完善网络电子信息安全性的主要途径

梁　群

（单县财政局，山东 单县 274300）

摘　要　现阶段，我国网络信息技术迅猛发展，新一代互联网框架及技术进入快速变革发展阶段。电子信息技术依托于网络信息技术的快速发展，发展速度也进一步加快。随着技术发展，网络电子信息安全问题也越来越严峻，成为制约技术稳定发展的重要因素。因此，加强网络电子信息安全性是非常必要的。本文通过对电子信息技术进行概述，分析了在电子信息技术应用中面临的网络安全问题，从而提出了完善网络电子信息安全性的主要途径，为有效解决网络电子信息安全问题提供参考。

关键词　电子信息技术　网络安全　杀毒软件

中图分类号：TP393.08　　**文献标识码**：A　　**文章编号**：1007-0745(2022)08-0026-03

随着网络信息技术时代的到来，计算机网络技术呈现出快速发展的势头，作为以该技术为支持的电子信息技术也获得了快速发展。然而，近年来，受各类外界因素以及技术本身的因素影响，网络电子信息在实际运行中存在较为显著的安全隐患问题，一旦发生信息泄露，就可能造成相关人员的人身安全损害及财产损失，对社会稳定及国家安全都具有不良影响[1]。因此，加强完善网络电子信息安全是非常重要的。在强化网络安全中，电子信息技术的合理应用对于提高网络安全水准，保障网络信息系统安全发挥着重要作用。相关技术人员需要加强对电子信息技术的关注与认知，科学分析其存在的安全隐患，制定有效的应用途径，维护网络信息安全。

1 电子信息技术概述

电子信息技术就是负责进行数据收集、存储、处理的技术，在其技术应用中，一是能够通过信息技术实现在短时间内快速地进行信息收集和处理，从而使得信息传播的便捷度显著提升。与以往的信息传播模式相比较，对于电子信息技术的应用能够实现对信息处理规模与处理质量的大幅提升。二是在传统的人工信息处理过程中，通常难以完全保证对信息处理的准确性，信息处理受影响因素非常多。而通过运用电子信息技术，则可以有效避免人为因素等众多因素的影响，大幅提升信息处理的准确性。三是在应用电子信息技术进行信息处理中，通常会涉及种类繁多的信息类型，覆盖社会各行各业，而通过信息数据的广泛覆盖与收集，也能够为当前大数据技术的应用与分析提供可靠的依据。四是在网络信息技术快速发展过程中，电子信息技术的应用优势也越来越凸显，对于社会经济发展起到了非常关键的作用[2]。

正是由于电子信息技术自身存在的优势特征，其在网络环境下的应用也越来越受到人们的欢迎。在网络安全实际应用中，电子信息技术的应用范围非常广泛。具体包括：

第一，在设备研发领域的应用。在设备研发领域，电子信息技术的应用能够帮助研发人员更好地了解用户需求，从用户角度出发进行设备研发，以提高用户对产品的满意度。例如在工程系统升级中，通过研发设备为用户提供更丰富的感知体验，充分发挥了电子信息技术的积极作用。同时，运用电子信息技术还可以有效提高电子设备的质量，为设备的运行与应用提供了重要基础，促进了信息工程的稳定[3]。

第二，在信号传输领域。在信号传输过程中，广域网技术是电子信息技术应用的重要形式之一。广域网技术是当前互联网技术的重要组成部分，其应用为突破信息传输的局限性，扩大网络覆盖使用范围具有重要作用。在信号传输中，电子信息技术的应用有效突破了传统模式的限制，进一步拓宽了信息的传递空间与应用空间。例如在企业进行信息交互中，利用相关技术既可以为企业内部信息沟通共享提供可靠畅通的平台，同时还可以促进企业之间的相互沟通交流，打破信息交流的时空障碍，为企业发展发挥促进作用。尤其是在网络环境下，互联网技术的快速发展使得相关技术需求进一步提升，确保网络电子信息技术应用的安全性，对于社会稳定具有重要意义。

第三，信息共享领域。在当前信息已经实现了高

度共享的环境下，电子信息技术成为最具有发展前景的一项优势资源，如何加强技术应用，提高信息利用和信息共享成为其发展的重要方向[4]。就目前而言，电子信息技术在信息共享领域中：一是可以为网络安全管理提供可靠的信息内容安全保障，并且还能够借助大数据云服务器功能，实现信息的海量存储与备份，有效保障网络信息的安全性。二是为促进信息解读方法的多元化提供了可靠技术，网络信息技术的作用为信息传播打破了时空限制，从而实现信息的高效共享。

