关于电子信息工程技术的应用与安全防护方案分析

唐 超

（河北大学物理科学与技术学院，河北 保定 071002）

摘 要 电子信息工程技术是新时代科技进步与革新背景下的产物，其中集成了多种技术，具有高速性、精准性的特征，当前在社会生产与人民日常生活中得到了广泛的应用。电子信息工程技术能够提高信息处理效率与精准度，在物联网技术、传感技术、信息集成技术等领域都具有极高的应用价值。但在大数据时代背景下，互联网中的任何信息与数据都有被窃取的可能，因此，电子信息工程技术领域要将安全防护作为现阶段主要研究方向，为企业与个人的信息安全提供保障。

关键词 电子信息工程；技术应用；安全防护

中图分类号：TP3 **文献标识码**：A **文章编号**：1007-0745(2023)07-0028-03

伴随着电子信息技术的持续发展与革新，当前已经在多个领域内得到了应用，并成为各个领域中不可替代的组成部分。同时电子信息工程技术也成为人们在日常生活中不可缺少的一项重要元素。计算机网络技术是电子信息工程技术的核心，在一定程度上，计算机技术的发展与进度，能够为电子信息工程技术的研发提供技术支撑。但也正是基于计算机与互联网技术，使电子信息工程技术存在着数据泄漏与窃取的风险。当前，电子信息工程的安全防护成为社会中探讨度很高的话题之一，为保障企业与人民群众的信息安全，电子工程技术研发人员就要做好安全防护对策，为电子信息工程技术应用领域的扩张提供安全保障。

1 电子信息工程技术的应用

1.1 在物联网技术中的应用

物联网是一种基于互联网技术和信息传感器等技术的互联模式，将生活与工作相关的多种设备、装置等连接在一起，实现信号定位和智能识别等功能，目前已经成为人们日常生活中广泛应用的一种技术。随着电子信息工程技术的不断升级和革新，监管功能的推广和普及也在很大程度上保障了物联网技术在数据信息方面的安全性。然而，基于计算机与互联网技术下的物联网技术与工程在实际应用中不可避免地会存在漏洞。因此，在电子信息工程技术的未来发展中，必须集中精力解决和完善这一问题。

1.2 在信息集成技术中的应用

将相关信息进行整合分类，将其输入统一的集成系统中，作为大数据存储在后台，通过对收集到的海量信息数据进行整理分析，并结合相应的规则和算法实现最终的结果输出，这是信息集成技术的主要应用形式。虽然这项技术在本质上并不复杂，但其所需的人力、资源与资金量却是十分惊人的，在结果数据的调取和输出中有着一定的难度[1]。为降低运行成本，就需要借助先进信息技术对数据进行收集与管理，并通过计算机和网络等设备实现信息之间的交互。目前在信息集成技术中，已经融入了电子信息工程技术，实现了时间、资源与资金成本的降低，同时对收集整理到的数据信息进行分类整理，以便于后台人员随时调取和参考。对于操作人员而言，在对数据信息进行整理分类时，必须秉持严谨认真的工作态度，以确保数据不会发生泄漏。

1.3 在电子通信工程中的应用

在电子信息工程技术的实际应用和操作中，信息处理是至关重要的环节，电子信息工程技术需要高度重视数据信息的完整性和准确性。在通信工程中，可能受到外部网络的攻击，从而影响到信息收集和处理工作的实效性，因此必须对这一问题加以重视。通信工程信息网络安全中的重要组成部分之一，在实践中可灵活运用计算机技术，保障电子工程信息处理工作的顺利进行[2]。在当前阶段，通信行业面临着较大的挑战，因此需要做好安全防护工作，以实现信息安全管理目标。虽然目前密钥技术和防火墙技术能够有效地预防一部分安全问题，但必须认识到，网络威胁难以完全消除，因此必须提前制定针对性的通信安全管控措施。

1.4 在产品设计中的应用

在产品设计中必须使用计算机软件，CAD软件是一种常见的计算机设计软件。该软件具备在计算机中进行产品建模的功能，同时也能够为电子信息工程设计提供精细处理方面的技术支持，从而使得产品的概念和规划更加精准、科学。随着信息技术的不断革新，计算机处理软件也出现了多样化的发展趋势。其中，自动化技术的运用较为广泛。产品设计人员可运用自动化技术，高效处理信息数据，从而提升电子信息工程设计的准确性，在提高设计效率、优化产品质量等方面均具有显著价值。

