# 电力信息网络安全防范措施

朱 峰
周口龙润电力（集团）有限公司 河南 周口 466000

**摘 要：**电力信息网络作为现代社会的重要基础设施，对电力系统的稳定运行、国家安全和经济发展具有重大影响。然而，网络安全威胁不断增加，电力信息网络正面临空前的挑战；因此，研究和加强电力信息网络的安全防护至关重要。我们需要深入探讨电力信息网络安全的现状，并寻求有效的防范措施，以保障其安全稳定运行，这不仅能够确保电力系统的可靠性，还能为国家的安全和经济的稳定发展提供重要支撑。

**关键词：**电力信息；网络安全；防范措施

引言：随社会进步，我国电力企业发展显著，本文详述了电力信息网络安全的重要性、现状及防范措施。电力信息网络的安全对国民经济和社会稳定至关重要。为保障网络安全，提出了一系列防范措施：安装防火墙、管理漏洞、使用加密技术、执行访问控制策略、加强密码账户管理、进行安全更新与补丁管理，并建立灾备恢复系统。这些措施构建了电力信息网络安全的全面保障体系，旨在为相关领域提供有价值的参考。

## 1 电力信息网络安全的意义

电力信息网络安全在当今社会具有极其重要的意义，随着信息技术的迅猛发展，电力系统越来越依赖于网络通信技术，而网络安全问题也随之日益凸显；电力信息网络安全不仅关乎电力系统的稳定运行，更涉及到国家安全、社会稳定和经济发展的大局。（1）电力信息网络安全是保障电力系统稳定运行的基石，电力系统是国民经济的命脉，一旦网络遭受攻击或出现故障，可能导致电力供应中断，进而影响各行各业的生产和生活[1]。（2）电力信息网络安全对于保护国家安全和人民利益至关重要，电力系统作为国家关键基础设施，其安全稳定直接关系到国家的战略安全，如果电力信息网络存在安全漏洞，可能会被敌对势力利用，对国家安全构成严重威胁。（3）电力信息网络安全也是推动电力行业数字化转型的关键，随着智能电网、物联网等新技术在电力行业的广泛应用，电力信息网络的安全性和可靠性显得尤为重要。

## 2 电力信息网络安全的现状

### 2.1 系统漏洞与自建系统的安全风险

电力信息网络系统中的漏洞问题，尤其是自建系统中的安全风险，是当前网络安全领域需要高度关注的问题，这些漏洞往往源于系统设计或配置的不当，如同系统中的隐形裂缝，给攻击者可乘之机。特别是自建信息系统，很多时候并没有经过专业的安全设计与严密的测试。在设计这些系统时，可能过于注重功能的实现，而忽视了安全性这一关键要素。例如，输入输出验证可能不严格，导致恶意输入能够轻易绕过验证机制；访问控制可能设置不当，使得未授权用户能够访问敏感数据；数据加密措施可能缺失或不足，造成数据在传输或存储过程中被窃取或篡改的风险增大。这些漏洞的存在，对电力信息网络的整体安全构成了严重威胁，每一个漏洞都可能成为攻击者入侵的入口，一旦攻击成功，可能导致重要数据的泄露、系统的瘫痪，甚至对电网的稳定运行造成影响。

### 2.2 违规外联与内部威胁

在电力信息网络安全的语境中，违规外联构成了一个严重的风险点，当未经注册的存储设备或外网终端被接入内网时，它们可能携带病毒、木马等恶意软件，进而对内网环境造成污染。比如，一个未经安全检查的U盘，在插入内网计算机后，有可能自动执行其中的恶意代码，从而感染整个网络系统；同样令人担忧的是，如果外网终端能够直接接入内网，那么它就有可能成为一个潜在的攻击入口，攻击者可能会利用这个入口绕过防火墙等安全设施，直接对内网发动攻击。除了违规外联带来的风险外，内部威胁也是一个需要高度关注的问题，内部人员可能出于各种复杂的动机，如追求经济利益、满足报复心理等；通过网络窃取机密信息、泄露敏感数据或更改重要配置。这种来自内部的威胁往往更加难以防范，因为内部人员通常拥有合法的访问权限，这使得他们能够轻松地绕过许多安全防护措施。

