络环境的安全性[9]。最后是要对现有的评估体系进行不断的升级和优化，准确分析出现有监测模式存在的不足，并以此制定出更加合理的监测体系，增强总体的网络安全风险处理能力，提高网络安全管理的稳定性和实时性。

（二）完善网络管理机制，为网络安全建设提供规范管理

为保证网络安全建设工作的落实，需要加强网络管理机制的建设，以更具体系化的管理制度规范从业人员的行为模式。在完善的网络管理机制的作用下，可以做到管理职责的明确化落实，实现管理流程的优化，进一步提高总体的网络信息管理水平。同时，也应当加强对于网络安全管理者的培训工作，优化计算机技术人才培养机制，加强人才培养力度，为计算机信息管理工作提供更多的技术型专业人才，保障信息管理活动的专业性。还需要重视员工监管机制的建设，保证计算机信息管理人员的工作透明度，避免因监管不当出现的网络安全风险。

（三）优化网络信息技术，为网络安全建设工作提供技术性支持

首先，应当对信息系统防御配置进行优化，让网络活动的安全性得到有效提升。通过对防火墙技术、访问控制技术等系统防御配置的全面优化，实现网络安全防御体系的全面性升级，为网络安全提供更强力的保护机制。其次，应当优化身份验证系统，避免信息管理账号的盗用。在必要时对身份验证信息进行复杂化处理，保证信息安全。利用科学技术对指纹、面部、声纹、虹膜等生物特征进行读取判定，避免由非本人操作带来的风险。最后，要对信息加密技术进行优化，通过更加高级的加密算法，如3DES、AES、IDEA 等[10]，增强重要信息或私密信息的防护水平。

五、结束语

综上所述，在计算机技术和互联网技术高速发展的背景下，对网络安全进行建设和管理活动有利于保障自身的信息安全，避免信息的泄露和损坏。在网络安全建设的过程中，需要充分利用计算机信息管理技术的综合特征，提高网络安全管理活动的综合效率，从预测评估、制度规范、技术支持等多个方面加以优化，确保网络安全的有效落实。

参考文献

[1] 柳冠军 . 探究计算机信息管理技术在网络安全中的实践应用 [J]. 电脑爱好者（电子刊），2021(3):1392.

[2] 朱迪 . 计算机信息管理技术如何在网络安全中的应用 [J]. 商情 ,2021(10):173.

[3] 王迪 . 计算机信息管理技术在维护网络安全中的实践探索 [J]. 信息记录材料 ,2020,21(7):204-205.

[4] 陈美倪 *, 毕路路 . 计算机信息管理技术在网络安全中的应用探究 [J]. 国际计算机科学进展 ,2022,2(1).

[5] 齐雪 . 浅谈计算机信息管理技术在网络安全中的应用 [J]. 中国新通信 ,2023,25(1):91-93.

[6] 夏泽暄 . 计算机信息管理技术在网络安全中的应用 [J]. 信息记录材料 ,2023,24(6):98-100.

[7] 汪升华 . 计算机信息管理技术在维护网络安全中的运用 [J]. 网络安全技术与应用 ,2023(7):113-115.

[8] 李晓江 . 计算机信息管理技术在网络安全中的应用 [J]. 电脑知识与技术 ,2022,18(8):40-41,43.

[9] 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(8):159-161.

[10] 贾康炜 . 计算机信息管理技术在网络安全中的应用分析 [J]. 现代工业经济和信息化 ,2022,12(6):106-107,169.