2 电子信息工程技术应用中常见的安全隐患

2.1 数据信息管理系统受到外部攻击

根据以往数据信息盗窃记录的统计结果来看，黑客通过非法手段入侵系统并攻破防火墙，从而窃取计算机数据信息管理系统中的数据，是一种常见的网络安全问题。这种行为对数据的安全性构成了极其严重的威胁，导致信息保密工作失去价值，并会对个人、企业乃至于国家造成严重的不利影响。随着计算机与互联网的广泛应用，人们的依赖程度日益加深，这也推动了互联网向多元化的方向不断发展，然而，网络中存储的信息和数据的安全性却无法得到有效保障。如果不能保护好这些信息数据，就很容易使一些不法分子利用计算机网络从事违法犯罪活动，给国家和人民群众的财产造成重大损失[3]。因此，在网络安全工作中，必须注重计算机信息数据管理系统的保护工作。在当今社会背景下，计算机信息安全问题已经成为社会关注的焦点，当计算机系统遭到恶意破坏时，不仅会导致人们的信息被窃取，更会对群众的生命和财产造成严重的威胁。

2.2 网络黑客攻击

网络黑客攻击手段一般是利用计算机病毒对私密网络空间进行攻击，从中窃取并破译关键信息，不仅会对个人利益造成影响，甚至在一定程度上对企业或国家的安全构成了威胁。随着计算机病毒的快速发展，黑客的攻击方式也变得越来越隐蔽，用户在使用计算机时，稍不留神就会使病毒入侵到个人计算机中，导致用户的个人信息被窃取。

3 电子信息工程技术安全防护对策

3.1 身份认证技术

在电子信息工程技术的应用中，可借助身份识别系统以个人身份信息作为登入计算机系统的验证内容。当有人非法登录时，计算机系统将拒绝访问，只有在通过身份认证后才能进入计算机信息系统。这种安全防护方式的目的在于防止不明人员登入计算机系统，并确保计算机系统的内部安全。身份验证可以采用人脸识别或手机验证码的方式，防止身份验证信息被窃取。手机验证码登录已成为电子信息工程技术中广泛应用的一种身份认证方式，这种方式能够保证密码不会被窃取，同时也能在系统内留下登录痕迹。如果该用户在计算机系统中进行了非法行为，能够将其作为报警的证据。此外也可使用数字签名技术。在数字化文档中以数字签名作为身份验证依据，确保个人身份的真实性。数字签名技术的独特之处在于其能够对所有接收到的信息进行严格的验证和识别，目前已经成为现代网络通信中的重要安全保障系统之一。

3.2 数据加密技术

目前，数据加密技术已广泛应用于多个行业和领域，其中链路加密是一种加密通信线路，主要用于信息传输。链路加密技术可以保证在网络通信中，数据信息始终处于加密保护状态下，并且能够掩盖数据信息传输的起始端、数据信息传输的频率、长度等相关参数，避免数据在传输期间被不法分子窃取和攻击，提升网络通信的安全性。然而，在实际应用中，链路加密只能用于信息传输的两端，在使用中存在一定的局限性，并可能对整个网络通信产生一定的干扰，从而降低数据信息的传输效率。在网络通信的前期加密中，一般使用端对端加密技术，这种加密技术能够确保数据信息由终端接收之前，不会进行任何解密处理，整个通信过程都是通过秘密文件的方式进行，当接收者获得数据信息后，必须使用密钥对文件进行解密，才能获得解密后的明文数据信息[4]。端对端加密与传统的网络加密技术相比具有较大优势，应用端对端加密技术，能够提高网络通信过程中的流畅度，即使在某个节点受到不法分子的攻击，导致数据文件被窃取，其中的明文数据信息也不会出现泄漏或丢失。

3.3 防火墙技术

应用防火墙技术，可以有效地避免外部网络的恶意入侵，从而提高网络安全性和稳定性，并为电子信息工程技术创造安全、绿色的运行环境。在使用防火墙时，也要同步使用安全防护软件，实时监督并记录各种网络活动和行为，并及时处理任何非法访问或异常数据，建立完善的网络安全防御体系，保障电子工程技术运行稳定，防止黑客或病毒等攻击事件发生。此外，借助防火墙技术，可以划分单位的内部网络，避免因局部安全问题导致单位内部网络整体发生瘫痪[5]。利用防火墙系统能够全面监管网络数据传输和信息读

取，记录下计算机系统每次访问记录并生成日志，这些日志可作为管理人员的安全防护参考内容，使管理人员可以从系统内获得有关网络安全状况的一手资料。当网络存在异常或遭到恶意入侵时，防火墙能够及时发出警报，在第一时间报告异常状态，为管理人员提供处理依据。

