计算机信息安全技术及防护措施

黄　波
四川卫生康复职业学院　四川　自贡　643000

摘　要：随着计算机科技的不断发展，计算机信息已经成为人们日常生活及企业、机构的重要资产之一。与此同时，网络攻击、黑客入侵、病毒感染等安全问题也日益严峻，对计算机信息安全的保护提出了更高的要求。本文将详细介绍计算机信息安全技术及防护措施，希望为读者提供有益的参考。

关键词：计算机；信息安全技术；防护措施

1 计算机信息安全技术

1.1 密码学

密码学是计算机信息安全的核心技术之一，它是通过加密技术保护敏感信息，使其在传输、存储或使用过程中不被非法获取或篡改。密码学主要包括对称密钥加密和公钥加密两类技术。对称密钥加密是指使用相同的密钥进行信息加密和解密。其优点是加密解密速度快，但缺点是密钥容易被破解，安全性不够。公钥加密是指使用一对密钥进行信息加密和解密。公钥是公开的，而私钥只有信息接收方知道。公钥加密的优点是密钥更加安全，但缺点是加密解密速度较慢。

1.2 防病毒技术

防病毒技术是指通过特定的软件或硬件设备，对计算机系统中的病毒、木马、间谍软件等进行检测、隔离和清除，从而提高计算机信息系统的安全性。防病毒技术主要包括实时监控、定期扫描和病毒库更新等措施。实时监控是指运行在计算机系统中的软件，能够实时监测计算机软件和文件的变动，并及时进行病毒检测和清除[1]。定期扫描是指定期对计算机系统中的文件和软件进行全面扫描，以查找和清除潜在的病毒、木马等。病毒库更新是指更新防病毒软件的病毒库，及时查找和清除最新的病毒。

1.3 防火墙技术

防火墙技术是指运行在计算机系统中的硬件或软件设备，通过对网络流量的监控和控制，来保护计算机网络和信息系统的安全。防火墙技术主要包括包过滤和应用程序过滤两种技术。包过滤是指根据预设规则对数据包进行过滤和阻挡。它可以控制网络流量协议、目的IP地址、源IP地址和端口等。应用程序过滤是指根据应用程序类型对流量进行控制和监测。它可以防止未授权的应用程序访问网络。

1.4 安全监控技术

安全监控技术是指通过设备、软件或方法对计算机网络进行全面监控和分析，以发现并解决网络安全问题。安全监控技术包括网络流量监控、入侵检测和漏洞管理等技术。网络流量监控是指通过对网络流量进行定期监测和分析，及时发现异常流量和攻击行为，有效保护网络系统的安全。入侵检测是指通过设备和软件等工具对网络系统进行检测和分析，以发现并及时报告入侵事件，保障网络系统的安全。漏洞管理是指通过定期检查网络系统中的漏洞，并及时修复和升级相关软件和设备，以保障网络系统的安全性[2]。

2 安全技术防护的主要内容

2.1 网络安全防护

网络安全防护是计算机信息安全技术防护的重要组成部分。其主要内容包括网络防火墙、入侵检测与防御、网络隔离与穿透技术、网络安全审计与监控等。网络防火墙是一种常见的网络安全防护手段，它可以对网络流量进行过滤，阻止恶意流量进入内部网络。入侵检测与防御技术则是对网络进行实时监测，及时发现并阻止入侵行为。网络隔离与穿透技术则是对内部网络进行分区隔离，提高网络的安全性和可靠性。网络安全审计与监控技术则是对网络运行情况进行实时监测和记录，及时发现并处理异常情况。

2.2 数据安全防护

数据安全防护是计算机信息安全技术防护的核心内容之一。其主要内容包括数据加密、数据备份和恢复、数据权限管理等。数据加密是保护数据安全的重要手段，通过加密技术可以将敏感数据转换成无法识别的密文，防止未经授权的访问和窃取。数据备份和恢复则是对重要数据进行定期备份和恢复，确保数据不会因为意外事件而丢失。数据权限管理则是对不同类型的数据设置不同的访问权限，确保只有经过授权的用户才能访问敏感数据[3]。

2.3 终端安全防护

终端安全防护是计算机信息安全技术防护的基础。其主要内容包括终端安全认证、防病毒软件、安全补丁管理等。终端安全认证可以确保只有经过授权的用户才能访问终端设备，防止未经授权的访问和攻击。防病毒软件则是对终端设备进行实时监测，及时发现并清除恶意代码。安全补丁管理则是对终端设备进行定期更新和升级，修复系统漏洞和缺陷，提高终端设备的安全性和可靠性。

