·医师论坛·

医院信息化建设过程中的网络安全管理与相关维护方法略谈

李　忠

中国人民解放军联勤保障部队第 940 医院信息科　730050

〔摘　要〕现阶段，我国政府部门正在积极努力的倡导医院构建信息化管理系统，并且出台了多项政策方面以及资金方面的扶持文件，其最终目的就在于有效的提升我国整体医疗服务质量。而目前我国诸多医院已经在开展信息化建设活动。当医院完成信息化建设目标之后，就需要有效的开展网络安全管理以及各项系统及硬件设备的维护，这是保障医院信息化建设质量以及各项信息化管理系统能够持续有效且稳定运行的基础保障。此次研究主要就医院信息化建设过程中的网络安全管理与维护方法做了简要的分析。

〔关键词〕医院；信息化建设；网络安全管理；维护；策略

〔中图分类号〕R197.3　　〔文献标识码〕A　　〔文章编号〕2095-7165（2020）05-189-01

目前，在医院信息化建设当中，LIS 系统、CIS 系统以及 HIS 系统都在医院当中得到了广泛的普及，并且发挥出了显著的应用成效，使得各项医疗信息的整合工作、存储工作、分类工作以及处理工作实现了统一管理，不仅极大地提升了医院各项管理的精准性以及时效性，同时还极大地提升了医院的服务质量。但是保证医院信息化建设成效以及各项信息化系统能够稳定运行的基础保障就是优质的网络安全管理以及维护。因此，相关的医院信息化建设管理人员需要健全网络安全管理制度，优化革新网络安全管理及维护方法，充分挖掘杀毒软件的优势功能三方面着手进行具体的管理与维护工作。

一、健全医院网络安全管理及维护制度

健全的管理制度不仅可以保证网络安全管理的规范性，同时还有助于医院信息化建设质量以及成效的提生。基于这一情况，相关的网络安全管理人员在实际工作期间必须要重视安全管理及维护制度的健全工作。为此，首先，需要落实连带责任追究管理制度，该项制度的制定是为了明确各个管理人员的职权，降低管理缺位以及交叉管理问题的出现，具体而言，需要明确规定各个管理人员的工作职责以及相应的管理权限，在出现问题之后，保证能够快速找到责任主体，分析问题出现的原因，如果是因为人为疏忽或者操作失误所造成的，那么需要追究相关责任人相应的责任。其次，需要落实奖惩制度，该项制度的制定是推进医院信息化建设的重要措施，可以有效的提升工作人员的工作积极性，具体而言，需要明确规定在医院信息化建设期间有突出表现，并提出一些具有建设性意见的人员，医院将为其提供升迁机会，并会给予其一定的物质奖励。而对于一些时常做出违规管理行为的人员要基于一定的惩罚。另外，还要适时风险管理制度，对于各个信息化建设环节进行风险预估，预估出可能出现的网络安全风险，并提前制定出预防措施，然后将这些信息进行有效的宣传，不断的强化每一位管理人员的风险意识以及网络安全管理及维护意识。

二、优化革新医院网络安全管理及维护方法

科学合理的网络安全管理及维护方法是保证医院信息化建设成效以及信息系统应用成效的基础保障。因此，需要医院网络安全管理人员重点革新网络安全管理及维护方法。首先，医院网络安全管理人员需要有效实施物理隔离方法，具体而言，将医院内部较为重要的部门所用到的电脑进行硬盘以及网线隔离处理，实施单独的网络设计方法，有效的将防火墙系统应用到一包上传的服务器和 HIS 服务器中间，降低数据外泄风险问题出现的概率，同时还要有效的运用 VLAN 技术进行交换机以及服务器的维护管理，并在此基础上绑定相关设备的 IP 以及 MAC 地址，以此来有效的避免网络安全问题出现。其次，由于信息化建设目标完成之后，大量的数据信息被存储之后会因为一些不稳定因素而导致信息数据丢失问题出现，基于这一问题，相关的网络安全管理人员需要定期的对数据进行备份存储处理，并对各项备份信息进行权重分析，并实施分级别保护措施。最后，需要有效进行操作系统安全防护，有效实施双机容错以及双机热备系统，为保证电压稳定性需要有效运用 UPS 主机装置进行供电。同时还要落实权限设计模式将各项信息数据的访问权限进行细致的划分，并明确规定不同级别的工作人员拥有不同的访问权限级别，以此来降低数据乱改越权管理问题出现。

三、充分挖掘杀毒软件在网络安全管理及维护中的优势功能

杀毒软件是网络安全管理及维护工作有效开展所需要用到的一种重要工具，该种软件的主要作用就是清除系统当中的病毒系统，避免病毒入侵以及软件系统问题出现，从而提升信息系统在医院当中的应用成效。而要想有效的运用杀毒软件来提升网络安全管理及维护的质量，首先，必须要科学合理的步入常规性软件，结合医用信息系统的兼容性以及其所需功能来选取杀毒软件，以此来保障信息安全系统的整体性。于此同时还要定期的对杀毒软件进行升级处理，并找到专业的系统管理人员进行升级操作，并将软件系统的内部模块划分为，药方、病房、医疗技术以及管理等多个模块，实施具有针对性的病毒防护方式。其次，要有效的运用杀毒软件深入防护恶意软件，尽可能的降低客户端的软件系统下载量，降低漏洞数量以及漏洞风险出现的概率，并及时有效的进行更新系统处理，有效运用防火墙系统，智能筛选主机安全数据，借助杀毒软件来扫描测验相关应用程序是否安全，如果检测出来应用程序存在风险，那么就需要及时的删除该应用程序，并快速的进行全盘病毒扫描，避免恶意软件存留于系统当中问题出现。

四、结束语

综上所述，现阶段，在我国医疗领域当中掀起了一场信息化改革的浪潮，各个地区的医院在政府部门的大力引导下都在积极努力的开展信息化建设工作，并且取得了显著的成效。但是由于我国医院信息化建设的起步时间相对较晚，在医疗领域当中并没有一套完善且健全的网络安全管理体系以及维护管理体系，进而导致仍然有诸多问题存在于其中，导致信息化系统很难充分的发挥出其应有的优势作用，甚至还会提升医院所承受的信息风险强度。因此，相关的管理人员需要从制度，方法以及软件系统的应用三方面着手进行医院信息化建设过程中网络安全管理及维护方法的研究，结合具体的管理需求以及关键管理环节，制定出具有针对性的优化措施，以此来保证信息系统能够充分发挥出其应有作用，提升医院服务质量以及效率。

[参考文献]

[1] 王鹏，马锡坤，吴艳君 . 基于防火墙的网络安全技术在医院网络中的应用 [J]. 电子设计工程 .2017(21)

[2] 董睿 . 医院网络信息的不安全因素分析及防护措施分析 [J]. 电脑知识与技术 .2018(07)

[3] 张宏萌，黄留然 . 新形势下医院网络的安全问题分析与对策 [J]. 中小企业管理与科技 (上旬刊).2019(08)