Engineering Technology and Development, 工程技术与发展 (5)2022,4
ISSN:2661-3506 (Online) 2661-3492(Print)

我国电子信息工程技术发展措施研究

孙宏伟
山东省人民政府机关保障中心　山东　济南　250011

摘　要：近年来，我国的计算机电子信息工程技术突飞猛进，结合其以往的发展历程来看，该技术在处理数据时具有显著的全面性与严谨性，可以利用该技术对海量的信息数据资源进行筛选，然后将有用数据传输至计算机控制系统中，全程实现自动化，有效提升企业的日常用运作效率。

关键词：电子信息；工程技术；未来发展途径

1 引言

实现企业信息管理系统化可以提升企业信息管理的效率。结合实际情况而言，企业在日常经营发展过程中常常需要处理大量的数据资源，而信息资源的管理具备复杂性与琐碎性，传统型的人工处理信息方式工作效率低下，而且有一定的可能性会出现数据遗漏、损坏等现象。但是随着计算机应用技术的出现，则有效解决了传统信息处理方式下的诸多难题。电子信息技术可以缩短信息管理的时间，减轻工作人员日常工作压力，提高信息处理的效率。

2 电子信息技术的应用

2.1 自组织网分层结构

自组织网属于一种分层式的结构类型，由多个簇共同构成，每一个簇含有一个簇首与多个簇成员。各个簇的簇首不但可以形成一个更高级别的网络结构，而且可以通过分簇的形式形成子网络结构。

2.2 自组织网的路由表及协议

通信技术的核心元素是路由技术，路由表是多个不同的节点路由技术的重中之重，通常来说，在自组织网络结构中可以通过不断改变路由表连接来保证通信畅通。

2.3 基于遗传算法的自组织网络组网过程

（1）确定角色，通常情况下，初始化的集群通过随机选择的方式确定，集群内的节点会对集群的适应度造成巨大的影响。（2）变量的空间离散可以借助二进制算法完成。（3）基于以上步骤在网络节点中随机选择n个群体作为父代，在对其编码以后将n个群体纳入至几何函数内，从而确定出其中的优秀个体。（4）借助交叉概率Pc完成父代群体的杂交处理，使用变异率Pm对子代进行变异处理。（5）当上述步骤完成以后可以获取到一个新的父代，则需要再次进行步骤（3）中的操作，而后进入到下一个流程中。

3 安全防护方案

3.1 系统概况

结合某市的电子政务信息管理系统对问题展开深入调研，该系统首个阶段的设计任务是构建出OA（OfficeAutomation，办公自动化）、公文传输管理模块，然后逐步将电子政务网络进行拓展，打造出面向全市的垂直化管理网络系统。该系统第二阶段的设计任务是构建出全市通用的认证管理平台，该平台的主要功能是个人的身份证认证。

3.2 技术手段

（1）数据加密技术现阶段，我国的计算机数据加密技术发展已经比较成熟，这种利好的局面为电子政务系统的建设提供了巨大的便捷。使用数据加密技术可以对部分重要、敏感的数据信息进行加密处理，以保证信息数据不会遭到外部环境恶意盗取，借助数据加密技术在共同网络中搭建出一条安全性比较高的通信渠道，保证安全数据始终处于安全的状态下，确保系统内的用户数据安全不会受到影响，同时可以促进电子政务系统的进一步发展。数据加密技术的出现对于公文传输、受控文件的管理具有重大的现实意义。在数据传输之前，操作人员会结合加密协议指定的公钥来对数据进行加密处理，这种设计方式促使只有特定的用户才可以对数据信息进行解密。在数据加密技术的运用下，管理系统的管理员与普通用户之前可以建立出一种量化的信任机制。这是管理员也不具备访问敏感信息的权限，但其可以切实维护系统正常运行。

（2）数字签名技术电子政务管理系统的行政管理职责需要增设数字签名功能，这个功能必不可少，其相当于现实生活场景中的公章、签字，具备真实性。数字签名技术的运用促使行政人员的签名具备合法性，电子签章与纸质版签字盖章具备同等法律效应。所以，数字签名技术是办理行政业务的前提基础，也是保证行政审批结果具备权威性、真实性以及合法性的重要保证。

3.3 安全解决方案

（1）搭建出特定的CA中心（CertificationAuthority，CA证书）。CA中心的搭建可以实现数字证书传输与接收功能，且地区内不需要再设置线下管理中心，在一定程度上降低了行政成本与管理压力，同时保证数据的安全性。

