信息安全环境下计算机软件的开发与应用策略

韦焯思
广东培正学院　广东　广州　510830

摘　要：网络和信息安全不仅关乎电子政务健康发展，也同国家安全保障体系建设密不可分。随着“互联网 +”技术迅猛发展，海量数据蜂拥而至，对信息安全建设提出了更高要求。计算机软件开发及应用是保障信息安全建设的根源所在，必须深化研究相关理论。立足于信息安全背景，深入研究计算机和软件开发及应用的现状十分必要。

关键词：信息安全环境；计算机软件；开发；应用策略

现今，网络与信息技术的身影已经无处不在，在给人们生产生活带来极大便利的同时，网络信息安全问题也不可避免的出现在人们的视野，个人隐私安全也受到了极大挑战。因此，在互联网络高速发展的今天，维护互联网络安全就显得尤为重要。本文就信息安全环境下计算机软件芙蓉开发与应用策略进行探究希望能为计算机软件开发和使用提供一定的参考。

1 计算机软件的概述

在计算机发展历程中，软件开发一直居于重要地位。具体而言，计算机软件的开发应用能够实现计算机技术层面的创新，也深刻影响计算机远程操控和长期发展。现阶段，计算机信息安全问题受到广泛关注，一个完善的保障系统能够维护计算机信息安全，对计算机软件的开发应用有着重要促进作用。与硬件制造不同，软件是由软件开发人员通过相关知识、技术与智力而开发的。通常情况下，硬件产品偶尔存在误差，不会引起较严重后果，而软件产品不允许存在一点误差，优劣并不能即时区分，直到程序开始运行才能知道，这给许多企业生产和管理带来诸多困难[1]。

计算机软件是程序和文档的共同集成，是用户与硬件之间的接口界面，依照性能用途可分为系统软件和应用软件。系统软件是计算机硬件系统的基层软件，负责管理计算机系统中的各类硬件和软件资源，保障协调计算机工作的正常进行。应用软件是为达到某种特定用途而开发的软件，即为满足不同领域、不同需求的用户而开发的软件。换言之，应用软件是利用计算机解决既定问题而设计的程序集合，可供多用户使用。

2 计算机软件技术开发与作用

相关技术人员在研究和开发计算机软件时应该了解现有的计算软件开发技术。当前在技术软件开发中有C语言、VB技术、Java技术。在这三种技术中， 我国计算机技术人员对C语言 运用较多并且该技术也较为成熟。C语言的使用范围较大，不仅包括符号，还包含运算处理和一致性，对C编程的实现有着很大的帮助。其次，Java技术是可以跨平台进行使用并且安全性比较高，很多计算机软件的开发都要借助Java技术，该技术能够在一定程度上弥补C语言技术上的缺陷，并且可以改正编程的错误，具备垃圾回收的功能。最后，VB技术是软件编程语言范畴的技术，主要是对企业软件的快速开发以及对传统编程界面的可视化转变，该技术对计算机软件的开发和使用有着很大的帮助[2]。

计算机系统对软件的开发和使用有着较强的依赖性，所以软件技术的开发对计算机技术的进步非常重要。首先，当计算机内部缺乏软件支持是就很难发挥其系统的作用。但是并非所有的软件都能够与计算机系统完美结合，由于计算机之间的差异性，一些计算机在使用软件时会不匹配，这种不兼容的情况，对计算机的系统产生消极的影响。所以，相关技术人员在开发计算机软件时，应该根据不同计算机的特点进行，确保软件的开发能够为计算机系统带来更大的好处，充分发挥计算机系统的价值。

3 信息安全环境下计算机软件开发与应用受到的冲击

3.1 信息安全性

在网络信息的安全隐患下，软件开发人员在开发软件时首先要关注软件对个人信息的保护性，这也是软件开发的核心要求。所以，相关技术人员在设计软件系统时，应该确保软件本身可以防范病毒以及信息被盗的风险。但是就当前的信息攻击手段和软件的开发形式来看，在软件开发技术进步的同时各种新型的信息攻击和窃取手段也在更新和优化，最为明显的是大数据和云计算技术。这两项技术在为人们带来便利的同时，也使用户的个人隐私遭受安全隐患问题。云计算和大数据依托于ATP，并且在用户使用软件的过程中会自主监测用户的使用习惯和兴趣爱好。这也意味着在这种背景下，软件