3.4 储存数字证书

CA系统兼容市面上的多种浏览器，并支持直接将数字证书保存在USBKey中，具有出色的灵活性。并且基于其良好的保密性以及完整性等特征，被广泛应用于电子商务领域中。USBKey具有与传统U盘基本相同的外形，方便携带和保存，当USBKey连接到计算机时，需要输入一个安全口令，这使数字证书的安全性得到了一定程度的提高，同时也避免了他人的窃取和使用。此外，USBKey采用了高度安全设计方案，数字证书不会轻易地从USBKey被中移出，从而有效提升了整个信息网络的安全性。

3.5 加强终端审计保护

很多系统终端管理员对终端审计的理解不足，将其简单视为对用户行为的监控。实际上，终端审计的功能并不只是记录用户访问记录和操作行为，而是在用户历史信息的基础上进行深层次分析，从中找出电子信息工程技术的缺陷与漏洞，从而为网络与系统的长期运行提供优化和升级[6]。利用终端审计功能监管用户的登录、打印、下载、异常登录与违规行为，从而充分彰显安全管理为核心的审计原则。终端审计能够实现有效的身份认证和权限分配，并通过相应的规则完成数据加密处理，从而保障了电子文档以及相关设备的安全性。此外，终端审计所具备的控制功能十分丰富，包括但不限于移动存储、文件操作管理、操作行为管控、文件打印下载控制等多个方面，为用户提供了全方位的安全保障。这些管控行为均属于合法范畴，可有效地避免多数违规行为的发生。

3.6 加快产品创新升级

在智能化技术迅猛发展的背景下，要不断加大电子设备、电子信息工程技术以及安全防护技术的探索与研发，推动技术与产品的创新升级，从而提高电子设备与电子信息工程技术的安全性能[7]。如革新服务器防火墙和计算机防护软件，提高其安全性和覆盖范围，满足多种电子设备与电子信息工程技术应用领域对于安全防护产品的需求。此外，也可以研究新的安全策略，实现电子设备与信息通信系统之间的融合，为人们提供更加安全可靠的互联网环境。另外，要顺应时代发展趋势，不断探索5G技术和智能化技术与电子信息工程技术的融合，开发和设计出更加安全可靠、使用更加便捷的电子设备。

3.7 安装计算机安全保护程序

程序的正常运行是支撑计算机中电子信息工程技术稳定运行的必备条件，要想完成这一目标，计算机系统需要具备完善的信息安全保密程序，防止病毒或网络漏洞对系统造成危害。现如今大部分的计算机都安装了不同的信息保密程序，在使用和操作的过程中，信息保密程序需要进行注册，编号、等级划分、修改密码、解除密码，在系统的设定中，程序代码明确地规定了对应的保密制度，也就是密码的尝试次数和浏览记录清除工作。常见的计算机安全保护程序是计算机安全防护软件，如瑞星、360、鲁大师等，这些软件安装与使用简单，在一定程度上能够发现计算机中的病毒与安全漏洞，并进行病毒消除与漏洞修复等操作。

4 结语

在现代化信息技术的持续发展背景下，电子信息工程技术在各行业与领域中的应用优势愈发明显，目前电子信息工程技术已经成为生活与生产中不可替代的一部分。但也要注意到，虽然电子信息工程技术为人们的生活带来了极大的便捷，但同时也伴随着大量的信息安全隐患，所以目前电子信息工程领域的当务之急就是在技术革新的同时，加大安全防护力度，提高对各类信息安全风险与隐患的应对与处理能力，推动电子工程信息技术的健康发展。

参考文献：

[1] 侯祥，赵岩，徐明远．电子信息工程技术的应用与安全防护方案[J]．电子世界，2022(01):208-209.
[2] 郭鹏．电子信息工程中的计算机技术应用及其安全研究[J]．电子元器件与信息技术，2021,05(09):9-10.
[3] 朱三妹．电子信息工程技术的应用和安全管理[J]．电子元器件与信息技术，2021,05(09):169-170.
[4] 李松宇．电子信息工程技术的应用与安全管理[J]．科技资讯，2021,19(27):14-16.
[5] 俞五炎，史业宏，雷宇，等．计算机电子信息工程技术的应用与安全分析[J]．无线互联科技，2021,18(13):85-86.
[6] 刘国祥，周卫红，李佩佩，等．计算机电子信息工程技术的应用和安全[J]．电脑编程技巧与维护，2021(05):40-41.
[7] 刘沂震．我国计算机电子信息工程技术的应用和安全研究[J]．信息记录材料，2021,22(01):46-47.