维护网络安全在计算机信息管理技术中的应用策略探究

尹浩然

（北京邮电大学理学院，北京市，100080）

摘要：本文主要针对维护网络安全在计算机信息管理技术中的应用展开研究，通过其中存在的不足，重点论述了几点针对可行的应用策略，主要包括提高人员的安全防护意识、加强网络安全管理制度的构建、积极构建网络安全管理平台、加强网络安全风险控制、积极培养计算机网络技术人员等，旨在充分发挥出计算机信息管理技术的应用价值，从而发挥出对维护网络安全的推动作用。

关键词：网络安全；计算机信息管理技术；应用策略

现阶段，在科学技术不断发展的推动之下，信息化时代应运而生，其技术的优势性突出，使国民生活方式出现了翻天覆地的变化。在信息化时代出现后，大大提高了人际交往和沟通水平，而且对于现代化社会发展也具有着大大的促进作用。但是在网络病毒和黑客技术越来越常见，对于计算机网络安全产生了很大的影响和制约，一旦不及时采取治理措施，极容易对人们正常的生产生活活动产生不必要的威胁，甚至很难确保用户自身权益。因此，应提高对维护网络安全的高度重视，将其与计算机信息管理技术结合在一起，使之成为统一整体，确保良好的应用效果。

一、计算机信息管理技术中维护网络安全存在的不足之处

（一）网络检测和管理技术水平比较弱化

现阶段，在社会大环境的影响下，信息安全问题已经成为了社会大众共同关注的话题之一，对当前互联网技术的发展趋势进行分析，网络病毒强度越来越强化，同时病毒的破坏性也愈发突出。因此加强网络管理非常有必要，及时解决和处理网络操作中的异常情况。在网络监控和管理过程中，信息管理技术尚未得到了广泛应用，其应用价值并不显著，这时如果监督管理者不加以重视，极容易导致潜在风险的出现[1]。而一旦面临黑客和病毒的趁虚而入，将会严重损失到网络信息，从而对个人和企业的信息安全造成影响。

在时间不断推移过程中，网络安全问题的复杂程度越来越突出，而且信息管理技术的发展速度极其迅猛，如果信息管理和监控技术缺失，极容易丢失诸多重要文件信息，甚至泄露重要机密。所以必须要加强信息管理技术中监控技术的应用，防止突发事件的出现。

（二）内部管理力度缺失

在信息系统内部，管理制度较不完善，而且制度的执行力度明显比较薄弱化，一定程度上极容易导致内部工作人员“钻空子”，比如内部人员擅自对上网设备进行安装，并没有过渡地关注系统安全管理控制点。同时，借助隧道技术，与外部人员相互勾结。对上述现象的原因进行分析，主要是因为内部管理力度不足，严重威胁到网络的安全性，而且其防范难度性较高，所以务必保持时刻警惕和重视。

（三）访问控制效果难以保证

现阶段，对网络上的病毒进行分析，大都借助于各种网络输入进行传播。借助一定的访问控制，对于防范病毒入侵具有明显的效果，当前信息管理技术，可以不断提高网络站点检测水平，确保高度的安全性[2]。但是在实际上，一些技术人员并没有保护好可能出现潜在风险的网络站点，同时用户的重视程度也有所欠缺，在进入网站时，具有盲目性和随意性特点，在使用网络过程中，有害访问和外来入侵经常出现。基于此，对于相关技术人员来说，必须要加强计算机技术的合理应用，加强特定对象和访问权限的设置，对黑客执行信息设备进行抵挡，在对信息设备权限予以明确后，有助于网络安全性的提升。

此外，在计算机信息管理技术创建过程中，具体对象尚未进行明确设定，对信息获取的影响程度并不大，所以针对于“色情事件”，主要由于社交网站 Facebook 网，对于信息获取的控制力度不足，造成黑客趁虚而入，而诸多色情、淫秽图片的大量出现，对用户正常使用网络产生了巨大的不良影响。

（四）加密技术的完善性不足

要想实现信息安全目标，加密技术发挥着明显的优势，而且在网络管理支撑技术中也占据着重要地位。对于加密技术来说，通过信息向密文的转换，接收方必须通过解密，确保密文得到还原，形成明文[3]。但是由于网络技术发展速度较快，以往传统加密方法并不适用，尤其在数据安全这一方面，所以应不断创新、与时俱进，给予网络安全强有力的保障。