的开发以及信息安全的难度也在不断升高。

3.2 运行稳定性

当前，大部分开发的软件在整体运行的过程中，会对计算机的原有软件和系统的工作造成一定程度的干扰。这类负面的干扰主要呈现为：一是对计算机内部系统的软件以及信息的原有信息的安全保证机制失去效果，致使系统没有足够的安全保障能力。二是开发的软件对于计算机原有软件来说属于外来物，所以会对计算机的原有构架产生影响，其最直接的结果便是软件在后期的运行过程中会因为底层的结构遭受破坏而无法按照原有的设定进行工作，软件运行的不稳定性，降低了计算机的安全性能[3]。

3.3 管理流程性

在网络环境中，信息的处理应该根据特定程序，在相对安全的环境中完成工作任务。在目前的信息管理工作中，那些原有的工作流程看似已经完成了对信息的管理和处理工作，但是从实际的工作角度出发，原有的信息管理流程只是对信息投方者的监管，并没有将其他信息的投放纳入信息管理的框架中去。除此之外，当前，现有的信息管理流程的工作机制与流程运行下的工作机制有着很大的区别。 这也就代表着，如果信按照当前的模式对信息进行处理，很难确保信息的安全性。

4 信息安全环境下计算机软件开发与应用策略

4.1 合理的应用信息加密技术

信息加密技术是利用一定数字或物理手段对传输过程中的电子信息进行加密，保证用户网络信息的安全性，并维持系统运行稳定。信息安全背景下，信息加密技术在计算机软件开发中的应用可进一步加强计算机的保密性。信息加密技术可通过实时监控和追踪制止黑客对计算机内部的攻击行为，有效避免恶意病毒软件的侵入，从而保证用户信息安全。针对不同学科领域，计算机软件开发可采用不同信息加密技术。对传输信息的加密处理能够实现文字信息与密文信息的转变，读取人需要获取正确解密方式才能实现对信息的解读。密钥是计算机信息加密的基本方法，且数量多、私密性强，原因是计算机信息传输量较大，且密钥的基本形式极其相似。如果被泄露，那么将会导致信息被窃取的风险。为高效保证信息安全，用户应尽量做到一个信息一个密钥，即降低同一密钥的使用频率。为此，相关工作人员可建立一个网络安全密钥配置中心，帮助各用户在与配置中心交流过程中仅可获得一个安全密钥，继而计算机用户将会提高对信息保密工作的需求，同时避免同一密钥的多次使用，以保证密钥安全性。此外，量子加密技术可通过自身量子态变化即时检测计算机是否受到攻击的，同时能够加大对密钥的保护性。当黑客攻击系统时，量子态会即刻发生特定变化。用户可根据量子态的变化及时判断信息是否被攻击，并采用对应措施，尽可能减少在数据信息方面的损失[4]。

4.2 加强病毒入侵检测

信息安全背景下，病毒入侵检测是对计算机防火墙的完善补充。通过阻挡网络黑客对计算机系统的攻击，提高计算机系统的安全管理效率，为计算机的安全使用营造良好环境。病毒入侵检测技术可通过收集信息连接网络中的不同关键点， 并进行分析。一旦计算机系统出现与网络安全行为不符的情况，便会被及时发现。 同样地，病毒入侵检测的应用主要通过采集计算机安全系统信息，并将获取的信息引入监测系统进行分析，进而判定系统中是否存在病毒程序。 一般情况下， 病毒是通过数据传输和网络接入而形成的。基于病毒的感染性质特性，病毒入侵检测须与其有联系的网络平台进行全面监测。当数据信息存在威胁性，则实行排异处理，再彻底检查计算机系统，确保没有影响计算机系统的正常运行。一旦发现计算机系统中存在病毒因素或者程序， 需要对其彻底分析，并增添相应防火墙。

此外，面对当前计算机盗版软件占据主导地位，而正版软件使用相对较少的问题，应加强计算机软件优化配置，从根本上解决计算机信息安全问题。企业应定期更换计算机硬件设备，且软件安装过程中尽量选用正版软件，并定期修复漏洞。

