基于新形势下计算机网络信息安全存在的威胁及对策分析

郭绍南
（天门职业学院，湖北 天门 431700）

摘 要：在社会经济高效化的发展过程中，加快了信息化时代的革新进程，使计算机网络的整体使用范围日益拓展，渗透于各行业领域当中，突出了计算机网络系统的优势和效用。在使用计算机网络的过程中，能够为生产、生活带来便利性，但在个人隐私等方面，若无法加强对计算机网络系统的监管，则容易造成信息安全隐患等方面的问题。在新形势时代背景的影响下，本文对计算机网络信息安全现状和相关特点进行分析，提出应对计算机网络信息安全威胁有效对策，仅供参考。

关键词：新形势；计算机网络；信息安全；严重威胁；应对措施
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1004-7344(2022)40-0145-03

0 引言

在科学技术水平不断提升的过程中，为计算机网络技术的使用提供了广泛化的空间支持，为社会生产和日常生活带来了极大的便利。随着信息安全威胁的日益突出，在软件漏洞、黑客入侵以及病毒干扰的作用下，无法保证信息安全性，当出现信息泄露或者篡改等现象时，无法维持和谐、稳定的社会氛围。在应对计算机网络信息安全威胁的过程中，需要积极顺应新形势的革新要求，加大对信息安全问题的防范力度，在多种技术的共同作用下，实现对计算机网络信息有效防护。

1 分析计算机网络信息安全应对现状

在新形势时代背景的影响下，若出现网络入侵等情况时，可以对此类现象予以细致划分，通常是以黑客攻击和信息泄露这两种形式为主。在上述两种形式的破坏作用下，会对计算机网络系统带来严重的损坏，并且形成了具备破坏性的负面作用，导致系统持续处于瘫痪的状态，无法保障重要文件的安全性，并且会带来信息、数据泄露等问题。通过对影响计算机网络安全的威胁因素予以全面分析，可以看出通常情况下包括技术、人为等因素，在难以设置完善法律法规体系的情况下，同样会对计算机网络安全造成威胁。不仅如此，不法人员还会利用线路入侵的形式，在违反法律、法规的情况下，对关键信息进行窃听，所以对网络系统带来了严重的破坏，不利于保障网络信息的安全性。结合我国的计算机网络认证系统予以分析，可以看出整体的系统缺乏完善性，在难以落实管理工作的基础上，导致相关技术用产品失去了原有的效用，无法加强对网络安全系统的充分管理，若缺乏规范化的管理系统和监管体系，则会提高网络入侵等问题的发生概率[1]。

2 分析计算机网络信息安全的相关特点

2.1 完整性

网络信息在传输的过程中，需要坚持完整性的基本原则，为信息的交换和储存奠定良好的基础，避免对信息的处理过程造成不良影响。对系统内部予以严格管控，保障数据信息的原始面貌，确保生成方法具备准确性，为网络信息的储存和传输提供便利性支持。不仅如此，在网络信息的传递过程中，应减少数据信息修改等问题的出现，降低随意修改情况的发生概率，对数据信息破坏问题予以全面规避。

2.2 可用性

信息在被访问的过程中，需要确保单位和个人能够具备授权，并严格按照规定要求，对实际所调取的信息予以充分使用。若网络系统在运行过程中，受到了病毒入侵等破坏问题时，需要及时采取有针对性的修复措施，确保计算机系统能够尽快恢复使用。在计算机系统的运行过程中，若需要从中提取出必要信息，需要合理规避网络系统损坏等问题的出现[2]。

2.3 保密性

在储存信息的过程中，需要坚持保密性的原则，从而才能够提升信息安全系数。为此，应要求操作人员能

够严格按照规定，避免随意出现信息调取情况，减少信息泄露问题的发生。在管理计算机网络信息的过程中，应避免网络信息泄露等问题的出现，确保单位和个人能够具备授权之后，才可以将信息授权给单位和个人进行使用，并要求单位和个人能够明确掌握信息安全相关规范[3]。

