

信息安全背景下计算机软件技术开发与使用的措施

聂红伟

太原航空仪表有限公司 山西 太原 030006

【摘要】随着我国经济的发展,网络 and 现代信息技术得到了普及,但是信息的安全也成为了人们关注的问题。所以,在当前网络和信息安全隐患的环境中,计算的软件开发和使用应该更加注重安全性。只有计算机的软件足够安全,才能在最大程度上避免用户信息泄露的情况。所以,相关技术人员在开发和研究计算机软件时应该首先考虑软件运行的安全性和稳定性,为用户带来更好的使用体验,并推动我国计算机技术和软件开发的进步,为社会经济的发展贡献力量。

【关键词】信息安全; 计算机软件技术; 开发使用
引言

在互联网信息技术时代,个人、企业、社会国家的信息安全性和保密性受到的威胁越来越多。在计算机软件开发的过程中,不仅要保证数据信息传输的效率质量,还要确保整体运行环境的安全性。为了避免数据信息泄露,保证良好的计算机开发和运行环境,必须要进一步把握安全技术。

1. 计算机软件开发与安全技术

计算机软件开发是技术人员编写软件系统或软件程序的过程,在开发的过程中包含要求捕捉、规划、分析设计及测试等程序。计算机程序软件的开发离不开互联网技术的应用,突出的开放性是造成安全隐患的主要原因,当前,计算机系统软件也处于快速更新迭代中,内部病毒的种类不仅越来越多,而且千奇百怪,在软件编写和应用的过程中,常会被病毒侵害,致使内部信息泄露,用户造成难以弥补的经济损失、名誉损失。因此,在计算机软件程序的开发中,必须要重视安全技术,以此来有效防御外来的风险,实现全方位的安全防护,保证计算机运行过程中稳定性和安全性。

2. 计算机软件的主要安全隐患

2.1. 软件运行隐患

计算机软件运行过程需要及时满足计算机本身的功能需求,若系统运行过程中有部分木马、蠕虫、病毒入侵计算机,可能会给予不法分子一定机会。比如不法分子可通过破坏防火墙,窃取计算机软件中的客户资料、用户信息,导致软件本身出现瘫痪现象,实现计算机软件破译的目的。为了消除软件运行过程中的安全隐患,工作人员应当及时完善软件本身的功能,分析出不同软件的运行需求,在安全防护支持下消除软件运行隐患。

2.2. 人为因素

人为因素主要是由于个人或企业内网、计算机软件

动态被不法分子破译,不法分子修改了用户本身的基本资料,或者是随意读取了不同形式的文件,影响了企业的正常发展,也可能会导致企业机密信息遭到泄露。另外,计算机软件病毒也会危害软件的功能性和安全性,一旦病毒入侵商业或个人电脑,致使部分信息遭到破坏,限制了企业的发展。因此,工作人员应当做好计算机黑客病毒的防护工作,尤其是要确定针对性、广泛性攻击的特点,在网络监管、杀毒软件的支持下快速确定出黑客的基本资料,消除虚拟网络对计算机疯狂攻击的影响。

2.3. 系统设备受损

当计算机系统设备受损或出现运行故障时,会给整个计算机运行系统造成严重的影响,不仅会使研发人员的数据信息丢失,还会延误整个程序项目开发的进程,甚至对研发系统网络造成严重破坏。在以往的计算机软件程序开发项目中,系统设备受损的情况相对复杂,例如,人为操作技术的干预、电路故障、线路老化等,如果在开发设计中未采用有效的安全技术对这些故障干扰进行有效控制,就会造成整个计算机网络的运行故障,甚至电脑硬件系统出现瘫痪,直接造成研发项目责任方与用户的经济损失,因此,在进行开发计算机软件的过程中,程序编写人员应全方位检查计算机的系统硬件设备。除了定时设备清洁除灰,还要做好电路的检查,加强设备养护,从源头上提供更安全的运行环境。

3. 信息安全背景下软件技术开发与应用对策

3.1. 软件开发升级工作

为了全面实现软件开发工作的升级,相关技术人员应该积极研究计算机本身的系统,对不同的运行系统和建设方法并提出自己的建议。其次,信息的处理和使用也应该根据软件的工作流程和专业性,对信息做进一步的分析。比如,一款属于工业作业的软件,那么在使用和分析该软件时就应该分析其在不同情况下的运行状况以及对信息的收集和分析能力。当发现该软件在性能

上存在漏洞时,技术人员就应该及时对软件进行升级和补充,确保其安全性,使其能够在网络环境中长久工作。此外,软件的运行方案也应该做出相应的调整和升级,只有这样才能使软件更好地运用于实际生活中。

3.2. 防火墙和信息加密技术

防火墙技术属于相对传统的计算机安全技术,然而却是能够有效隔绝恶意攻击的重要安全技术,其本质是一个在内网与外网之间安装的通行保护屏障。该技术在使用的过程可以把不安全的网络信息彻底隔绝或隐藏起来,以此来为整个计算机运行网络构建出一个安全稳定的环境。在计算机软件运用的各个环节,涉及内部网络内所有的访问与传输信息都必须要通过防火墙的持续检测,且待检测达标后,才允许开展访问。从某种层面上来说,防火墙具备有效规避和阻挡木马病毒、违法分子以及恶意程序等内网访问行为的实力,可以切实为计算机软件开发工程提供了优质且安全的环境。不仅如此,对于开发工作来说,防火墙还可以作为极其牢固的数据保护屏障,根据内部的各种网络性能的需求,做出合理且智能的划分并对关键网段进行隔离,以此来保证计算机系统的平稳安全运行。

3.3. 应用病毒检测技术

计算机病毒对计算机系统的伤害是致命的,所以相关技术人员在进行软件开发时应该利用病毒检测系统,

帮助计算机系统分析数据,当发现计算机数据遭受威胁时及时进行排异处理,禁止有害数据进入到计算机系统中去。这种对病毒检测技术的应用是从源头上禁止危害信息入侵的方法,对计算机系统的安全有着重要的作用。因此,相关人员在开发软件时应该充分利用病毒检测技术。此外,在开发信息软件时,相关人员还可以将防火墙技术应用到计算机系统中,提高计算机系统的安全性。

4. 结束语

综上所述,为了消除计算机软件技术安全问题隐患,工作人员应当了解到软件技术安全隐患的直接影响,探讨出正确的、创新的、科学的、合理的处理思路和处理方式,在发现问题、评估问题的基础上解决软件技术隐患,以期进一步提高软件的功能性。

【参考文献】

- [1]许海楠.信息安全环境下计算机软件开发[J].电子世界,2021(19):13-14.
- [2]窦青嵩.浅谈信息安全环境下的计算机软件开发研究[J].信息记录材料,2021,22(01):27-28.
- [3]付国龙.探究信息安全环境下计算机软件的开发[J].信息与电脑(理论版),2020,32(01):65-66+69.
- [4]王亚辉.软件开发过程中的信息安全管理[J].信息系统工程,2019(09):70.