大数据背景下计算机网络安全及防范措施分析

杨洋
云南省曲靖农业学校

[摘　要]随着大数据时代的到来，我们的生活环境发生了巨大的变化，在通信技术和计算机网络的全面覆盖下，我们迎来了信息的高度共享时代，但与此同时，我们的计算机网络安全也面临着诸多威胁。在大数据背景下，计算机用户之间的信息交流量非常庞大，而这些数据信息都会在计算机网络系统中留存，但是当前的计算机网络安全管理还存在诸多问题，如安全管理体系不完善、数据安全管理不规范、数据存储安全性低、网络病毒威胁计算机安全、网络安全防护工具更新慢、网络安全管理人员基本素养有待提升等，导致计算机网络安全问题频发。对此，在当前的时代背景下，有必要重视计算机网络安全问题，强化计算机网络安全管控。

[关键词]大数据；计算机网络安全；防范措施
【DOI】10.12252/j.issn.2096-627X.2021.10.1117

近年来，大数据在我们工作和生活中的应用范围愈发广泛，其所承载的价值也越来越高。在新时代的网络环境背景下，大数据与计算机网络技术的发展相辅相成、互相依存，同时也创造出了更多的价值。在计算机网络的迅速发展中，保障网络的安全性是极为重要的一项任务，然而在面对大数据时代下高频、海量的数据信息交互时，计算机网络安全也迎来了新的挑战。就此而言，在当前大数据背景下，我们必须要将网络安全的防范工作重视起来，在进行数据信息的交互、存储过程中，保障计算机网络系统信息的安全，进而推动计算机网络技术和大数据技术的进一步融合发展，为我们的工作和生活带来更多便利。

一、大数据背景下计算机网络安全防护的重要性

如今，在大数据技术的支持下，计算机网络技术也得到了进一步的发展，计算机网络用户之间的信息交流激增，这些庞大、复杂的数据量都将通过计算机网络系统进行储存和交互，随着信息交互形式朝着多元化和高速率方向发展，计算机网络安全问题也越来越突出，成为用户应用计算机网络的重要阻碍。

当前，各个行业也实现了长足的发展，有效推进了信息化、智能化在各个行业的展开。基于大数据和网络技术的发展，信息数据的交流传递速度大大提升，同时大大增强了数据信息的时效性，在信息数据的高效利用下，有效推进了各个行业的升级转型，尤其对于新业态行业中，大数据在其中的应用价值更加明显。但与此同时，信息安全方面的威胁为计算机网络信息系统的进一步推广带来了一定的阻碍，网络安全防范体系的不足导致用户信息难以受到有效保障，可能会发生信息泄露、信息丢失等网络安全问题，严重影响工作效率。

我国的互联网开启新的发展模式，加强计算机网络安全防范措施，能够将大数据的作用更好、更有效地发挥出来，对于大数据的进一步发展也具有积极意义。作为一种信息化资源，大数据具有一定的共享性和普遍性特征，加强网络安全防范措施，同时也是对大数据信息资源的保护，能够有效保障这些信息数据的可靠性、完整性和保密性，进而提升数据信息资源的利用效率。而如果不重视网络安全防范的话，则这些数据信息会面临着泄露、丢失的风险，这也会一定程度上影响大数据的使用和发展。此外，大数据的经济潜力巨大，经由数据的采集——加工——分析等一系列流程后，能够帮助解决我们生活和工作中的诸多问题。然而一旦发生信息泄露，则会对数据采集工作产生严重影响，数据信息也将失去其实际效用。就此而言，在大数据的环境背景下，我们必须要正是计算机网络安全工作，深入探究当前的网络安全问题，并据此不断优化网络安全防范措施，进一步提升大数据背景下网络中信息数据的安全性。

二、大数据背景下计算机网络安全存在的问题

（一）安全管理体系构建不完善

安全管理体系是网络安全的基本保障，能够为网络安全防范工作提供可靠依据和统筹方案。但在实际的网络安全管理中，安全管理体系的构建仍不够完善，国家法律法规对于网络安全方面的相关规定仍比较笼统，不够详细，缺乏用户网络安全保护和个人信息安全保护等方面的系统化法规制定，导致计算机网络安全管理体系的构建缺乏政策支持，难以发挥指导作用。