3 新形势下计算机网络信息安全所面临的威胁

3.1 计算机网络信息系统漏洞问题

在网络系统的运行过程中，由于容易受到外界干扰因素所带来的影响，若无法保障连接形式的正规性与合法性，则会为系统安全漏洞的产生提供可能性，导致不法分子会侵入网络系统，从而不利于保障信息的安全性。计算机网络系统在运行的过程中，由于整体的网络运行系统具有复杂特性，会根据实际所接收到的指令，确定相应的运行结果，并完成信息的查找和分析作业。在计算机设备更新的过程中，使计算机的网络功能得到了强化，不法分子在研究计算机设备时，延伸出多种不同类型的入侵渠道，且攻击手段呈现出了多样性和复杂化的特点。对于部分不法分子来说，当其已经掌握网络信息系统时，能够借助网络信息系统的运行模式制造安全漏洞，并且可以利用任何一个终端设备，对特定的网络信用户信息系统进行攻击。通过窃取信息、篡改数据的形式，满足不法分子的利益需求，而这一类利益缺乏合法性[4]。

3.2 尚未加强对计算机网络信息安全的监管

网络用户的数量呈现出了大幅度的上升趋势，且计算机网络系统中所呈现出的网络活动具有多样性，在开展计算机网络信息安全管理工作时，容易为此项工作带来较大的难度，且整体的难度梯度日益上升。与此同时，网络信息安全监管平台在运行的过程中，若无法发挥监督管理等方面的职能优势，则会对平台监管机制的建立造成严重影响，难以保障监管平台和管理机制的健全性，提高了网络信息安全问题的发生概率。部分计算机网络信息安全管理人员在整理用户网络信息时，由于并未坚持严格性与严谨性的审核要求，所以导致网络信息安全管理工作失去了原有的效用，不仅无法保证信息安全系统设置的实效性，还会为不法分子的入侵创造了可能性，导致信息泄露等问题时有出现，使计算机网络系统受到信息安全问题的严重威胁。

3.3 计算机网络用户信息安全意识尚未加强

现阶段，计算机网络系统中的应用软件类型具有丰富性，且更新和创新效率普遍较高。在开展网络社交活动时，需要依赖计算机网络终端设备来完成，并满足居民的日常消费需求。需要注意的是，虽然部分软件在操作过程中，能够为日常的生产、生活和工作提供便利，但由于网络信息安全问题随之出现且日益突出，所以在应用快捷类支付软件时，容易导致部分网络用户信息存在泄露现象。例如：对于支付宝这一软件来说，此类支付应用软件具有快捷性，所以呈现出了普及化和广泛化的应用优势。在群众行使交易行为时，为支付宝等软件的应用提供了空间支持。若用户的安全意识尚未得到有效加强，那么在无法合理保障自身信息安全的情况下，容易为隐私信息泄露等威胁提供可能性，使不法分子通过窃取用户信息，使用不合法的形式，导致用户需要承担严重的经济财产等损失[5]。

4 新形势下应对计算机网络信息安全威胁的有效对策

4.1 完善信息安全防护技术

在计算机网络系统的运行过程中，由于存在不稳定性特征，所以网络信息安全问题具有突发性，需要积极的引进先进的网络信息安全技术，实现对网络信息安全问题的有效应对。例如：在使用网络加密技术、网络防火墙技术的过程中，在上述安全技术的共同作用下，能够有效应对病毒攻击，减少系统漏洞产生的可能性。为此，在使用防火墙技术的过程中，能够结合计算机网络系统的实际情况，对外部访问信息进行管控，以实时化的运作形式，加大对外部访问信息的拦截力度。同时，还应及时采取有效措施，通过对病毒的有力管控，提高计算机网络系统运行阶段的安全系数。

4.2 合理应用网络加密技术

在使用网络加密技术的过程中，需要遵循严格性与严谨性的要求，对信息的传输过程加以管控，避免信息在传递阶段被不法分子所窃取，通过提高计算机网络系统的保密性能，保障信息数据传递的安全性。在开展网络安全管控作业时，应基于层次化的形式，使加密技术能够涵盖多样化的基本层次。通过扩大加密技术的应用范围，使其能够结合网络安全监督作业，加大加密技术与网络安全监管体系的融合力度，为网络加密技术的应用提供广泛的空间支持，提高网络安全监督以及管理工作的实施水平。例如：在使用 TCP 协议以及 IP 协议的过程中，上述两种协议的应用具有广泛性，但仍然容易出现漏洞和问题。其中，对于 IP 协议来说，由于此类协议当中本身存在一定程度的安全问题，所以需要在使用网络加密技术时，应针对 IP 协议中的安全

