关于无线电通信安全问题探析

马美丽　黄晨宁

1.喀什地区无线电管理局 新疆 喀什 844000

2.新疆维吾尔自治区无线电监测中心 新疆维吾尔自治区 830000

【摘　要】我国无线电通信技术不断发展下，人们对便利的使用需求量也在日益增加，因此不断提升企业信息安全是当前企业面临的重要问题，同时有效地提升企业运行效率，增加了电网安全。近年来，随着无线电技术的不断发展，通信技术在无线电中发挥着重要作用，但工作中涉及信息和数据关系到供电的稳定性和安全系数。因此，只有不断提高安全水平，才能保证通信技术中的信息安全。

【关键词】无线电；通信；安全防护；应用措施

1.无线电通信安全防护原则

强化无线电安全防护原则是加强信息安全重要保障，我国城市电力信息网本质上是一个面向服务的电力系统单元。因此，无线电通信技术自身的工作能力是相对统一的，只有通过发送信息和通信才能实现。根据安全防护原则，采取切实可行的安全技术措施。（1）要在工作中保证数据网络的安全运行，保证网络通道中数字序列的同步，借助网络专用设备实现公共信息网络和物理层的安全管理。（2）在电力系统信息安全技术中，员工必须按照基本的安全原则工作，在加强无线电绩效沟通的信息系统中，详细讨论和了解影响性能通信信息系统开发的许多重要因素，包括一些网络管理要求、技术标准和网络管理的具体结构，为了增强数据的准确性，无线电通信技术的应用可以有效地实现数据内容传输，强化信息安全性。

为了树立强烈的安全风险意识，能源供应商需要组织全体员工逐级签署“安全函”，并对安全从业人员、研发人员等专业人员进行全面的安全应对，签署具体的承诺申请表，确保能源供应企业的安全和信息安全，并向员工详细介绍《安全法》的背景。同时，企业扮演着基础设施运营商、网络运营商、网络产品和服务提供商的角色。因此，安全的法律责任就显得尤为重要，每个能源供应商都应该认识到遵守法律的重要性。

2.无线电通信安全防护应对措施

2.1.中心站

在无线电的发展过程中，无论信息传输还是信息输入，如果总部受到外界的攻击，就会出现网络瘫痪。主要是通过一套完整的安全防护及监测系统来解决或避免网络瘫痪问题，它可以及时监控工厂内异常的数据流，同时，也可以及时判断是否有外部入侵行为，一旦出现异常，就会给出警告，并且在未来我们可以继续优化安全防护及监测系统的性能实践经验。通过使用物理层的技术措施可以限制非法干扰的发生，无论是对用户还是供电服务，都可以保证信息安全，进而提高电力系统的安全性和隐蔽性。

2.2.无线终端漏洞

无线通信技术的进一步发展是无线通信技术发展的必然要求。版无线电通信技术在使用无线终端过程中，其终端类型较多，再加上系统信号较为开放在应用过程中较为容易出现问题。另外，终端系统对于访客的身份认证不仔细，使一些非法登录电网频繁的人员可以获取信息，造成无线电信息安全无法得到保证，也影响了电力系统的正常运行，因此，无线终端在开发过程中，要保证身份认证的多样性和访问人员的控制，只有这样才能不断促进无线终端系统在无线电中的应用。

2.3.通信系统加密技术及其优化

为了更好地解决信息安全和通信问题，通常采用加密技术来解决信息安全问题。关键在于，数据信息的具体内容只能通过加密来探索。例如：对于企业通信系统数据加密的文件必须使用系统加密的方法，增加信息的安全保障。其主要目的是防止外来人员通过信息中心窃取企业信息，增加企业信息安全。信息加密的常用方法有标准加密算法和公钥算法，选择两种方法对信息加密过程中要选择适合的加密方法，如果加密方法选择的不适当会降低信息的安全性，我国在选择信息加密安全一般采用明文加密的方法，但该方法在应用过程中仍存在一定的问题。

加密技术的优化。为了进一步提高信息安全性，工作人员在使用性能自动化技术时，不仅要保证终端用户的安全意识，还要保证信息在运输过程中的安全性。工作人员应进一步优化加密技术，保证加密技术在无线电工作中的应用。在进行自动化通信技术过程中，操作人员必须经过严格的规范流程，才能进入到终端系统中，

避免无关人员接触到终端系统，降低安全隐患的发生。另外，还要选择适当的加密技术，不断优化加密技术的应用，提升信息安全性能，还要加强技术人员对加密方法使用的进度。

2.4.系统恢复

现阶段，在实际操作过程中，电力网络频频出现不同情况，这是很难避免的，例如不法分子的恶意袭击，往往蓄谋已久。与此同时，不法分子通常具备较高的网络技术水平，但企业并非专门攻克安全技术的，非常容易出现错误和漏洞，大幅提高此类风险的规避难度，目前的企业难以有效预防相应风险。不过，部分电力安全威胁还是能够避免的，一些情况下甚至能够杜绝。例如，在电力网络系统运用过程中，一些工作人员尚未形成安全意识，没有掌握专业的计算机知识，没有掌握网络配置，无法熟练操作应用软件，当进行实际操作时，极易导致带有病毒的 U 盘、硬盘接入系统，将病毒带入网络系统中，从而使电力网络受到病毒的威胁。这类威胁是可以避免的，需要企业加强对工作人员的培训，使其具备较强的安全意识，及时查杀软件中的病毒，健全规章制度，一旦有工作人员将病毒带入电力网络中，企业应当对其进行批评和惩罚。针对该情况，企业为防止病毒侵入电力网络，应采取有效措施。因此一旦外带病毒侵入电力网络，势必以极快的速度传播，从而对电力网络服务系统产生极大的不良影响，导致其无法运行，若服务系统被破坏，便不能保障日常工作的有序开展。因此，企业技术人员应该科学合理地应用系统恢复技术，以此让系统有序工作，确保电力网络的顺利运行。另外，相关技术人员需要及时、全面清查电力网络中的病毒，尽量增强其安全性，利用系统修复这一方法减少经济损失，优化安全等级，从整体上提升电力网络的安全防御水平。

3.结语

随着我国无线电通信技术的不断发展，通信安全也在不断提升其人们的需求量也在增加。通信技术中的数据信息安全已成为保障无线电通信技术中的重要内容之一。其中，病毒常常成为威胁企业信息安全的因素，导致信息泄露、信号弱等问题，因此，只有不断提升无线电通信信息安全保障，及时做好信息维护工作，增加人员信息安全意识，才能做好安全管理工作并提升无线电通信技术信息安全为我国企业发展奠定坚实的基础保障。

【参考文献】

[1]张开阳. 无线电通信的安全及防护措施研究[J]. 信息周刊, 2020(5):1.

[2]周广峰. 无线电通信安全防范措施[J]. 数码设计, 2020, 9(16):1.