基于大数据的新型电力系统网络信息安全防护策略研究

陈 健
内蒙古电力（集团）有限责任公司包头供电分公司，内蒙古 包头 014030

[摘要]随着科学技术的不断发展，电力系统的网络信息安全也面临着更大的挑战。电能是一种较为新型的清洁可再生能源，能够为人类的生活生产提供基础的物质保障。保证电力资源的稳定供应不仅是满足居民正常生产生活的需要，也是保证国家经济稳定发展的需要。在大数据技术不断发展的今天，应该不断加强电力系统的网络信息安全防护工作，保证居民的用电安全。居民用电安全得以保障，才能够进一步保障国家经济的发展。文中主要从大数据技术飞速发展的背景出发，探究电力系统网络信息安全的防护策略。主要阐述了电力系统网络信息安全面临的困境、电力系统安全防护的关键技术以及大数据技术在新型电力系统网络信息安全防护的策略，希望为新型电力系统网络信息安全提供一些有用的参考。

[关键词]大数据；电力系统；网络信息安全；防护
DOI：10.33142/hst.v6i4.9164 中图分类号：TP393.08 文献标识码：A

Research on New Power System Network Information Security Protection Strategy Based on Big Data

CHEN Jian
Baotou Power Supply Company of Inner Mongolia Electric Power (Group) Co., Ltd., Baotou, Inner Mongolia, 014030, China

Abstract: With the continuous development of science and technology, the network information security of the power system is also facing greater challenges. Electric energy is a relatively new type of clean and renewable energy, which can provide basic material guarantee for human life and production. Ensuring the stable supply of electricity resources is not only to meet the needs of residents' normal production and life, but also to ensure the stable development of the national economy. With the continuous development of big data technology, the network information security protection of the power system should be constantly strengthened to ensure the safety of residents' electricity use. Only by ensuring the safety of residents' electricity use can we further ensure the development of the national economy. This paper mainly explores the protection strategy of power system network information security from the background of the rapid development of big data technology. This paper mainly expounds the difficulties faced by power system network information security, the key technologies of power system security protection, and the strategies of big data technology in the new power system network information security protection, hoping to provide some useful references for the new power system network information security.
Keywords: big data; power system; network information security; protection

引言

对于电力系统来说，网络信息安全是十分重要的，如果出现网络信息安全泄露的问题，就会导致较为严重的后果。电力企业在保证稳定的电力供应的同时，也应该注重新型电力系统网络信息安全的防护，保护网络信息安全。电力企业在实际运行过程中，只有充分保护新型电力系统网络信息的安全，才能够提高供电的工作效率以及提高所供电能的质量。随着大数据技术的发展，电力企业逐渐呈现出一种智能化的发展趋势，这就使得电力系统的稳定运行与电力系统网络信息安全具有很大的关联性，如果电力系统的网络受到不法人员的攻击，就很有可能对电力企业如造成较为严重的后果。因此，基于大数据背景下，电力企业应该积极加强对新型电力系统网络信息的安全防护，积极探索新型电力系统网络信息安全防护的策略[1]。

1 大数据技术概念概述

大数据技术是指一种在信息获取、信息存储、信息管理、信息分析与处理等方面能够同时进行的一种技术，大数据技术的特征主要表现在四个方面，数据规模大、数据流转速度快、数据类型十分多、数据价值密度低。在大数据诞生并被广泛运用到各个领域中之后，大数据具有的战略意义就不再仅仅是能够掌握海量的信息数据了，而是能够从获取的信息中分析、处理出企业所需要的信息内容，并进一步对这些企业需要的内容进行专业化的处理。简单来说，如果大数据作为一种产业，那么这一产业就是为了能够实现盈利的目的。从技术方面来看，大数据技术和云计算的关系可以说是一个硬币的正反面，大数据不能够简单地运用计算机实现信息处理，要实现有效的信息处理，就必须实现分布式架构。而从巨大的数据资源中挖掘出所需要的信息的这一过程也必须借助云计算的一些功能，例如分布式处理功能、云存储与虚拟化技术等。云计算和大数据的结合促进了云时代的到来，云时代的到来又进一步促进了大数据技术的发展[2]。

2 影响电力系统网络信息安全的因素

随着大数据技术的不断发展，电力系统的网络信息面临着许多的风险因素，因此，对于电力企业说，加强新型电力系统网络信息安全防护，是其当前的一个重点工作。影响电力系统的网络信息安全的因素主要有：管理因素、病毒因素、恶意攻击、操作失误等。要想进一步加强新型电力系统网络信息安全防护，就应该充分意识到这些影响新型电力系统网络信息安全的因素，最大程度上避免因这些因素导致的新型电力系统网络信息安全问题。以下是对影响电力系统的网络信息安全的因素的具体阐述。