（2）CA中心在业务办理以后会自动根据用户的个人身份证颁发一张数字证书，这种数字证书具备唯一性，这就意味着可以取消简洁化的身份验证流程。

（3）在电子政务信息网中设置WEB（WorldWideWeb，

全球广域网，也称为万维网）系统，要求用户在登录该系统时必须提供数字证书，并启动HTPPS协议，有效保证政务信息传输的可靠性与真实性。

（4）设置访问控制授权功能，用户可根据自身的实际情况真实填写相关信息，例如姓名、年龄、部门等，根据用户的安全级别设置相对应的访问权限。

（5）对文件进行加密保存。借助数字证书将原本的信息全部传输至PKI（PublicKeyInfrastructure，公开密钥基础设施）认证的网络环内。

3.4 认证中心的设计

此次研究的电子政务网认证中心由5个子系统组成：CA认证中心、KMC（KeyManagementCenter，密钥管理中心）密匙管理系统、证书管理系统、数据库以及注册中心。认证中心属于一个完整性的PKI认证体系，可以高效完成对用户身份认证、访问权限控制功能，在这整个过程中数据的安全性得到保证，在很大程度上提升了整个电子政务网的安全性运行效率。

3.5 数字证书的存储

CA系统适用于各种类型的浏览器，具备较高的兼容性，且可以直接将数字证书保存在USBKey中。在实际运行时，为了进一步提升电子政务网内部的安全性，开发人员在经过全面的调研分析以后选择使用USBKey。USBKey外形与常规性的U盘基本上相同，便于携带与保存，但是USBKey连接至计算机时需要输入安全口令，不会轻易被他人窃取使用，在一定程度上提高了数字证书的安全性。此外，USBKey基本进行了高级别的安全设计，保证数字证书不会轻易被导出至USBKey以外，同样起到了提升整个电子政务网的安全性的目的。

3.6 重视终端审计保护

终端审计功能的作用至关重要，其主要是为平台内的管理员提供用户登录平台以后的访问记录、操作行为等具体信息，为管理员的监管工作提供了巨大的便捷。大部分的管理员对于终端审计的认知不够深刻，将其简单理解为对用户行为的监控，严格意义上来讲，终端审计并非是单一性的记录用户的访问记录与操作行为，其更多的是对用户的历史信息展开深入的分析，探索出电子政务网存在的不足之处，以便于电子政务网在长期运行的过程中不断得到优化与升级。为了加大对电子政务网的安全管理力度，可以借助终端审计来介入用户的登录、打印、下载、异常登录、违规行为的监管，这一点可以淋漓尽致展现出以安全管理为核心的审计原则。此外，终端审计具有诸多控制功能，例如移动存储控制、文件操作管理、操作行为管控、文件打印下载控制等。这一系列的管控行为都基于合法背景下进行，可以在很大程度上避免大部分的违规行为出现。

3.7 提高应急响应方案解决问题的水平

（1）确定出紧急时间的级别与具体类型。结合电子政务自身的特点来预估可能会发生的安全事件，例如产生的原因、安全事故的特点、安全事故爆发后造成的影响等。（2）建立应急管理小组。应急管理小组应负责协调指挥，加强各方面的交流与沟通，结合实际情况迅速作出合理的治理决策，合理分工，明确指出各相关人员的具体职责。（3）搭建出科学完善的预警监测机制。对重要的基础设施、核心系统、重要模块进行严格监管，并建立完善的应急处理制度，加强对网络安全的监管力度，保证每一位安全管理人员建立起安全防护的基本意识。（4）对应急处理的流程进行细化处理。在实际组织应急活动的过程中，应结合安全事件的实际情况制定具有针对性的应急方案，然后组织人员有序开展应急处理作业，将事故损失降至最小。（5）制定应急善后机制。在最大程度上发挥出应急响应以及恢复机制的效能，且应兼顾安全事故爆发以后的恢复工作。（6）排练与优化应急处理方案。对所制定的应急处理方案进行实践，结合实践情况优化不足，以保证应急方案可以切实发挥出最大的效能。

4 结语

综上所述，此次研究主要是针对电子信息技术的实际运用效果与安全防护效果进行深入研究分析。在经过调研分析以后发现，电子信息工程技术在现代化社会中的应用范围非常广泛，已经发展成为了一种常规性的通用技术。

参考文献：

[1]杨航，刘明朗，向星达.计算机网络技术在电子信息工程中的应用[J].南方农机，2017（3）：128-131.

[2]龚爱军.浅谈自动化技术在电子信息工程设计中的应用[J].城市建设理论研究（电子版），2019（16）：46-48.

[3]张文涛.电子信息工程技术的发展前景及其应用浅析[J].电脑知识与技术，2019（31）：112-114.

[4]徐子涵.电子信息工程技术在工业设计中的应用研究[J].轻纺工业与技术，2020（1）：86-91.

[5]申红.计算机网络技术在电子信息工程中的应用探析[J].花炮科技与市场，2019（4）：31-37.

[6]张杰.现代化技术在电子信息工程中的应用探讨[J].赤峰学院学报（自然科学版），2016（4）：50-53.