最新安全技术与管理论文(模板8篇)

公司宣传语要具备感染力，能够打动人心，引发客户的情感共鸣，激发购买欲望。确定目标受众，分析他们的心理需求和价值观，抓住共鸣点。以下是一些广受好评的公司宣传语范例，希望可以激发您的创作灵感。

安全技术与管理论文篇一

摘要:

随着我国电力能源的发展，电气技术也在不断提升，电力设备在人们工作及生产生活中扮演着重要角色。工程质量是保证电气工程发展的基础，而安全管理则是整个电气工程运行的核心。针对电气工程的施工技术问题及安全管理进行系统性分析，提出电气安装工程技术要求及安全管理措施，希望可以为我国电气工程发展提供有效参考。

关键词:

安全技术与管理论文篇二

摘要：随着社会的发展与科学的进步,计算机被广泛应用于人们的日常生活中。但随之而来的网络信息安全问题也日渐显现。本文针对网络信息安全技术管理的计算机应用展开研究,通过技术、管理等方法,增强网络安全,避免危险因素影响人们的日常生活。

关键词：网络,信息,安全,技术

计算机是现代办公、生活的重要工具,其遍布于社会活动的每个角落,带给人们高效、便捷的服务。但同时,安全问题也引起了人们的关注,加强计算机网络信息安全技术管理能够提高

其利用效率,充分发挥计算机的功效,是保证政府、国家安全管理部门以及人民生活的隐私与重要数据不受侵犯的首要任务。

1、计算机网络安全问题概述

现代社会的互联网应用范围比较广泛,且其本身具有一定的自由性、共享性、开放性等特点,能够为人们的生活、办公带来高效的服务,并提升了数据采集与传输的速度,在当今世界可谓是时代进步的标志,技术发展的必然手段,因此,使得互联网在使用过程中存在无限的发展潜力,但同时也带来了一定的安全隐患。其中与病毒的攻击最为明显,主要表现为通过各种技术手段进入用户计算机内,并进行恶意破坏或篡改数据、窃取数据等非法行为[1]。而病毒则主要表现在广泛使用的软件中,其本身具有一定的复制功能,被广泛的扩散到计算机每一个角落。其中病毒的主要特点表现在传染性、繁殖性、潜伏性以及破坏性。主要传播方法是不法分子利用计算机固有的软件进行编程等操作,并通过某种途径侵入计算机内,修改程序系统进而造成破坏。其次一些网络安全问题还有木马破坏、计算机信息泄露等问题。以下简单根据上诉几种问题提出相关解决办法。

2、基于网络信息安全技术管理的计算机具体应用

2.1人工智能防火墙安装

随着科学技术的发展,人工智能技术被广泛应用于各个领域。在计算机领域中,人工智能技术的使用常表现在防火墙技术。普通的计算机防火墙技术无法做到针对各种病毒甚至违法行为进行实时分辨,且缺乏一定的学习功能,创新功能,未能做到跟随时代发展而变化。无法为用户提供安全的网络环境,无法保障网路信息的可靠运行,目前已被逐渐取代。

而人工智能防火墙技术则能够实时学习新技术与新知识,根据

每次病毒的侵入总结相关经验并完善自我抵御能力,在不断的总结中发展自我,提升自我。同时,能够针对人们日常收发邮件、网络环境等方面进行实时侦查,确保用户在互联网环境内的`安全使用。针对可疑入侵来源能够做到自行分辨,并对用户进行提醒,确保不妨碍用户的正常使用。当发现外来入侵源时能够及时作出防御、修护等举措,抵御外来危险的入侵。当抵御不成功时,能够及时备份计算机内相关数据,以免丢失带来不必要的麻烦。