### 2.3 安全防范意识薄弱

在电力信息网络安全管理中，安全防范意识的薄弱确实是一个亟待解决的问题。（1）一些信息管理人员对新兴的安全威胁缺乏了解，随着网络技术的飞速发展，

新的攻击手段层出不穷；然而，由于部分管理人员未能及时跟进最新的安全动态和技术发展，他们可能无法有效识别和防范这些新的攻击手段，这就使得电力信息网络系统暴露在潜在的安全风险之中。（2）一些管理人员在日常工作中忽视了安全规定的重要性，例如，他们可能会随意点击来自不明来源的链接或下载未知的附件，这种行为极易导致恶意软件的感染或敏感信息的泄露。此外，一些管理人员在使用网络服务时也可能存在不当配置或未及时更新安全补丁的情况，从而增加了系统被攻击的风险。（3）对安全培训和演练的重视程度不够也是导致安全防范意识薄弱的一个重要原因，部分管理人员可能认为安全培训和演练是浪费时间或资源的活动，因此未能积极参与其中。

## 3 电力信息网络安全的防范措施

### 3.1 安装防火墙

在电力信息网络的安全保护措施中，防火墙的安装和配置是至关重要的一环，防火墙是网络安全的基础设施，能够监控和控制进出网络的数据流，有效地阻止非法访问和潜在的网络攻击。在安装防火墙时，我们首先要明确电力信息网络的具体安全需求，并据此选择适合的防火墙类型：包过滤型和代理服务器型防火墙各有优势，包过滤型防火墙处理速度快，而代理服务器型防火墙则能提供更细致的安全检查[2]。选定类型后，接下来的重点是细致配置防火墙规则，规则的设置需要精确到位，既要能够抵御外部威胁，又要确保内部网络的顺畅运行；通过分析日志，我们可以及时发现异常流量或潜在的攻击行为，进而采取相应的应对措施。此外，定期更新防火墙的规则库和防御策略也是必不可少的，网络安全威胁日新月异，只有不断更新和完善防御体系，才能确保电力信息网络的安全稳定运行。

### 3.2 实施漏洞管理

在电力信息网络的安全管理中，漏洞管理占据着举足轻重的地位，鉴于电力信息网络系统的错综复杂性，难以避免地会存在一些潜在的安全漏洞，这些漏洞若被不法分子利用，可能会引发严重的安全问题。因此，实施漏洞管理的首要任务是进行定期的漏洞扫描，我们借助专业的扫描工具，能够系统地探测网络系统中的潜在漏洞。这些工具能模拟多样化的攻击情景，从而揭示出可能被攻击者利用的弱点，一旦发现漏洞，我们需要对其进行深入的分析和评估，根据漏洞的严重性和潜在危害来制定相应的修补方案，并迅速付诸实施。除了进行定期的扫描和修补外，建立漏洞管理的长效机制也至关重要，这包括构建漏洞数据库、制定紧急响应方案、加强安全培训和提升全员的安全意识等；通过这些综合性的措施，我们能够确保电力信息网络系统的持久安全。

### 3.3 使用加密技术

电力信息网络中的数据传输安全，无疑是系统安全的重要组成部分，加密技术，作为一种经过验证的数据保护手段，在电力信息网络中的应用显得尤为重要。它确保数据在从一个节点传输到另一个节点时，即使经过多个中间环节，也能保持其完整性和机密性，选择适合的加密技术是关键；不同的加密算法有其特点和适用场景，AES（高级加密标准）以其高效和安全性被广泛应用，特别是在对称加密领域。而RSA等非对称加密算法，在密钥交换和数字签名方面有着独特的优势，在电力信息网络中，我们需要根据数据的性质和传输需求，灵活选择最合适的加密算法。除了算法选择，密钥管理也是一个不可忽视的环节。如何安全地生成、分发、存储和更新密钥，直接关系到加密系统的可靠性，一个完善的密钥管理体系，能够大大降低密钥泄露或被破解的风险。端到端的加密方式，进一步强化了数据传输的安全性，这种方式意味着数据在离开发送端之前就已经被加密，直到到达接收端才被解密。在整个传输过程中，数据始终保持加密状态，从而极大地减少了数据被非法访问或篡改的可能性。

### 3.4 实施访问控制策略

在电力信息网络中，访问控制策略构成了安全防护的核心，这一策略的核心目的是确保信息和资源只能被授权的人员访问，从而维护数据的完整性和机密性。实施访问控制的首要任务是明确划分不同用户或用户组的权限。这种权限的划分是细致且严谨的；例如，网络管理员因工作需要可能持有最高权限，可以对系统进行深度的设置和更改，而一般员工则仅能访问完成其本职工作所需的数据和功能。这样的设计防止了敏感信息和核心系统被非授权人员接触，除了权限分级，身份验证也是访问控制中的关键环节。现代身份验证机制，如多因素认证，结合了密码、指纹、动态令牌等多种方法，大大提高了系统的安全性，确保仅有真实用户能够登录。此外，为了应对可能的安全风险，如用户忘记注销或离开工作站时，实施会话超时和自动锁定机制显得尤为重要，这些功能在用户离开一段时间后自动结束会话或锁定工作站，从而防止他人恶意利用。为确保访问控制策略的有效性，还应定期对其进行审查和更新，这包括验证每个用户的权限是否与其职责相符，以及及时撤销那些不再需要或已过期的权限，从而保持整个系统的安全性和高效性。

