电力系统计算机网络信息安全防护研究

史英
（国网朔州供电公司，山西　朔州　036002）

【摘　要】当前，随着信息技术的不断革新和发展，电力系统正逐渐向智能化方向发展。目前，电力企业生产经营活动均以计算机网络为依托，因此，对网络信息的安全防护就显得尤为重要。这就要求有关人员不断提高自身的素质，增强安全防护的成效。本文就电力系统中计算机网络的信息安全防护问题进行了探讨，并给出了相应的防护对策，以期对提高电力系统的防护水平，保证电力系统的稳定运行起到积极的作用，为我国电力行业的发展提供一定的帮助。

【关键词】电力系统；计算机网络；信息安全防护

前言：

为了保证电力系统的正常稳定运行，保证电网的正常运行，确保用电安全。在电力系统中，计算机网络信息的安全性是一个重要的课题。在电力系统中，计算机网络是一种重要的信息资源获取的方式，其安全性直接关系到电力系统的正常运行，也关系到电网的供电可靠性。因此，加强对电力系统中计算机网络信息安全研究与保护工作的探讨是非常重要的一项工作。

一、电力系统计算机网络信息安全防护的重要意义

当前，我国电网开放程度不断提高，计算机网络技术的应用领域不断拓展。电力系统保护，流量监测，电力稳定性等多个领域都有了长足的进步，促进了电力系统的稳定和可靠，提高了电力系统的安全性。随着网络信息技术的不断发展，电力系统中的黑客也越来越多，这对电力系统的安全性构成了严重的威胁，影响了电力系统的正常运转，造成各种数据的巨大偏差，严重的甚至会造成电力运行设备的失效。特别是随着国内电力市场的逐步开放，人们可以通过第三方平台与电力公司进行实时交易，这就使得黑客更加肆无忌惮地对电网进行攻击，给电力系统的正常运行带来了巨大的负面影响。计算机网络信息的安全防护是一个非常重要的课题，需对其进行深入研究。

骇客可以按照预设的数据传送速度和长度、加密的数据种类和功率流等特定信息来对数据进行整理，还可以将数据与电力系统中的各种装置相连接，避免干扰它们的正常使用。加强对计算机网络的信息安全防护，可以有效地防范各种威胁，并利用加密、认证等技术手段来消除这些威胁。有些黑客甚至会根据电力系统的数据流进行二进制码转换，对各个独立运行的系统进行解密，从而控制整个电网。综上所述，在这种情况下，对电力系统的计算机网络信息安全防护就成为一项非常重要的工作。

二、电力系统计算机网络信息安全防护中的问题

（一）网络病毒入侵影响正常操作

在网络安全方面，病毒入侵是一种非常普遍的现象，它会对计算机的正常运行造成很大的影响。违法者们编写了一种病毒，然后利用这种特殊的代码或者命令，对计算机进行攻击，从而获得相应的信息数据，对电力企业的运行造成了非常严重的影响。这种病毒的杀伤力极强，严重的话，甚至会让一台计算机陷入死循环，导致整个计算机的性能下降，从而导致电力系统的正常运行出现问题。随着科技和电子技术的进步，病毒的等级也在不断提升。目前，计算机病毒入侵的方式已经发生了变化，可以通过银行卡和电子邮件进行攻击，这不但大大提高了防御的难度，还极大地降低了网络数据的安全保障能力。入侵计算机的网络病毒具有很强的破坏力，尤其是在病毒持续升级的情况下，它可以窃取用户的个人资料，从而威胁到人们的隐私和财产。当病毒侵入计算机后，难以消除，因而具有很强的隐蔽性。一开始的时候，这台计算机还能正常使用，但时间一长，就会出现故障，对计算机的使用造成影响。如果病毒入侵到计算机后及时地清理，则不会对计算机的正常使用造成影响。

（二）计算机的使用操作不规范

信息技术已经走进了每一个家庭，人们可以利用因特网来搜集各种信息，这就意味着计算机网络具有

比较明显的开放性。但是，在现实工作中，网络上的信息必须经过一些技术的筛选。工作人员在工作中，因为缺乏风险控制意识和防控能力，尽管已经采取了一些拦截手段，但仍然存在着一些缺陷，造成了计算机信息安全方面的较大隐患。这样就会使计算机安全性变得非常脆弱，甚至可能遭到非法的攻击。因此，那些拥有重要信息资料的单位应该加强对信息数据的保护，提高自己的风险防范能力，采用比较复杂的密码和相关的措施来进行工作，从而保证信息数据的安全。但是，有些工作人员认为自己的工作经验比较丰富，因此在工作中并不注意规章制度，造成了信息资料泄漏的可能，对电力系统的运行造成一定的影响。尤其是在对安全性有很高要求的电力行业，如果计算机的使用方法不符合标准，就会造成很大的安全隐患。