2.2计算机加密技术

现如今,计算机网络信息安全防范中,计算机加密技术相对来说比较稳妥,且有一定的技术保障,其能够提高互联网传输过程中的数据安全度数与实用性,是一种主动抵御外来危险入侵的防御策略,可以说是利用最小的成本为互联网信息安全提供最大的保护;能够针对数据传输加以限制,进而将原始数据在硬件或软件方面进行加密设计,使得原文变为代码形式,再通过解密行为还原原文。其中主要分为私用秘钥与公共秘钥两种加密技术。私密秘钥主要为由一个钥匙加密组成,也就是说加密与解密钥匙为同一个,其过程相对简单且代码生成效率较高,但是因仅有一组秘钥,因此保管起来相对存在缺点,一旦秘钥泄露其保密措施也就不存在意义了。而公开秘钥加密技术则加密与解密为两个秘钥,由两个人或一个人保管,即便其中一串秘钥丢失若得不到另一串秘钥也无济于事。其优点是具有一定的保密性,且加密技术较为严谨,一般情况下数据不会发生丢失现象。但是其编程过程存在一定难度,且效率低下,编程时间较长。一般银行系统、工商系统的数字签名较为常见。该技术的使用在人们日常生活也较为常见,如社交软件中的qq□微信、微博等的用户名与密码组合而成才能登陆。而银行系统则为了确保取款、转账等日常银行账户往来为本人亲自操作,常采取此加密技术,也就是数字签名。这种双重保障技术能够确保所有操作为本人进行,且能够保证本人不存在抵赖可能。双重加密技术中建议以编程形式进行加密,并转化为文本进行显示,一旦其中某组符号、编程格式等发生篡改行为,

那么所显示出的文本也将发生一定的变化,这样也就能够保证该加密技术的有效性。

2.3完善计算机信息管理制度

无规矩不成方圆,社会任何角落都需要制度的约束。网络信息安全问题大至国家信息小至个人隐私都有可能受到一定的威胁,因此,在技术方面严格加强,也应辅助以管理制度、法律效应的监督完善[2]。计算机信息安全管理制度是其在网络环境中安全运行的重要基础,能够有效保证其环境的稳定。制定完善的管理制度与法律法规,使得其在使用过程中能够有法可依,有制度约束。阻止不法分子入侵计算机系统,进而保障计算机的硬件、软件有一定的保障,在信息传输过程中能够受到一定的保护。加强网络巡查范围与巡查次数,防止恶意破坏行为的见缝插针。如现在微信的管理不仅仅依靠国家法律,更是微信团队的自身加强防范。虽然市面出售各种多开软件,防封多开等微信外挂技术,但是由于微信严查猛打,以致很多微商的账号被封。且一旦被封三次将永久封号,这对用户的惩罚是非常严重的。以此便有效管理了微信网络信息安全,由于微信内绑有用户的个人信息、银行卡等隐私,一旦被各种微商进行利用将出现巨大风险。因此严查微信多开能够有效规范微商行为,进而减少微信个人隐私外泄的可能,进一步做到网络信息安全防范工作。

2.4加强身份验证技术

计算机使用过程中加强身份验证能够有效保证数据的安全性,且针对基本信息进行保护。针对一切保密文件、保密数据都加强身份验证功能,以此避免不法分子采取不正当手段入侵电脑的可能,防止其窃取用户基本信息。而国家、政府等保密性极强的企事业单位相关数据更应以身份验证技术来完成所有工作。下级不得借助上级身份私自使用电脑,以防止数据窃取的发生。以及区分内外网使用,加强数据防范意识,避免不法分子趁虚而入。现如今国税、地税等系统都采取金税三期软

件,所有关于企业的数据都需要身份认证方可操作。而银行、工商等系统也纷纷使用的身份验证技术,以提高数据保护能力,每个人仅拥有属于自己的身份信息,才能进入自己职权内的数据系统进行操作,即便同属于一个单位也无法数据共享,以此有效避免了同事间的非法行为,确保网络信息环境的安全性。可靠性、稳定性。

3、结语

综上所述,网络信息安全技术管理的计算机应用要与时俱进,跟随现代化发展的脚步,利用先进的科学技术统治网络信息环境,提升技术使用范围与适应范围,同时完善监督管理机制,以确保计算机软件、硬件等设施不受外来入侵的影响,增强智能化使用范围,以提升网络信息安全。

参考文献

[1]刘祥.基于网络信息安全技术管理的计算机应用分析[j].电子制作,(12):74.

[2]桂美坤,李俊.基于网络信息安全技术管理的计算机应用探析[j].科技创新与应用,2016(3):70.