（二）数据安全管理不够规范化

目前来看，网络数据的安全管理还不够规范化，在网络安全技术专业审核方面的力度还不够，不重视专业培训和考核的开展，导致相关技术人员在实际操作中缺乏规范意识，网络安全维护工作落实不到位。

（三）网络安全防护工具更新速度慢

近些年，随着网络技术的不断进步，黑客制作的网络病毒也越来越多样化，这些病毒依附于各类网站链接之上，传播速度非常迅速，且危害性极大，一旦计算机被网络病毒感染，就很容易被入侵数据库，造成大量数据的泄露和丢失，损失巨大。但是就我国网络安全防护工具的发展现状来看，其更新速度较慢，通常等到病毒已经大面积危害用户网络安全后才进行针对性的更新处理，远远落后于网络病毒的更新水平，进而导致用户的网络信息安全和经济安全难以得到有效保障。

（四）计算机网络安全管理人员基本素养有待提升

计算机网络安全管理人员是落实网络安全措施的主体，其职业素养的不足会对实际的网络安全管理工作造成直接影响。但目前来看，很多网络安全管理人员的专业技术水平偏低，在工作中并未意识到自身工作的重要性，导致遇到突发安全事件时应对能力不足。此外，因为自身素养的不足，其对于用户的号召力度也不够，无法为用户提供专业的网络安全防范指导和推广，导致网络安全管理工作难以高效展开。

三、大数据背景下计算机网络安全防范措施

（一）加快安全管理体系的构建与完善

针对当前网络安全管理体系不健全的现状，急需从法律层面加强网络安全相关法律法规的制定，整合零散的网络安全防范措施和指导性建议，促进网络安全管理体系的科学完善和合理构建。现阶段，我国计算机安全管理体系的构建在法律层面还存在很多漏洞，导致许多不法分子利用法律空隙盗取私密资料，威胁网络安全。对此，应该加大网络安全方面的立法力

度，促进安全管理体系的完善。首先，应该由相关责任部门结合大数据背景下的计算机网络安全实际问题以及目前已有法律法规，进一步制定详细化安全管理体系构建方案，保证网络安全管理工作科学、高效地展开。在进行网络安全管理过程中，相关人员需要充分考虑广大计算机网络用户的使用需求，根据用户群体的实际网络安全问题及管理情况制定相应的管理体系，比如根据用户信息泄露问题严重，就可以制定相应的身份验证制度、信息存储制度等，强调用户的信息安全以及私密资料的数据管理，使广大用户正视网络安全风险及其危害，强化其安全管理意识，并逐步构建“法律指导+实践运行”的安全管理体系。

（二）推进数据安全管理的规范化

强化计算机网络安全管理，就需要不断推进数据安全管理的规范化，以提升计算机网络安全管理工作效率。首先，需要将各方可利用的资源进行充分调动，进一步提升网络安全技术专业审核力度。可以通过专业的培训机构展开网络安全技术专业培训，并对相关人员的技术水平进行专业考核，构建规范化的专业网络安全管理部门，推进安全管理工作的规范化发展。其次，应该积极转变传统的安全管理机制和管理形式，优化网络安全管理方法，对网络应用中可能存在的安全隐患进行及时排查，并遏制安全问题的发展，保障网络的安全性。此外，要注重网络安全管理结构的规范化调整。依托大数据背景下我国互联网的实际运行情况，针对性设定多项管理方案和方法，并保证能够根据网络安全的现实问题提出具有针对性且详细的解决方案，进而实现网络安全管理水平的有效提升。

（三）增强数据存储的安全性

数据存储是计算机网络系统的重要功能之一，但是在当前的大数据背景下仍面临着很多的存储安全问题。为了保障网络数据存储的安全性，首先，相关网络安全管理部门应该加快引进现代化技术，借助先进技术进行网络数据备份、网络监控、风险预警等。比如可以利用硬盘、云空间等加强数据备份的安全性。同时，还要强调技术推广工作，通过多元化的宣传教育，让更多的用户了解并掌握这些先进技术，保证这些技术能够在广大用户间实现高度普及，并能够将技术用于日常生活和工作中。其次，应积极鼓励计算机网络用户优化自身学习观念和网络安全管理理念，积极配合网络管理部门展开学习，完善自身对于网络安全存储技术和相关知识的认识，学会选择合适的技术工具进行数据存储。如果发生存储数据被盗取或被攻击的情况，用户应该积极上报，并及时借助现代化技术进行自主数据保护，避免数据无法挽回的情况发生。