（三）计算机程序存在较大问题

在利用因特网进行信息检索的过程中，外部的网络环境可能给计算机系统带来不同程度的破坏，增加了安全风险。首先，计算机操作系统包括三层：CPU、内存和外围设备管理，每个层次上都有相应的程序或者模块。如果电力系统的防护水平不高，就会造成系统易受黑客攻击，严重时还可能影响到计算机的正常工作，导致信息资料的泄漏。其次，计算机上的大部分程序都是由人来完成的，一旦写错或者遗漏，就会造成计算机上的漏洞，病毒和黑客就会趁机入侵计算机，造成信息和数据的损失。此外，若计算机中安装有病毒的程序，则会对计算机的使用造成影响，不但不能有效地保护计算机网络信息的资料，还会造成计算机内的信息资料随病毒一同被盗。

（四）缺乏对网络信息安全的重视

虽然最近几年，电力部门对网络信息安全的重视程度有所提高，但仍然没有得到足够的重视，相关工作人员的安全意识也不高。在计算机网络安全管理工作中，经常不能端正自己的工作态度，导致在平时的工作中存在着比较严重的安全隐患。另外，个别的电力系统维修人员在管理和检查计算机网络方面，缺少耐心和细致的态度，没有进行定期的检查，在处理和排除系统中的安全隐患方面，也存在着一些问题。此外，还缺少日常的归档工作，这使得电力系统的网络信息存在着很大的安全风险，一旦受到攻击或者其他突发事件，电力系统网络信息的稳定和精度都会受到影响。

三、电力系统计算机网络信息安全防护的有效策略

（一）应用有效的防火墙技术

为了使用户能用上安全高质量的电能，必须对电力系统各个环节进行有效的信息控制，提高对电力生产过程的监控、调控、保护和调度。如何有效地防范计算机病毒的入侵，保证电力系统的安全运行，具有十分重要的意义。当前，随着信息技术的不断发展，网络信息安全防护已经成为一种有效的手段。

首先，要和有关部门或者公司合作，研究出一套非常先进，非常可靠的防火墙。这种防火墙技术能够在网络信息安全防护中起到一定的作用，并且需要定期对其进行维护和更新，以保证这种技术能够切实地发挥作用。这样可以使电力系统中的每一个环节都能更好地工作，防止病毒入侵对系统的正常运行造成影响，保证电能生产工作的高效进行，为用户提供更安全、稳定的电力。其次，要提高防火墙的利用率，增加它的类型，做好这项工作，才能确保网络信息的安全性。与此同时，在电力系统的每一台计算机中都应该使用防火墙，根据数据信息的需要，构建各种防火墙，以便电力系统的输电、配电和变电工作能够更好地进行，为用户提供更优质、更安全的电力。只有如此，才能充分利用防火墙的功能，保证电力系统的信息安全。

（二）设置稳定的拦截系统

先进的设备和强大的安全防护能力，是保证电力系统平稳运行和提高经济效益的关键，使发电和用电之间达到最好的平衡。在使用电力系统时，需要时刻对其进行扫描核实，以确定 IP 地址的正确性。因此，用户在使用时，必须有一定的权限，才能确保操作的顺畅。但是，也有不少犯罪分子利用计算机中的恶意病毒，对计算机进行攻击，使计算机无法正常工作。因此，电网必须建立一个拦截系统，监控和管理陌生的、异常的 IP 地址，并阻止他们的登录。通过这种方式，可以将电网中的信息安全风险降到最低。

在这个过程中，还可以让防火墙加入到工作中来，对可能会对网络信息系统造成影响的连接或者应用进行拦截，找出潜在的隐患，并向操作员汇报，从而使电力系统的工作更加准确、稳定。在构建系统的过程中，还需要对一些可能含有病毒的软件进行及时处理，防止它们与电网相连，减少木马等病毒的

