电子信息技术应用于网络安全维护工作的建议

牛　静

（山东省单县卫生健康局，山东 单县 274300）

摘　要　互联网技术在社会经济高速发展的今天获得飞速提升，更为细化的电子信息技术也在该时代背景下产生并不断发展进步，为我国网络工程建设带来了较大推动力量，但也形成了一定程度的新挑战，尤其在网络安全这个重要领域，电子信息技术的应用能否采取恰当的方式方法极为重要。本文将以电子信息技术的核心特征为切入点，分析现阶段电子信息技术应用于网络安全维护工作过程中存在的问题，对如何提升电子信息技术对网络安全维护工作的整体应用水平提出参考性建议策略。

关键词　电子信息技术　网络安全维护　信息收集　信息整合　数据运行

中图分类号：TP393.08　　**文献标识码**：A　　**文章编号**：1007-0745(2022)08-0029-03

电子信息技术作为一种较为新型的技术模式，是以计算机网络技术为基础逐渐产生并不断发展起来的。在近些年，互联网的全面普及推动信息化时代的形成，国内国际环境严峻复杂，自身与外界的影响因素逐渐增多，都对电子信息技术提出了新挑战与高要求。若电子信息技术存在安全漏洞并不断增多，信息泄露的可能性就会无限放大，造成人民利益甚至国家利益的重大损失，不利于人民生活安全与社会和谐稳定的态势形成与巩固。所以，电子信息技术工作者应首先建立与网络安全维护工作的紧密联系，树立始终保持网络安全的维护理念，深化对电子信息技术的认知，提高对电子信息技术的重视程度，以自身综合素养的全面提升推动网络安全维护工作的发展进步。

1 电子信息技术的主要特征

电子信息技术在社会经济高速发展的时代背景下产生并不断进步，为企业、机构、部门、群众带来了便捷高效的生活并逐渐改变着人们的生活方式与习惯，对社会经济的发展形成了一定程度的推动与促进作用。这些都离不开其自身独特的优势特征[1]。

1.1 信息收集的全面性

在市场环境日渐复杂，市场竞争日益激烈的今天，不论从政府的工作调节还是各个企业的优化发展等方面都面临着庞杂数据的收集与分析这个必不可少的环节。如果始终保持传统的方式方法，侧重于依靠人工手动搜集、统计、分析，很难保证最终信息整合工作的整体质量。而电子信息技术的出现很好地解决了这个难题，电子信息技术可以依托其信息收集全面性的特征，使数据在收集过程中不会轻易出现丢失的状况，并且其可以对所收集到信息进行全方位、系统性、自动化的处理，确保最终信息整合工作的整体质量[2]。

1.2 信息整合的高精准度

信息收集工作在传统的方式方法中不仅会时常出现胡乱采集、错误采集、遗漏采集等各种问题，其采集到的最终数据也处于凌乱的状态，没有形成有序性。这些都对信息处理的工作人员造成较大的工作压力，不利于信息收集整合工作的顺利高效开展。而电子信息技术的恰当性应用可以为信息收集工作人员多方位、多渠道的提供信息，增强信息的全面性、准确性、有序性，以此来推动最终信息整合工作的高精准度。具体工作人员通过对电子信息技术此优势特征进行有效应用，可以提高对信息反复核查工作的效率，提高信息处理的科学性、合理性，很大程度上降低信息处理的失误概率，始终保持信息整合的高精准度，逐渐提升信息整合工作的最终质量。

1.3 数据运行的高效性

电子信息技术不是停滞或一成不变的状态，始终与时代发展步伐保持一致，不断提升与进步。其将信息收集整合方式与技术功能方面进行高效融合，始终追求对庞多繁杂的电子信息数据进行最快速、最合理的分析与处理，以实现数据整体运行的高效性与合理性[3]。

