大数据背景下信息通信网络安全管理策略研究

赵文浩
中国机械设备工程股份有限公司　北京　100000

摘　要：近年来，伴随着网络信息科技的迅速发展，信息通讯技术早已运用到各行各业和行业，在各方面都可以发挥重要作用功效。云计算技术的快速发展不但促进了信息通讯技术的突破，还对信息通讯网络安全管理给出了一个新的更高规定。仅有融入互联网时代，深入推进信息通讯网络安全管理自主创新，才能获得很好的效果，保证信息通信网络一直处于稳定安全的环境里。

关键词：大数据背景；信息通信；网络安全；管理策略

引言

大数据环境下，尽管信息通信网络技术实力不会改变，网络日益开放，信息传输速率变的越来越快，但有关安全问题不可忽视。为了确保网络通讯的安全性和信息的品质，务必制订完备的管控机制和对策，采用多元化的方式，充分保证网络运转的可靠性和稳定性，符合大众需求，确保客户的合法权利。

1 大数据背景下信息通信网络安全管理现状

1.1 信息通信网络安全管理意识比较薄弱

虽然大部分单位和个人大体上早已适应互联网时代，对信息通信网络的安全工作有了一定的高度重视，但依然存在信息通讯网络安全管理观念严重不足的问题，特别是对信息通讯网络安全管理观念严重不足的问题。意识到人工智能的开放性、整合性和互动性，无法重视在信息传播方式中搭建更精准的网络安全管理体制，数据信息信息资源保护不足，如一些开发计算机单位和个人。通讯中应用了一些盗版，网络防火墙基础建设比较小，非常容易遭受电脑病毒攻击。智能手机迅速发展也使云计算技术的应用更为普遍：一部分客户使用手机时，疏忽信息通信网络的安全工作[1]，随便开启联接，造成侵略与控制智能机，造成更多的财产损失。

1.2 缺乏先进的网络安全设备

随着信息通讯技术实力的不断提升，对通信网络的安全性给出了更为明确的规定。必须积极主动开发和引入前沿的安全工作设备和设施，以尽快达到人们对于通信网络安全要求。但经营过程中，目前安全工作设施设备科技含量还需要进一步提升。虽然在我国十分重视安全隐患，根据各种方式提升了通信网络的安全标准，但有关设施的专业技术和特性并不健全。网络安全管理管理体系存有众多系统漏洞，为犯罪分子带来了机会。通讯系统常常遭受网络黑客和病毒进攻。除此之外，已有的安全防护体系并不健全，造成很多关键信息泄漏，对消费者造成威胁，对于企业及相关部门组成严重危害。

1.3 信息通信网络安全管理体系不够完善

完善的信息通讯网络安全管理管理体系对提升和优化互联网时代信息通讯网络安全管理和现代化发展具备强有力推动作用，但一些单位和个人还比较弱，尤其是在这些方面，很多企业都还没专业大数据安全管理平台、管理方案、安全管理机构和管理者。比如，很多公司早已设立了“大数据运营和综合服务平台”来充分发挥人工智能的作用和功效，但却没有创建专门“大数据技术安全管理平台”。云计算技术的迅速发展，让网络黑客盗取信息变得越来越非常容易。一些单位和个人都还没意识到这一点，信息通讯网络安全管理组织管理体系、工程项目管理体系、防止机制和操纵服务体系还欠缺规章制度。

2 大数据背景下信息通信网络安全技术分析

2.1 收集与分析技术

大数据技术相关技术的应用通讯网络系统中，在一定程度上依靠运营环境自身的实际需要，这务必对于数据信息与对应的顾客执行精确的精准定位操作，并且在数据信息收集与对于数据信息的探索层面开展更进一步的处理方法操作，从而保证完成根据针对通讯网络系统经营过程中无线天线的抗干扰性信息数据信息执行全方面的搜集与分析操作[2]，确立并精准定位在其中发生的出现异常情况及其数据信息层面的差异，主要目的是确保通讯网络系统在相对较高的高效率中进行运行，并且必须将其和GPS相关技术性执行特殊层面上的结合操作，进一步开传出对于数据信息自己的三维立体规定性跟踪作用。

2.2 数据信息存储系统

数据信息的储存做为大数据技术相关技术的应用通讯实践应用中的重要环节，无论是数据信息的收集、剖

析层面，或是在之后的数据标准化及其文件存储层面，相关的存储系统一直以来都是科研人员关注的焦点具体内容。在数据信息开展存放的一个过程当中，务必有意识的形成对应的数据库系统。

