大数据视域下计算机网络安全防范研究

罗　银
（天府新区信息职业学院，四川 眉山 620564）

摘要：随着信息技术的飞速发展，现今，在社会中的各个领域中，大数据技术都已经被运用其中，并且发挥中愈加明显的作用，扮演中越来越重要的角色。大数据技术具有非常显著的特点，它的功能性、开放性以及渗透性都非常的强大，为了能够使计算机网络安全防范工作能够与大数据技术更好地进行配合工作，必须要采取一些至关重要的方式来加以升级和优化。本文重点分析了在大数据视域下计算机网络安全防范的现状，并且在此基础上注重分析了大数据视域下计算机网络安全防范中存在的问题，最后就如何加强在大数据视域下计算机网络安全防范的有效路径进行分析，希望为广大朋友提供一些有价值的参考和借鉴。

关键词：大数据视域下；计算机；网络安全

随着信息技术的高速发展，大数据技术已经融入人们生活中的各个领域之中，并且在教育、经济、建设方面都取得了显著的成效，可以说大数据技术对于人们生活发展具有显著的促进作用。但是它在帮助人们提升工作效率，加快企业发展的同时，也存在一些问题，比如说安全问题，随着不法分子的利用此漏洞，导致信息数据丢失、隐私信息泄露等问题时有发生。这也就要求我们在大数据视域下，必需要加强网络安全防范工作。因此，如何提升网络安全防范能力已经成为社会普遍关注的问题之一。在大数据视域下，整体的计算机网络安全防范的情况有所进步，很多单位以及相关企业对于网络安全防范措施非常重视，不断地对计算机网络防范机制进行升级和优化，使得现今网络安全防范的水平有了极大的极大的改观，但是，随着信息技术的发展，网络安全防范依旧存在一些问题需要解决，若企业以及相关的单位对此并不重视，就可能会造成更加重大的经济损失。因此，在大数据视域下，必须要采取积极有效的态度去应对网络安全防范问题，构建一个健康、稳定以及安全的网络环境，为人们的生活交流以及社会经济的良好发展铺好安全基调。

一、大数据视域下计算机网络安全防范的现状

在大数据视域下，从整体上来看，网络安全防范随着科学技术的不断创新和发展，计算机网络安全防范整体的防范水平也在随之升高，并且在此过程中，也逐渐形成相对比较完善的计算机网络安全防范体制，不管是政府单位，还是各个行业，计算机网络安全防范的体制在不断地进行优化，这使得计算机网络安全防范工作也正在朝着好的方向发展。

现今，在大数据视域下，计算机网络安全防范现状主要表现在：

随着我国经济实力的不断发展，人们生活水平逐渐提升，群众素质也在逐渐提升，使得人们愈加重视网络安全防范工作。很多单位以及相关的公司已经建立了专门的机构，旨在强化对本企业或者本单位的网络安全防范体系，并且专门投入一定资金，配发了先进的计算机网络安全防范设备，使得计算机网络安全防范水平水涨船高。但是依旧存在一部分企业，对于网络安全防范工作并不重视，网络安全防范意识并不强，片面地认为自己所处的环境是安全的。

此外，在计算机网络安全防范工作中，具体的网络防范方式多种多样，非常地多元化，其中，最为重要的就是大数据技术所带有的开放性特点，如何针对黑客以及网络病毒的攻击进行有效的防范已经成为当前重点研究问题。截至如今，各种计算机技术层出不穷，安全软件、APP 等目不暇接，比如说鲁大师、360 安全卫士等软件，这些功能强大的防范软件被广泛地运用，可以有效地针对网络安全问题进行防范，能够高效地阻止黑客以及一些木马病毒的入侵。除此之外，还有其他的网络安全防范软件，这使得计算机网络安全防范的手段更加的丰富，有力地阻止网络安全问题的蔓延。随着网络安全防范工作的逐渐加深，防范效果逐渐获得强化，可以将一些人工智能技术运用在网络安全防范领域之中，并且已经取得了不错的效果。经过一些科研团队的研究和发展，可以将智能防火墙技术、入侵检测及时以及专家系统等技术运用在计算机安全防范之中，使得它的融合性、综合性以及互动性更为强化。由于将人工智能以系统应用在计算机网络安全防范之中，极大地提升防范能力，但是同时，在将人工智能运用在计算机网络安全防范中也同样存在一些问题，比如说它的运用和操作并没有形成一套体系。