安全技术与管理论文篇三

安全维护管理策略主要体现在以下几方面：健全和完善规章制度、广播电视节目的技术环节管理、强化广播电视人员培训以及加强对广播电视播出系统的维护。

3.1健全和完善电视广播的各项规章制度

广播电视安全播出过程中需要借助一定的规章制度作为管理基础，这些规章制度将会对安全播出工作直接产生影响。在不同的工作环节应有不同的规章制度，因此，需要根据工作

特点对制度进行完善。构建完善、明确的管理目标，依托这些目标开展管理工作，实现节目安全播出。开展具体工作时，通过完善的规章制度约束员工的行为，落实各项监督机制，通过维护广播电视的安全性，保证节目正常播出。此外，通过落实各项规章制度，可以为安全播放提供一个和谐的环境。

3.2强化节目播出各环节技术管理工作

民众作为广播电视节目的受众，其需求呈现多元化。通过及时传递新闻消息，还在很大程度上影响着社会的精神文明发展，对指导社会舆论走向具有重要意义。广播电视的安全播出对播出技术具有较高要求，同时对节目本身质量要求也不断提高，除节目本身价值外，还承载着更多东西，如教育意义、价值普及等。就负责广播电视节目的工作人员而言，一定要有足够的安全意识，在整个节目制作过程中，严格遵守操作规范和相关的规章制度，争取在大家的不断付出和努力下，使节目内容呈现出更积极向上的一面。节目制作完成后，还需要进行细致的剪辑，待部门审核和验收等工作完成后才能播出。在这一过程中，安全检验的一个重要环节就是最终的验收工作，需要严格按照广电总局颁发的规定进行验收检查，确保最终播出质量和效果。

3.3通过培训提高技术人员专业素质

技术人员专业素质直接影响节目播出的安全性，因此，需要重视对技术人员的.培训。随着科技水平影响力的不断提升，广播电视安全播出同样对技术产生较大依赖性。因此，相关部门应定期组织人员进行培训考核，通过邀请专家讲座以及同行之间的相互学习，有针对性地提高从事广播电视职业人员的素养，提高安全播出的可靠性。相关部门还应通过建立激励机制，激励员工进行自行学习，通过明确行业发展需要，以及掌握新兴技术和先进设备，为广播电视的安全播出做出更大贡献。也只有强化广播电视技术人员培训教育工作，才能确保技术人员专业素质满足岗位需求，及时掌握先进的技

术，为节目安全播出保驾护航。

3.4做好播出系统的维护与保养工作

广播电视节目播出通常采用的是连续播出的方式，因此，对播出设备具有较高要求，长时间使用设备导致设备故障率不断提高。在实际生产工作中，故障问题是影响广播电视节目的重要方面。为降低故障影响，需要定期对播出设备进行维护和管理，消除设备运行隐患。随着科学技术进步及互联网技术发展，广播电视播放时不断使用新设备与技术，这对技术维护人员的要求显著提高，需要其不断更新与完善技术知识储备。考虑到以上诸多因素，有必要采取有效措施做好广播电视播出系统的安全维护工作，主要涵盖以下内容。一是制定定期检查、维护制度。通过定期检查与维护的方式，确保数据库、服务器等设备正常运行，确保相关数据的安全，并将其作为数据核心，加强保护，提高广播电视播出的安全性。二是视频播放设备是传输广播电视内容的重要平台，因此，需要对视频播出服务器进行定期检查，同时对读写磁盘的存储情况进行严格检查。视频播放器对整个广播电视顺利播出具有决定性作用，由于每天播出的内容存储量庞大，这种理论性错误发生的概率不断提高。另外，频繁使用磁盘进行存储，将会对磁盘造成损伤，容易导致信息数据缺失。因此，对磁盘的检查应该做到及时，并根据情况做出更换处理。避免磁盘受损影响节目顺利播出，给企业或个人造成经济损失。

4结语

综上所述，广播电视节目在丰富人们精神生活的同时，也受到多种因素的影响，导致安全播出存在一定风险。因此，完善规章制度，提高人员素养，积极完成设备检修，对于保证广播电视安全播出具有极其重要的意义。

参考文献：

[2]刘晓.广播电视安全播出技术及运用实践探寻[j].数字技术与应用,2017(10):206,208.

[3]林远江.广播电视安全播出技术的发展与展望[j].西部广播电视,2017(9):192.

[4]张伟明,康海龙.加强广播电视安全播出技术维护管理探析[j].科技传播,2017(2):14,68.

