论电子计算机的信息数据安全

张子牧
长城（天津）质量保证中心有限公司　天津　300000

摘　要：随着信息技术的快速发展，电子计算机在各行各业中的应用越来越广泛，数据安全问题也日益凸显。电子计算机信息数据安全不仅关乎个人隐私保护，更涉及到国家安全、经济发展等多个方面。本文围绕电子计算机信息数据安全展开论述，从技术层面、管理角度和物理层面三个方面探讨保障数据安全的有效措施，旨在为提升电子计算机信息数据安全水平提供理论支持和实践指导。

关键词：电子计算机；信息数据；安全

引言

在信息化时代，电子计算机已经成为人们生活和工作中不可或缺的工具。然而，随着数据量的快速增长和网络环境的日益复杂，电子计算机信息数据安全问题愈发严重。数据泄露、非法访问、病毒攻击等事件频发，给个人和企业带来了巨大的损失。因此，加强电子计算机信息数据安全保护，对于维护国家安全、保障个人权益、促进经济社会发展具有重要意义。

1 电子计算机信息数据安全的重要性

电子计算机信息数据安全的重要性在当今信息化社会愈发凸显，它涉及到个人、组织乃至国家的核心利益。随着科技的快速发展，电子计算机在各行各业中的应用越来越广泛，成为现代社会不可或缺的一部分。因此，保障电子计算机信息数据的安全，对于维护社会秩序、促进经济发展、保护个人隐私等方面都具有重要意义。首先，电子计算机信息数据安全对于维护社会秩序至关重要，在现代社会中，大量的政府事务、商业活动和个人生活都离不开电子计算机。如果信息数据遭受泄露、篡改或破坏，将可能导致严重的社会混乱。例如，政府机密信息的泄露可能危及国家安全，商业机密的泄露可能导致企业破产，个人信息的泄露可能引发诈骗等犯罪活动。所以，保障电子计算机信息数据安全，有助于维护社会的稳定和谐。其次，电子计算机信息数据安全对于促进经济发展具有重要意义，随着信息技术的快速发展，电子商务、云计算、大数据等新兴业态蓬勃兴起，为经济发展注入了新的活力。然而，这些新兴业态的发展也离不开信息数据的支撑。如果信息数据无法得到有效保护，企业的商业机密、客户的个人信息等都可能面临泄露的风险，从而影响企业的正常运营和市场的公平竞争。最后，电子计算机信息数据安全还关系到个人隐私的保护，在信息化社会中，人们的日常生活、工作和学习都离不开电子计算机。人们通过电子计算机存储了大量的个人信息，如照片、视频、聊天记录等。如果这些信息被不法分子获取或滥用，将对个人造成极大的困扰和损失。因此，保障电子计算机信息数据安全，有助于保护个人隐私不受侵犯，维护人们的合法权益。

2 影响电子计算机信息数据安全的因素

2.1 技术层面的因素

技术层面的因素是电子计算机信息数据安全的基石，它涉及到数据传输、网络体系、系统安全以及应用层面等多个关键环节。在信息化社会，数据的安全传输至关重要，一旦数据在传输过程中被非法窃取或篡改，就可能造成无法挽回的损失。因此，确保数据在链路上的安全，防止黑客或入侵者通过窃听、截取等手段获取敏感信息，是技术层面需要考虑的首要问题。一方面，网络体系和系统的安全漏洞是另一个需要重点关注的技术因素，随着网络技术的快速发展，网络攻击手段也日益复杂和隐蔽。黑客可能利用系统漏洞，通过注入恶意代码、发动拒绝服务攻击等方式，破坏数据的完整性和保密性，甚至可能造成整个系统的瘫痪。另一方面，在应用层面，由于资源共享的普遍性，信息安全风险也相应增加[1]。许多组织或个人在共享资源时，可能未能充分意识到信息安全的重要性，导致重要信息泄露。例如，在云计算环境中，多个用户共享相同的物理资源，如果云服务商的安全措施不到位，就可能导致用户数据被非法访问或滥用。此外，随着移动设备的普及，移动应用的安全问题也日益突出，许多移动应用可能存在权限滥用、数据泄露等安全隐患，对用户的隐私和信息安全构成威胁。