3 大数据背景下信息通信网络安全管理管理策略

3.1 提升信息通信网络安全管理观念

针对做好互联网时代信息通信网络安全管理而言，非常重要的便是需要对此项工作给与十分重视，充分发挥各个方面的积极意义，充分打造出具备突破性的信息通信网络安全管理体制，进一步加强有关资金投入幅度，勤奋使信息通信网络安全管理完成更大突破。在具体执行过程中，需要对信息通信网络安全管理开展科学布局、系统软件计划和创新融合，从防范与控制信息安全隐患、数据安全风险、网络安全风险层面，努力提高信息通信网络安全管理的整体性。

3.2 健全防护系统的前提安全防护

在复位环节中，工作员能设客户的管理权限，便于更强提升系统安全性能。例如，为防止操纵系统设定，导致网络安全问题，以避免故意原素登录系统。此外，当设备在检验环节中，查验到该问题的时候，一定要立即采取相应的防护措施，才能保证应用系统的安全性[3]。比如，针对信息进行数据加密，提高其安全，数据信息信息只可以收货人查询，那样立即信息被阻拦，第三方也无法读取具体内容。

3.3 做好黑客防范，提升硬件配置设备维修管理

黑客对信息和通信网络组成关键威协。针对网络安全管理，应加强黑客违法行为的防范，积极主动开发和运用有关的防范技术性，减少黑客进攻风险。黑客进攻技术性具备极高的专门性、多元性和非理性因素，要坚持实事求是，搭建多样化的防范技术标准体系和防范体制，才可以避免黑客违法行为的产生。此外，硬件配置是信息沟通交流的基本，因而，要高度重视日常运行维护，不断完善检修管理方案。规章制度建设要综合考虑硬件配置、机器设备的运转要求及特性，融合机器的技术说明，高效地确保了检修管理方案和全面的合理化和合理性。除此之外，还需要做好设备日常维护与维护，及早发现和清除系统异常，保证信息通信相关工作的稳定性。

3.4 完善信息通信网络安全管理模式

想要保障信息通讯网络安全管理方面获得更强成果，就必须不断完善和优化信息通讯网络安全管理机制。融合信息通讯网络安全检测新举措，进一步增加信息通讯网络安全检测幅度，及时掌握信息通讯网络安全趋势，详细分析评定安全性情况。信息通信系统，借助深度神经网络模块和人工智能技术提升安防监控。收集剖析机器设备、数据流量和节点个人行为等数据，以建立“安全性即时聊天”管理框架[4]。在提升信息通讯网络安全管理机制层面，还要加快构建“网上”与“线下推广”结合的信息通讯网络安全方式，积极主动构建信息通信系统造就生态环境保护。安全性，恪守大数据基本。提升信息通讯网络安全项目生命周期一站式管理模式基本建设，从确保数据资金安全的战略层面考虑，搭建安全性“三位一体”管理机制信息通信系统大数据安全性、安全通信运用和信息安全性。

3.5 数据水印技术的应用

移动互联网科技的迅猛发展和成长，大家应对的不仅是各种各样文字信息，以及各种声频、短视频、图象等信息，传统加密算法对其数据开展数据加密时已无法融入大数据时期。更改。应用数据水印技术性保护区音频视频信息，将一些具备验证功能性的暗含信息融入被照顾的数据中，能通过专业设备和探测器载入。声频信息，此数据有可能是特有标志、创作者系列号、数字公司序号等，以保障有关数据的著作权。此外，因为水印科技的安全性，水印不容易被盗取，不会受到客户工作中环境的作用，与此同时水印技术性具有极强的唯一性，水印具有极强的偶然性，不容易被拷贝精确，使用方便[5]。在水印技术性中置入水印或数据识别系统，完成水印技术性数据管理方法分权限设置，使不同类型的客户见到不同类型的水印信息。

3.6 提升风险防范能力

健全风险管理系统。健全通讯网站运营风险管理制度，融合岗位工作职责制，明确风险管控有关工作规定、工作要求和工作内容，合理促进管理方案的实行，形成长效高效的体制运作模式。对专业以及相关系统软件设施规划、设计方案、执行、运行管理和损毁环节，执行项目生命周期风险管控，健全管理制度规定，规范工作流程，保证系统运维安全性，防止运送网络安全受管理方法要素风险管控危害[6]。与此同时，关心新技术应用、新机器，在设计环节便对设备开展风险评价，避开技术性、机器设备、设备自身带来的损失。

3.7 构建专门的信息通信网络平台

在大数据环境条件下，想要提高通讯的安全性和稳定性，确保互联网的正常运转，必须建设专用通信系统平台，进一步提升数据质量。要充分调动信息科技功效，完成精确建设。需要把物联网技术与互联网紧密结合，将二者融进日常生活与生产过程中，充足达到大家