入侵和迅速复制的可能性。通过对相应措施的实施，可以促进电力系统信息化、提升控制子系统的性能、保障电能质量、提升电网安全运行、提高产能、改善工作环境。

（三）注重对主机的防护

在所有的工业领域中，电力系统是非常的大领域，它的层次十分复杂，对实时性的要求也非常高，因此，在对信息安全管理和控制的研究上，必须采用更有效的手段，采用可靠的优化手段，推动电力系统监测和调度自动化的发展。尤其是在电网中，智能配电系统的工作，必须以主机为基础，主机在其中发挥着重要的作用。因此，对主机的保护是非常重要的，在保证信息安全的同时，也要加强对主机的保护，确保网络信息的安全性和稳定性。从使用者的用电量中抽取出来的有关资料，都要经过主控计算机的汇总和处理。如果主机受到了攻击或者病毒的入侵，就会发生数据丢失的情况。针对这种情况，可以采用软硬件相结合的方式进行信息安全防护，提高系统的自检能力，及时发现隐患，并云备份用户的相关信息，从而保证系统的安全。另外，还可以采用外接装置来实现物理上的隔离，使危险的装置不会直接和主机发生直接接触，从而确保了电力系统的正常运行。

（四）加强对网络信息安全的重视程度

随着电子、计算机和信息技术的不断发展和发展，计算机网络信息安全成了一个越来越重要的控制环节，它可以增强对电力系统的调控能力，推动电力系统的现代化。因此，加强对电力系统信息安全管理的研究，对于保障电力系统的供电质量和电力系统的安全运行至关重要。电力系统中的计算机网络安全问题将影响到整个电力系统的正常运转，因此，为了确保网络信息的准确和真实，就必须提高对网络信息的安全性的关注。

首先，要提高有关工作人员对网络信息安全的认识，使人们对计算机网络信息的重要性有更深地认识。其次，在平时的工作中，要对工作人员进行专业的培训，使各种工作人员能够更好地了解自己的职责，充分利用自己的优势，提高工作的积极性。最后，要根据特定的时间段，有目标地对电力系统中的计算机网络信息安全进行分析和检测，确定计算机有没有安全隐患，一旦发现病毒，要确定病毒的种类和排除方法。

（五）加强电力系统信息安全防护宣传教育

客观上，除上述防范措施之外，更应该重视对有关人员的教育和训练。之所以这么说，是因为他们的整体素质参差不齐，也就是说，在遇到同样的问题时，他们的处理方法也有很大的不同。这样的差距很容易造成电力系统的瘫痪。而且，缺乏对员工的规范管理，很容易导致信息泄漏。要解决这个问题，就必须有计划地开展信息安全的宣传教育，使他们的信息安全意识能够得到切实地增强。除此之外，还必须禁止在非涉密计算机上进行涉密操作，并明确每个人的责任。此外，还需要建立一套科学、合理的监管体系，对电网的安全状况进行细致地检测，从而将隐患消除在萌芽状态。

四、结语

电力系统既要达到经济性，又要确保电能质量，又要提高设备利用率，使各种能源资源得到合理利用，减少网损，获得良好的经济效益。在此过程中，必须加强对电网信息安全的重视，并采取相应的对策，保证电网的正常运行。总之，在网络信息时代，为了提高电力系统的网络信息安全，就必须对其进行一些改进和升级，采用主动应对的方法，在其尚未形成危害之前，对其进行修复。为了更好地解决网络信息安全问题，必须采取合理的防火墙技术设置，注重主机的保护，以及加强对网络信息的安全防护。只有如此，才能对电力系统主动地保护，防止因外界的攻击和安全隐患而导致的网络信息遗失。

参考文献：

[1] 李岳泽 . 关于提高电力系统计算机网络信息安全水平的研究 [J]. 科学技术创新，2018（22）：88-89.

[2] 赵妍，刘娜 . 电力系统计算机网络信息安全的防护探究 [J]. 数字通信世界，2019（1）：124-124.

[3] 戴宙 . 提高电力系统计算机网络信息安全水平的研究 [J]. 中国新通信，2019，21（17）：151-151.

[4] 程晓岩，丛鹏，赵子鉴 . 电力系统计算机网络信息安全的防护分析 [J]. 价值工程，2020，39（9）：250-251.

[5] 孙宏意，许轲 . 电力系统计算机网络信息安全防护问题分析 [J]. 中国标准化，2019（6）：227-228.

[6] 马小龙 . 电力技术监督在电力生产安全中的应用研究 [J]. 电力系统装备，2021（14）：46-47.