计算机系统以及计算机网络安全的研究

张兴东

华电能源股份有限公司牡丹江第二发电厂　黑龙江　牡丹江　157015

【摘要】如今，计算机技术在人类社会的各个领域都扮演着不可替代的角色。由于网络的开放性，该设施为网络犯罪提供了机会，并且信息安全威胁正在逐渐增加。

【关键词】计算机系统；计算机；网络安全

如今，网络安全正成为人类研究的焦点。在世界各国遭受上，经常发生计算机病毒或黑客攻击，这破坏了信息人们的正常生活。因此，加强网络安全性变得越来越重要，并且预防性计算机病毒在世界各国越来越受到关注。

1 维护计算机系统和网络安全的必要性

计算机系统安全性，是指保护计算机以获取内部信息，设备和功能的工作。保护计算机信息安全，防止未经授权访问，更改和盗窃计算机内部信息。设备安全性主要与计算机的物理安全性及其支持设置有关。硬件安全性可以为系统提供可靠的内容管理环境。保护功能包括在正常运行期间检查系统并从故障中恢复的能力。网络安全主要是指内容的安全和信息传输的安全。信息内容的保护包括信息的可靠性和机密性。传输安全性是指用于通过网络传输信息的计算机安全管理技术。在当今社会，维护计算机系统和网络的重要性和必要性变得越来越重要。人们的生活越来越依赖互联网，并且社会各个领域的日常工作和商业与互联网有着千丝万缕的联系。同时，来自病毒和黑客的威胁正在上升。网络安全影响着整个社会的经济发展。社会和个人应特别注意网络安全的重要性，提高对安全措施，计算机系统和技术资源的认识，以实现网络安全，并确保信任网络的人们的稳定和社会生产的发展[1]。

2 计算机的系统安全问题

实际上，如果您的计算机出现故障，则不能保证计算机的安全性。该漏洞的核心是未经过管理人员许可的情况下，却可以访问高层次软硬件。这是计算机系统中的第一类缺陷，包括物理漏洞，软件漏洞和不兼容的漏洞。其中第一种是管理人员不许访问的地方，而在系统集中的过程中，各部分之间存在许多差异，并且安全性能无法满足相关标准。此外，计算机系统中的漏洞主要存在于数据库，开发工具和应用程序等操作系统中。一旦系统正式运行，随着时间的流逝，系统中的缺陷就会变得明显。要完全消除漏洞，请根据系统版本和当前状态仔细分析漏洞，并找到彻底消除漏洞的方法。系统安全性对于确保计算机的稳定运行非常重要，所谓的系统安全性的本质是存储在计算机中的信息，可以在计算机系统和所有连接的系统运行时对其进行正确处理。您可以继续正常运行，当然，外部环境也会影响计算机系统的行为。例如，一些员工的技能水平较低，并且会犯一些操作错误。根据调查，由于工作不正确，导致出现系统错误。例如，某些意外删除的任务会从系统中删除一些信息，数据和重要程序，例如有害软件和病毒软件。随着科学技术的进步，病毒软件也变得非常强大。许多病毒程序通过使计算机系统瘫痪的缺陷渗透到计算机系统中，不仅使您可以正常使用计算机系统，而且还会泄漏和损坏您的个人信息。在正常情况下，影响计算机网络安全性的因素可以分为几个主要方面。首先，是计算机犯罪，故意更改或删除对计算机网络上的所有者有用的信息或破坏网络通信设备。其次，比如极端天气事件（例如强风暴和地震）之类的环境影响影响了计算机系统网络的正常使用。第三，关于计算机病毒的影响，如果计算机系统正在运行，则病毒的存在会使计算机系统瘫痪，并损害软件系统和用户信息。情况很糟时就是这种情况。它还会损坏您的计算机[2]。

3 计算机网络安全隐患

3.1 网络检测和管理技术水平较低

根据结果，黑客入侵和病毒的迅速传播是信息时代网络安全的两个主要威胁。为存在而开发在线安全系统的复杂性已经对构建相对安全的在线环境产生了很大的影响，并且还在不断增长。随着社会的发展和时代的到来，计算机网络趋向于与科学技术的进步保持同步，而忽略了可以传递给电脑黑客的日益增长的电脑黑客或干扰水平。别小看他尽管存在这种网络发展状况，网络安全仍需要对网络进行即时监视，以根据目标技术逐步提高和提高技术人员的整体专业水平和专业资格。关于计算机网络安全的当前状态，网络安全监视技术日益暴露出越来越多的问题。由于技术人员的数量有限，网络运行的安全性受到严重损害，并且难以及时确保、高效的预期效果，大量数据丢失对网络，专业和个人工作以及增长的预期影响已受到严重影响[3]。