4.3 云计算环境下的计算机安全保护

云计算的环境以及网络的复杂性很容易产生一些安全问题，所以在这些环境下需要提高计算机软件对信息的辨别能力。因此，相关人员在开发软件时不仅要从技术方面下手，还要优化云计算环境下的管理制度，确保计算机信息的安全。 此外，计算机是软件载体，所以只要计算机足够安全那么病毒以及不良信息就无法通过网络侵害计算机，因此计算机软件开发人员在进行软件开发和使用时应该严格把握计算机的硬件设施和芯片的质量，防止硬件上携带病毒侵害计算机。 只有在云计算环境下确保计算机的安全，才能为用户提供更好的使用体验，并推动计算机软件开发技术的进步[5]。

4.4 数据集中化安全防

在我国信息技术飞速发展的同时用户信息也面临着安全问题，这些信息不仅包括用户的个人信息，更有国家相关信息，所以加强计算机信息安全的任务非常重要。因此，计算机软件开发人员应该利用数据的集中化

管理，提高信息的安全性。首先，要对数据进行集中化全方位的监控、分析，维护网络安全。其次，需要相关人员对信息和数据的边界做好防护工作，整合软件资源。此外，软件在实施的过程中也要发挥维护计算机信息的价值。

4.5 强化信息安全保护

复杂的网络环境下，用户的个人信息以及企业的信息频复杂的网络环境下， 用户的个人信息以及企业的信息频高度依赖现代信息技术和电子移动设备，所以和各种APP层出不穷。人们借助计算机技术和各种软件实现了社交自由、购物自由，但是这些软件大多需要用户实名登记，并且对用户所使用的电子设备有着访问的权限，像相册、录音、定位等，方便人们生活的同时也对其个人信息造成了一定的隐患。因此，加强用户的网络安全意识是非常重要的。首先，用户在使用软件时涉及到转账信息等个人财产问题应该谨慎起来， 提高安全认知。其次，对于重要的文件应该设计安全指数较高的密码，并在计算机上安插安全系统，确保信息的安全性，避免信息泄露。此外，为了防止不法人员窃取密码，用户应该避免同一密码多账号使用，减少损失。最后，提高网络安全意识，不要点击和浏览不明网站。这些方式是在使用过程中避免信息的泄露以及病毒的入侵，对用户个人隐私的保护有着重要作用。国家还应该加强对网络环境的监控严厉惩罚信息窃取者，为用户营造较为安全的网络环境。软件开发人员在开发软件时也应该重视软件的安全问题，尽可能提高自身的专业素养，确保所开发出的软件具有较高的安全值数，维护用户的信息安全。另外，计算机技术人员应爱时时关注软件的安全性，及时发现软件中的漏洞，分析问题并找出最佳的解决方案，优化软件。只有提高软件开发者以及用户的网络安全意识，才能最大程度上避免信息的泄露，促进计算机技术的进步，使我国计算机技术在互联网环境下健康持续发展。

4.6 提升工作人员素质

信息安全背景下，计算机行业对软件开发人员专业技能和职业素养的要求与日俱增。一方面，软件开发过程中，企业要求相关研发人员可通过积极参与培训教育不断提升自身专业技术和知识，从而研发先进、优质的计算机软件。另一方面，随着信息技术的高速发展，计算机行业竞争愈演愈烈。企业内部人员流通较大，一旦企业内部研发人员出现职业道德低下的问题，易导致核心技术泄露或者软件漏洞问题的出现。因此，信息安全背景下，第一，企业在开发软件过程中需要不断提高相关技术人员的道德素养，以保证软件开发的正常运行，从而推动行业长期发展。第二，专业技术人员能够定期维护计算机，保证计算机软件得以长期合理应用。第三，软件开发人员可定期实行跟踪研究，并根据情况实行检测，从而全面了解软件实际使用情况，对软件使用过程中存在的问题及时更正。第四，高水平的技术研发队伍在开发软件时会将创新因素融入开发过程，以提升计算机创新价值。

结束语

总之，随着我国经济的发展，网络和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。因此，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。

参考文献

[1]钟琨.新时期计算机软件开发技术的应用及发展趋势[J].网络安全和信息化,2022(2):28-30.

[2]方自远.安全环境下计算机软件的开发与应用分析[J].无线互联科技,2019,1 6(18):46-47.

[3]薛茹.信息安全环境下的计算机软件开发探讨[J].南方农机,2019,50(09):238.

[4]谢雨博.信息安全环境下计算机软件的开发与应用探究[J].无线互联科技,2021,18(07):43-44.

[5]王建齐.信息安全环境下计算机软件的开发研究[J].无线互联科技,2021,18(7):54-55.