计算机信息管理技术在网络安全中的应用

张　利

（紫光华三集团有限公司，浙江 杭州 310056）

摘　要　随着我国经济和技术的不断发展，计算机的管理技术被更多的应用到了企业实践中，提升了企业的技术效率和生产效率。计算机信息管理技术能在一定程度上提升互联网技术的安全性，但是目前网络环境日益复杂，仍然存在很多不安全的因素，这就直接导致企业的互联网安全问题频发。互联网的安全问题可能对企业的财产安全造成一定的威胁，对于人民群众的生活也有着比较大的影响。本文从网络安全的应用情况出发，进而分析目前网络安全的主要问题，从而得出网络安全的重要意义和未来的发展策略，以期能够为互联网安全的发展提供新的思路。

关键词　计算机信息管理技术　网络安全　信息技术　信息安全

中图分类号：TP393.08　　**文献标识码**：A　　**文章编号**：1007-0745(2022)08-0019-03

我国的信息技术发展已经进入了新的阶段，更多的网络信息技术被研发出来并被应用到了各个领域，促进了多个领域技术含量的提升。但是网络的发展除了带来新的发展机遇，还带来了一定的挑战。目前网络安全问题频发，侵犯了我国人民群众的基本权益，也对企业的发展带来了一定的阻碍。

因此，网络安全问题成为当前计算机管理技术领域所面临的主要问题，充分解决网络安全问题，将计算机信息管理技术应用到网络安全当中，能够有效地促进社会的安全和稳定。

1 网络安全和计算机信息管理技术的内涵

1.1 网络安全

网络安全指的是网络领域内的个人信息和资源等的安全，同时信息传递的安全和软件安全也是网络安全的范畴。软件安全指的是软件的稳定性，能够为获得权限的访问用户提供对应的服务，同时保障软件使用者的信息不被窃取。资源的安全则主要指的是企业和个人的服务器等网络设备的安全，为了使得个人和企业的服务器不受到外部攻击的影响，就需要使用网络安全技术来进行保障。信息的安全主要氛围信息的传输安全和储存安全，账号密码等信息作为用户的私密信息和关键信息，对于用户自身有着较高的价值，如果个人的信息在传输中被窃取，将对个人的财产安全造成较大的威胁[1]。

1.2 计算机信息管理技术

计算机信息管理技术属于信息技术的一个子领域，其中包括信息安全性评估、访问控制技术和防火墙等技术内容。信息安全性评估指的是对信息安全的预防措施，信息安全性评估是对网络安全性和网络状态的一种检测，通过发送某种不具备意义的字符串到固定的服务端，就能够得到网络的状况和安全情况，如果该信息被拦截或者是存在被拦截的风险，就需要及时对网络漏洞进行修补，这样就能够有效地降低网络运行的风险，能够为实际的用户创造更为安全的用网环境。访问控制技术指的是对网络信息的拦截技术，这种技术通常被应用在浏览器上，服务器会首先对将要访问的网站和传输的信息进行安全性检测，如果发现被访问网站存在风险，就可以向用户发出警告，这样就能够防止用户访问不安全的钓鱼网站。防火墙是现代操作系统的核心技术之一，运用防火墙技术能够有效地屏蔽不安全软件的信息传输，智能防火墙技术还能对正在传输的数据进行判断，当出现信息风险的时候，防火墙就会自动预警并终止信息传输，起到对用户信息的保护作用。

2 计算机信息管理技术在网络安全中应用的实际状况

2.1 应用现状

计算机信息管理技术是现代信息技术中的重要内容，也是国家重点研究和建设的互联网技术之一。互联网对于用户来讲存在着便捷之处，但是同时互联网也会对用户造成一定的威胁。互联网技术如果被用到实处，就能够有效地改善人民群众的生活水平，同时也能够带动经济和社会的发展。但是现在越来越多的不法分子企图通过互联网技术获取违法财产，严重情况下还可能会对企业财产和社会带来不良影响。网络安全指的是互联网传输数据的安全性，诸如银行等重

点的网络应用的数据受到国家的严密保护，如果被不法分子篡改其中的部分数据，很可能会导致公民个人财产受损，严重情况下还会对社会秩序产生不利影响[2]。目前我国信息技术的更新速度很快，但是各种诈骗技术和黑客技术也在不断地发展，这对现代网络环境来讲是一种新的挑战，同时也对计算机信息管理技术的发展带来了一定的挑战。

