计算机网络安全问题及对策分析

陈国栋
广东科贸职业学院　广东　广州　510430

摘　要：现今，随着互联网技术迅猛发展，虽然人们的信息交互效率和质量得到了显著的提升，但其中存在的各类型风险问题却更为显著。因此，如何控制计算机网络运行过程中的风险问题，提升计算机网络运行过程中的安全管理效率，成为推动我国计算机网络行业安全发展的切入点。基于此，文章从计算机网络安全的内容出发，对计算机网络面临的安全问题进行分析，并且基于现代科学技术，对未来计算机网络安全的防范对策进行探讨，以期为提高计算机网络安全管理质量提供参考。

关键词：计算机网络；安全管理问题；防范对策

1 计算机网络安全的主要内容

计算机网络安全是指通过采取必要措施，保护网络系统的硬件、软件及其系统中的数据不受未经授权的破坏、更改或泄露，确保系统连续可靠正常地运行，网络服务不中断。其涉及多个方面，包括网络设备的安全配置、访问控制、加密通信、身份验证、防火墙、入侵检测和防御等技术和措施。其目标是保护网络和其上的信息资源，确保网络的正常运行和数据的安全性，旨在确保网络的保密性、完整性和可用性，以防止未经授权的访问、恶意软件、数据泄露、网络攻击和其他安全威胁对网络和其相关资源的损害。以下是计算机网络安全的主要内容：

1.1 安全

计算机网络相对于传统的数据传输模式而言，文件传输速率更快，且在计算机网络安全的前提下有着更高的效率。但是，由于数据和文件的传输完全依赖于计算机互联网，常常受到计算机网络安全的影响和威胁，传输文件越多，受到威胁的概率也就越大。所以，只有不断完善计算机网络安全技术，才能保障传输文件的安全性。因此，要不断提高和完善计算机网络安全技术，以保障工作文件和工作数据的安全性，避免相关资料的泄露[1]。

1.2 完整

由于计算机网络在文件和数据传输过程中，是以虚拟代码形式为传输载体的，代码自身具有不确定性和不稳定性，因此容易在传输过程中出现缺失。这就要求计算机网络具备完整保留文件的功能。不完整的文件和数据将无法被修复，这也会对计算机使用人员或企业带来一定的损失。所以，在引进计算机网络安全技术时，需要保障文件和数据在传输过程中的完整性，减少文件和数据受到攻击和威胁。

1.3 保密

计算机网络在运行期间，互联网作为计算机网络工作的主要载体，具有开放性和分享性，由此，计算机在网络工作中可能会出现数据共享的情况。这也要求计算机网络安全技术能够为计算机用户提供保密性服务。计算机网络安全技术可以对上传到计算机网络上的数据、文件、图片等信息材料进行加密，帮助使用人员在计算机网络运行期间获得更佳的保密体验。提高计算机网络安全技术的保密性能，保护个人的隐私和信息，避免信息泄露和被窃取的现象发生

2 计算机网络安全防护的重要价值

网络安全问题所涉及的领域相对较多，关系到的综合性学科也较为复杂，其中，不仅涉及到了计算机网络科学，同时也与通信技术、密码传输技术、信息安全防范技术以及应用数学技术等多种技术之间具有密不可分的关系。简而言之，计算机网络安全的防护工作是一门相对综合性的学科和系统性的工程。网络安全工作主要是指网络系统的硬件以及软件设备和系统中所存储以及交互的相关数据信息能够得到有效的保护，并不会因偶然的系统运作故障或恶意攻击等原因而出现信息更改、信息泄露、信息破坏等问题，确保计算机平台能够连续并安全正常地运行，保障网络服务不中断。

计算机网络安全防护的重要性主要体现在以下几个方面：（1）保护个人隐私：网络安全可以防止个人信息被窃取或滥用，避免个人隐私的泄露。（2）维护企业利益：保护企业数据免受泄露、网络攻击和其他安全威胁，避免经济损失和声誉损害。（3）国家安全保障：网络安全对于保护国家基础设施，如电力网络、水供应系统、电信网络等至关重要，攻击这些基础设施可能会导致重大灾难。）（4）知识产权保护：网络安全能够

防止未经授权的抄袭或转载，以及其它侵犯知识产权的行为，这对于保护企业和个人的知识产权都非常重要。（5）维护网络连通性和正常：保护网络系统的正常运行，确保网络服务的连通性和稳定性。因此，计算机网络安全防护对于个人、企业和国家都具有重要的价值。