第四，安全维护领域。在当前网络环境下，人们对信息安全的关注度和需求进一步上升。在网络环境中，不法分子会通过对信息的窃取或对系统攻击获取信息，来谋求不正当经济效益，造成受害者的重要信息丢失或泄露，对信息传播与应用造成了非常不良的影响。加强电子信息技术的安全防护成为当前技术发展亟待解决的问题。合理利用电子信息技术，加强网络电子信息安全的防范与保护，是当前电子信息技术发展的重要内容。

2 网络电子信息技术常见的安全风险问题

2.1 电子信息技术的应用安全不规范

目前，现有的电子信息技术发展十分迅速，其技术优势也非常多，但在其实际应用过程中，也存在一些缺陷，影响了网络电子信息的安全性。在网络环境下，电子信息技术的应用为人们带来了极大的便利，但其也成为不法分子进行网络攻击的技术手段，来窃取信息、破坏信息技术系统等。这不仅对用户正常使用电子信息技术进行网络信息的传递产生了不利影响，更重要的是对用户的信息安全造成了严重的困扰和威胁。

2.2 系统运行方面存在安全问题

在互联网快速发展过程中，电子信息技术在各行业领域的应用已经基本实现了普遍覆盖，各类应用主体可以通过计算机来解决日常繁琐事务，有效提升了工作效率，推动社会生产力的快速提升。但同时，电子信息技术的应用也同时出现了一些网络安全隐患。在实际应用过程中，如果相关人员不能全面了解技术应用的安全隐患问题，一旦遇到技术故障就会无从下手，从而导致自己的电子信息安全系统变得非常脆弱，增加了被不法分子非法入侵、攻击的可能性与成功率。这种情况不仅可能会造成网络电子信息的泄露与丢失，同时还可能引发相关主体巨大的损失[5]。对于企业单位来说，一旦其内部电子信息遭到泄露或丢失，就可能引发巨大的经济损失。而对于个人来说，如果个人隐私信息遭到泄露，则可能陷入电信诈骗的泥沼，轻则经济损失，重则还有可能引发生命悲剧。因此，电子信息技术的应用中对系统运行的安全性保障十分重要，一旦发生电子信息泄露丢失等问题，就可能会引发严重社会问题。

2.3 相关技术人员的安全防护存在问题

在企业及各类机构对电子信息技术的应用中，大部分都存在一定的安全防护不到位的情况，出现这种问题的主要原因之一是相关技术人员在安全防护中存在一定的问题。一是由于网络电子信息安全防护的制度不健全，相关单位对电子信息技术应用管理的重视度不足，没有建立完善的信息安全防护管理制度，从而导致相关人员在信息采集、处理等过程中较为混乱，为不法分子入侵提供了机会。二是没有制定完善的应急解决措施，一旦发生突发性网络安全事故，相关技术人员不能立即根据实际情况做出反应，导致网络电子信息安全问题扩大化，不能及时控制并消除影响。三是相关技术人员缺乏高度网络安全维护意识，在其实际工作中，不能时刻将维护电子信息安全作为工作的首要前提，对电子信息安全进行维护与管理，从而使导致电子信息泄露的漏洞较多，技术安全性不足。

3 完善网络电子信息安全的主要途径

3.1 强化身份认证的准确性，确保个人信息安全

在电子信息技术的应用中，为充分保障网络下电子信息的安全性，不会被不法分子随意窃取，技术应用人员应当建立个人专属的信息安全防护体系，并加强对身份认证的重视，严格核实用户身份，促进真实用户与网络用户的紧密关联。一是采取短信验证码进行身份认证。当前，在身份认证中短信验证码认证方式应用非常广泛，用户需要根据自己的身份证办手机号，然后验证方通过向指定手机号中发送四位或六位数字的短信验证码，相关用户根据验证码数字输入指定地点，从而完成用户的身份认证[6]。这种认证方式效率与安全性都比较高，只要用户保护好验证码，就能够有效保障相关信息的安全性。二是采用身份识别卡进行验证。通过在识别卡中输入用户的相关信息数据，通过验证机器进行扫描后即可完成身份验证。这种身份验证的方式较为简单、快捷，但是风险性相对较高，如果用户发生识别卡丢失等问题，就可能被捡到卡片一方轻松盗取相关信息，并且要重新建立识别卡和找回丢失的信息数据存在一定的难度。三是设置密码。

通过在计算机中设置密码，可以由单一个体或者是特定群体掌握，只要在计算机中输入密码，就可以获取相应的电子信息。但如果密码被破解或者泄露，其他人就能够随意打开系统获取电子信息，并且当用户忘记密码时，还需要繁琐的过程才能找回密码，造成使用不便。