2 现阶段电子信息技术应用于网络安全维护工作过程中存在的问题

2.1 技术使用没有形成规范化，存在安全隐患

电子信息技术以其时代先进性与有效性为优势，是其他的一些信息数据整合技术无法比肩的，社会各机构、企业、部门都将其广泛应用于工作各环节问题

处理中，较大程度提高了办公效率与发展速度。但电子信息技术作为一把双刃剑，在带给企业、群众便利高效生活的同时也带来了新的风险，相关工作人员对此新型技术的具体应用也被赋予更高的要求及更严峻的挑战。电子信息技术的相关工作部门、机构也将承担起更多的责任，因此对电子信息技术的具体应用问题应摆在更加关键的位置，对其进行深度的研究与思考。电子信息技术的应用在现阶段越广泛，意味着问题与风险也就越多，一些不法分子开始利用电子信息技术进行违法犯罪活动，个人信息、企业机密等被盗问题时有发生，甚至政府层面的办公治理环境也受到了一定程度的影响。首先，网络不法分子通常会使用病毒植入等技术手段侵入电子信息系统，以至于个人无法使用相应的电子数据信息，使网络信息系统进入完全瘫痪的状态，从而造成网络用户的信息及隐私在一定程度上泄露，对用户信息安全产生极大威胁。其次，高端网络黑客群体比普通不法分子的危害性更为巨大，其出于各种目的对网络的正常运行秩序进行侵入破坏，电子信息技术在具体应用方面会形成较大阻力，难以弥补的破坏漏洞需要进行耗时耗力的研究修复工作 [4]。最后，各企业自身硬件设备更新换代与电子信息技术的发展更新在步调上没有形成一致。电子信息技术紧跟时代步伐不断发展进步，而企业自身硬件设备没有进行及时的更新工作，以至于新的电子技术无法与旧的硬件设备相融合，难以发挥其最大价值效果，甚至由于旧设备无法与新技术相匹配而强行应用导致运行卡顿、崩溃等状况的发生。

上述现阶段存在的情况都使得电子信息技术的应用难以形成规范化，相关工作人员在具体应用工作过程中面临着各种压力与难题，为网络安全问题埋下了较大隐患。

2.2 信息系统存在一定安全隐患且相关人员经验不足

随着科技的进步，互联网技术也更加的先进和纯熟。在企业的运行和发展中是离不开互联网信息技术的，信息技术为企业发展提供了很好的契机和平台，还可以节约人力成本，但同时也带来了一定的安全隐患。在新型的网络环境中，部分工作人员不能较快地积极地去适应环境的变化，从而导致网络系统中出现较多的安全隐患问题。但是又由于很多工作人员在进行计算机的实际操作时会出现一定的失误，造成信息系统瘫痪，同时他们在面对突发事件或具有较高难度的系统障碍时会感到手足无措，不能及时有效地处理问题，在此时，很多的网络病毒就会趁机而入，网络黑客更是会利用这个机会窃取公司机密和个人相关信息。如果企业中存在这样的系统漏洞，相关机构必然会遭受巨大的威胁，对于企业的安全运营也必然会造成巨大的影响，使企业遭受严重的经济损失，削弱企业的核心竞争力，最终阻碍企业的发展。如今，各个企业间也会利用竞争对手的网络系统中的漏洞来窃取相关机密信息，以此来抢占更多的市场份额。所以，为了企业的健康向上发展，不断地完善和强化网络系统是极其有必要的。

2.3 部分工作人员网络信息安全意识淡薄

为了能够在最大程度上维护网络信息安全，建立和完善一支认真严谨的维护团队是极其重要的。但由于部分工作人员的网络信息安全意识淡薄，给网络病毒和黑客可趁之机，造成企事业单位机密信息和用户个人信息的泄露，企事业单位和个人的信息安全都受到了严重的威胁。

2.4 互联网信息技术具有隐蔽性和欺骗性

随着信息技术的快速发展，计算机的防病毒能力也得到了相应的提升。对于一般的普通的病毒，使用计算机自带的杀毒技术就可以将其杀死，但是在现如今，计算机病毒也在不断地变化，网络犯罪分子对其进行了新的伪装，使病毒可以根据计算机的相关配置设置相应的网络诈骗技术，盗窃用户个人信息。例如，黑客可以侵入某个网站，更改网站用户登录协议，窃取用户信息，继而采取不同的方式进行诈骗。黑客还可以设置隐藏的点击点，若用户进行点击就会盗取用户的信息，从而实施网络犯罪 [5]。

3 提升电子信息技术对网络安全维护工作整体应用水平的建议

3.1 规范技术使用，保证使用安全

在如今的社会，电子信息技术与其他技术相比较而言，电子信息技术具有很多的优势，其适用范围较其他技术而言也更广，各个工作领域都有使用它的人群和受众。在信息技术快速发展中，新型技术的使用在相关领域也为技术人员相应地带来了工作环境的挑战，在这个背景下，各个相应的工作部门和机构都应该展开全面的与之相关的多方面的思考。对于人们的日常生活来说，不管是公司还是个人，电子信息技术的使用为人们的起居住行带来了极大的便捷，但是也不乏有许多道德败坏的不法分子利用电子信息技术的便捷做违法的事情，所以为了企业发展和用户个人信息安全，都应该规范技术使用。首先，对于企业来说，应加强自身系统的维护，及时地更新相应的硬件设施