2.4 应用安全防护

应用安全防护是计算机信息安全技术防护的重要组成部分。其主要内容包括应用程序安全、访问控制、身份认证等。应用程序安全可以确保应用程序不会因为漏洞和缺陷而被攻击者利用。访问控制则是对应用程序进行权限管理，确保只有经过授权的用户才能访问应用程序。身份认证则是对用户进行身份验证，确保用户的身份真实可靠，防止未经授权的访问和攻击[4]。

2.5 应急响应机制

应急响应机制是计算机信息安全技术防护的重要组成部分。其主要内容包括应急预案、应急响应小组、应急演练等。应急预案是对可能发生的突发事件进行预先准备和安排，确保在突发事件发生时能够及时响应和处理。应急响应小组则是由相关人员组成的专门小组，负责对突发事件进行调查和分析，制定相应的处理措施。应急演练则是对应急预案进行模拟演练，检验应急预案的可行性和有效性，及时发现并处理存在的问题。

3 计算机信息安全技术防护的重要性

随着信息技术的快速发展和计算机的普及，计算机信息安全问题越来越受到人们的关注。计算机信息安全技术防护的重要性在于，它可以有效地保护计算机信息的安全和隐私，防止黑客攻击、病毒传播、数据泄露等威胁，保障人们的正常生活和工作秩序。

3.1 保护计算机信息的安全和隐私

计算机信息安全技术防护可以有效地保护计算机信息的安全和隐私。通过各种技术手段，如加密技术、访问控制技术、网络隔离技术等，可以防止黑客攻击、病毒传播、数据泄露等威胁，保障计算机信息的安全和隐私[5]。

3.2 保障人们的正常生活和工作秩序

计算机信息安全技术防护可以保障人们的正常生活和工作秩序。一旦计算机信息受到威胁，可能会导致系统崩溃、数据丢失、机密信息泄露等严重后果，影响人们的正常生活和工作秩序。通过计算机信息安全技术防护，可以有效地避免这些问题的发生，保障人们的正常生活和工作秩序。

3.3 防止国家机密信息和军事信息的泄露

计算机信息安全技术防护可以防止国家机密信息和军事信息的泄露。在现代战争中，信息已成为重要的战斗力量，而计算机信息安全技术防护可以有效地保护国家机密信息和军事信息的安全和保密性，避免被敌方获取，从而保障国家的安全和利益。

4 计算机信息安全因素分析

4.1 黑客攻击

黑客是指一些具有高超的计算机技能和知识的人，他们通过各种手段入侵他人的计算机系统，获取机密信息或者破坏系统。黑客攻击是计算机信息安全的主要威胁之一，他们可以利用各种漏洞和弱点，进入系统并进行破坏[1]。黑客攻击可以分为两种类型：一种是主动性攻击，即黑客通过各种手段入侵系统，获取机密信息；另一种是被动性攻击，即黑客只是监听系统中的通信，获取传输的数据信息。

4.2 病毒传播

病毒是一种恶意程序，可以破坏计算机系统的正常运行。病毒可以通过各种途径传播，如电子邮件、网络下载、U盘等。一旦病毒进入计算机系统，它就会在系统中繁殖并破坏系统中的文件和数据。病毒传播对计算机信息安全的威胁非常大，它可以导致系统崩溃、数据丢失、机密信息泄露等严重后果。

4.3 数据泄露

数据泄露是指未经授权的个体或者组织获取到敏感信息或者机密信息。数据泄露可能通过各种途径发生，如黑客攻击、内部人员操作失误、外部人员窃取等。数据泄露可能会导致严重的后果，如商业机密泄露、个人隐私泄露等。

5 计算机信息安全防护措施

5.1 加强安全意识教育

首先，政府、学校和企业应该加强计算机信息安全教育，提高人们的计算机信息安全意识[2]。在这方面，政府、学校和企业可以开展各种形式的计算机信息安全教育活动，如举办讲座、开设课程、发放宣传资料等，提高人们对计算机信息安全的认知和了解，培养良好的计算机信息安全意识。其次，政府和企业应该加强对员工的安全培训，提高员工的信息安全技能和安全意识。在这方面，政府和企业可以开展多种形式的安全培训活动，如举办技能比赛、开展安全演练、开设安全课程等，提高员工的信息安全技能和安全意识，使员工具备应对常见信息安全风险和威胁的能力和意识。最后，政府和企业应该建立健全的计算机信息安全文化体系，营造良好的计算机信息安全氛围。在这方面，政府和企业

可以采取多种措施，如制定计算机信息安全规范和制度、建立信息安全举报和处置机制、开展信息安全宣传和教育活动等，营造良好的计算机信息安全文化氛围，提高人们的计算机信息安全意识和技能。