文档为doc格式

安全技术与管理论文篇四

摘要：网络数据库集数据计算、处理、存储、管理与应用于一身，在相关技术得到迅速发展的同时，也获得了各界的广泛关注与实际运用。在信息化程度日益加深的先进，对数据库进行安全管理，也成为了网络信息系统建设的重要环节。本文将对数据库的安全问题进行探讨，并分析相应的安全管理技术和策略。

关键词：计算机技术；网络数据库；安全管理技术

引言：

数据库安全管理的工作重心应始终放在保证用户信息数据的完整性、一致性、安全性和保密性等方面，通过对硬软件的规律维护、用户账号验证、审核访问操作、数据管理，备份与恢复、建设网络防护系统等措施开展安全管理工作。对此，管理人员应积极加强工作能力的培养，切实落实管理步骤，保证信息安全。

1目前网络数据库存在的安全问题

1.1软硬件的稳定与安全问题

硬件的质量与状态是确保数据库运行稳定性与安全性的前提，若出现硬件故障和问题，可能会导致数据库系统崩溃，信息数据丢失或损坏；系统与软件的安全问题表现在版本落后、漏洞没有及时修复等，若无法及时解决，则可能造成信息数据遗失、或遭泄露、篡改等。

1.2账户认证环节缺乏有效管理

目前数据库的用户密码强度普遍偏低，在账户配置等方面留有隐患，加之账户审核与认证环节缺乏有效管理，严重威胁了数据库的安全。

1.3信息数据加密、备份与恢复工作不到位

数据库运营应时刻防范黑、客攻击和病毒、木马等的入侵，同时也应加强信息的加密、备份与恢复工作，否则可能导致库内信息被轻易破译，或在遭遇非法操作与攻击时无法及时恢复应有状态，对用户造成损失。

1.4管理制度与体系不够完善

目前与网络信息安全相关的管理制度依旧不够完善，法律对影响信息安全行为的打击力度不足，且由于数据库运营方安全管理体系建设不足，安全管理工作多由信息管理员兼任，导致了管理人员工作能力与精力不足、工作效率低、管理措施落实不到位等问题[1]。

安全技术与管理论文篇五

房地产行业是我国的龙头行业，对经济的增长做出了很大的贡献。在房地产行业得到迅猛发展的同时，保证建筑安全和质量是房地产开发应当重视的问题。而如何确保建筑施工过程符合规范、建筑质量达标一直以来都是一个难题。建筑施工是房地产开发的基础，而贯穿全过程的技术管理是房地产

企业管理的重中之重。只有加强施工过程中的技术管理，才能确保建筑质量、有效提高房地产的经济效益。本文就如何加强房地产施工全过程的技术管理进行了分析，并提出了建议。

1施工过程技术管理的发展现状

安全技术与管理论文篇六

建筑工程现场管理指的是通过科学合理的手段对现场人员、设备等进行分配和管理，保证施工的顺利进行。以下将对建筑工程现场施工的安全管理措施进行分析。

1．1制定完善的施工现场安全管理制度

施工单位在建筑工程施工现场施工阶段，要制定完善的现场安全管理制度，保证整体现场管理的.顺利进行。此外基于安全管理的细节以及其他管理要求，要做好内容制定工作，从建筑工程现场实际管理情况出发，进行安全岗位责任管理。此外需要将表面的安全管理进行落实，以对施工岗位、施工

人员以及施工内容进行有效管理，保证施工人员能观察落实现场安全管理。如果存在违规操作或者管理制度不合理的现象，必须严格进行惩罚，保证现场施工安全管理的有效性和完善性。如果存在严重的安全隐患，在施工阶段需要将其控制在有效的范围内［1］。

1．2强化对施工现场隐患因素的控制

施工单位对现场施工安全管理中，要掌握存在的安全隐患因素，对常见的事故影响因素进行分析和控制，从根源上避免出现严重的安全事故，进而提升施工现场整体管理力度。从具体情况来说，施工单位需要明确对各种隐患因素进行分析，做好基础排查工作，选择经验丰富的工作人员对存在的各种安全隐患进行排查。此外选择而经验丰富的施工人员做好安全管理和分析工作，以可能存在的安全隐患管理为基础，采取有效的措施完成对上述隐患以及影响因素的控制，加强对上述隐患以及影响因素的定期检查，保证建筑工程施工现场不会因为粗心大意而出现安全事故［2］。

