电子信息工程与网络安全浅析

康　昉
商水县自然资源局　河南　周口　466100

摘　要：随着互联网的快速发展和应用，网络安全问题成为一个日益严重的全球性难题。电子信息工程又是现代社会发展的主要驱动力之一，而随之而来的网络安全问题就愈加凸显。如今，以安全为前提的电子信息技术和网络应用成为共识，这使电子信息工程所涉及的领域更加广阔。保护电子信息技术安全，保证网络操作稳定，维护用户数据和信息安全，这些都需要网络安全管理来实现。只有将电子信息工程和网络安全有机结合起来，才能更好地保障社会安全，推动经济与技术的可持续发展。因此，加强电子信息工程网络安全管理工作，切实提升网络安全保护意识和技能水平，成为当前和未来一段时间内非常必要的任务。

关键词：电子信息工程；网络安全；防护措施

引言：随着信息社会快速发展，电子信息工程和网络安全已成为建设数字化世界的重要领域。电子信息工程是信息技术、电子技术、通信技术等多种技术的综合体现，已经在生产、生活、科学、文化等领域得到广泛应用。但随之而来的是网络安全问题的增多，信息泄露、网络攻击、网络欺诈等问题屡屡出现，给个人和企业的利益造成严重影响。因此，加强电子信息工程与网络安全的研究和应用已成为技术与社会发展的重要命题。

1 电子信息工程概述

电子信息工程是一个综合性技术领域，涉及了电子技术、通信技术、计算机技术、信息处理技术等众多方面，主要负责研究和探索电子信息相关领域的技术和方法，开发相关产品和系统，解决各种电子信息问题，推动电子信息科学技术的发展和应用。目前，电子信息技术正在以惊人的速度发展，它已经在社会各个领域中的应用得到广泛的关注。在现代工业、交通、通信、军事、医疗、家庭、教育等方面，电子信息工程都在起着越来越重要的作用。电子信息工程的主要研究方向包括：电子器件、电路与系统设计、电子测量技术、数字信号处理、通信技术、可编程逻辑器件、微电子系统、集成电路设计与测试、嵌入式系统、计算机网络、物联网、数据通信、信号处理、无线通信等。随着信息产业的快速发展，电子信息工程面临着严峻的挑战。首先，科技更新换代迅速，电子信息产品和技术发展十分迅猛，如何跟上时代步伐成为工程师必须面对的难题。其次，技术成本不断上升，尤其是大型工程项目的研究和开发成本庞大，必须注重技术创新和成本控制。最后，与科技更新同步，安全问题也成为电子信息工程面临的主要挑战之一，如何保证信息的安全性、有效性和可靠性也是目前亟待解决的难题。为解决上述问题，电子信息工程需要不断深入探索其核心技术的开发，积极推动其应用的创新和发展，加强与其他相关领域的合作和交流，提高工程师的综合素质并积极应对安全问题。在未来，电子信息工程将继续保持强劲的发展势头，不断为人们的生产和生活带来更多的便利和创新，促进社会进步和经济发展[1]。

2 网络安全技术的发展与应用

2.1 网络安全技术发展的历程

随着互联网技术的不断发展和应用，网络安全问题也越来越突出。网络上出现了各种各样的安全问题，如数据泄露、黑客攻击、病毒攻击和网络钓鱼等。在这样的背景下，网络安全技术应运而生。网络安全技术主要涉及密码学、防病毒技术、防火墙技术、入侵检测、网络访问控制和网络应用安全等方面。

2.2 网络安全技术的主要内容

网络安全技术的主要内容包括：密码技术、访问控制技术、安全规划与管理、网络攻击与防范、网络入侵检测和网络应用安全等。（1）密码技术是网络安全技术的重要组成部分。密码技术主要聚焦在数据加密和解密算法上。数据加密其实是生成密钥，然后将要传输的数据进行加密，这样加密的数据将不会被第三方窃听或者攻击者获取。（2）访问控制技术主要是对设备或人员访问的控制和安全保护。它可以通过身份验证、访问控制、审计跟踪等手段确保网络安全和数据资产的保护。例如：在企业内部，管理员可以对员工的电脑进行安全设置，避免非法人员访问系统和数据资产。（3）安全规划和管理主要是对网络安全的策划、设计和监督。对网络安全的规划和管理上，实现技术上的安全性、组织上

