信息系统的网络安全技术及实施方法分析

周友江

（苏州科技大学天平学院，江苏 苏州 215011）

摘要：随着网络信息技术的发展与普及，信息系统中的网络风险与安全问题得到了更多的关注，不仅影响着信息系统的应用与普及，还会造成经济方面的效益损失，因此，信息系统的网络安全技术发展与实施显得尤为重要，需要基于当下的网络安全工作现状，对安全技术实施方法进行探究，寻找信息系统的网络安全技术优化方案。

关键词：信息系统；网络安全技术；实施方法；分析

一、网络安全技术

对网络信息系统的安全性进行优化前，需要对计算机网络的组成进行明确，计算机网络的组成分为硬件与软件，设计网络资源、网络服务、信息共享等领域，要对网络安全技术进行维修或应用，促进计算机网络信息系统的安全性提升。计算机网络新题系统的安全性需要较为严格的保护，专业维护人员需要对软硬件进行优化、保护各类数据信息，实现网络信息系统的安全运行，防止信息泄露。随着现代社会的生活方式改革，网络安全问题受到了越来越多的重视，信息系统网络中的信息量不断增加，网络传播速度也飞速提高，这就带来了信息网络安全质量要求的提升。网络安全受到的威胁逐渐增加，还提高了网络信息系统中的信息不可预测性。对计算机网络的成效进行优化时，需要应对多样化的调整，建设网络的过程中，也要设计应对网络入侵、网络瘫痪等问题的策略，针对网络系统信息化采取专业的技术方法，减少损失与利益上的问题。

网络安全技术有着三个较为明显的特征，首先是技术的多样化。网络安全技术是一种防御性的措施，一旦出现入侵，才会进行被动防御介入，因此，如果采取较为单一的安全技术，就会容易受到破坏或入侵，影响整体的技术质量。其次，网络安全技术与机制会不断进行变化，随着信息系统的发展，信息网络安全技术的质量与效果也会受到影响。网络安全技术的优化与普及过程中，还需要不断的对机制进行更新迭代，保障应用的最终效果。信息网络系统的普及与发展会影响系统的速度，也会使得安全技术与机制不断地改变形式与种类。第三，网络安全问题中，技术性与复杂性较强，随着信息系统的发展加加速，网络安全的技术型也在不断变化，因此，规范化的标准建设工作需要得到重视。

二、信息系统的网络安全技术分类

（一）虚拟网络技术

虚拟网络技术是局域网交换技术下的分支，通过对局域网通讯范围的限制，能够促进网络监听工作的效果提升。虚拟技术会提升对入侵手段的反制能力，但让虚拟交换设备复杂，容易受到攻击对象，例如假冒的 MAC 地质、攻击手段的多元化。

（二）防火墙技术

防火墙技术主要通过对网络间的访问进行加强，防止用户利用违法方式亲人，减少信息系统的受损问题，为减少信息系统的损失、信息泄露，需要优化防火墙的防护能力，防范防火墙以外的攻击途径。例如，内部的用户防范能力不足，会导致感染病毒的软件或文件传播。信息安全技术中应用中防火墙，能够实现维护简单、可靠性墙的优势得以落实。在信息安全威胁中，代码感染或系统漏洞这两种问题最为危险，需要计算机软件与技术发展并不断更新，满足用户的安全需要，强化新技术的应范围并保障系统运行的安全性。

（三）数据加密技术

数据加密技术主要是资料密码法，这种方法主要是对计算机数据进行加密，使得合法接触者能够获得还原的消息。这一技术通常采用加密乏，关注加密迷药，只要接收与发送方能够进行解密，中间的传输节点中，无法读取数据。数据加密技术也是针对计算机网络的加密，这种技术在日常计算机应用过程中十分常见，密码的强度也会有所差异。部分技术人员会采用非对称性技术，减少密码间的联系，加强加密技术的实际效果。

（四）访问控制技术

访问控制与认证的技术配合，能够实现数据系统的安全性提升。认证是实现一致性的方法之一，主要的内容有认证技术、体系、安全性，认证作为计算机安全技术中的应用，被广泛使用，也是网络安全的重要保障。访问控制是对系统与资源的管理与保护，是对身份认证进行授权，并控制访问权限，进而实现数据安全与完整性。