问题加以整改，加大对地址假冒等问题的管控力度，发挥出网络加密技术的应用优势[6]。

4.3 建立健全信息安全保密对策

首先，通过对信息安全保密对策予以细致化分析，从涉密分级保护对策这一层级入手，为了完成信息安全保密等方面的工作，需要设置完善的计划管理方案，并对相关技术的应用提出较高的要求，促进安全监测作业的顺利进行，保障涉密分级保护对策设置的规范性与完善性。其次，在制定安全保密动态防护对策时，通常需要对网络系统中的不安全因素进行监督，并提出有针对性的管控措施，保障整体规划的合理性与科学性，制定更加完善的应急方案，突出信息保密工作的重要作用，提高计算机网络系统的安全系数，减少信息安全等问题的出现。最后，在建立安全保密纵深防御对策的过程中，需要强化网络管理人员的监督意识，根据网络系统的安全区域进行全面分析，并形成合理的区域划分形式，对安全域边界予以密切关注，提高监控作业的整体水平。

4.4 打造科学的计算机安全防护体系

在设置计算机防火墙的过程中，发挥出防火墙的优势和效用，并保证计算机防护作业的有效性，通过形成有力屏障，对外部的网络安全隐患进行过滤，避免入侵的计算机网络系统，减少对信息安全的严重威胁。在开展计算机网络安全防护工作时，需要从计算机软件和计算机硬件这两个方面入手，采取有效的安全隐患排除措施，对计算机系统中的潜在问题和安全隐患予以全面排除。用户在使用计算机系统的过程中，需要结合实际情况，及时安装计算机防火墙等防护体系，并对防火墙中的预警和提示予以高度重视，通过严格执行防火墙警告，采取有效措施，保障计算机系统的安全性。另外，还可以积极应对外部网络中的不安全因素，避免计算机系统出现瘫痪等现象，在计算机安全防护体系的运行阶段，及时结合外部网络病毒问题进行预警，保障预警操作的及时性和高效性，使计算机网络系统运行人员能够采取有效措施，加大对计算机网络信息的保护力度。

4.5 增强用户的安全意识

在计算机网络系统的运行过程中，部分网络信息安全问题通常是由人为因素所导致，这就需要用户能够有规划、有目的的强化自身的防范意识和安全意识。在操作计算机网络系统时，引导用户采取正确的运行方式，加大对信息的管控力度，保障信息数据的安全性，避免不法分子或者木马病毒对计算机网络系统带来侵害。不仅如此，还需要定期组织计算机网络信息技术人员开展培训活动，以网络培训的形式，扩大此类培训活动的宣传范围，使用户和技术人员都能够参与到网络培训活动中，借助专业化和多样化的培训内容，强化网民的安全意识，并调动技术人员的积极性与主动性。在管控计算机网络系统的过程中，应提出有针对性的管理措施，在法律法规的指导下，对相关法规内容予以完善。以计算机网络系统安全化管理为主要目的，促进网络道德教育工作的广泛推行，引导广大网民积极、主动的投入网络道德教育活动中，通过全面掌握计算机网络信息安全问题严重性，强化用户的安全意识。在技术人员和网民的共同配合下，实现对计算机网络信息安全威胁的有效管控，全面规避系统入侵问题。

5 结语

计算机网络系统在运行的过程中，容易出现信息安全等方面的问题，且此类问题具有复杂特性，由于带来信息入侵问题的影响因素相对较多，在制定防范措施时，应对相关干扰因素进行综合考虑，制定合理的防范方法。现阶段需要结合计算机网络系统的运行现状，对其中可能会存在的网络信息安全威胁进行探究，通过顺应新形势的革新趋势，提出有针对性的应对措施，并加大对网络信息安全问题的防范力度，保障计算机网络信息安全应对措施的实效性。

参考文献

[1] 高铭泽.探析新形势下计算机网络信息安全性的提升策略[J].湖北农机化，2020(6)：19.
[2] 王林军，魏敏敏.新形势下计算机通信网络安全防护策略[J].时代经贸，2019(36)：95-96.
[3] 丁永尚，艾旭升.新形势下高校网络安全建设实践研究和设计[J].内江科技，2019，40(11)：52-53.
[4] 范伟康. 新形势下计算机网络信息安全存在的威胁及对策研究[J].电子元器件与信息技术，2018(9)：61-64.
[5] 吴亚峰. 新形势下计算机网络信息安全存在的威胁及对策研究[J].中国战略新兴产业，2018(32)：92.
[6] 苏东楠.新形势下计算机网络信息安全的技术发展问题[J].信息系统工程，2018(6)：104.

作者简介：郭绍南(1984—)，男，汉族，湖北天门人，本科，讲师，研究方向为计算机。