基于大数据时代计算机网络安全防范探讨

龚　瑞
仙桃职业学院　湖北仙桃　433000

摘　要：在现代科学技术高速发展的背景下，已经全面进入了信息时代，在信息时代中计算机技术、互联网技术具有重要的作用，使得社会生产模式与人们的生活方式发生很大变化。但是结合当前计算机网络的实际情况来看，存在着一定的安全问题，为了强化计算机网络安全防范，可以通过大数据技术构建相应的防范模式。因此，本文将对基于大数据时代计算机网络安全防范进行深入地研究与分析，并结合实践经验总结一些措施，希望可以对相关人员有所帮助。

关键词：大数据；计算机；网络安全；防范方法；优化措施

Discussion on computer network security prevention in the era of big Data

Rui Gong
Xiantao Vocational College, Xiantao, Hubei, 433000

Abstract: Under the background of the rapid development of modern science and technology, it has fully entered the information age. In the information age, computer technology, Internet technology plays an important role, making the social production mode and people's way of life have undergone great changes. However, according to the actual situation of the current computer network, there are some security problems. In order to strengthen the security prevention of the computer network, the corresponding prevention mode can be built through big data technology. Therefore, this paper will conduct in-depth research and analysis on computer network security prevention in the era of big data, and summarize some measures combined with practical experience, hoping to be helpful to relevant personnel.

Keywords: big data; computer; network security; prevention methods; optimization measures

计算机网络已经成为现代社会的重要组成部分，工业生产、企业管理以及个人都需要使用计算机网络，在很大程度上促进了社会发展。但是受到计算机网络特点的影响，容易发生一些安全性问题，比如网络病毒、恶意攻击等，导致计算机用户的个人隐私泄露，甚至会引起财产损失。为了提升计算机网络安全防范力度，需要加强对大数据技术的应用，通过大数据技术构建相应的防范体系，能够有效提升防护效果，全面保障计算机网络安全，为用户使用计算机网络提供充分保障。

作者简介：龚瑞（1985年7月－），男，汉，籍贯：湖北仙桃。学历：大学，职称：高校讲师，研究方向：计算机网络技术，网络安全。工作单位：仙桃职业学院，邮编：433000。

一、大数据背景下计算机网络安全相关内容分析

在现代信息技术发展的推动下，我国各行业得以飞速发展，大数据技术、计算机技术以及互联网技术的应用，为生产生活带来了许多便利条件。在大数据时代下，数据处理能力全面提升，为大量且复杂的数据处理工作提供了全面支持，是传统计算机信息技术不具有的能力与优势。虽然大数据技术使得各项数据处理能力增强，但是由于计算机产生的数据总量较大，且安全防范能力较弱，从而产生了安全性问题，计算机数据风险问题全面增加，对社会生产以及群众生活造成了很大负面影响，所以在大数据时代下，必须做好计算机网络安全防范工作，构建完善的防范体系，全面保障计算机网络安全性。在大数据时代下，计算机网络具有高效化的资源共享功能，在计算机网络应用日益普及的情况下，数据安全问

题日益凸显，且由于我国计算机网络用户大幅度增长，网络安全问题的影响范围更广，造成的后果与损失更加严重，所以必须做好计算机网络防范工作。大数据技术的处理能力，为计算机网络安全防范提供了相应的支持，通过将大数据技术与计算机网络防范相结合，能够构建更加完善的防范体系，更好地保障计算机网络用户的个人因素数据，避免出现数据泄漏问题，从而为用户提供安全的计算机网络环境，是大数据技术具有的重要优势，为此需要以大数据技术为基础构建相应的防范体系[1]。

二、大数据时代下计算机网络安全存在相关问题分析

在大数据时代下，数据已经成为重要的资源，为了避免数据安全问题发生，需要加强大数据技术的使用，但是在多种因素的影响下，当前计算机网络安全还存在着一些问题，具体包括如下几项：

2.1 计算机网络安全管理制度不够完善

计算机网络的发展已经与许多行业融合，与社会发展之间具有密切的关系，是一项不可缺少的重要技术，但是当前相关部门对于计算机网络安全问题不够重视，没有构建完善的计算机网络安全管理制度，缺乏相应的法律法规支持，从而导致计算机网络安全问题难以有效解决。计算机网络安全问题对于社会发展会产生很大危害，需要相关部门制定完善的管理制度，确保各项防范管理工作全面落实，才能够提升计算机网络安全安全性，但是当前在制度方面还存在着一些空白，导致计算机网络安全难以得到保障。