3 计算机网络安全存在的问题

3.1 信息内容交互中存在安全隐患

随着计算机和互联网的融合，信息的传播方式越来越便捷，人们对电脑的存储能力也有了更高的要求[2]。因许多数据和信息都需要进行交流，不可避免会下载和安装一些应用软件，而某些病毒和恶意软件就可以通过这些操作来侵害用户的电脑，这给电脑带来了一定的安全隐患。随着电子商务的日益普及，许多企业和软件利用人们不愿意付费的心理，以免费下载的名义或者刻意在信息共享较多的平台植入链接等方式来推广自己的产品，更有甚者，为达到目的，设计一些恶意程序捆绑下载，给用户的计算机带来安全隐患。随着移动支付的普及，企业和个人的隐私信息受到了严重的威胁，一旦被盗取或泄露，将会带来巨大的损失。

3.2 计算机使用者的安全意识薄弱

计算机用户作为计算机网络安全的应用主体和调控对象，其综合素质对计算机网络安全性能存在巨大影响。如果计算机用户在使用期间不遵守安全规范，比如解除安全保护措施、未能按照规定增强系统访问的安全性，导致计算机在运行期间发生病毒侵害或者出现安全漏洞，有时还会出现不法分子侵入计算机网络安全并窃取计算机网络中的文件数据等现象，这些都不利于保障计算机安全系统的有效建立，有碍于高质量的信息存储和传递。

3.3 黑客攻击的现象增多

由于计算机网络本身就存在系统漏洞，加之用户安全意识薄弱，下载不知名的软件或者点击不安全的网页，这些都有可能对计算机网络的安全带来巨大的威胁，也给专业的黑客带来了攻击计算机的机会。互联网黑客善于利用黑客技术，远程强行进行监控、侵入、干扰、破坏计算机系统，造成计算机系统瘫痪。计算机网络容易成为黑客攻击的目标，且黑客通常是通过木马病毒或者系统病毒攻击破坏计算机网络[3]。黑客都是通过木马或者攻击性病毒，以链接或者软件的形式诱导计算机使用者点击和下载，从而侵入计算机网络实施非法攻击行为。

3.4 相关部门的监管力度有待提高

计算机网络安全是一个非常重要的领域，需要得到相关部门的监管和保护。然而，在现实中，一些部门可能存在监管力度不够、监管不力等问题，这可能会对计算机网络安全造成威胁。因此，提高相关部门的监管力度是非常重要的。为了提高监管力度，可以采取以下措施：（1）加强法律法规的制定和执行。制定更加严格的法律法规，明确监管责任和义务，加大处罚力度，确保监管的有效性和权威性。（2）加强监管队伍建设。建立一支高素质、专业化的监管队伍，提高监管人员的素质和能力，确保监管工作的有效开展。（3）加强社会监督。鼓励社会各界积极参与，对违反法律法规的行为进行举报和投诉，形成全社会共同关注计算机网络安全问题的良好氛围。总之，提高计算机网络安全领域的监管力度是维护网络安全、保障国家安全的重要措施。只有加强监管力度，才能确保计算机网络安全工作的有效开展，保护国家和人民的利益。

4 计算机网络安全防范策略

4.1 创建良好自然环境

近年来，计算机网络逐渐占据人们日常生活的大半部分，对衣食住行都有影响，越来越多的个人信息被计算机网络平台中心所储存，虽然可以有效保障各类信息数据使用的高效性和精准性，但为了保障用户以及相关企业可以在使用数据信息时具有完整性和安全性，企业和个人都应为计算机网络运行系统营造良好的应用环境。首先，要落实相应防雷电、防水患、防火的应对举措，可以根据实际情况对相关仪器设施进行有效安置，防止计算机网络所使用的相关仪器设备受自然环境所影响[4]。其次，要对计算机网络在应用中所产生的信息数据做好及时保存和备份，以便保障信息数据的完整性。最后，使用计算机的人员也要对周围环境卫生进行有效保护，从根本上降低计算机运行区域受到外界环境因素影响的概率，为计算机网络正常使用，营造良好的应用环境，保证计算机网络得以顺利、安全、科学地进行使用。

4.2 合理应用防火墙技术

防火墙技术作为计算机网络安全技术中的基本技术之一，其负责监控和管理计算机网络的访问记录，是维护计算机网络安全的重要技术手段，对计算机网络安全的维护起着至关重要的作用。在计算机网络运行过中，及时阻止和处理不法分子和安全隐患的访问，并发出相应的警报，以此保障计算机网络安全。另外，根据计算机网络安全的使用等级，不断提升防火墙的规格和级别，以提高计算机安全防护能力。防火墙主要用于互联网接触的计算机网络，其作用是过滤和筛选不合规的IP地址，并拦截部分违反计算机工作规则的数据包。为了确