三、信息系统的网络安全问题分析

（一）网络运行环境

社会环境、自然环境都会为计算机网络信息系统的运行造成影响，也是系统会受到在主要影响之一，会对网络安全带来较大的问题。例如自然环境因素，如果产生水灾、火灾等自然灾害，网络信息系统就会受到较大的影响，难以保障计算机运行的安全，还容易引发其他问题。利用计算机网络进行浏览过程中，如果对网站的安全性考虑不足，就容易导致信息泄露，也有针对系统的攻击，引发网络瘫痪，损害网络信息体统，破坏网络运行环境。同时，信息系统的网络安全需要相关技术人员的素质提升。网络建设工作中还有着一定的不足，例如网络管理人员的要求需要提升，寻找专业认识的指导等。

（二）网络入侵问题

我国在发展信息科技的同时，也培训了大量计算机产业的相关人才，这些专业人才为社会的发展打下了重要的基础。但也有一部分掌握了计算机专业知识的人，忽视法律与道德标准，基于计算机技术手段攻击网络信息系统，引入科技手段进行犯罪，导致计算机网络信息系统在运行的同时受到入侵，引发网络安全问题。部分非法入侵的网络黑客甚至会截取机关单位的重要信息，窃取国家机密，给社会发展带来负面影响。

（三）信息共享问题

信息系统网络技术的发展使得更多人能够享受到科技发展的成果，实现信息的共享与交流，计算机技术发展的实际过程中，多数人逐渐通过计算机终端与服务器进行连接，实现资源共享，为用户提供了大量的便利。但信息共享的初衷，一些用户在获取资源的同时会受到网络攻击，个人数据信息被窃取，破坏网络信息的安全，造成利益方面的损失。现代社会中，信息系统的网络

安全问题主要体现在数据被窃取与控制方面，基本都是由于安全漏洞引起的，没有对信息进行加密处理，使用过程中没有设置密钥。

四、信息系统的网络安全技术及实施方法分析

（一）优化网络架构工作

信息系统网络的安全技术中，物理方面的隔离措施是最重要的，网络安全技术会提升网络与数据的安全性，实际的实施过程中，基于物理的网络机构能够实现内部与公共网络间的隔离，强化抵御能力、优化系统性能。在进行内部网络架构的优化时，可以考虑自身的系统要求，对内部的重要模块进行专门管理，设置独立服务器，将备份服务器与分级服务器配置齐全，组成内部网络的服务器，便于内部网络的隔离，切断对外的出口，保障信息安全。同时，外部公共网络的建设中，用于对外业务的以太网、管线为主构建外部公共网络，与内网进行隔离，外部网络不收发内部信息数据，减少内部数据的泄露可能性，提升数据的安全性。要解决信息系统网络通讯的流畅性，需要确保网络通信技术的稳定性与安全性，进而建立起更加健全的保障体系。可以对计算机设备的维修、养护进行明确的规定，促进工作的标准化，也能够有效避免操作失误等问题。

（二）建设病毒防御系统

随着社会的发展进步，信息系统在生活实践中起到了重要的作用，信息网络安全问题，是计算机网络发展中的新问题，也对系统的正常运行造成了影响。计算机网络系统有着一定的开放性特点。能够进行跨区域、跨系统的使用，也能够实现多个程序与数据的流通，在信息网络技术分析中，需要针对信息网络系统，设计抵御病毒的系统，防范病毒与安全风险的同时，提升整体系统的安全性。实际应用过程中，病毒防御软件也能够对网络设备，例如硬盘、服务器进行管理，实现对病毒的有效智力。内部服务器则需要专门安装病毒防御软件，定期对软件中的内容进行更新，强化防御系统的质量，减少病毒带来的安全风险。

（三）建设网络安全秩序

用户在计算机网络的应用过程中，需要对自身的信息安全提供保障，实现信息网络系统中的良好秩序，计算机网络操作要规范自身行为，遵守一定的秩序。用户是计算机网络信息系统中的重要组成部分，应当重视自身的日常操作、提升安全保护意识，使用网络过程中保持良好秩序。用户也要重视对网络环境的维护与创造，减少信息系统安全问题的发生几率。网络安全部门也可以共同参与进秩序的建设与管理工作之中，以更加严格的秩序对信息系统的操作进行约束，制定合适的安全秩序维护条例。同时，相关部门也要严格执法，遵循网络信息建设工作的秩序，针对违规人员进行处罚，使得用户对自身的行为进行自觉规范，共同营造良好的网络秩序。