3.5 加强密码和账户管理

加强密码和账户管理是电力信息网络安全不可或缺的一环，密码作为保护用户信息的第一道防线，其重要性不言而喻。为了提高账户的安全性，我们必须坚决执行强密码策略，这意味着，用户设置的密码应具备足够的复杂性，不能是简单的、容易被猜到的字符串。我们要求密码必须包含大小写字母、数字和特殊字符的组合，这样的密码更难以被破解，从而为用户提供更强的安全保障。除了强密码策略，多因素认证也是我们提升账户安全性的重要手段，传统的单一密码验证方式存在被盗取或猜测的风险，而多因素认证则通过引入额外的验证步骤，如指纹识别、面部识别或动态令牌等，显著增强了身份验证的过程，这种多层次的身份验证方法使得非法接管账户的难度大大增加，从而为用户数据提供了更全面的保护[3]。此外，账户管理还涉及对用户账户的细致监控和定期审计，我们的系统能够实时监控用户的登录行为和活动，一旦出现异常登录或可疑操作，系统会立即发出警报，以便我们及时介入并采取必要的安全措施。这种主动的监控机制有助于我们迅速发现并应对潜在的安全威胁，确保电力信息网络的整体安全。

3.6 进行安全更新和补丁管理

安全更新和补丁管理是电力信息网络安全的重要环节，旨在修复已知的安全漏洞并提升系统的防御能力。第一，应定期检查并更新系统和应用程序的安全补丁，这些补丁通常包含对已知漏洞的修复和改进，可以防止攻击者利用这些漏洞进行攻击；为了确保补丁的及时应用，可以建立自动化的补丁管理系统，以减少人为操作的延误和错误。第二，除了应用安全补丁外，还应定期更新系统和应用程序的版本，新版本通常包含对旧版本中存在的安全问题的修复和改进，可以提高系统的安全性。第三，为了确保更新的安全性，应在更新前进行充分的测试，以确保新补丁或版本不会引入新的问题或风险；此外，应建立应急恢复计划，以便在更新出现问题时能够迅速恢复到之前的状态。第四，为了提高安全更新和补丁管理的效率，可以与其他安全措施相结合，如使用安全信息和事件管理（SIEM）系统进行集中监控和报警，以便及时发现并应对安全问题。

3.7 建立灾备和恢复系统

建立灾备和恢复系统对于电力系统信息网络安全至关重要，这一系统不仅能够在遭遇安全事件或灾难时保障数据的完整性和业务的连续性，还能有效减轻潜在损失，并迅速恢复正常运行。在构建灾备和恢复系统时，我们首先要做的是对重要数据进行全面备份，这些数据包括但不限于用户信息、交易记录、系统配置等，它们都是电力信息网络运行的核心。通过定期备份，我们确保了数据的完整性和可恢复性，即使在最坏的情况下，也能迅速恢复数据，避免信息丢失。除了数据备份，配置恢复策略也是灾备计划中的关键一环，我们根据电力系统的特点和可能面临的风险，制定了详细的恢复策略，这包括确定恢复的时间目标（RTO）和数据恢复点目标（RPO），以明确在发生灾难后应恢复到何种状态，并在多长时间内完成恢复。此外，我们还定期进行恢复演练，以检验灾备计划的有效性和可行性，通过模拟各种可能的安全事件和灾难场景，我们评估系统在实际情况下的恢复能力，并根据演练结果不断调整和优化恢复策略。

**结语**

电力信息网络安全是确保电力系统稳定运行的基石，也是推动电力行业数字化转型的关键。面对日益复杂的网络安全环境，我们必须采取综合性的防范措施，从防火墙安装到漏洞管理，从加密技术的应用到访问控制策略的实施，每一个环节都不可忽视。通过加强密码账户管理、及时进行安全更新与补丁管理，以及建立完善的灾备恢复系统，我们能够构建一个全方位、多层次的电力信息网络安全保障体系，从而确保电力系统的安全稳定运行，为国家的经济发展和社会稳定提供坚实支撑。

**参考文献**

[1]林诚.浅谈电力信息网络安全防范措施[J].中国新技术新产品,2020(15):33-34.

[2]柏楷.电力企业信息网络安全建设的要点及其实践[J].企业改革与管理,2020(13):203-204.

[3]代鹏飞,吴明.关于大数据环境下企业信息网络安全研究[J].科技传播,2020,10(04):103-104.