2.1 电力系统管理不善

通过对电力系统管理过程的分析，可以从中分析出两个方面的风险因素，首先就是对网络信息管理者的有效管控。要保证电力系统的网络信息安全，首先应该要保证对电力系统网络信息管理者的有效管控。简单来说，就是应该要严格约束电力系统网络信息管理人员。对于电力企业来说，电力系统网络信息安全防护工作与电力系统网络信息管理人员的管理质量密不可分。在当前的许多电力企业中，还没有充分重视对电力系统网络信息管理人员的管控，没有对其进行合理的工作分配，这就导致一些电力系统网络信息管理人员以及一些系统使用者都能够随意进入核心机房。另外，一些电力系统网络信息管理人员不具备相应的安全管理意识，在对电力信息系统的网络进行管理时，操作较为随意，从而导致一些信息风险。其次就是在一些电力企业中，存在网络账号随意转借的情况，由于没有建立起较为严格的管理制度，一些电力系统网络信息管理人员为了工作方便，有时会将自己的网络账号转借给其他人，从而导致一些网络信息安全问题[3]。

2.2 病毒因素引发电力系统网络信息安全问题

随着信息技术的进步，网络病毒也发展得更加快速，许多电力企业的电力系统经常会出现一些病毒，往往导致电力系统网络信息安全受到威胁。由于计算机病毒是以代码的形式存在的，传播方式比较多，例如U盘、网络、软件等都可能会导致病毒的传播，当电力企业的电力系统受到计算机病毒的影响，就很可能出现一些信息泄露的问题。目前，我国的电力企业采用的网络模式是双网双机模式，采用这种模式将能够将电力系统的内网和互联网有效隔绝，从而能够有效避免计算机病毒的感染。但是，如果计算机病毒是处于一种可移动的存储载体中，那么当这一可移动的存储载体被运用于电力系统中之后，还是会使电力系统遭受计算机病毒的入侵。如果电力系统遭受了计算机病毒的入侵，可能会使电力系统的一些大型文件夹遭到破坏，导致一些重要的网络信息丢失[4]。

2.3 恶意攻击引发电力系统网络信息安全问题

对于电力企业来说，电力系统的网络还会遭受恶意攻击，这也是一种影响电力系统网络信息安全的重要因素。一些不法人员往往通过电力系统防护漏洞对电力系统进行攻击，攻击者可以从一些防护漏洞观察电力企业的一些重要网络信息，还可以通过防护漏洞，对电力企业的内网进行连接，做出一些盗取电力企业重要信息资源或者删除电力企业重要信息资源的行为。当电力企业遭受严重的恶意攻击时，往往会出现电力系统重要网络信息丢失的情况，对电力企业的发展造成严重威胁。当前电力企业遭受的恶意攻击模式主要有缓冲区溢出攻击模式、拒绝服务攻击模式等。

2.4 人为操作失误引发电力系统网络信息安全问题

对于电力企业来说，电力系统的网络信息安全还会受到人为操作的影响，如果一些电力企业的工作人员在操作电力系统时，出现一些失误，也可能会引发电力系统网络信息安全问题。比如，在配置电力系统的网络服务器或者网络设备时，出现配置不当，就可能会导致电力系统出现一些安全漏洞。另外，一些电力信息系统的使用者，在操作信息系统时，可能会因为操作失误，引发网络中断问题。以上所述都是因人为操作失误可能引发的电力系统网络信息安全问题。

3 基于大数据背景下的电力系统网络信息安全防范策略

基于大数据背景，电力系统的网络信息安全面临着较为严峻的挑战，因此，电力企业也应该随着信息技术的发展，采取一些积极措施，加强对电力系统网络信息安全的防护。根据影响电力系统网络安全的因素进行分析，笔者也提出了一些加强电力系统网络信息安全防护的措施，这些措施主要有：创建有效的数据采集层、保证数据存储设计效果、有效设计数据分析层、做好数据显示层的设计工作、加大安全管理力度、预防恶意攻击行为、科学防治计算机病毒等，以下是对加强电力系统网络信息安全防护的措施的具体阐述。

3.1 创建有效的数据采集层

要进行有效的电力系统网络信息安全防范，首先应该利用大数据技术在电力系统中创建出有效的数据采集层，保证数据采集层在充分发挥数据采集作用的同时还具有较高的安全性。要创建有效的数据采集层，在设计数据采集层时，就应该根据相关的网络信息安全要求进行设计，使数据采集层的设计充分满足网络信息安全的要求。构建了有效的数据采集层之后，采集到的数据就能够具有更高的安全性。在构建电力系统的数据采集层时，应该对采集层的结构数据、半结构数据、非结构数据这三种数据之间的关联效果进行充分地把握，进而保障各项数据的安全性。

3.2 保证数据存储层的设计效果

对于电力系统的网络信息安全来说，数据的有效存储是保证电力系统网络信息安全的重要因素。因此，在对电力系统的数据存储层进行设计时，使电力系统的数据存储

层具有较高的科学性和安全性，强化信息存储层的存储效果，最大程度上避免出现信息泄露。

在进行电力系统的数据存储层设计时，应该满足以下要求：数据存储层与数据库需要具有较高的关联性，从而能够使存储的重要数据信息进入数据库的时间最短，从而达到保护电力系统网络信息安全的目的。数据存储层与数据库需要具有较高的关联性，还能够使电力系统管理人员需要查询一些电力信息时，能够及时有效的查询到。

