电力企业信息安全管理

张 浩
镇江供电公司信息通信公司，江苏镇江 212001

摘 要 近年来，国家电网公司提出了“坚强智能电网”的发展战略，对公司信息化水平有了更高的要求。建立健全信息安全保障体系是加快推进信息化工作的前提。本文结合地市公司面临的信息安全方面的威胁，从安全制度建设、人才队伍建设、防护系统建设、系统安全建设、个人安全建设和信息保密建设等六个方面介绍了地市公司在信息安全管理上的一些做法。

关 键 词 信息安全；安全防护；信息保密
中图分类号 TP39 **文献标识码** A **文章编号** 1674-6708（2013）83-0024-02

1 电力企业的信息安全

1.1 什么是信息安全

信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。

通常来说，信息安全就是要做到五个方面内容：一是进不来，通过设置系统口令、屏保口令等使恶意人员无法进入；二是拿不走，对系统用户有权限区分，低权限用户无法越权获取高权限用户资料；三是看不懂，对重要文件进行加密处理，保证信息不曝露给非法用户；四是改不了，确保只有得到允许的人才能修改数据，其它人无法改动；五是走不脱，使用审计、监控等手段，使得攻击者、破坏者无法走脱。

1.2 信息安全总体要求

公司信息安全坚持“双网双机、分区分域、安全接入、动态感知、精益管理、全面防护”总体防护策略，执行信息安全等级保护制度，防止因信息系统本身故障导致信息系统不能正常使用和系统崩溃，抵御黑客、病毒、恶意代码等对信息系统发起的各类攻击和破坏，防止信息内容及数据丢失和失密，防止有害信息在网上传播，防止公司对外服务中断和由此造成的电力系统运行事故。

2 地市公司信息安全管理

2.1 信息安全面临的威胁

随着信息技术的发展以及公司信息化建设的推进，地市公司面临的信息安全威胁越来越多样化。目前，信息安全面临的威胁主要有：一是人为无意失误，如管理漏洞、安全意识不强，操作不当等；二是人为恶意攻击，如计算机病毒等恶意代码；三是软硬件的漏洞和“后门”，如操作系统、数据库及应用系统本身存在的缺陷和漏洞；四是设备故障；五是自然灾害。

2.2 信息安全管理

2.2.1 安全制度建设

地市公司要根据上级公司的相关要求，结合本公司所面临的信息安全威胁，从网络、终端、应用、管理等各方面建立完善一整套信息安全管理制度。管理制度主要包括：《计算机机房安全管理制度》、《安全责任制度》、《网络安全制度》、《系统安全风险管理和应急处置制度》、《操作权限管理制度》、《用户登记制度》、《重要设备、介质管理制度》、《信息发布审查、登记、保存、清除和备份制度》等等。这些信息安全制度在公司信息安全工作中起着根本性、指导性和全局性的作用。

地市公司要根据实际情况制定信息安全通报制度，加大全体员工对信息安全的重视程度，提高信息安全的管理效率。通报分为例行通报、紧急通报两类，通报内容包括：一是围绕信息安全考核指标的日常工作；二是信息安全的专项工作；三是信息安全事件的预警、响应、研判和处置情况。

地市公司要建立信息安全监督制度，要求各单位、部门对危害信息安全的各类危险源点进行自查整改。信通公司作为信息安全主管部门进行现场检查和远程检查。

地市公司要建立信息安全应急处置制度。为了正确、有效和快速地处理信息安全突发事件，最大限度地减少突发事件对公司生产、经营、管理造成的损失和对社会的不良影响，需要定期修订完善应急预案和开展应急演练。同时，地市公司还要定期组织全体信息运维人员学习应急预案，做到熟悉预案，了解如何应对突发事件，明确各自职责和处理程序，真正确保突发事件下的信息安全。

