大数据时代下计算机信息技术在网络安全中的应用分析

袁　睿
绿城科技产业服务集团有限公司　浙江杭州　310000

摘　要：大数据时代下，为信息传递方式、信息处理提供了重要路径，改善人类生产生活环境。大数据为计算机信息技术提供了网络安全保障，是经济社会健康发展的关键性技术。基于大数据时代，应通过提高计算机信息技术网络安全系数，体现其应用有效性，进而保护用户隐私、提升安全水平。本文围绕大数据时代下计算机信息技术在网络安全中的重要性进行分析，结合网络安全影响因素进行讨论，提出相应的应对策略，旨在提高信息技术的应用效能。

关键词：大数据时代；计算机信息技术；网络安全；应用

引言

大数据背景下，计算机信息技术已成为政治、经济、生活、教育、医疗、军事等领域的重要工具，引领着人类生活走向数字化、信息化。但大数据时代为人类提供高速、便捷服务的同时，也存在网络安全隐患。网络黑客技术高超、人数较多，通过计算机网络虚拟技术隐藏身份，再通过技术手段盗取网络用户个人信息、窃取其隐私，导致用户重要信息泄露，给用户带来不同程度的损失。因此，依托大数据背景，技术人员巧妙运用计算机信息技术保障网络安全，切实提高网络用户的整体水平。

1 保护网络安全的重要性

互联网不但丰富了人们的日常生活，而且为人们带来海量信息和数据资料，为生产生活提供重要信息。在大数据时代下，网络安全成为人们重点关注的课题。“如何提升网络安全”“如何运用计算机信息技术保护网络安全”越来越被人们重视。基于此，利用计算机信息技术保障网络安全，能够促进社会发展、人们生活快速进入数字化、信息化环境，进而提高效率与质量。

在大数据背景下，计算机信息技术能够有效保障网络安全，使网络技术可以更好地为人们日常工作、休闲娱乐、商务洽谈、文化传播等方方面面提供技术保障。在网络安全保障中，计算机管理技术切合实际要求，对网络攻击予以精准防范，高效解决网络安全问题，提高网络安全可靠性和有效性[1]。

2 大数据下网络安全影响因素

2.1 网络病毒

在网络上传播，对服务器、客户端组件造成破坏的病毒，即可称之为网络病毒。网络病毒对网络体系造成不良影响，其在网络体系传播中对网络体系造成较大危害。基于此，网络病毒破坏对象主要为网络，是网络安全的“克星”。网络病毒能够在计算机运行过程中进行攻击、破坏，导致计算机系统代码错误、运行失控；网络病毒传播速度随着计算机运行速度而变化，即计算机运行速度快，则网络病毒传播速度快；计算机运行速度慢，则网络病毒传播速度慢。网络病毒对网络安全影响较大，使其自身防御系统处于瘫痪状态，导致系统出现崩溃，影响其正常使用的功能。

2.2 安全漏洞

外部系统支持计算机访问网络，并对关键部门进行访问，但若外部系统稳定性较差，则会导致网络安全漏洞。计算机正常使用过程中，软件、硬件共同操作系统，二者若出现问题，则使得计算外部系统稳定性降低。在计算机网络安全中，应定期进行下载、安装补丁的操作，对其漏洞进行修补，以此保证计算机运行稳定性。但是，若出现动态变化漏洞，普通安装补丁无法进行修复，导致网络安全问题严重，为网络黑客提供可乘之机。比如，企业网络安全系统遭遇安全漏洞，则会在黑客入侵后，造成商业信息泄露，机密文件丢失等问题，使得企业遭遇严重经济损失[2]。

2.3 管理缺陷

计算机管理缺陷是导致计算机网络安全的重要因素之一。一般情况下，计算机管理人员使用防火墙、杀毒软件等

保护计算机网络安全，但由于网络安全意识淡薄，忽略网络安全防护措施应用的重要性，导致网络安全问题频发。另外，部分计算机使用者认为安装网络安全防护软件容易导致设备性能障碍，对计算机系统自带的网络防护软件予以卸载，安装和使用盗版防护软件，导致个人信息泄露、网络安全问题等。由于计算机管理者人为因素，忽略安全防火墙、防护软件的系统安装，导致网络黑客入侵，使得重要文件、机密信息等丢失，为其带来不可估量的经济损失。