2.2 人为因素

人为因素在电子计算机信息数据安全中占据着举足轻重的地位，与技术层面的因素不同，人为因素更侧重

于强调人的行为和决策对数据安全的影响。这种影响可以分为无意威胁和有意威胁两大类，它们都以不同的方式对数据安全构成潜在或实际的危害。（1）无意威胁往往源于人们的疏忽或知识不足。例如，网络管理员在进行安全配置时，可能因为对系统的理解不够深入或操作不当，导致安全漏洞的出现。这种情况下，管理员可能并没有恶意，但由于其决策或操作的失误，给攻击者留下了可乘之机。同样，用户在设置口令时，如果缺乏安全意识，选择了过于简单或容易被猜到的密码，也会大大增加账户被非法访问的风险，这些无意的失误虽然看似微小，但却可能对整个网络系统的安全性造成重大影响。（2）相对于无意威胁，有意威胁则更为严重和直接。黑客攻击和计算机犯罪是这类威胁的典型代表，黑客利用病毒、木马等手段，蓄意破坏计算机网络和数据的安全，以达到窃取机密数据、破坏系统功能或进行勒索等目的。这种攻击往往具有明确的目标和精心的策划，因此其危害也更为严重。除了黑客攻击外，计算机犯罪也是另一个不容忽视的有意威胁，这类犯罪可能涉及内部人员滥用职权、非法访问敏感数据或进行数据篡改等行为。这些行为不仅可能导致机密数据的泄露，还可能对企业的声誉和客户的信任造成严重影响。（3）工作人员的职业道德水平也是影响数据安全性的一个重要因素，在数据处理和存储的过程中，如果工作人员缺乏职业道德或受到外部诱惑，可能会故意破坏或窃取信息数据以满足自己的私利。这种行为虽然较为罕见，但一旦发生，其后果往往非常严重。

2.3 物理层面的因素

物理层面的因素对电子计算机信息数据安全的影响不容忽视。这些因素不仅与计算机硬件设备的完好性和稳定性有关，还与数据存储和传输的环境条件密切相关。第一，自然灾害是物理层面威胁的典型代表，地震、火灾、洪水等自然灾害可能突然发生，给计算机设备带来毁灭性的打击。一旦硬件设备受损，存储的数据很可能也会随之丢失或损坏，导致无法恢复[2]。第二，除了自然灾害，物理损坏和设备故障也是物理层面常见的威胁，硬件设备的老化、磨损或不当操作都可能导致数据丢失或泄露。第三，电磁干扰也是物理层面影响数据安全的一个重要因素，电磁干扰可能来自于外部电磁场、雷电等自然现象，也可能来自于其他电子设备的工作干扰。这些干扰可能导致计算机设备的运行不稳定，甚至造成数据损坏或丢失。第四，电磁辐射和信息泄漏也是物理层面需要关注的安全隐患，计算机设备在工作时会产生电磁辐射，这些辐射可能被不法分子利用，通过专门的接收设备窃取敏感信息。同时，口令密钥等敏感信息的保管不善也可能导致数据泄露。

3 保障电子计算机信息数据安全的措施

3.1 技术层面的措施

在电子计算机信息数据安全的保障工作中，技术层面的措施无疑是最为基础和关键的一环。随着信息技术的飞速发展，数据安全所面临的挑战也日益复杂多变，因此，采取一系列科学、高效的技术手段来确保数据安全显得尤为重要。（1）加强数据加密技术的应用。数据加密技术通过采用先进的算法，将明文信息转化为密文形式，使得未经授权的人员无法读取和理解原始信息内容，这就像是给数据穿上了一层“隐身衣”，让攻击者即使截获了数据也无法得知其中的内容。对称加密和非对称加密是两种常用的数据加密方式，它们各有特点，可以根据实际应用场景选择合适的加密方式。（2）防火墙和安全检测技术的运用。防火墙技术就像是网络的“守门员”，能够监控和控制进出网络的流量，根据设定的规则过滤掉恶意攻击和非法访问[3]。通过配置防火墙，我们可以有效地阻止未经授权的访问和数据泄露。而安全检测技术则能够及时发现系统中的安全漏洞和潜在威胁，通过定期进行安全扫描和漏洞评估，我们可以及时发现并修复潜在的安全隐患，提高系统的安全性。（3）随着云计算、大数据、人工智能等新技术的发展，我们也需要不断创新和升级数据安全技术。例如，利用云计算技术可以实现数据的集中存储和备份，提高数据的可靠性和可恢复性；利用大数据技术可以实现对海量数据的分析和挖掘，发现潜在的安全威胁和异常行为；利用人工智能技术可以构建智能安全防御系统，实现对安全事件的自动识别和处置。（4）除了上述技术手段外，还有一些其他的技术措施也值得我们关注。比如，采用多层次的身份验证和访问控制机制，确保只有经过授权的人员才能访问敏感数据；建立数据备份和恢复机制，以防万一数据丢失或损坏时能够及时恢复；加强网络安全教育和培训，提高员工的安全意识和技能水平。