1．3制定合理的应急预案

施工单位要制定完善的施工管理体系，通过对建筑工程现场进行管理后，确定合理的处置方案，进而实现对施工现场的控制。如何降低施工阶段存在的不利因素，成为技术管理的关键所在，应急预案的落实能做好现状管理，施工单位需要建立专业的安全管理机构，对施工安全事故和类型进行对比和分析。强化现场施工的演练，能保证各项落实有序落实，提升施工管理整体优势。

1．4提升现场管理人员综合能力

施工单位在进行现场管理过程中，需要不断激发施工人员的安全意识，降低安全事故的发生几率。施工人员作为建筑工程的一线工作人员，对施工现象有详细的了解，针对具体阶

段出现的相关异常情况，需要做好强调工作，强化对不符合安全管理要求的施工人员的惩罚，保证施工人员具备安全控制意识，控制好自身安全。为了避免出现粗心大意或者其他想法，要提升建筑施工安全的安全程度，以综合评估为基础，做好整体管理工作。

2如何做好建筑工程施工现象的技术管理工作

施工单位在建筑施工阶段需要做好技术管理工作，强化设计单位之间的沟通和合作，保证施工技术管理符合要求。由于管理设计到的影响因素比较多，需要进行综合管理，最大程度满足安全和施工技术应用要求。

2．1制定完善的现场施工技术方案

施工单位在施工现场的技术管理过程中需要制定完善的施工技术方案，结合技术要求和方案应用准则，做好整体管理工作。从实际情况来说，以技术方案本质为例，只有做好后续管理工作，才能全面的对方案进行统计，同时施工技术的应用能对质量影响因素进行具体的分析和统计。对于施工阶段出现的各类问题，需要有效的对技术方案进行编制，以质量标准规定为例，需要有效的完善各项编制工作，保证施工技术方案符合管理指标，保证整体施工技术得到有效的控制［3］。

2．2落实现场施工图纸审核

施工单位在现场施工技术落实阶段，要做好现场施工图纸的审核和选择，以技术应用指标以及图纸设定要求为例，要对内容进行对比，结合施工技术过程中的具体要求，完成对施工图纸的优化处理。如果在设计过程中不存在意外情况，则要保证施工技术的应用标准符合施工图纸质量要求。施工单位和设计单位、监理单位等要完成施工图纸的会审工作，按照审核机制要求落实。

2．3做好施工材料和设备控制

施工单位在现场施工技术管理阶段，要做好对现场施工材料、施工机械的管理。

2．3.1材料管理在施工过程中，对材料有一定的要求，施工材料只有符合施工要求，才能满足后续施工要求。材料属性比较特殊，对于不同类型的材料要进行完善的管理。材料类型有很多，需要对材料性能、参数等进行审核，同时做好施工机械的调试工作，包括性能检验和材料属性分析等，保证施工材料和设备符合技术要求，为其提供优良的质量支持。

2．3.2设备管理施工阶段应用到多种类型的施工设备，在现有管理基础上要做好性能评估和分析工作。部分设备没有进行维护和保养，进而出现缺乏管理的现象，因此在调试管理过程中，需要对性能指标进行评价，按照参数调试要求进行，保证施工材料和施工机械能够为施工技术的应用提供更加优良的质量支撑。

2．4建立完善的安全管理技术体系

建立和健全完善的技术管理体系，能保证建筑施工的效率和质量。考虑到技术管理的特殊变化，需要成立专门考核小组，对施工管理人员的工作进行定期审核，如果实践阶段存在施工问题，要确保建筑工程的施工质量。其次做好图纸的审核工作，建立完善的审核制度，促进施工人员对工程设计进行了解，使其满足设计指标的具体要求。此外要完善技术管理和交底工作，分项工程施工结束后，进行验收，为下一阶段施工奠定基础。最后成立工程检验和评价制度，工程整体施工后，建筑施工技术管理部门制定完善的质量检验方案，结合建筑行业应用标准以及其他要求，对工程质量进行监督和检查，对于存在的各种问题，尽快进行处理，确保其符合工程质量要求［4］。