2.2 防范技术缺乏创新

计算机网络技术的应用，使得信息、数据传输效率加快，数据传输也是计算机网络最为主要的功能，但是在计算机网络中传递数据时，由于缺乏相应的防范技术，很容易出现数据被拦截、窃取等问题，从而导致用户个人信息被泄露，一些不法分子通过获取他人在计算机网络中传输的数据开展相应的违法活动，比如利用获取的信息盗取他人钱财等，外加我国部分计算机网络用户缺乏防范意识，导致该问题频繁发生。为了确保计算机网络安全性，必须加强对防范技术的创新，积极融合其他技术构建相应的防范体系，但是当前计算机网络安全防范技术整体创新性不足，采用的防范技术依然处于较为落后的水平[2]。

2.3 网络病毒与非法入侵方法能力不足

在计算机网络全面普及的背景下，随之而出现了大量的网络病毒与非法入侵事件，我国已经发生过多次重大的网络病毒、非法入侵等计算机网络安全问题，比如最为著名的“熊猫烧香”病毒事件，普通计算机网络用户难以有效抵御网络病毒。但是结合当前计算机网络安全防范的实际情况来看，在抵御网络病毒、非法入侵等方面的能力还存在着一定不足，计算机系统、网络系统等存在着许多漏洞，使得网络病毒、非法入侵有可乘之机，这些问题在计算机网络中较为普遍，且造成的后果与损失较为严重，需要通过融合大数据等技术，构建相应的防范体系，确保网络病毒、非法入侵等问题能够得到有效处理。

三、基于大数据时代计算机网络安全防范优化措施分析

结合上文的分析可以明确，在大数据时代下，计算机网络安全已经成为一项重要的问题，必须做好计算机网络安全防范与保障工作，才能够为用户提供安全的网络环境，促进社会稳定发展。但是受到技术水平等因素的限制，当前计算机网络安全防范工作中还存在着一定的不足，导致相关问题频繁发生。因此，本文结合相关实践经验，总结如下多项大数据时代下计算机网络安全防范优化措施：

3.1 制定完善的防范制度

为了确保计算机网络安全防范效果，需要相关部门制定相应的防范制度，为计算机网络安全防护工作开展提供支持。首先，需要提升群众计算机网络安全防护意识，政府相关部门需要加强对网络安全的宣传，使得群众认识到计算机网络安全的重要性，并学习一些基本的防范方法，以此提升整体防护水平，是最为有效的防范措施。其次，网络安全相关部门需要构建相应的防范制度，加强防范技术的研发与创新，积极融合大数据技术，构建相应的方法技术体系，并加强对新型防范技术体系的推广与宣传，将各项新型技术应用在网络安全防范中，为企业、工业以及个人用户等提供防范技术支持，从而能够提升全社会网络安全防护水平。最后，需要做好计算机网络安全防护相关法律法规的制定，为防护工作开展提供制度化的支持，确保防护工作能够全面开展，有利于构建更加完善、全面的防护制度与体系，以此方式提升计算机网络安全防范工作质量与水平[3]。

3.2 加强大数据技术与安全检测的融合

受到计算机网络特征的影响，大部分计算机网络安全问题都具有隐蔽性，普通用户无法准确察觉与识别相关问题，所以在计算机网络安全防范中，需要做好相应的检测工作，通过检测技术能够准确识别网络病毒、非法入侵等问题，但是传统的检测技术效率较差，检测范围、检测效果等存在问题，所以为了提升安全检测工作

质量，可以与大数据技术进行融合。大数据技术具有快速处理信息的能力，所以在对计算机网路病毒、非法入侵等检测时，能够快速检测大量的数据，在发现异常数据后，能够进行预警，并自动启动相应的防范措施，使得异常数据无法进入用户的计算机网络系统中，进而能够提升计算机网络安全防范效果。大数据技术的应用，为计算机网络安全防范提供了全新的思路，使得网络安全防范中的检测技术水平全面提升，为此需要结合计算机网络安全事件的基本特征，做好与大数据技术的融合工作，将大数据技术的优势全面发挥，通过大户数技术提升网络安全监测效率、检测方法，从而能够提高检测工作效果，是大数据时代下计算机网络安全防范的有效优化措施。