使其可以具有较强的兼容性，保证设备在使用的过程中不会出现卡顿或者崩溃，以避免工作人员在使用的过程中出现不规范操作的问题，杜绝网络安全隐患。其次，对于个人用户来说，应加强自身的警惕性，防患钓鱼软件，保护好个人信息和隐私，确保个人信息的安全。

3.2 加强相关人员的技术培训，增强其适应能力

如今，互联网技术已经成为人们日常生活和工作不可缺少的一部分。先进的信息化技术的使用可以使企业在市场环境中的运作效率更高，在市场中占据的份额也更多，同时也能够节省人力资源。为了使相关工作人员适应各种新型的工作环境，培训就成了一门必不可少的课程。培训课程可以提高工作人员的专业技术水平，确保企业网络环境安全，同时还可以提高工作人员的适应性，杜绝网络系统安全隐患。培训过程中应按照工作人员的擅长领域进行分组，并根据其自身的情况制定相应的培训计划，使各个工作人员在自己的专业领域都能得到大幅度的综合提升，最大程度地降低信息泄露的风险。在培训的过程中还可以提高工作人员应对突发事件的能力，使其在面对具有一定难度的突发事件时不会手足无措，能够做到及时修复问题，不给黑客有机可乘的时间，确保企业的运营安全，减少企业的经济损失。对于具有专项特长的人员来说，在培训的过程中应重点关注和培养，使其在后续的工作中能够发挥自己的才能，更好地抵御外来病毒入侵。

3.3 加强系统防护，确保信息安全

首先，应设置网络的访问权限，使没有权限的人不能进入网络系统中，同时设置权限还可以精确识别外界的具有危险的技术并对其进行阻拦，防止信息的泄露。其次，在防火墙的使用方面，应规范地、科学地使用。相关技术人员应将自己的工作经验与如今的防火墙技术结合起来，从以往的案例中汲取经验，从根本上解决问题，最大程度地确保企业信息安全。设立防火墙系统能够为电子信息系统建立起一个安全的屏障，降低网络黑客的攻击。在防火墙使用的同时也应对网络信息进行加密，为信息安全增加一层保障，使其能够更好地抵御网络病毒的攻击。最后，在查杀病毒方面，杀毒软件的使用是必不可少的。选择合适的杀毒软件，并对网络环境进行定期定时的病毒查杀，确保电子信息的安全性，保证网络设备在使用的过程中免遭病毒的侵害，防止信息的泄露。

3.4 完善相应制度，提升工作人员的网络安全防患意识

在企事业单位的发展中，建立和完善严谨的网络安全维护团队是极为重要的。在网络安全方面，技术人员需要有敏锐的发现问题的能力，同时也应该居安思危，提升自己的网络安全防患意识，降低网络信息泄露的概率。对于企业来说，制定符合自身发展需求的安全管理制度对其发展是极其有帮助的，同时相关负责人也需要意识到电子信息安全管理工作的重要性，强化内部人员的综合能力，在最短的时间内解决网络安全威胁问题，保证网络信息安全。

4 结语

电子信息技术在时代发展中产生并不断发展进步，同时又反作用于社会发展，产生一定的推动促进作用。此外，电子信息技术在为日常工作生活带来便捷性、高效性的同时也带来了新的风险与挑战。如何将电子信息技术更好地应用于网络安全维护工作中值得电子信息领域全体工作人员进行深度的研究与思考。应首先对电子信息技术的“全面性、高效性、高精准度”等最主要优势特征进行把握并不断拓展深化，其次要明确现阶段电子信息技术在网络安全维护工作中存在的“技术使用没有形成规范化，存在安全隐患、信息系统存在一定安全隐患且相关人员经验不足、部分工作人员网络信息安全意识淡薄、互联网信息技术具有隐蔽性和欺骗性”等问题，最后落实好“规范技术使用，保证使用安全、加强相关人员的技术培训，增强其适应能力、加强系统防护，确保信息安全、完善相应制度，提升工作人员的网络安全防患意识”等各项工作，促使网络安全问题在电子信息技术的科学化、合理化、规范化应用下得到有效解决。

参考文献：

[1] 盛俊 . 电子信息技术在网络安全中的应用研究 [J]. 网络安全技术与应用 ,2022(03):128-129.
[2] 董昊 , 李林泽 . 电子信息技术在网络安全中的应用分析 [J]. 通信电源技术 ,2020,37(21):211-213.
[3] 别雨航 . 电子信息技术在网络安全中的应用 [J]. 无线互联科技 ,2021,18(07):23-24.
[4] 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.
[5] 赵军 . 计算机信息技术应用与网络安全的思考 [J]. 卫星电视与宽带多媒体 ,2022(02):60-62.