3结束语

针对建筑施工现场管理存在的各种问题，在实践阶段需要做好基础管理工作，以现有管理机制为例，为了提升整体竞争力，获得长远的发展，必须做好施工安全和施工技术管理工作。建筑企业管理人员对现场管理要引起重视，做好安全和施工技术管理，保证工程的施工质量和安全落实。同时还要打击质量安全和建筑市场违法违规的行为，实现施工企业安全生产标准化、从业人员标准化和施工设施设备标准化，促进建筑安全施工形势好转。

参考文献

［1］徐朝明．做好建筑工程现场施工安全管理的策略分析□j□□城市建筑，(17)．

［3］谢兴国．浅谈建筑工程施工技术及现场施工管理□j□□江西建材，，(19)．

［4］于宏伟．房屋建筑工程现场施工技术与管理探究□j□□科技创新与应用，(01）．

安全技术与管理论文篇七

3.1防火墙技术的应用。目前，防火墙技术是较为常见且被普遍应用的网络信息安全保护技术。该技术主要针对网络中存在的不安全因素，作为内部网络保护屏障能够有效阻止外网用户在未经授权的情况下访问内部网络，从而防止非法入侵及信息泄露等事件的发生，确保内部网络信息的安全性。防火墙技术通过采取代理服务、状态检测等安全控制方法，将内部信息设置为封锁状态，强化信息安全等级。然后可以根据实际需要合理开放内部信息，这不仅对网络信息起到了良好的保护作用，还方便了操作者的一系列操作。3.2身份验证技术的应用。身份验证技术是当前一种新型的网络信息安全

保护技术，在计算机网络中确定操作者身份。此项技术主要利用特殊的识别技术对当前操作者进行特定的数据识别，以此来判断操作者是否具备使用权限。该技术特别重视对身份认证的需求，经过对相应参数的一一验证，有效保障了参数的有效性和准确性，体现了用户与计算机之间的信任验证机制。由于身份验证技术采用一对一的形式，因此，具有超强的针对性，能够在很大程度上避免非法入侵与恶意攻击等不法行为。对于网络用户来说，能够有效防止网络信息泄漏。现阶段，身份验证技术主要表现形式为生物特征、信任物体及信息秘密。上述验证方式中，生物特征的身份验证实用功能优良且安全系数最高。由于生物特征的身份验证形式有着较大的运行成本，而且操作起来较为复杂，因此，还没有得到普及和广泛应用。目前，网络用户所采用的身份验证方式以信息秘密的验证方式为主[3]。3.3防病毒技术的应用。防病毒技术是一种硬件技术，通过与操作系统的相互配合，保护缓冲区的漏洞以防病毒的攻击。现阶段，防病毒技术主要包括病毒预防技术、病毒检测技术与病毒清除技术。其中病毒预防技术就是通过技术手段阻止计算机病毒感染与破坏操作系统，实用性较强；而病毒检测技术就是利用信息技术手段来识别计算机病毒，以此来判断系统是否存在病毒，如果存在病毒，就会实施相应的处理方案。该项技术主要分为两种类型，第一种类型就是基于病毒程序的检验技术，将病毒的特征、关键词、程序段内容以及病毒蔓延方式作为检测标准。第二种类型就是对某个数据段或文件进行相应的检测与计算，并保存其结果。在之后的运行过程中，经常定期或不定期保存该部分数据段或文件，通过对比检验，能够及时发现文件中存在的数据异常情况。如果数据存在异常则代表病毒已感染了文件，必须及时采取有效的解决措施。3.4入侵检测技术的应用。入侵检测技术也是一种较为有效的网络信息安全保护技术，通过分析操作系统各项指标如审计数据、安全日志或行为等是否存在异常项，来判定具体的入侵行为。入侵检测技术主要包括误用检测模式与异常检测模式两种，一旦检测到入侵行为就会发出相应的报警信号，以此来确保网络信息的安全性。该项技术的顺利实施是建立在入侵检测

系统的基础上，入侵检测系统是由相应的软件、硬件所构成，用来检验计算机网络中是否存在违反安全策略的行为，其在计算机中的应用具有十分重要的现实意义。3.5信息加密技术的应用。信息加密技术主要借助物理或数学技术，对网络信息传输和存储加以保护。该技术以软件加密作为主要方式，最常见加密形式有计算机密钥、保密通信、防复制软盘等。在当前的网络环境中，信息加密技术对于保护网络信息安全起到积极促进作用，为电子信息的机密性和完整性提供保障。在实际应用时，将加密技术与用户密码相结合，能够有效保障网络信息安全。

4结语

综上所述，在互联网时代，网络信息安全面临诸多问题，如软件漏洞、电脑高手、病毒入侵、网络政治活动等，因此，应分析问题存在的原因，并通过应用各种行之有效的网络信息安全保护技术，来提升网络信息安全性，营造一个良好的网络环境。

参考文献

[1]王洁民.浅谈网络信息安全技术管理的计算机应用[j].中国新通信,,20(4):147.