保计算机在工作中通过的数据流符合计算机网络的工作要求，需加装内、外部网络的计算机网络安全防火墙。因此，与其他的网络安全技术手段相比，计算机网络防火墙具有更强的基础效应。此外，防火墙还能优化计算机网络安全设计，并记录系统在工作中的各种行为。

4.3 加强法律法规对相关行为的约束

由于计算机网络在近年来发展的速度较为迅猛，我国没有及时出台相应完善的法律法规对计算机网络安全行为进行严格制止和约束，造成计算机网络技术在应用中出现用户信息泄露问题，无法保证计算机网络应用安全性。为有效杜绝这一问题，我国相关政府部门要对计算机网络使用进行有效研究，并根据实际情况出台较为严格的法律法规，对计算机网络应用行为进行有效约束，从根本上确保了计算机网络运行的安全性和有效性。并创建完善的监督管理制度，对信息技术在实际应用中所产生的信息泄漏、黑客攻击、病毒入侵等影响计算机网络安全运行的问题进行严格管制和惩罚，以便保证计算机网络发展环境的安全性。

4.4 提高用户安全意识

制定并加强相关法律法规虽然可以对信息网络安全维护起到一定作用，但实际效果远远不够，要想从根本上保障信息网络使用的安全性，需要计算机用户自身安全意识得以具备。计算机用户具备基本的、良好的安全意识可以有效降低网络问题发生次数。因此，要对用户的安全意识进行培养和提高，确保计算机用户可以对生活常识进行把握，对网络上可能出现的诈骗情况进行有效察觉和警惕，对可能出现的违规操作进行杜绝。譬如，一些诈骗人员会充当银行员工对用户进行信息查询，如果计算机用户知道银行不会自主与用户进行沟通，并对用户的个人信息或验证码、付款码等进行收集，就不会在实际应用中受到诈骗。因此。相关人员要定期对计算机用户开展网络安全培训活动，以便计算机网络用户可以提高自身安全意识，从根本上杜绝网络安全问题发生。

4.5 强化系统维护管理技术

网络维护管理策略需要根据网络安全需求的不同做出相应的调整。于个人而言，可通过加密技术、加装杀毒工具等方式提高网络系统安全性。对于网络安全要求较高的单位，还需从网络系统建设上加强网络安全维护。首先，要提高管理人员对网络安全维护的重视程度，对计算机网络安全系统运行情况加以评估，进行定期精细化的维护管理，以保障当网络系统出现安全问题时，可第一时间采取措施进行处置，有效消除安全隐患；并且针对当前网络威胁的性质要充分明晰，了解其作用机制，制定科学有效的处理决策，及时更新网络安全系统，提高网络系统性能，避免网络安全问题的威胁损害；最后，不断培养网络安全维护人才，提高维护管理技术水平[5]。

4.6 加强网络信息安全的监管

虽然政府部门已加强对网络信息安全的监管，但随着网络技术的快速发展，虚拟空间依然为犯罪分子提供了可乘之机。因此，政府部门应采取更严格的措施来确保网络传输的安全性，以降低计算机使用者在信息交流过程中风险。同时，政府应制定严格处罚标准，严厉打击网络信息违法犯罪行为，并加强宣传，以减少这类犯罪行为的发生。

结束语

随着互联网信息技术的发展与应用，计算机网络在校内人员日常学习工作中发挥着重要作用。计算机网络具有双面性，一方面，计算机网络为人们的生活和生产提供了便利；另一方面，也对信息安全带来威胁。所以，在计算机技术不断发展和普及使用的今天，用户应加大对计算机网络安全的重视程度，加强计算机网络安全意识，积极利用计算机网络安全技术，做好网络安全维护，进而保障系统的完整性、安全性和稳定性，营造优良的网络环境和营商环境，提高计算机在工作与日常生活中的应用质量，助力经济和社会的发展。

结束语

[1]刘成.计算机网络安全技术在网络安全维护中的应用分析[J].网络安全技术与应用，2022(4):169-170.

[2]梁丰.计算机网络安全存在的问题及防范策略[J].计算机产品与流通，2020（7）：54-55.

[3]徐晨.计算机网络安全技术在网络安全维护中的应用分析[J].中国管理信息化，2022,25(8):189-191.

[4]夏文英.探究计算机网络安全技术在网络安全维护中的应用[J].数字技术与应用，2021,39(7):175-177.

[5]张良.试谈大数据时代的计算机网络安全及防范措施[J].信息通信，2020(7)：138-139.