2.2.2 人才队伍建设

信息安全工作需要必须的人力资源来支撑。地市公司要按照“谁主管谁负责，谁运营谁负责，谁使用谁负责”的原则，落实专门机构和人员负责信息安全工作。目前，地市公司的信息安全运维管理由信通公司负责，主要工作包括有系统的安全运维、信息安全的技术保障、信息安全事故应急处理及员工信息安全教育等。地市公司还应根据工作地点及人员分散的特点建立一只信息兼职队伍。通过信息兼职队伍的壮大及能力的提升，使信息安全迈上新的台阶。

2.2.3 防护系统建设

安全技术是信息安全的主体，信息安全离不开安全技术的实施和安全产品的部署。地市公司必须要部署防火墙、入侵检测系统、防病毒系统、桌面终端标准化管理系统等各种安全防护系统。这些系统的部署给信息安全提供了多层次、全方位的安全防护。

部署防病毒系统。Symantec endpoint Protection 提供端点安全解决方案，它实现防病毒、防间谍软件、防火墙、入侵防御和网络威胁防护等多种功能，并且通过策略的设置，可以防范安全违规事件的发生。它具有系统性和主动性的特点，能够实现全方位多级安全防护。

部署桌面终端管理系统。桌面终端系统应实现对公司内部终端的软硬件、数据保密的集中化和标准化管理，提高公司内部终端的安全性及维护管理的效率。

地市公司还应利用在网络设备上采取 IP 地址与 MAC 地址绑定的技术手段限制不明非法的设备接入到信息内网中。同时，

作者简介：张浩，助理工程师，研究方向：电力信息安全

（下转第26页）

磨床，数控加工中心，数控车床等等。我国数控机床产品已延伸到成套、复合领域。数控系统装置是数控机床的神经中枢，我国从上世纪 90 年代末开始，掌握基于通用 32 位工业控制机开放体系结构，一举登上当代同一起跑线，开发出能与加工中心、复合车削机床及齿轮机床配套的数控系统，特别是能控制五轴联动和具备网络化远程监测、诊断、操作功能的数控系统，并开发出弧齿锥齿轮数控加工。

总体来讲，我国机床产业进入转型期后，发展顺利，自主创新能力提升，整体产业实力有了质的飞跃。

7 数控设备制造业已成为中国工业的主导行业

在中国，机床行业已进入了创新活动的活跃期。中国的创新资源逐渐成熟，在某些领域已经到了由技术模仿跟踪转向主要依靠自主创新求发展，进而在产业发展制高点上挑战全球。我国有条件由一个技术消费国转变为技术创新国，带动传统产业的改造升级，由低端制造转向产业链，培育出一批批具有全球竞争力的企业和企业集团，进一步提高国家竞争力。

机床，是装备工业的母机，关系到国家整体实力，要率先取得更大的突破。国内一批装备制造的领军型企业，经过多年的积累和进步，具备了相当的基础，应该有信心、有志气完成这个突破。这是国家的期望、民族的希望和企业的社会责任。

8 我国数控机床行业的未来发展趋势

在中国机械工业中，机床行业位居“工具母机”的特殊地位，其水平也对机械工业中各行各业的升级具有特殊重要的意义。因此，机床行业的发展既取决于中国机械全行业总体发展形势，同时又影响着全行业的健康发展。

我国生产的数控机床不但在品种数量上有了很大的发展，而且在产品的技术水平和质量上也不断提高。五轴联动高档数控龙门镗铣床、五轴联动高档数控车削中心，是造船、电力、航空等行业急需的关键设备，近年来我国已开发研制成功，且作为成熟商品走向市场。我国数控机床通过多年的努力，在机床的外观造型、制造质量、产品可靠性和售前售后服务等方面也都有较大的改进和提高，进一步得到了各界用户的信任，从而赢得了越来越多的用户，随着数控机床技术水平和档次的不断提高，为国家重点工程和国防建设提供数控装备和成套设备的能力，也有明显的提高。