的安全人员建设与管理、安全日志进行监管等方面都要考虑到。（4）网络攻击与防范是在网络安全过程中必不可少的环节，可以通过使用防火墙等设备来进行防范。防火墙可以检测到网络安全威胁，并为用户提供安全的访问服务。（5）网络入侵检测是指在网络通信过程中，检测出可能的攻击行为，并做出最后的判断。它可以帮助网络管理员及时掌握网络安全状态，并对可能的攻击行为做出及时的处理。（6）网络应用安全是网络安全技术的重要组成部分。当用户使用各种网络服务时，都可能会遭到攻击，因此需要保护用户数据和账户安全[2]。

2.3 网络安全技术的主要应用

网络安全技术在现代生活中应用很广泛，主要体现在以下方面：（1）企业网络安全：在企业内部，网络安全技术可以用来保护企业的机密信息和资产，防止黑客攻击和病毒感染等威胁。（2）金融领域：网络安全技术在银行和证券等金融领域的使用非常普遍。网络安全技术可以进行客户身份验证和支付交易防范。（3）政府机构：政府机构是很敏感的机构，网络安全技术被广泛应用于政府网络安全管理。（4）个人网络安全：在日常生活中，可以通过使用防火墙和杀毒软件来保护个人计算机的网络安全。

3 电子信息工程和网络安全面临的挑战

3.1 新技术的不断涌现和快速更新

新技术的不断涌现和快速更新是电子信息工程和网络安全面临的重大挑战之一。随着新技术的不断推陈出新和技术变革的加速，现有的网络安全技术迅速失去应对新技术带来的风险和挑战的能力。新技术的快速涌现不仅扩大了网络安全事故的风险面，而且增加了电子信息工程和网络安全的管理和安全保障的难度。

3.2 信息泄露和数据安全问题

信息泄露和数据安全问题是电子信息工程和网络安全的重要挑战之一。在网络环境下，大量的数据交换和互联互通，信息泄露、数据被窃、网络攻击等风险也随之增加。这不仅对企业和个人的信息资源造成了巨大的威胁，也影响着经济和社会的发展。

3.3 跨境犯罪事件增多

跨境犯罪事件增多是电子信息工程和网络安全面临的一项重大挑战。网络跨界犯罪活动的范围和影响程度越来越大，让网络安全的防范变得更加困难。网络犯罪分子通常身在境外，通过境外服务器、钓鱼网站、虚拟货币结算等手段来窃取财产和个人信息，给社会和公民带来经济损失和人身威胁。

4 电子信息工程和网络安全挑战的应对措施

4.1 强化技术研发

强化技术研发是电子信息工程和网络安全发展的核心目标，可以有效提升网络安全的应对能力和技术水平。随着信息化、智能化、互联化等新技术不断出现，网络安全技术需要不断创新才能适应不断变化的网络安全形势和风险挑战。同时，针对当前存在的网络安全问题，也需要不断研究新的技术解决方案，才能更好地应对网络安全挑战。具体来说，强化技术研发可以采取以下措施：（1）提高技术创新能力。大力投资科技创新，提高技术创新能力。例如开展针对网络安全的尖端科研和技术攻关、制定新一代防护体系等。此外，也可以通过开展技术竞赛、合作创新等方式提高网络安全技能创新能力。（2）加强标准化。制定、完善网络安全行业标准规范，创新网络安全的管理方法和技术标准，既可以引导网络安全技术的科学发展，又可以提高网络安全技术的协调和规范水平。（3）加强学术研究。加强网络安全学术研究，总结前沿的网络安全技术和防御策略，及时发掘网络安全领域的新问题和新挑战，并提出相应的解决方案和研究建议。（4）推广应用。通过对新技术、新工具、新方案、新产品的不断推广，将先进的网络安全技术更广泛地应用于工业、商业和政府等领域。同时，也可以整合新技术创新和网络安全保障发展，不断提升网络安全的整体水平[3]。

4.2 加强科技团队建设

加强科技团队建设是电子信息工程和网络安全发展的重要保障，可以提高科技人员的素质和尖端技术水平，推进技术研发和应用，从而促进了网络安全的长期发展。在构建具有世界水平的科技团队的过程中，需要考虑以下几个方面：（1）建立人才培养体系。加强网络安全专业人才储备和专业化技术培养，建立健全的网络安全人才培养体系，为网络安全团队建设提供源源不断的人才支撑。可以通过实施以下措施实现这一目标：支持高校和科研机构开展网络安全相关的学科和专业建设，引导优秀人才走向网络安全领域。建立网络安全知识普及和技术培训平台，提升网络安全行业人才的技术水平和综合素质。搭建科技团队交流平台，建立互联网企业、高校和科研机构之间的合作机制，培育人才及知识共享。（2）加强创新研究。通过持续推进技术研发、研究新技术和应用，进一步增强科技团队在网络安全领域的创新能力和核心竞争力，可以采取以下措施：加大科研资金投入，鼓励科技人员进行前沿技术研究，提升网络安全技术水平。推动学术、产业和政府的联合，建立跨行业、跨领域、跨地区的科技团队协作机制，提高