（五）应变能力有待提升

借助于经济和技术的大力扶持和推动，大大提升了互联网的发展速度，在硬件或软件处理方面，网络信息技术要通过不断发展变化，确保与社会发展需求相符，但是在实际上，互联网技术的改变，很难影响到数据管理技术，所以不利于存在问题的及时解决，也无法落实针对性原则，从而威胁到互联网网络安全水平。

二、维护网络安全在计算机信息管理技术中的应用策略

（一）提高人员的安全防护意识

网络内部安全问题的发生，对其原因进行分析，主要是因为管理者对网络安全的了解甚少，甚至对于网络安全比较漠视，所以要想维护网络安全，既要加强计算机信息技术的应用，也要引导公众树立清晰明确的安全意识。首先，相关工作人员应明确计算机管理技术和维护网络安全之间的关系[4]，加强器安全意识的渗透，将计算机信息管理技术在维护网络安全的作用发挥出来。此外，还要对信息管理技术进行积极研究，进一步拓展信息管理技术的应用范围，使网络安全水平得到有效强化，从而将信息管理技术的促进作用进行展现。

（二）加强网络安全管理制度的构建

在网络安全问题方面，计算机信息坚持不容忽视，在网络发展过程中，必须要基于安全视角，加强安全体系的构建和规范。基于此，可以将网络安全要素挖掘出来，确保网络环境的设计符合标准性要求[5]，不断提高安全保障体系的完善性。要想不断提高网络运行效果，应对网络安全体系进行不断完善，给予网络安全一定的保障。此外，在技术发展过程中，用户应正确认识和看待安全管理内容，加大监督和控制力度，防止安全风险的出现，致力于网络安全系数的提升，从而将网络安全管理制度的法律性保障作用充分发挥出来。

（三）积极构建网络安全管理平台

要想推动网络安全目标的顺利达成，必须要引导网络用户树立高度的网络安全意识。具体来说：

首先，应加强法律规则的制定，一旦网络环境问题出现异常，及时加以解决，并且第一时间封禁非法网站，面对网络滥用行为的出现，应加强内部监禁，同时给予相应的惩罚。其次，对于网络管理者来说，应注重自身专业水平的增强，加强自动化管理模式的应用，杜绝安全问题的出现。同时加强专业技能的学习也是至关重要的，将自身技术水平提升到全新的高度，并加强信息管理技术最新成果的融合，确保信息管理技术与互联网社会发展趋势保持高度的一致。最后，社会应严格监督用户网络，在用户使用互联网过程中，网络安全问题难以避免，所以用户应大力杜绝垃圾网站，一些网站如果存在潜在风险，会给予用户相应的提醒，所以用户应提高其重视程度[6]，防止病毒渗透到电脑之中，以免造成不必要的损失问题。此外，应及时加密处理重要文件信息，这也是网络安全的重要实施内容之一。

（四）加强网络安全风险控制

要想不断提高计算机网络系统使用功效，必须要注重各种网络安全风险的防范，积极开展风险监测和防御等一系列工作，以免对计算机网络系统的正常运行造成不利影响，给予维护网络系统安全一定的扶持。详细来说：

首先，在网络系统方面，应加强监测系统的设置，针对于网络信息数据，可以实现第一时间监测，面对异常数据的发现，应加强强制停运措施的应用。同时加强信息访问的检测控制也是至关重要的。在信息访问的检测控制过程中，既要注重访问信息的内容和数量，也要提高对信息访问者的关注程度。基于此，可以不断提高检测控制效果，满足维护网络安全的内在需求。

其次，应加大风险预测力度，不断完善预警机制，及时处理安全风险。在计算机使用方面，一旦出现系统漏洞现象，极容易丢失和损坏重要信息数据，所以应积极防护操作系统，其中，应积极设置扫描软件[7]，全方位、多角度领域地监测计算机，针对于使用者身份，应进行积极验证，防止相关威胁的出现影响到计算机的正常使用。

最后，加强操作系统的安全防护。众所周知，在计算机网络中，操作系统的作用不可小觑，如果操作系统存在薄弱环节，安全问题在所难免，所以应将操作系统的安全防护工作落实下去，推动计算机网络安全水平的提升。比如应积极设置安全防护系统，将其与计算机操作系统结合在一起，确保漏洞得到及时修复，并防止病毒和黑客病毒趁虚而入。此外，在计算机网络系统安全方面，应对入侵检测系统等进行不断优化，从而将安全隐患“拒之门外”。