机床行业将以国家“信息化带动工业化”为契机，用信息技术和复合技术提高数控机床的性能和关键功能配套产品水平，加快产品结构调整，通过引进先进技术、合作生产、合资经营，实现与国际接轨的跨越式发展。

（上接第24页）

还应制定网络接入设备审批制度，严格控制和管理接入信息内网的设备。

2.2.4 系统安全建设

系统安全分为物理安全和运行安全两个部分。

物理安全主要是指主机存储设备、网络设备、安全设备及机房辅助设备安全。设备放置在专门的信息机房内，通过门禁系统及机房监控系统保证这些设备自身的安全。地市公司应制定机房管理、机房出入人员管理等制度，对设备安全管理、机房环境管理、人员出入访问控制管理等做出详细的规定。同时，地市公司还应指定专人负责各类设备的管理工作，定期联系专业厂家对设备进行巡检，做到问题早发现，早解决。

运行安全主要是指业务应用系统、网络系统及数据库系统等运行安全。主要系统应采用双机的方式来建设。所有的系统都有专人负责，地市公司定期对系统的运行状态进行巡视、备份等工作。同时，地市公司还要对设备的账户安全、网络安全、服务安全、日志安全等方面开展加固工作，保障系统的安全稳定运行。

2.2.5 个人安全建设

地市公司应从管控与培训两个方面开展个人信息安全建设。

所有终端设备应统一安装桌面终端管理系统、防病毒系统和补丁升级系统等安全防护系统。地市公司要每日安排专人监控终端设备，发现问题及时整改，保证桌面终端注册率、防病毒安装率，补丁安装率是 100%。

教育培训是提升员工个人信息安全意识和技术水平的重要手段。通过开展安全讲座、建设专题网站、印发宣传手册和巡展宣传展板等多种形式加强信息安全知识的宣传，使每个员工懂得信息安全违规行为的防范知识。

2.2.6 信息保密建设

地市公司要严格执行“涉密信息不上网，上网信息不涉密”的保密要求，对发现的违规失密、泄密事件严肃处理。信息保密工作主要有：一是强化信息保密教育培训，使员工明确信息保密安全防护要求；二是加强对终端和网络的保密管理，防止敏感、涉密信息的丢失以及有害信息在网上传播。

3 结论

信息安全本身包括的范围很广泛。大到国家军事政治等机密安全，小到如防范商业企业机密泄露、防范个人信息的泄露等。信息安全对企业而言只是相对的，我们只能够使企业的信息越来越安全，但不可能做到绝对的安全。为了保护公司的信息安全，我们必须对自己公司的信息安全情况有一个清醒的认识，高度重视信息安全工作，制定并执行相应的安全保障方案，从技术、管理、工程和人员等方面提出安全保障要求，确保信息系统的保密性、完整性和可用性，降低安全风险到可接受的程度，将公司的信息安全防护水平提高到一个新的阶段。

（上接第27页）

在我们国家钢结构住宅仍然只是处于一个发展的阶段，，目前还有很多的问题是需要专业的建筑人员去多多发展和完善的。我们看到在我国技术集成化以及产业化是我们国家住宅业发展的必然趋势，钢结构住宅体系正是符合这种趋势的住宅结构，同时也是我们国家实现小康社会的住宅的最终目标要求，可以看出钢结构住宅的发展前景是良好的。可以相信，在本世纪钢结构住宅一定可以快速发展，由混凝土结构、砖混结构长期以来一统天下的格局即将改变，钢结构施工、制造企业必将会快速发展。

参考文献

[1]建设部科技发展促进中心1.钢结构住宅设计与施工技术[M].北京：中国建筑工业出版社，2011.

[2]刘承宗，周志勇.我国轻钢建筑及其发展问题探讨[J].工业建筑，2009，30(4).

[3]陶忠，何保康.发展我国新型轻钢结构建筑体系[J].中国工程科学，2008(3).

[4]张亦静.发展轻钢结构存在的问题与对策[J].株州工学院学报，2010(5).