研发创新能力。建立高效的研发流程管理机制，加强团队协作与信息交流。（3）提供优厚的薪酬福利。建立激励、优评和薪酬制度，鼓励人才团队不断进取、创新，进一步增强科技人员的凝聚力和创造力。可以通过以下方式实现：设立合理的奖励机制，对科技人员的技术能力、科技成果等方面进行评估，并给予奖励、晋升等优惠政策。提供优厚的薪酬待遇和完善的福利体系，从而吸引优秀的科技人才加入到网络安全团队中。

4.3 加强法律法规和监管

加强法律法规和监管是保障网络安全的核心保障之一。在当前不断升级的网络安全威胁和挑战下，加强法律法规和监管的能力，将有助于打击网络犯罪行为，维护公民、企业和国家的网络安全利益。具体而言，可以采取以下措施：（1）加强网络安全相关法律法规制定。加强网络安全相关法律法规的制定和完善，形成完整的法律法规体系，加强对网络安全领域的监管和约束。制定网络安全政策和标准规范，规范政府、企业和个人在网络空间的行为。（2）建立有效的监管机制。建立健全的网络安全专项监管机制，落实行政管理、技术监管和市场竞争等方式，加强网站运营者、网络服务提供者和用户在网络空间中的监管，打击违法和犯罪行为，保障网络空间的公平有序和安全稳定。（3）建立跨部门的网络安全协调机制。建立跨部门合作的网络安全协调机制，推动政府和工业界的联合防范和应对网络安全威胁，提升网络安全防护能力，防止网络安全隐患导致的严重社会和经济后果。（4）加大网络安全执法力度。通过加强执法力度，提高网络安全的惩治力度，对网络犯罪行为进行有效打击。可以通过加强执法机构的建设和技术支持，加强网络安全行业和执法机构之间的协调合作，形成有效的打击网络犯罪的力量[4]。

4.4 注重用户教育

注重用户教育是保障网络安全的重要一环，通过加强对用户的安全意识和安全行为培训，可以起到很好的预防和避免网络安全事件发生的作用，同时也能够增进用户对于网络安全的了解和认识。具体而言，可以采取以下措施：（1）加强用户安全意识教育。通过开展各类安全意识教育活动，提高用户的安全意识，让用户了解网络安全风险，认识网络威胁以及如何使用互联网资源的注意事项等。（2）开展网络安全应急演练。加强用户针对网络安全风险的应急处理能力，开展网络安全应急演练，提高用户处理网络安全事件的能力。（3）强化网络安全规范制定。要求用户遵守网络安全规范，加强网站、应用、平台和系统的安全设计，让安全成为一种习惯和生活方式。（4）推广网络安全科普宣传。加强网络安全知识的科普宣传，扩大用户对网络安全的认识，增强用户的维权意识和安全意识。（5）加强用户合法权益保护。保障用户的合法权益是加强用户教育的重要环节之一，只有让用户自我保护和行为规范化，才能真正从根本上保障网络安全。

结束语

随着信息时代的到来，电子信息工程与网络安全已经成为当今世界最前沿的科技领域之一。电子信息科技的快速发展，为网络安全威胁的增多提供了条件和滋生土壤，网络安全的威胁和挑战日益严峻。电子信息工程与网络安全的研究和应用，需要坚持科学、精益求精的原则，促进创新和技术进步。加强人才培养，建立健全的社会保障体系，加强创新研发和应用，以及提高法律法规和监管能力，都是保障电子信息工程和网络安全的有效方法。我们应该不断深入研究电子信息工程和网络安全，积极探索创新发展之路，为促进科学技术发展、推动社会进步、维护国家安全和人民幸福奋斗。

参考文献

[1]段智霞,王景.电子信息工程发展及其安全保障的研究综述[J].信息网络安全,2021,2(3):56-60.

[2]张胜男,赵旭,李勇.电子信息工程中的网络安全攻防技术研究[J].国际电子商务,2020,6(2):52-55.

[3]王丽华,张玉龙.电子信息工程中的网络安全管理[J].电子科技,2021,40(1):109-112.

[4]贾晓辉,李松海.电子信息工程中的网络安全问题及其对策[J].现代化商业,2020(12):154-156.