2.2 存在的问题

首先，我国的网络检测水平仍然处于一个较低的水平。根据有关调查数据显示，我国主要的网络安全威胁在于黑客的入侵和电脑病毒的影响，这两种不安全的因素都可能会对人民群众的财产造成严重的影响。为了能够及时发现侵入和病毒，就需要加强网络检测水平，及时发现当前网络中的波动情况，如果发生黑客入侵等情况，有关人员也可以在第一时间开展信息安全的攻防战。但是我国的网络检测水平仍然不足，很多工作人员不具备相应的计算机信息管理技术，无法及时地检测到网络环境中存在的威胁，因此就导致了网络环境的不安全性。

其次，我国普遍存在着内部管理不到位的现象。这种现象出现的原因主要是由于管理制度和管理体系的缺失，相关的管理人员的综合素质和技术水平没有达到要求。管理制度的缺失导致了相关的管理人员在参与网络安全建设的时候，缺乏工作的根据和管理的依据，因此很多管理性工作都流于形式，无法充分发挥计算机信息管理技术在网络安全中的实际作用。技术人员的综合素质和技术水平不达标将影响其工作能力，部分工作人员缺乏良好的职业道德，有一小部分人甚至会以个人利益为由来牺牲部分的集体利益。更有甚者在工作过程中收受贿赂，协助他人进行网络数据的窃取，这直接对网络安全造成了威胁[3]。

最后，我国技术的灵活程度不足。计算机信息管理技术随着时代的发展也在不断地发展，在应用的过程中也解决了部分的安全隐患问题，计算机信息管理技术的水平也在不断地提升。但是在实际应用过程中，计算机信息管理技术的灵活程度不足，很难针对某些特别的网络安全问题做出对应性的应变。黑客技术和病毒等网络安全威胁因素也在不断地更新迭代，很多威胁性的手段都有着不同之处，对于网络信息也有着一定的针对性，所采取的信息攻击方式也有着较大的不同。为此，计算机信息管理技术虽然获得了一定的提升，但是缺乏灵活性导致了技术手段很难应对复杂的网络环境。

3 计算机网络技术对网络安全的重要意义

相较于计算机信息管理技术，计算机网络技术指的是目前常用的网络协议和其他互联网底层技术。这些技术通常情况下不会和用户进行直接的交互，但是对于网络安全而言也发挥了重要的作用。计算机信息管理技术是基于计算机网络技术的，例如防火墙技术就需要和底层的互联网协议进行交互。黑客和病毒等网络威胁手段都是针对计算机网络技术的薄弱之处进行攻击，例如僵尸网络就是通过病毒来感染大数量的服务器和个人电脑，通过这些服务器或电脑之间的联合形成僵尸网络，僵尸网络通常情况下被用来攻击更大型的服务器，通过频繁的发送响应请求从而使得服务器响应能力受阻，服务器将无法满足用户的实际需求。僵尸网络的应对需要用到流量监测技术，通过对流量类型进行分类就能够有效地将僵尸网络流量屏蔽，从而保障用户的真实请求不被影响。从这可以看出，计算机网络技术对于网络安全有着重要意义，同时也是网络安全的基础。

4 计算机信息管理技术在网络安全中的具体应用

4.1 打造行之有效的信息化管理平台

无论对于个人还是企业而言，网络安全问题都是一个较大的威胁，同时网络安全问题还可能会危机国家和社会的安全和稳定。为了能够营造良好的网络环境，政府也需要承担起责任，发挥起自身在网络安全建设方面的职责，积极维护网络空间环境的安全，提高对维护网络环境的财政支出，构建信息化的管理平台，为企业和个人提供良好的网络化管理平台。信息化平台的工作人员需要承担起建设网络安全环境的宣传职责，利用多种网络化的传播渠道，向公众传播网络安全的重要意义，规范人们的用网习惯和安全意识，这样能够有效地减少相关威胁事件发生的频率。信息化平台的工作人员还需要针对常见的黑客攻击和病毒种类进行总结，并对这些影响网络安全的因素进行归纳，制定好防范措施和突发情况下的解决措施，这样当用户在利用网络环境的时候，如果遇到相似的网络威胁事件，用户就能够在最短的时间内发现威胁事件的种类，从而能够在很短的时间内做出响应，能够减少网络威胁事件的不良影响[4]。

4.2 打造完备的网络安全管理制度

通常情况之下，计算机网络数据是计算机信息管理技术的对象，管理的主要内容是数据的收集过程和数据的传输等。这几个环节的联系都是比较密切的，

因此如果想要提升计算机信息管理技术在网络安全领域的应用程度，就需要加强计算机信息管理技术的管理，对此就需要制定一定的管理制度，这样在出现具体情况的时候就可以有比较明晰的处理办法。在实际的管理进程之中，相关的工作人员需要对网络的运行状态进行动态化的监测，同时对网络环境的运行情况和安全性进行合理的评估，这样就能够确保某些加密信息都是在安全环境中传输的，数据的传输安全性就会受到保障。