3.2 内部管理不到位

内部管理系统的缺乏和内部人员的综合能力直接关系到内部管理问题的出现。由于员工无法实施特定且详细的、高效的预期效果，，因此网络安全管理内容的实施无法实现有效的网络安全应用程序的预期效果。缺乏成熟和高素质的内部员工。从在线数据库中窃取基本

内容时，网络数据的安全运输也因此难以得到保障，各类严重程度不同的网络安全事件频频发生。

4 计算机网络安全防范策略

4.1 要建立完善的网络安全系统

最重要的方法是为计算机病毒和黑客安装防火墙。在 IT 操作中，防火墙实施实时保护。如果发生病毒攻击或黑客入侵，第一个问题就是防火墙发生了什么。防火墙会及时发出警告和阻止。如果有可能以数据形式传输危险信息。您需要在计算机的防火墙中对其进行编码。如果配对异常，将很快发出警报。在计算机上工作的过程是启动内部程序和应用程序的过程。如果发现未知或无法区分的信息，则可以通过运行内部防火墙来减轻安全威胁的影响。个人无法访问其个人网络帐户。此操作还可以删除系统，这些系统将在未经授权的情况下自动删除。用户使用计算机时，它将执行早期检测，更新防病毒和防火墙系统以及更新内部软件。下载程序时，用户必须首先确定软件的安全性，然后执行安全性管理并立即响应与维护磁盘存储的安全性有关的任何问题。

4.2 强化用户安全防范意识

频繁出现网络安全问题的主要原因是缺乏用户安全意识。因此，相关部门有责任以普遍接受的方式对用户进行安全性教育并尽可能延迟使用计算机安全性。创建一个信息平台。首先，信息平台的相关管理人员需要一定程度的在线交流和分析。这将为管理人员充分了解其功能并维护信息平台网络的安全性创造必要的条件。它有助于提高人们对网络安全性的认识，并促进个人和网络的安全使用。其次，信息平台人员必须进行了解与分析，以识别常见的网络安全问题和诸如特洛伊木马病毒审查之类的一般网络安全问题，以便更多的人可以找出导致它们的原因。确保进一步实现居民用完安全。另外，最重要的一点是提高信息平台上的员工的培训质量。促进和确认正确的价值观和职业道德是信息平台机制平稳，稳定运行的严格条件。专长和专业知识技能是任何工作的先决条件。提高员工工作的整体质量有助于对可疑代码进行分析并做出有效响应，以确保信息平台的在线安全。

4.3 要加强杀毒软件的运用

防火墙是用于防御网络病毒的有效系统，但是如今，许多新病毒可以轻松绕过防火墙并危及计算机的安全性。因此，除了防火墙设置之外，根据对新病毒特征的分析，还需要安装防病毒程序以防止各种病毒并改善针对病毒的计算机防病毒软件的管理。例如，在害病毒“想哭”扩展迅速阶段，当一位外国工程师在终端上工作时不小心打开了病毒清除开关时，他找到了一种控制病毒的方法。注意病毒的传播。由于技术的进步，不经意触发该病毒自杀开关，并且管理变得困难。如果最终用户发现了勒索病毒的痕迹，他们可以请专业技术人员来提取信息。由于病毒具有副本，因此防病毒程序会在计算机启动并运行时对其进行检测，并采取措施来防止计算机运行。研发人员逐渐开发了防病毒技术，以提供更高的网络安全性。因此，技术人员应鼓励使用防病毒软件，以确保计算机的安全使用[4]。

5 结束语

通常，在信息时代，随着计算机网络用户数量的增长，在计算机网络技术以前所未有的水平发展的环境中，网络安全问题逐渐使人们在使用网络时的注意力转移。加强网络安全管理，保护个人信息，提高资产安全性，保护受威胁企业和国家的网络安全运营，确保企业或国家机密安全。通常，解决网络安全问题是当前的首要任务。计算机网络技术及其重要性显而易见，确保整个安全系统的正常运行非常重要。

【参考文献】

[1] 张玥，胡璨．大数据环境下计算机网络安全技术的优化策略 [J]．中国信息化，2021(04):74-75.

[2] 童瀛，姚焕章，梁剑．计算机网络信息安全威胁及数据加密技术探究 [J]．网络安全技术与应用，2021(04):20-21.

[3] 庄世伟，王斌．计算机网络信息安全管理策略探析 [J]．网络安全技术与应用，2021(04):157-158.

[4] 杨国富．计算机网络信息安全与管理初探 [J]．网络安全技术与应用，2021(04):158-159.