3.3 利用大户数技术加强数据传输防护

大数据与计算机网络相结合已经成为时代发展的必然趋势，这种形式也增加了计算机网络安全事故发生的概率，所以要加强病毒预防与处理软件的开发，比如针对数据传输的有效抵御计算机病毒的软件，通过数据加密与访问控制技术，能够实现对数据传输的有效保护，通过对授权方式、入网访问控制等多方面技术的不断升级，对新书传输的主体与客体之间的访问过程进行高级别的规则约束，对于其他的动态信息，可以通过密钥进行控制的方法来不断完善数据加密技术，并且对数据进行科学的处理与变换，能够有效组织一些非法授权的人利用软件对用户数据进行访问和修改，这样的方式能够在很大程度上确保用户数据传输的安全，而且维护与管理的成本较低，可以实现对计算机网络安全的有效保护。计算机网络安全的维护与管理要具有高度的针对性，对不同的环节采用不同的维护与管理方式，不断创新和升级相关技术，才能实现最大程度的对计算机网络安全的维护与管理，保护我国网络信息的安全。大数据技术对于信息传输保护具有重要的作用，需要加强相关技术创新，为数据、信息传输提供全面的安全防护，避免数据传输过程中出现丢失、窃取等问题，从而保障用户个人数据安全，是大数据技术的重要应用方式，需要加强大数据方法技术的研发，为计算机网络用户提供更加良好的环境[4]。

3.4 提升交换网络安全防范力度

为了提升计算机网络安全性，不仅需要完善的制度与技术体系，同时需要采用有效的计算机网络安全防范措施，确保交换网络安全性。交换网络是指网络内部互联设备，存在着一定的安全风险，需要做好安全保障工作。路由器与交换器在默认状态下，不需要输入指令就能够直接登录，这就为非法入侵提供了便利条件，是计算机网络安全中存在的一个漏洞。交换网络在计算机网络中具有重要的作用，所以为了保障其安全性，需要配置交换器与路由器登录管理权限，确保网络不会受到入侵；同时，需要加强网络访问控制技术的应用，对计算机网络设备的安全进行管控，利用检查命令等方式，实现对输入、输出数据的访问控制，并结合大数据技术的数据处理优势，能够提高交换网络数据处理效率，在防范非法入侵方面具有重要的作用，可以全面提升交换网络安全性，确保内部网络不受到非法入侵等问题的影响，为用户的隐私数据、个人网络等提供全面的防护[5]。木马病毒、非法入侵等具有隐蔽性与随机性，无法做好提前预防，所以一般都是在对计算机网络产生破坏后才会发现，所以为了确保交换网络安全，需要结合大数据技术，构建交换网络数据安全防范系统，加强对交换网络的数据监测与分析，是提升交换网络安全水平的有效措施，可以避免多项计算机网络安全问题发生。

四、结束语

综上所述，本文简要阐述了大数据时代下计算机网络安全相关内容，并对当前计算机网络安全防范中存在的问题进行分析，最后提出并总结了多项科学有效的防范优化措施，希望能够对计算机网络安全领域起到一定的借鉴与帮助作用，全面提升计算机网络安全性，构建更加安全的网络环境，推动社会发展与建设，同时促进我国计算机网络领域技术创新。

参考文献：

[1]常祖国.探讨大数据时代的计算机网络安全及防范措施[J].网络安全技术与应用，2022（003）：35-35.

[2]庞涛.大数据时代的计算机网络安全及防范措施[J].百科论坛电子杂志，2022，40（1）：225-227.

[3]张晓玲.大数据时代下计算机网络安全防范技术探究[J].计算机应用文摘，2022，38（8）：101-104.

[4]颜玲，彭维龙.基于大数据时代的计算机网络安全防范措施研究[J].电子元器件与信息技术，2021（02）：3-3.

[5]蔡畅.基于大数据时代的计算机网络安全防范措施研究[J].数字通信世界，2022（009）：12-12.