4.3 强化管理人员的网络安全管理能力

网络技术人员对于网络安全性具有决定性作用，其能力和综合素养的高低是决定工作效果的重要因素。因此，加强网络空间管理人员的安全管理能力，对网络空间安全的构建是必要的。为此，有关企业和政府就需要对从业人员的网络技术水平进行定期的评估，同时针对当前计算机信息管理技术进行培训，不断提高从业人员的技术水平，这样就能够有效提高有关人员的计算机信息管理技术应用能力。在定期培训之外，有关单位还需要对计算机信息管理技术从业人员的能力进行定期的考核，同时可以针对考核内容设置一些奖励性的指标，并结合激励制度，对表现较好的技术人员进行物质或者精神上的奖励，这样就能够促进团队内成员的互相学习，能够带动技术在工作人员之间的流通，促进管理人员网络安全管理能力的提升 [5]。

4.4 提升加密技术水平

加密技术对于网络数据传输具有重要的意义，能够有效保障数据传输的安全性。目前在实践中运用频度最高的加密技术氛围节点加密技术和端对端加密技术等，这些加密技术都有着各自的优缺点，同时所适应的数据类型也有着一定的差别。但是目前黑客入侵手段也在不断向着多样化发展，这种单层的加密形式已经很难防御某些高流量的黑客入侵。因此在进行加密的过程中，可以针对数据的优先度和重要程度，对数据进行双层加密或者是多层加密，这样就能够有效地防御黑客的入侵，数据传输的安全性将会大幅度的提升。加密技术的嵌套可以采用多种不同加密技术，这样加密技术就能够产生环环相扣的效果，大幅度增加数据加密的效果。

4.5 提升抵御风险的能力

计算机网络中存在着各种各样的运行风险，这些风险对用户数据都会造成不同程度的威胁。为了能够增强计算机信息管理技术在网络安全中的应用，就需要加强系统的风险抵御能力。目前随着云技术的发展，很多运算并不一定需要在本地机器上进行开展，相关的工作人员可以利用某些大型系统来进行计算机网络安全的管理，通过定期查杀的方式来对网络环境中或者是本地机器中的文件数据进行查杀。如果发现某个文件存在着安全问题，就可以采用物理隔离的方式来将可疑文件和其他正常文件进行分隔，这样就能够在最大程度上减少病毒对本地机器的影响，从而能够保障数据的安全 [6]。

4.6 提升技术水平

目前黑客入侵和病毒的更新迭代速度越来越快，为了能够有效应对新型的病毒和黑客入侵，就需要不断地提升计算机信息管理技术的水平。提升技术水平可以通过团队研发实现，因此企业或者政府中就可以成立计算机信息管理技术团队，团队主要负责计算机信息管理技术的迭代升级，使得当前计算机信息管理技术能够应对当前绝大多数网络威胁事件。此外，不同企业和政府之间可以加强信息的相互流通，可以派遣团队内成员去其他企业和政府去交流学习，这样能够促进计算机信息管理技术在不同团队之间的流通，能够有效带动技术水平的提升。

5 结语

计算机信息管理技术对于网络空间的安全具有重要的意义，实现良好的计算机信息管理技术效果就能够有效保障信息安全。目前病毒和黑客入侵手段的迭代速度比较快，为了能够适应入侵手段的升级，计算机信息管理技术也需要对应进行技术迭代，通过多种措施结合的方式来进一步保障网络空间环境的安全。

参考文献：

[1] 杨曙光 . 计算机信息管理技术在网络安全中的应用 [J]. 网络安全技术与应用 ,2015(04):40-41.
[2] 高喜桐 . 计算机信息管理技术在维护网络安全中的应用策略探究 [J]. 计算机产品与流通 ,2019(04):21,112.
[3] 张丹丹 . 网络安全中计算机信息管理技术的应用探究 [J]. 电脑编程技巧与维护 ,2020(12):157-158,161.
[4] 欧晓萍 . 计算机信息管理技术在工程造价信息管理中的应用 [J]. 中小企业管理与科技 (上旬刊),2021(02):195-196.
[5] 马良 . 维护网络安全中计算机信息管理技术的实践与探索 [J]. 电脑编程技巧与维护 ,2018(08):118-119,130.
[6] 李健 , 李小虎 , 焦志勇 . 浅析计算机信息管理技术在维护网络安全中的应用 [J]. 中国新通信 ,2020,22(20):63-64.