二、大数据视域下计算机网络安全防范存在中的问题

（一）计算机网络安全意识相对比较薄弱

在大数据视域下，经过调查发现，现今，比较突出的问题就是计算机网络安全防范的意识相对比较薄弱，很多个人以及单位对于计算机网络安全问题可以能带来的影响并不关心，他们对此并没有一个深刻的认识，因此，在生活、工作以及学习过程中，并没有养成良好的计算机网络安全防范意识和习惯，可能会导致计算机网络安全防范工作无法提升实效。另外，还有一部分单位，它们只是停留在口头上，并没有付诸行动，认识到计算机网络安全防范的重要性，但是它们的行动力不足以支撑构建防范体系，致他们对自身的一些重要数据、商业信息以及商业资源的保护等问题并不重视，导致出现了很多严重问题，对自身企业以及单位造成重大的经济损失。对计算机网络防范工作不重视，还表现在对系统漏洞、计算机网络漏洞的忽视，比如说使用一些盗版的计算机技术，在网络防范层面投入较少，这些行为必然会导致计算机安全防范工作受到阻滞，非常容易被黑客以及网络病毒所攻击，造成不必要的损失。

（二）计算机网络安全防范机制不够完善

随着大数据技术的发展，它已经完全融入到计算机网络领域之中，并且它的数据收集和数据分析能力十分的出众，只有具备完善的计算机网络安全防范机制和措施，才能够使计算机网络领域更加的顺畅，提升企业的综合效率。从整体网络安全防范的运行情况来看，很多企业以及单位存在严重的计算机网络安全防范问题，它们并没有建立强大的、坚固的计算机网络安全防范制度和体系，这导致它们非常容易受到网络病毒以及黑客的攻击。计

算机网络安全防范机制不够完善，导致出现这一情况的另一原因是在使用计算机的过程中，并没有科学化以及规范化的使用，技能掌握也并不全面，对于计算机网络的使用规则和使用方式没有正确的认识，在大部分时候，很多计算机安全问题都是由于人为操作不当导致的，这才使一些犯罪分子得手。在数据时代，精通计算机技术的黑客非法盗取信息将更为简易，若人们并没有构建坚固的网络防范机制，这会给犯罪分子造成可乘之机。

（三）网络安全防范技术陈旧

在大数据视域下，各种信息技术更新换代非常的快速，对于网络安全防范工作来说，在构建和完善网络安全防范机制的同时，还要运用先进的防范技术，只有在技术层面不断地与时俱进，才能更好地做出网络安全防范，并且取得有效的成果。但是，经过调查，部分公司以及相关的单位并没有及时地将自身的网络安全防范体系进行升级和优化，没有做到与时俱进，在技术投入和资金投入方面并没有做到位，很多公司的网络防范技术比较陈旧，同时它们也并不重视网络防火墙的设置，并且在数据存储、计算机防范工作方面结合得不够紧密，存在极大的网络安全隐患。

（四）网络安全防范工作缺少创新

随着信息技术的发展，尤其是大数据技术的不断进步，这更加剧了网络安全防范工作的创新，只有不断地对网络防范进行创新和优化，才能在现今大数据视域下取得良好的网络防范成效。但是很多企业以及机构对于修复网络漏洞工作不予以足够的重视，相关的网络安全防范软件的实效性还有待提升。

三、大数据视域下计算机网络安全防范的有效路径分析

（一）提升计算机网络安全意识

在大数据视域下，为了更好地开展和推动网络安全防范工作的顺利进行，首要的工作就是提升全体的网络安全防范意识，只有这样，才能在网络安全防范工作中实现突破。在实施过程中，不管是个体，还是单位，大数据技术对于计算机网络安全防范的影响都要深刻地意识到，并且可以采取一些必要的方式对其进行优化和升级。要科学设计和系统安排计算机网络安全防范工作，并且对信息风险、数据风险、网络风险等进行重点的防范和控制，着重推动计算机网络防范工作的优化和升级。