3.2 管理角度的措施

在电子计算机信息数据安全保障工作中，除了技术层面的措施外，管理角度的措施同样重要，建立完善的信息安全管理制度，不仅能够有效提升数据安全防护能力，还能为企业或组织的稳健发展提供坚实保障。首先，制定详细的信息安全政策、流程和规范是管理层面工作的基石，这些政策和规范应明确数据安全的目标、原则和要求，为各级人员提供明确的工作指引。同时，政策中还应规定数据的分类、存储、传输和使用等方面

的具体要求，确保数据在整个生命周期中都得到妥善保护。通过制定这些详细的政策，可以确保数据安全管理的责任落实到人，避免出现管理空白和职责不清的情况。其次，定期进行信息安全风险评估和漏洞扫描是管理层面的重要环节，通过风险评估，可以及时发现和识别潜在的安全威胁和漏洞，为制定针对性的安全措施提供依据[4]。而漏洞扫描则能够发现系统中存在的安全缺陷和漏洞，为修复和完善系统提供重要参考，这些工作应定期进行，并根据实际情况进行动态调整和优化，以确保数据安全的持续性和有效性。此外，加强员工的信息安全培训和教育也是管理层面不可忽视的一环，员工是数据安全的第一道防线，他们的安全意识和技能水平直接影响到数据的安全状况。因此，定期开展信息安全培训和教育活动，提高员工的安全意识和技能水平，对于防止因人为失误或疏忽导致的安全事件具有重要意义。培训内容可以包括数据安全知识、安全操作规范、应急处理流程等方面，以确保员工在工作中能够自觉遵守安全规定，有效防范安全风险。

3.3 物理层面的措施

在电子计算机信息数据安全领域，物理层面的措施扮演着至关重要的角色，物理层面的安全措施旨在保护硬件设备、存储介质以及整个信息系统免受物理威胁和损害，从而确保数据的完整性、保密性和可用性。（1）机房和数据中心作为计算机设备的重要运行环境，其安全性直接影响到数据的安全。因此，机房和数据中心应选址在地质稳定、环境适宜的地方，并采用抗震、防火、防水等防护措施，确保设备在遭受自然灾害时能够稳定运行。此外，机房内还应设置合适的温湿度控制系统、电源保障系统等，为设备提供稳定可靠的运行环境。（2）采用多层次的身份验证和访问控制机制是物理层面安全的重要手段，通过身份验证，可以确保只有经过授权的人员才能进入机房或数据中心，从而防止未经授权的访问和操作。同时，采用访问控制机制，可以限制不同人员对数据的访问权限，确保敏感数据不会被非法获取或篡改，这些措施可以有效降低人为因素对数据安全的威胁。（3）对重要数据进行备份和恢复是物理层面安全的必要措施，由于自然灾害、设备故障等突发事件可能导致数据丢失或损坏，所以定期对重要数据进行备份至关重要。通过备份，可以在数据丢失后迅速恢复，确保业务的连续性和数据的完整性。并且，建立灾难恢复计划，制定详细的应急处理流程，可以在突发事件发生时迅速响应，最大程度地减少损失。（4）加强物理层面的监控和防护也是必不可少的，通过安装视频监控系统、门禁系统等，可以实时监控机房和数据中心的安全状况，及时发现和处理异常情况。此外，加强设备的物理防护，如使用防盗锁、加固设备等，可以防止设备被盗或损坏。

结语

综上所述，电子计算机信息数据安全是一项长期而艰巨的任务，而通过技术层面的措施、管理角度的措施以及物理层面的措施的实施，可以有效地提升电子计算机信息数据的安全性，为信息化社会的发展提供有力的保障。未来，随着技术的不断进步和应用的不断拓展，电子计算机信息数据安全将面临更多新的挑战和机遇。我们要保持高度警惕，不断创新和完善数据安全保护措施，确保数据安全成为信息化发展的坚实基石。

参考文献

[1]叶华雄.大数据下计算机网络信息安全与防护分析[J].中国科技信息,2020(12):52-53.

[2]衡立业.数据加密和异常数据自毁技术在网络信息安全中的研究[J].网络安全技术与应用,2020(06):35-36.

[3]杨鑫源,毕文静,苏艺铄.大数据时代背景下财产隐私安全存在的问题及其对策分析[J].价值工程,2020,39(15):210-212.

[4]王勇.安全管理技术在计算机网络数据中的有效应用分析[J].电子测试,2019(18):75-76.