（四）推动安全防护工具的更新

就当前我国的信息安全技术发展水平来看，其在技术的研发、引进和推广方面始终处于落后状态，导致大量的病毒入侵网络，严重影响了网络环境的稳定性。对此，必须要加快安全技术的研发和引进，不断推动安全防护工具的更新，并进一步强化技术工具的推广，解决当前网络病毒泛滥的问题，提升网络信息的安全性。首先，相关技术公司应加快安全防护工具的研发，通过引进先进的安全防护技术，结合我国的实际网络环境和病毒水平，及时更新防护工具，针对性解决目前所存在的网络问题。比如，可以加快设计研发病毒查杀软件，并及时更新病毒库和技术库，保证在用户使用网络的过程中，能够及时发现病毒风险，并阻止病毒的入侵，保护应用的信息安全和经济安全。其次，相关互联网公司要加快构建专业的技术人员队伍，深入探究病毒预警技术和截取工具的研发，一旦发现不明原因的侵入，截取工具将迅速反应，抑制病毒的传播感染速度和范围；预警系统则及时发出预警，并将病毒相关信息实时传输到技术管理部门中，由管理部门制定针对性的解决方案，实现网络安全的全面防护。

（五）重视计算机漏洞的及时修复

在当前的大数据背景下，要保障网络安全，还需要及时修复计算机所存漏洞，防治病毒、黑客利用漏洞侵入计算机盗取信息。首先，对用户来说，其可以在计算机上安装相应的修复软件，借助软件进行漏洞的科学查找和修复。在这一过程中，用户需要了解修复软件的具体工作原理和工作流程，并合理利用软件进行漏洞的修补，避免遗漏。此外，开发商还应该进一步加强相关修复软件的研发，保证修复技术与当前的网络发展和网络安全需求相适应，并及时更新修复软件的技术，进一步扩大修复软件的普及性。此外，还有不断增强计算机网络系统补丁技术，针对计算机的漏洞进行有效修复。

（六）提升网络安全管理人员的基本素养

目前，我国网络安全管理人员的整体素养不足，技术水平难以应对大数据背景下的诸多网络安全问题，且难以对广大用户形成有效引导。就此而言，需要网络安全管理部门找那个是相关管理人员的素质培养，不断优化部门整体的安全管理水平，提升管理成效。首先，网络安全管理部门应该定期安排线上、线下的先进技术培训和实践锻炼机会，鼓励相关管理人员积极参与培训活动和实践活动，学习先进的安全管理技术的理念，不断拓展自身的网络安全视野，正确认识自身工作的重要性，提升自身的技术能力，优化职业素养，使其能够更好地应对突发网络安全事件。其次，可以设立网络安全培训课程，并通过多渠道推广课程，吸引广发计算机网络用户参与课程学习，课程内容应包括常用的网络安全知识以及防范办法，帮助用户树立网络安全意识，并掌握基础的安全防范技术和手段，进而提升计算机网络系统运行的安全性和可靠性。

四、结语

总而言之，在当前的大数据环境下，网络信息数据迅猛增长，网络技术和计算机技术在迎来新发展的同时，也面临着越来越多元化的网络安全问题，对我们的信息安全和经济安全造成了严重威胁。对此，网络安全管理人员和计算机网络用户必须要重视网络安全防范，通过加快安全管理体系的构建与完善、推进数据安全管理的规范化、增强数据存储的安全性、推动安全防护工具的更新、重视计算机漏洞的及时修复、提升网络安全管理人员的基本素养等手段，不断提升计算机网络安全管理水平，强化防范措施，有效规避网络风险问题，优化网络安全环境，保障计算机网络系统的稳定运行。

参考文献：

[1]袁一帆.探讨如何实现大数据时代的计算机网络信息安全[J].网络安全技术与应用,2021（12）:174-175.

[2]石书红.大数据背景下计算机网络信息安全管理及防范措施[J].普洱学院学报,2020,36（06）:15-17.

[3]徐大海.大数据时代背景下计算机网络安全防范应用与运行分析[J].计算机产品与流通,2020（06）:33-34.

[4]冉小青.分析计算机网络安全面临的威胁及其防范措施[J].计算机产品与流通,2020（05）:59.

[5]洪家幸.大数据背景下计算机网络安全问题与防范措施分析[J].数码世界,2019（10）:236.