2.4 黑客攻击

计算机使用者一般习惯于将数据信息存储于计算机中，为后续使用提供方便；这一习惯无形中为网络黑客窃取资料提供便利条件。一些黑客为了经济利益或恶意报复，频频对目标对象计算机进行攻击，通过攻击夺取用户有价值的信息，并将其泄漏出去，导致计算机网络安全问题频出，使得计算机出现瘫痪、漏洞等，最终导致其无法正常使用。另外，黑客对海量数据信息造成攻击风险，存在较大的网络安全隐患，使得计算机系统无法正常运行，造成使用者的操作困难。

2.5 操作不当

计算机使用者在使用计算机时，对计算机进行规范性操作，发挥其最大功用；但若对计算机进行错误操作，则使得计算机网络安全问题出现，影响整个体系应用效能。比如，计算机操作者对计算机不熟悉或个人操作习惯问题，导致一系列的安全隐患，使得计算机陷入网络安全问题之中。另外，操作者网络安全意识薄弱，在使用计算机期间容易泄漏个人隐私。比如，泄漏账号、密码等，导致重要信息丢失，使其存在一系列的网络安全隐患。基于此，计算机使用者应在现实操作中以网络安全为第一位，科学、正规地进行计算机操作，以此杜绝各类操作不当造成的网络安全问题。

3 大数据时代下计算机信息技术在网络安全中的应用

3.1 提升安全意识，防范网络病毒

提升用户安全意识，加大网络安全关注力度，能够有效防范网络病毒。大数据时代下，用户通过使用计算机信息技术保障网络安全，降低网络病毒侵害影响，使用户损失降到最低[3]。首先，用户应提升对个人上网安全的认知，提升用户对这一内容的关注度，使其认识到个人信息泄露的严重性。比如，泄漏个人信息会造成生命财产安全问题，影响个人信息安全等，从而加强用户的使用安全意识。其次，用户在防范网络病毒中，应设计高保密性密码对网络系统进行安全保护，避免非法入侵导致个人信息泄露，进而保护个人资料安全。比如，提高用户使用计算机信息技术保障网络安全的能力，使其能够在安全、合理的范围内防范网络病毒，提升计算机应用安全系数。同时应用计算机信息技术对网络病毒进行防范，最大限度保障和维护计算机系统安全，降低和避免网络病毒侵害。最后，增强网络用户规范操作意识，使其了解安全意识的有效性和可行性。计算机用户要不断增强网络安全意识，在具体操作中应用有效防范方法避免网络病毒侵害。比如，计算机用户在使用过程中，应用计算机信息技术做好网络安全工作，建立一个安全、绿色、健康的网络运行环境，抵制不良网站、不良信息带来的网络病毒，进而提升安全意识。

3.2 完善防御系统，查补安全漏洞

大数据时代下，信息技术快速发展，为计算机安全使用提供技术保障。在计算机使用过程中，网络安全影响面较大，不是影响“一位用户”“一台机器”，而是对整个网络系统造成安全影响。因此，相关部门监管人员应对相应网站、相应软件进行安全管理，逐步完善计算机网络安全防御系统。同时，推广应用相应的网络安全防御软件，对计算机用户群体展开密集排查和系统保护，及时筛查不法网站的系统漏洞，做好相应的处置、防御，以科学有效地防御系统抵制安全漏洞，提高用户使用安全性，为用户提供安全保障。政府部门加大对应用软件开发企业的长效监管，加大人员培训力度，分析系统风险隐患，提高系统运行安全性和平稳性，从根本上杜绝或减少安全漏洞造成的影响。通过运用计算机信息技术中的实时监测技术对网络信息进行分析和处理，进行信息采集与应用。一旦遇到信息不匹配问题，应进行二次检测，并配合入侵监测技术对危险信息进行扫描。其中，若对于网络安全中获取的损坏性信息，要通过信息技术进行修补；对不能进行修补的信息则通过“打包”的方式传输给管理员，由管理员进行专业化处理。比如，进行系统加固处理，关闭危险端口，禁止使用 139、445 等高危端口；防止 RPC 漏洞被利用；提升限制权限，通过注册表设置、命令行限制等降低权限滥用造成的安全漏洞。