3.2 加强对信息加密及防火墙技术的应用

通过使用信息加密技术与防火墙技术，能够有效提高网络电子信息的安全保密性。在组织或个人应用电子信息技术中，为确保信息安全性，防止黑客入侵、信息泄露等问题出现，相关技术人员可以通过设置专门的防火墙或信息加密，有效防范并抵御攻击。一是防火墙能够有效对抗他人对电子信息系统的攻击，建立起一个非常强大的安全防护网络。这是一种有效的安全防护技术，通过在计算机系统中建立防火墙，能够有效抵御外来的对系统的不良攻击，避免计算机病毒入侵。同时一旦发现与身份认证不符合的入侵，就能够立即将其进行隔离，从而防止网络电子信息受到损失。二是加密技术的应用可以对隐私信息数据进行多层加密，以提高信息安全的防护能力。在进行电子信息传输过程中，通过对传输的各类型的文件信息进行多层加密处理，能够有效防止信息数据被盗取的可能性。这两种技术都可以有效阻挡信息安全风险，加强对网络电子信息的安全保障。通过重视加强对防火墙和信息加密技术的应用，充分发挥电子信息技术应用优势，保障网络电子信息的安全性。

3.3 重视应用杀毒软件，消除信息安全隐患

在网络环境下，除了通过应用防火墙和信息加密技术进行电子信息保护之外，还需要定期对网络病毒进行清理，从而有效降低网络电子信息安全风险。在网络设备使用过程中，长时间的浏览各类网页可能会在不知不觉中产生病毒，通过安装杀毒软件，定期进行病毒查杀，能够有效保证网络设备不被病毒污染，为黑客攻击留下机会。首先，技术人员可以进行网络访问权限的设置。通过在网络设备上设置网络访问权限，就可以对是否发生外界不良攻击对网络安全造成的破坏进行有效检查与避免，通过权限设置将对网络的恶意攻击阻挡在外，进而也就避免了网络电子信息被盗取和使用。其次，定期进行垃圾清理。在杀毒软件中，需要安装清理能力较强的清理软件，定期清理网络设备及系统中积累的垃圾和病毒，提高设备及系统本身对病毒的抵抗能力，避免不良垃圾过多对系统造成伤害，导致电子信息安全风险。

3.4 加强管理，提升技术人员安全防护意识

加强对网络电子信息的安全防护，还需要建立严格的管理机制，提高信息技术人员的安全防护意识，重视合理运用电子信息技术，加强网络安全维护，从而降低电子信息的安全风险。首先，加强网络电子信息安全技术培训。相关单位可以对内部技术人员进行专业培训，包括网络安全的重要性及相关知识、具体防御技术等，使其能够在工作中重视安全防护技术的应用，并且能够在发生信息安全风险时第一时间采取有效的防范措施，将可能造成的损失降到最低。其次，建立网络电子信息安全防范小组，通过组建专门的防范小组，针对网络电子信息安全问题进行处理，一旦发生较为严重的外来人员入侵，则可以及时应对，防止发生电子信息泄露或丢失等风险。最后，建立安全管理制度。相关管理人员要重视对网络电子信息的安全管理，建立健全的管理机制，制定完善的电子信息安全防控方案。

4 结语

总而言之，我国网络普及程度越来越高，电子信息技术在人们日常生活与工作中的应用越来越广泛，其对于人们的重要信息采集也更加全面，一旦发生信息安全风险，所可能造成的影响都是非常巨大的。因此，加强网络电子信息安全性的防护与保障十分重要。相关技术人员在推进电子信息技术发展的同时，也要重视电子信息技术应用中的信息安全问题，防范网络风险，最大限度避免网络电子信息丢失或泄露造成的损害。

参考文献：

[1] 姚懿宸 . 电子信息工程技术的应用与安全管理 [J]. 电子技术与软件工程 ,2020(23):238-239.
[2] 王瑀珩 . 电子信息技术在网络安全中的应用分析 [J]. 网络安全技术与应用 ,2020(10):154-156.
[3] 郭伟伟 , 吴文臣 , 隋亮 . 计算机网络技术在电子信息工程中的应用分析 [J]. 数字技术与应用 ,2020,38(07):75-77.
[4] 贾弘 . 关于电子信息工程技术的应用和安全管理分析 [J]. 科技风 ,2020(05):100.
[5] 林婕 . 信息工程中计算机网络技术的安全问题及应用 [J]. 数码世界 ,2019(12):268.
[6] 陈柯宇 , 徐锦亮 . 我国计算机电子信息工程技术的应用和安全 [J]. 计算机产品与流通 ,2019(04):18.