（四）提高管理人员能力

信息系统的安全管理要求需要借助专业管理人员的操作技术来完成，进而从基础层面上提高网络信息系统的安全性。当下各个互联网行业都重视对高新技术人才的培养，促进人才的挖掘，实现人才与技术的集合，减少管理人员缺少的问题。当下我国的信息安全管理人员存在不足的问题，这就需要企业与各个部门加强人才培养工作的力度，提升专业人才的培训能力，实现专业培训工作的进步，使其充分掌握信息系统网络安全的管理运行要点，具备根据实际情况分析处理问题的能力。技术人员也要定期参与新的培训，提升自身的工作能力、丰富工作经验，提升网络安全意识。一些互联网行业相关的企业可以与高校展开合作，展开计算机网络安全的相关培训活动，为企业的发展打下人才基础。

（五）强化环境安全维护

环境安全的维护工作主要指物理层面的防护，例如自然环境、人为因素引起的计算机网络系统的安全问题，如水灾、火灾、地震等灾害，人为损坏等。具体的物理安全防护操作中，需要技术人员对服务器系统进行防水与防潮能力的检测，检查消防系统，对工作中存在的安全隐患问题进行指导。相关部门也可以构建物理安全防护的体系，例如设置自动报警装置，做好服务器、设备所在区域的消防、防火隔离措施，保障系统的安全性。同时，还可以配置门禁系统、对访问进行控制，进而提高系统的安全等级；设置温度湿度的智能控制系统、静电消除设备等，最大程度减少环境方面影响产生的损害。

（六）完善安全技术使用方法

信息系统网络安全技术的实施中，防火墙技术的应用是有较大的必要的，通过对网络的访问控制，能够防止外部的入侵，保护信息系统设备安全，减少数据信息的泄露。实际的安全技术应用过程中，还是需要从防火墙技术入手，提升信息网络的系统安全性。可以通过对防火墙的多层面、多维度构架，在以往的基础上构建新的防火墙，积累信息系统活动、服务器日志，减少用户的信息泄露风险。通过对信息的过滤、认证、筛选，能够加强内部网络的安全性，不断提升系统的防御能力。

处理内部系统的隔离与物理隔离外，还需要优化对外部风险的检测工作，强化信息网络安全技术的质量，实际的实施工作中，需要关注系统管理的实际需要，建设动态化的信息流动使用与控制工作。例如，在出现入侵问题时，要技术进行报警、切断网络，实现入侵者的记录与追踪，强化网络安全技术的质量。

计算机网络信息系统是对所用用户开放的系统，其技术的核心在于数据的传输应用，这就使得数据安全性成为系统应用的重点，除了对于技术与设备的应用外，还需要构建更加日常的安全防范方案，进而有效推进储存方式的安全与访问手段的安全，实现信息网络体系的优化。具体的实施中，一方面，需要对存储安全进行优化例如对网络设备进行精简，对相关的信息与数据进行备份，用于后续的风险处置分析。另一方面，也要对数据库进行备份，减少由于数据库操作失误、意外事故造成的问题，及时对数据进行恢复与完善，强化信息安全。

总而言之，网络信息化时代的到来，使得越来越多的人在日常生活中感受到了新技术带来的便利，为保障系统运行的安全，相关部门应当组织技术人员强化安全意识，提升安全管理水平，为网络应用营造出良好的环境，提升系统的安全性能。用户要提升自身的安全意识，学习更多安全操作，同时也要完善安全技术的应用，减少数据信息丢失、泄露的问题。未来的发展实践中，还需要对信息系统进行更多针对性的安全控制研究，为我国信息科技的发展提供助力。

参考文献：

[1] 王双燕 . 公众危机信息传播演化模型设计及规律分析 [J]. 中国安全生产科学技术，2023，19（5）：21-28.

[2] 赵勇 . 计算机网络信息安全的数据加密技术探讨 [J]. 信息系统工程，2023（6）：136-139.

[3] 叶婷，曾灶烟，董碧飞，等 . 面向云服务系统的网络安全评测方法 [J]. 信息通信，2020（2）：2

[4] 孙金阳 . 高校网络与信息安全体系和实施方法研究 [J]. 网络安全技术与应用，2020（1）：3.