3.3 网络安全管理，完善保护制度

网络安全管理是网络安全的基本前提。通过建立网络安全管理制度，约束和保障用户网络使用安全，以此提高计算机安全保护能力。在网络安全管理中，能够有效杜绝管理

缺陷问题，通过建立健全与时代相符的网络安全环境，应用网络安全制度，通过制度为相关人员提供依据，使其遵循制度原则提高安全管理效能[4]。基于大数据背景，计算机信息技术应用安全管理能够完善网络安全保护制度，净化网络安全环境，发挥计算机信息技术应用效能。比如，企业在计算机信息技术应用中，能够有效解决办公过程中的网络安全问题。在这一过程中，需要技术人员熟练掌握大数据属性，通过计算机信息技术保障网络安全，进而提高计算机用户使用安全性。基于此，加强安全管理工作中，一方面，领导层、各部门要做好相应的网络安全管理意识培养工作，使其能够明确计算机安全管理重要性，从而遵章办事，提高管控效能。结合计算机网络安全实际问题，做好发展规划、体现产品特色，科学构建合理性、安全性计算机网络环境。另一方面，以部门为核心，召开计算机信息技术在网络安全中应用的安全大会，不断增强计算机用户安全意识，使其能够在常态化操作过程中遵章办事，养成良好的计算机操作习惯，避免不良网站、网页的浏览，削减网络病毒侵害、提高网络安全管理效能。

3.4 设置防火墙，应对黑客入侵

大数据时代下，“黑客”已不是一个陌生的名词，黑客存在于网络的各个角落。人们应对黑客保持时刻警惕，针对计算机使用过程中容易受到黑客攻击的部分，要加强防御力度，有效避免黑客入侵造成的不良影响。比如，政府机关、企事业单位等是档案信息密集区，在使用网络过程中应结合大数据时代特点，做好黑客预防工作，设置专业、灵活的反黑客攻击防御系统，优化安全预警系统，从而降低黑客入侵可能性。同时，应对普通网络用户进行“反黑客”教育指导，通过科普相关的“反黑客”教育视频，提高其应对黑客入侵的专业技术能力。通过设置计算机安全防火墙，对黑客进行实时防护[5]。防火墙在网络环境下，能够结合数据访问全过程进行实时监控、管理和防御。通过防火墙等级的提升，能够提升网络安全系数，避免外部用户使用非法手段入侵网络系统，进而提高网络系统内部安全性，有效应对网络环境下信息泄露问题。同时，在使用防火墙过程中应不断强化防火墙的预设功能，根据功能目标进行程度分析，确保防火墙能够起到防御的作用。防火墙能够阻止危险信息阅览、危险插件安装，阻隔一切对网络系统造成安全威胁的信息，从而发挥防火墙的保护作用，体现计算机信息技术使用安全性。

3.5 规范操作行为，实现网络安全

安全管理规范直接影响大数据网络安全，基于此，在进行大数据计算机信息技术网络安全管理中，应通过严格执行操作标准科学管理网络数据安全。计算机用户在大数据下，要规范操作行为，保障网络安全，这是一项长期的、系统的工程，通过良好的操作习惯提高网络安全有效性。首先，加强设备管理。在常态化工作中，对计算机设备进行日常维护和安全保障至关重要，应定期对其系统进行病毒查杀，在局域网内部进行安全维护，通过设置防火墙，预防各类黑客攻击。在计算机系统中的病毒查杀中，通过安装杀毒软件提升病毒预防效能。对计算机软件应进行定期升级，提高软件应对网络病毒的能力，使其能够创造良好的软件预防“生态系统”。其次，优化操作流程。在计算机操作中，操作人员遵循计算机应用规范，巧用信息技术进行安全管理；合理进行操作与应用，杜绝浏览和使用非法网站，避免网站病毒侵害。比如，对网站弹窗广告予以忽略，防止网络病毒侵害。

4 结束语

大数据分析下，网络安全问题多种多样，为计算机用户带来使用困扰，造成一定损失，影响整个计算机生态系统科学应用，阻碍其可持续性发展。随着大数据处理技术的日益成熟，需做好计算机网络安全工作，充分发挥计算机信息技术作用，确保大数据背景下网络安全，促进计算机用户获得良好使用体验。大数据是信息时代的主流，在计算机信息技术应用中能够净化网络安全环境，提高网络安全系数，共同营造健康、绿色、安全的网络平台。

参考文献：

[1] 韩腾飞 . 大数据时代背景下计算机网络信息安全教学的创新研究 [J]. 电子元器件与信息技术 ,2025,9(01):180–182.

[2] 赵金金 , 孙正伟 . 大数据时代下计算机网络安全技术的挑战与对策研究 [J]. 软件 ,2025,46(01):178–180.

[3] 张妍 , 肖志勇 . 大数据时代计算机网络信息安全与防护策略 [J]. 数字通信世界 ,2025,(01):89–91.

[4] 张成挺 , 程超 , 叶万兴 , 等 . 大数据时代计算机网络安全技术的应用策略 [J]. 电脑知识与技术 ,2025,21(06):86–87+96.

[5] 韩璐 . 大数据时代背景下人工智能技术在计算机网络安全中的应用研究 [J]. 科技资讯 ,2025,23(04):44–46.