的需要，提高效率和生活品质。在建设本平台时，为确保平台的正常运转，必须制订科学合理的平台建设整体规划，确立平台的设计目的，积极主动健全和改进平台的功效，严苛保证网络信息安全。在硬件软件开发中，必须引入性能健全、作用相对稳定的元器件与技术。除此之外，还应注意病毒感染和黑客入侵等意外事件产生的影响，进一步提高平台的安全性[7]。为了能严格控制来源于外部浏览个人行为，务必设定专门网络防火墙，并且在发现异常前进行硬件配置防护，以充分保证传送数据的安全性，标准浏览个人行为。为了能进一步提高通信系统平台的安全性和稳定性，必须对设备连接端口号进行全面的的评估和操纵。一旦检测出外界侵略，务必第一时间关闭端口，并采取相应的预防措施，全面保障设备和平台的安全性。除此之外，还要有效管理平台的建设成本费。公司在购置设备时，不但要了解设备的性能，还需要充足控制和设备有关成本。在成本管理上，公司一般采用下列方式：一是降低通讯网线端口和配电线路总数，二是减少通讯间距。这不但减少了平台的建设成本费，也减少了后期维护费用。在规划硬件配置时，企业需要考虑系统及设备间的兼容模式。在引进设备时，除开要了解设备的功效和安全性，还需要确保设备与设备中间连接和通讯，确保数据的合理传送，完成资源整合共享。

3.8 定期诊断和修复网络漏洞

通过对当前网络安全事件的调查分析，发现大部分安全隐患源于自身的安全问题。因此，安全人员应该收集更全面的信息并建立数据库来识别安全系统风险。基于此，还应加大手机、电脑软件扫描力度，对内部文件、外部设备（U盘、硬盘）等被访问文件进行安全保护。如发现异常，应立即报告并立即处理。基于此，有必要对以往的安全事故进行客观的分析、预测并提出相应的对策，从而科学合理地利用各种资源，保障数据传输的安全[8]。同时，为保证系统的绝对安全，需要构建防护体系，根据不同类型的系统漏洞制定相应的防护方案。

3.9 完善信息通信网络安全管理体系

健全完备的信息通信网络安全管理体系，对提高信息通信网络安全管理水平具有强有力的支撑作用。单位要着力加强信息通信网络安全管理工作合力，建立专门的信息通信网络安全管理机构，配备专业的信息通信网络安全管理人员，配备通信网络，制定健全完善的信息通信网络安全管理制度。信息通信网络安全管理体系，如建立“大数据网络信息安全管理中心”。加强信息通信网络安全共建，进一步完善和完善信息通信网络安全管理流程体系，有效实现“内外网”分离。为加强对网络信息通信用户的教育培训，既要强化其风险意识，又要引导其按规定程序和要求开展工作，有针对性地开展不同部门之间的协调与合作。

结束语

综上所述，大数据与信息通信安全技术相结合，可以通过多种方式全面监控各种工况下产生的所有数据，从而提高监控效率和信息质量。信息通信速度有了很大提高，但也带来了一些安全问题，因此，我国需要加强网络安全管理体系建设，制定行之有效的管理措施，切实保障信息通信网络安全。特别是在大数据方面，对信息通信网络安全管理措施的探讨，能够促进我国信息通信网络安全事业的扎实发展。

参考文献

[1]姚杰，李浩鹏.大数据背景下信息通信网络安全管理策略研究[J].科技资讯，2021,19(31):7-9.

[2]张婧.大数据背景下信息通信网络安全管理策略研究[J].长江信息通信，2021，34（10）：145-147，150.

[3]董克彬，朱曈，杜广让. 基于大数据背景的通信网络安全管理策略研究[J]. 网络安全技术与应用，2022(1):56-57.

[4]刘子铭.大数据背景下信息通信网络安全管理管理策略研究[J].网络安全技术与应用，2021(11):55-56.

[5]江育锋.大数据背景下信息通信网络安全管理策略研究[J].长江信息通信，2021，34（3）：158-160.

[6]许沙，丁丽华，王鑫. 大数据背景下信息通信网络安全管理策略研究[J]. 中国设备工程，2021(19):45-46.

[7]李源浩.基于大数据的信息网络安全研究综述[J].中国安全防范技术与应用，2021（3）：74-77.

[8]王金京.大数据背景下信息通信网络安全管理策略研究[J].数字通信世界，2021（1）：105-106，113.