安全技术与管理论文篇八

计算机与互联网技术的普及和应用，使人们的生活方式发生了巨大的改变。大数据时代，网络信息大爆炸，在提高人们工作效率、丰富业余生活的同时，也带来了一定的安全隐患。现阶段，网络信息安全存在诸多问题，制约了计算机与网络技术的进步，因此，应提高对基于网络信息安全技术管理计算机应用的重视。

1当前计算机网络信息安全问题的具体表现形式

1.1计算机软件存在漏洞。由于软件设计具有现时性与局限性，在信息技术发展过程中，会逐渐呈现出软件存在的漏洞和缺陷，一旦不法分子利用这些漏洞做出违法行为，将会造成信息泄漏。而且随着网民数量逐年攀升，增加了计算机软件的使用频率和范围，如果计算机软件出现漏洞，将会导致严重的网络安全问题。1.2感染计算机病毒。当前，我国计算机系统遭受病毒感染情况日益严重。由于计算机病毒类型多样，危害形式也呈现多样化，而且具有超强的潜伏能力和破坏力，难以做到对病毒的有效防范。根据国家计算机病毒应急处理中心的日常监测情况来看，计算机病毒表现出非常活跃的形式。我国大部分计算机用户都曾感染过病毒，感染次数较多，病毒对数据造成的破坏力也较强[1]。1.3电脑高手的恶意攻击。当今社会中，存在着数量众多的.电脑高手，他们或单独行动攻击目标电脑，或有组织、有团队地进行集体犯罪。网络信息系统具有开放性，极易受到攻击，导致电脑高手的攻击行为异常猖獗，对其进行位置追踪定位会花费大量时间，不利于及时抓获犯罪嫌疑人，这给我国网络信息安全带来了极大的挑战。1.4网络政治活动频繁。近些年来，一些国内外的反动势力通过互联网拉帮结社，并展开了一系列非法活动，其行为猖獗频繁，目前仍无法将这股势力连根拔除。特别是有些非法组织，利用网络渠道，大肆宣传歪理邪说，企图扰乱社会人心，影响社会的正常秩序。

2造成计算机网络安全问题的原因分析

2.1网络的开放性。网络信息传播速度非常快，具有开放性的特点，使得网络上的信息人人都可以共享。在给人们带来便利的同时，也造成了一定程度的信息安全问题。如果这些共享信息被某些不法分子所利用，开展网络犯罪活动，将给人们带来不可挽回的损失。而且很多网民自身缺乏较强的安全意识，给不法分子提供了可乘之机。2.2病毒感染的风险长期存在。随着网络技术的发展，病毒的传播形式也在不断变化。当前，病毒能够通过网页、邮件、文件等各种途径大肆传播和蔓延。由于病毒带有自动启动功能，通常会潜入被感染电

脑系统的核心或内存中，进一步破坏计算机系统，严重的还会中断计算机网络数据传输，导致系统瘫痪无法运作。2.3防范机制不够规范。我国很多单位在管理制度上都缺乏完善的安全防范机制，在运行过程中，欠缺切实可行的安全检查与保护制度。由于制度的不完善滋生了内部管理人员的违法犯罪行为。与此同时，信息安全的保障法规还不够完善。所制定的法律法规实用性差，细节问题不够明确。基于上述现状，网络上个人信息与商务信息的安全性很难得到保障[2]。2.4缺乏高水平计算机人才。想要确保计算机网络信息安全，则需要计算机领域的高精尖人才。我国计算机技术起步较晚，人才培育机制还不够完善，使得我国计算机技术研发与管理方面的专业人才十分匮乏。基于此种现状，对于网络安全的维护很难达到预期效果。此外，我国计算机人才的薪资制度与晋升制度还不够科学合理，导致计算机人才流失情况严重。