3.3 保证数据分析层的效果

在电力系统中，网络信息数据一般在经过采集、存储之后，还会进入数据分析层。数据分析层主要就是对采集到的网络信息数据进行分析，为相关人员提供较为准确有用的信息。因此，在设计数据分析层时，需要充分考虑到数据信息的安全，对数据分析层进行科学合理的设计。如果需要分析的数据较多，设计人员就应该拓宽数据分析层的数据处理空间，如果需要分析的数据比较复杂，设计人员应该使数据分析层的数据分析环节更加地精密。对于当前的许多电力企业来说，数据的分析内容主要包括数据学习方面、聚类分析过程、关联性分析等。为了保证数据分析法的有效性，在进行数据分析层设计时，应该充分保障涉及内容间的关联性。

3.4 保证数据显示层的设计效果

要进行有效的电力系统网络信息安全防范，还应该保证数据显示层的设计效果，使数据显示层达到相关的设计要求。电力系统对数据显示层的要求主要就是，显示层要能够全面展示出电力企业各个时期基础数据的全部信息，通过对全部信息进行分析，能够判断出这些信息是否具有相应的安全性。在进行电力系统的数据显示层的设计时，应该充分重视人机交互效果，保证数据管理人员在对各项数据展开分析时，能够得出准确的判断。

3.5 加大安全管理力度

要进行有效的电力系统网络信息安全防范，还应该加强对电力系统网络安全的管理力度。可以从大数据技术出发，完善相应的电力系统网络安全管理制度，并组建相应的电力系统网络安全管理机构。创建完善的网络安全管理制度，首先就是要制定相应的安全指标，根据安全指标，加大对电力系统的网络账号的会影响网络信息安全的因素的管理力度。其次，还应该加强对员工的培训，提升员工的网络信息安全意识，规范员工的工作行为。最后，还应该严格禁止网络账号外借以及将工作之外的存储载体用于企业内部计算机上等行为，如果出现这些行为，就应该采取较为严厉的处罚措施。

3.6 科学防治计算机病毒

计算机病毒是随着计算机问世以来始终存在的问题，对于电力企业来说，计算机病毒会对电力系统的网络信息安全造成严重的威胁。因此，电力企业要进行有效的电力系统网络信息安全防范，就应该科学防治计算机病毒，提升计算机病毒的防治效果。要提升计算机病毒的防治效果，首先可以引进专业人才，对电力系统的网络防火墙进行加固和维护。其次就是禁止网络账号外借以及将工作之外的存储载体用于企业内部计算机上等行为。最后就是不断提升电力系统网络信息的加密等级和防病毒等级，使电力系统网络信息在受到病毒入侵时，能够避免遭到破坏。

3.7 预防恶意攻击行为

电力企业要进行有效的电力系统网络信息安全防范，还应该对恶意攻击行为进行有效预防。要预防恶意攻击行为，可以关闭电力系统中一些不需要使用的服务端口，当发现电力系统防护系统存在漏洞时，应该及时对漏洞进行修补。要预防恶意攻击行为，还可以引进一些专业人才，对电力系统的网络防火墙和入侵检测系统进行加固和维护。防火墙能够有效阻止一些恶意攻击行为，入侵检测系统则能够及时识别出恶意攻击行为，并对其进行阻挡。防火墙和入侵检测系统能够避免很大程度上的恶意攻击行为，达到有效的电力系统网络信息安全防护。

4 结语

随着科学技术的不断发展，电力系统的网络信息安全也面临着更大的挑战。对于电力系统来说，网络信息安全是十分重要的，如果出现网络信息安全泄露的问题，就会导致较为严重的后果。电力企业在保证稳定的电力供应的同时，也应该注重新型电力系统网络信息安全的防护，保护网络信息安全。本文首先对大数据技术进行概念进行阐述，接着论述了影响电力系统网络信息安全的因素，随后提出了一些在大数据背景下进行电力系统网络信息安全防范的策略，希望能够为维护电力系统网络信息安全提供一些帮助。

[参考文献]

[1]高雪松.基于大数据的电力信息系统网络安全探究[J].中国科技投资,2020(1):33-34.
[2]徐建梅.基于大数据的电力信息系统网络安全探究[J].今天,2020(4):0231-0232.
[3]李东耀.基于大数据的新型电力系统网络信息安全防护策略研究[J].中国科技期刊数据库工业A,2023(4):4-5.
[4]李佳.基于大数据的电力通信网的安全防护系统探讨[J].中国战略新兴产业：理论版,2019(22):1-2.

作者简介：陈健（1980—），男，汉族，内蒙古包头人，大学本科，华北电力大学，电气工程及其自动化专业；副高级工程师，现就职于内蒙古电力（集团）有限责任公司包头供电分公司。