5.2 加强网络安全防护

首先，政府和企业应该加强对网络安全的投入，提高网络安全防护的能力和水平。在这方面，政府和企业可以增加对网络安全技术研发的投入，引进先进的网络安全技术和设备，提高网络安全防护的技术水平。同时，政府和企业应该建立健全的网络安全管理制度，规范网络安全的日常管理和操作流程。其次，政府和企业应该加强对网络攻击的监测和预警，及时发现和应对网络攻击事件。在这方面，政府和企业可以建立完善的网络安全监测和预警系统，对网络攻击行为进行实时监测和预警，及时发现和应对网络攻击事件，减少网络攻击造成的损失和影响[3]。同时，政府和企业应该加强对网络安全的宣传和教育，提高人员对网络攻击的防范意识和能力。最后，政府和企业应该加强对外包服务的安全管理和监督，确保外包服务的安全性和可靠性。在这方面，政府和企业可以采取多种措施，如对外包服务提供商进行安全评估和认证，签订安全协议和保密协议，加强对服务过程中安全事件的处理和应对等。通过加强网络安全防护，政府和企业可以有效地保障计算机信息安全，防止网络攻击、病毒木马、间谍软件等安全事件的发生，确保网络的稳定性和安全性。

5.3 加强数据备份和恢复工作

首先，政府和企业应该加强对数据的备份和恢复工作，确保在发生意外事件时能够及时恢复数据。在这方面，政府和企业可以建立完善的数据备份和恢复机制，对重要数据进行定期备份和存储，避免数据的丢失和损坏。同时，政府和企业应该采用先进的数据备份和恢复技术，确保数据的完整性和可靠性。其次，政府和企业应该加强对数据的保护和管理，确保数据的机密性和完整性。在这方面，政府和企业可以采取多种措施，如对重要数据进行加密处理，限制人员的访问权限，加强对数据使用过程的监控和管理等。此外，政府和企业应该加强对内部人员的教育和培训，提高人员的安全意识和防范能力。最后，政府和企业应该建立健全的数据管理制度，规范数据的采集、存储、使用、共享和销毁等环节的操作流程和安全要求。通过加强数据备份和恢复工作，政府和企业可以有效地保障计算机信息安全，防止数据泄露、篡改和丢失等安全事件的发生，确保数据的可靠性和稳定性[4]。

5.4 加强法律制度建设

首先，政府应该制定更加完善的法律法规和标准规范，明确计算机信息安全的责任和义务。在这方面，政府可以制定《计算机信息安全法》、《网络安全法》、《数据保护法》等法律法规，明确计算机信息安全的法律责任和义务，规定相关企业和个人必须采取的安全措施和应对突发事件的预案。同时，政府可以制定更加详细的标准规范，如《个人信息保护规范》、《网络安全等级保护规范》等，明确保护信息安全的技术要求和操作流程。其次，政府应该加强对违法犯罪行为的打击力度，严厉惩处违法犯罪分子。在这方面，政府可以建立专门的计算机信息安全执法机构，加强对违法犯罪行为的查处和打击，坚决维护计算机信息的安全和保密性。同时，政府可以加强国际合作，共同打击跨境的计算机信息安全犯罪行为。最后，政府应该加强对计算机信息安全的监管力度，及时发现和处理计算机信息安全问题。在这方面，政府可以建立计算机信息安全监管机构，对涉及计算机信息安全的单位和个人进行监管，及时发现和处理计算机信息安全问题，确保信息安全得到有效保护。通过加强法律制度建设，政府可以为保障计算机信息安全提供有力的法律支持，加强对违法犯罪行为的打击力度，保障公民的合法权益和国家的安全稳定[5]。

结束语

计算机信息安全是一个综合性较强的领域，需要采用多种技术和措施来保障信息安全。本文从密码学、防病毒技术、防火墙技术、安全监控技术等多个方面详细介绍了计算机信息安全技术。同时，本文还针对计算机信息安全因素，提出了一些防护措施。在未来的信息化时代，加强信息安全的防护措施，将成为各个企业和机构不可或缺的重要工作。

参考文献

[1]周力，王晓东，陈晨.计算机信息安全技术及防护措施[J].计算机科学与应用,2020,12:1-5.

[2]中国互联网协会.信息安全技术指南——计算机信息安全等级保护[M].北京:电子工业出版社,2021.

[3]李晓明，王建.计算机网络安全技术及防护措施[J].网络安全技术与应用,2021,6:1-5.

[4]张涛，李超.计算机信息安全技术及主动防护措施[J].计算机应用研究,2022,4:1-5.

[5]国家互联网信息办公室联合公安部.计算机信息安全保护指南[R].2022.