例如，为了更加有效地防止网络黑客来盗取相关信息，应该要加强网络防火墙的构建和完善工作，可以通过提升防火墙的防御力，来确保网络环境的安全。同时为了更加有效地防止网络病毒对计算机的上海，必须要对相关的杀毒软件以及防火墙软件进行及时的更换和优化，通过不断地更新病毒库，升级防范软件，才能使计算机网络环境更加的安全，从而获取更好地网络防范实效。对于一家企业来说，必须要重视网络安全防范工作，帮助员工树立网络安全防范意识，并且对他们进行针对性的培训和教育，使他们形成网络安全意识和数据安全意识，在使用计算机的过程中，要做好防范工作，防患于未然。

（二）完善计算机网络安全防范机制

大数据技术具有很多的优势和特点，其中它的开放性功能比较显著，为了更有效地对计算机网络进行控制和防范，必须要加大力度完善计算机网络安全防范机制，通过使网络安全管理工作得到进一步的强化，从而使网络安全防范工作的效能获得最大限度地提升，对于那些比较频繁使用计算机或者网络规模较大的企业来说，更应该要完善计算机网络安全防范机制，同时，充分发挥出防范制度的稳定性、长期性以及规范性作用，使它的防范体系制度更加的完善和健全，同时形成计算机网络安全防范合力。

例如，在防范网络黑客的过程中，为了取得更好的防范实效，切断网络黑客的侵入渠道不是最为主要的，可以通过使用内外网隔离的方式，来有效地防止网络黑客的侵害，提升网络安全性。此外，在构建安全防范机制时，除了要构建和完善相关的防范制度之外，还要加大对计算机网络安全防范工作的投入，并且使各个部门之间共同构建协同防范体系，使防范体系的作用发挥最大的作用。

（三）优化计算机防范技术

在当前大数据视域下，对计算机网络安全防范工作来说，优化和创新是非常重要的，因此，必须要对计算机网络安全防范技术层面进行及时的升级和创新，提升它的实效性，并且在防范方面具有针对性。在实施的过程中，必须要防范技术进行深度的研究，比如说提升网络信息资源利用效率的算法就有 RSA 加密算法、聚类算法等，将网络防范的机密性和安全性作为重点，同时还要对专家系统、智能防火墙技术、垃圾网络安全防御、神经网络系统等人工智能技术进行实践和探索，同时还要根据网络安全防范的具体情况，加强相关的融合性建设，通过将多种技术进行有效融合，将计算机网络中的不安全、不稳定的因素进行最大程度的防范和限制。

四、结语

综上，由于大数据技术具有非常多的特点，比如说互动性、融合性以及开放性等特点，随着它的发展和进步，导致计算机技术也伴随着这些特点而产生，这也对计算机防范工作具有重要的作用。因此，在大数据视域下，如何进行加强和优化计算机网络安全防范工作，已经是社会中各个行业必须要面对和重视的问题，否则，一旦出现网络信息泄露等问题，那么对于相关企业、单位甚至国家都会造成严重的伤害和巨大的经济损失。因此，我们必须意识到网络安全防范工作的重要性，同时要树立起强大的计算机网络安全防范意识，要坚持问题导向，运用创新的思维和观念，通过提升计算机网络安全意识、完善计算机网络安全防范机制以及优化计算机防范技术等多种方式，推动计算机网络安全防范工作的开展，打造一个安全性高的网络环境，从而为人们的网络信息交流以及社会经济的良好发展打下坚实基础。

参考文献：

[1] 郑州 . 大数据背景下计算机网络安全风险与防范研究 [J]. 无线互联科技，2021，18（24）：19-20.

[2] 陈洪超 . 大数据背景下计算机网络安全防范策略研究 [J]. 机械设计，2021，38（12）：160.

[3] 熊永亮 . 大数据环境下计算机网络安全防范研究 [J]. 电脑知识与技术，2021，17（34）：46-47+50.

[4] 王丽华 . 大数据背景下计算机网络安全问题与防范措施研究 [J]. 软件，2021，42（11）：134-136.

[5] 齐红 . 大数据时代下计算机网络安全防范的研究 [J]. 中小企业管理与科技（上旬刊），2021（10）：104-106.

[6] 傅望 . 大数据背景下计算机网络安全防范措施探析 [J]. 网络安全技术与应用，2021（06）：153-154.