（五）加强多种先进信息方式的应用

1.信息加密方式

针对于信息数据，加强各种加密算法非常重要，防止信息窃取等不良行为的出现。在科学技术发展的推动下，以往传统数据加密方式并不适用，与当前时代需求有着明显的差距。因此，应对国外先进技术和经验加以学习，不断创新加密算法。在加密系统中，非对称性质的加密方法（“公开密钥”）有着良好的应用价值。对该密钥进行分析，RAS 公开密钥技术、DSA 数字签名技术等得到了充分体现[8]，加密和解决者掌握的密钥内容具有明显的差异性。当前在诸多领域中，RSA 公开密钥密码技术算法、PGP 混合加密算法等非常值得应用，其实施效果显著。需要注意的是，管理人员要想取得良好的应用成效，应贯彻落实好具体问题具体分析原则，确保加密算法选择的合理性、适用性，从而构建安全稳定的网络环境。

2，信息认证技术

在维护网络安全方面，信息认证技术的重要意义不言而喻，可以对认证的信息发布者进行准确判断，而且在传播过程中，还可以防止信息更改现象的出现，贯彻落实信息的准确性需求，并做到完好无损[9]。通常来说，验证信息、身份确认以及数字签名等是信息认证的重要类型，所以应结合实际情况予以采纳。

3. 防火墙技术

对于防火墙技术来说，具有较高的应用价值，该技术在实际操作过程中，具有极大的便利性，而且更新速度较快，价格也比较隔离。在数据监测过程中，防火墙技术具有较高的有效性，可以限制不规范的访问，其权限限制性突出。此外，防火墙技术在网络内外部均扮演着重要角色，可以对网络外部信息展开全面观察，且保护具有全天候性质，从而方方面面地维护网络安全。

（六）积极培养计算机网络技术人员

对于技术人员来讲，其专业性和相关职业意识，关系到互联网的安全系数。网络安全问题，与人民群众的切身利益之间有着密切的联系，而且也是企业核心竞争实力的重要影响因素之一，所以专业人员应提高认知能力，确保自身的专业水平得到提升。所以相关单位应引导 IT 网络技术人员提高对相关会议的参与热情，并加强激励措施的制定[10]，如果员工具有显著的创业能力和知识水平，应给予相应的物质奖励和精神奖励，反之，应实施一定的处罚。相关工作人员在计算机管理方面，应树立高度的风险防范意识，有效控制和防范风险，保证网络安全得到有效维护。

此外，基于社会视角，社会应对技术队伍建设保持高度的关注度，致力于队伍专业水平的提升，实现网络环境的优化，基于此，可以确保网络安全水平的稳步提升。

三、结束语

综上所述，在计算机信息管理技术应用过程中，明确提出了对于维护网络安全的要求，这在计算机信息管理技术中发挥着不可比拟的作用和优势，切实维护好社会大众的合法权益，防止不安全因素的出现。但是也要注意，应不断更新和升级计算机信息管理技术，确保与时代发展趋势和发展方向相一致。

参考文献：

[1]郭亚鹏.计算机信息管理技术在维护网络安全中应用策略探究[J].计算机产品与流通,2020(10):84.

[2]王捷,王峰.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].电脑知识与技术,2020,16(04):15-16.

[3]闵星.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].信息与电脑(理论版),2019(09):7-8.

[4]张莎莉,洪月,韩柳.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].中国新

通信,2019,21(08):144.

[5]邵力.计算机信息管理技术在维护网络安全中的应用策略探析[J].计算机产品与流通,2018(05):15.

[6]阎靓.计算机信息管理技术在维护网络安全中的应用策略[J].电子技术与软件工程,2018(04):209.

[7]吐尔逊艾力·巴孜力江.计算机信息管理技术在网络安全中的运用[J].网络安全技术与应用,2017(11):5+7.

[8]蔡猛,陈志忠,王骏.计算机信息管理技术在维护网络安全中的应用策略[J].电子技术与软件工程,2017(21):190.

[9]骞巍.计算机信息管理技术在维护网络安全中的应用策略[J].信息与电脑(理论版),2017(09):200-201.

[10]陈文兵.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].电脑知识与技术,2015,11(36):35-36.