新时期通信网络系统安全防护路径探究

张斌

广东南方通信建设有限公司，广东广州，510630

摘　要：近几年来，科学技术的发展让信息网络的依赖度越来越高，因此加强信息通信网络安全性非常具有现实意义。网络通信安全问题随着互联网的不断普及与应用得到了人们越来越高的关注。现阶段的通信网络安全通信网络结构的复杂性、通信设备种类、风向评估方式等因素导致网络通信存在安全风险隐患。对此，人们在应用计算机期间，需要增强安全防控的观念、意识，不但需要完善、健全网络安全管理系统。由此，全方位落实、贯彻计算机安全威胁防控，能够防止计算机发生信息盗取与截取、黑客入侵与攻击等方面的问题。基于此，本文主要探讨了新时期通信网络系统安全防护路径。

关键词：通信网络系统；安全防护；路径

中图分类号：F626.5　　**文献标志码：**A

0　引言

随着时代的发展以及社会经济的转型升级，计算机信息技术的应用范围以及重要性获得了大幅度的提升，通信网络系统安全防护作为关系到通信行业持续发展的重要工作环节，应当受到有关部门以及相关企业的高度重视与研究，除了应加强通信网络安全防护体系建设、数据加密技术研发以及加强通信网络环境监管等工作的开展，还应重视通信网络安全管理专业人才的培养，对通信网络系统安全防护水平的提升以及通信行业的健康、持续发展有着重要意义。

1　现阶段通信网络优化存在的问题

1.1　数据处理难度大

数据处理作为通信网络运营的关键点。在每个单位时间内，通信网络内部的基础数据层、数据访问层、数据记录日志等运行环节中都有着大量的数据信息需要同步处理，数据类型众多且处理环境复杂。随着通信网络的发展，通信网络的数据量一直在稳步增长，数据处理的难度也会随之加大，此时就需要对数据的处理方式或算法进行改良。与此同时，现阶段我国通信网络的主要架构模式为超密集结构，这种架构模式能高效地完成数据信息的采集，但缺乏对边缘性数据的敏感度，容易出现采集遗漏，从而导致通信数据缺失，影响后续数据分析、价值挖掘等环节的开展[1]。

1.2　软硬件设施安全问题

信息通信过程中，软硬件设施是整个网络运行的基础环节。对于硬件设施来说，无论是在办公还是学习中，都会涉及到计算机、存储设备、网络终端以及通信设备等方面。如果这些硬件设施存在安全风险隐患，例如：受到外界环境因素的影响而导致设备损坏，或是运行时间过长，导致设备处在故障状态，那么在使用过程中就必然会影响信息通信的整体质量。当设备存在安全隐患时，就会使得数据在传输的过程中面临着泄露、丢失的风险，严重的情况下还会损害通信网络的运行以及相关业务的正常进行。

1.3　通信数据安全防护不到位

通信数据安全防护工作是通信网络运营的重点。由于通信网络所需处理的用户数据过于庞杂，数据的安全问题不是仅靠单一的某条机制条例或者某项技术就能解决，而是需要一个完善的数据安全管理模式。目前我国通信网络的数据安全保障体系尚未健全，存在数据安全问题难发

现、难处理等现象，严重阻碍了通信网络的健康发展[2]。

1.4 存在病毒侵染风险

网络病毒、木马是最为常见的通信网络安全风险因素之一，不仅可以通过文件、网站等多种途径传播，还具有极强的隐蔽性特点，可以隐藏在内存以及计算机系统文件当中，如果计算机用户的网络安全意识较弱或者没有采取一定的病毒防御措施，很容易导致计算机被网络病毒和木马侵染，并通过计算机向网络中复制、传播，轻则会对计算机用户的网络使用体验造成较大影响，重则会致使计算机用户的个人数据信息被破坏或窃取，并为计算机用户带来一定的经济损失。

1.5 通信网络安全评估不合理

人们对通信网络的依赖性随着网络设施的发展完善而不断加深，网络的后端积累着大量的用户数据，需要进行处理，目前数据处理只能依靠网络后端的管理中心进行，这就为网络通信的安全带来了极大的管理风险。同时，在网络安全评估上还没有有效的数据分析方式，网络通信的风险等级还只能依靠相关分析人员的经验与直觉进行判断。而这样的风险评估方式并不具有精确性，也很难对风险进行及时的评估[3]。

2 新时期通信网络系统安全防护路径

2.1 优化通信网络架构

通信网络系统是由不同业务功能的系统接入基于IP的核心网络组成的信息平台，为了满足不同用户对于不同功能业务的需求，通信网络系统具有优秀的可拓展性和灵活性，其通信网络结构自下而上可以分为物理层、网络业务执行技术层以及应用层。不同的结构层都有各自的功能，他们的目的都是用以协调各项业务，为用户提供更加满意的服务。用户的申请、接入、业务执行等操作都需要大量的数据进行输入、处理和输出。此时大数据技术的应用便是强化了网络架构中的数据处理功能，通过设置数据处理中心，可以开拓更多数量的数据传输渠道，使得通信网络能更加高效、高质量地完成各项数据处理操作。

2.2 构建通信网络信息数据存储体系

第一，政府信息化管理部门要加强通信网络领域的基础设施建设，通过建设统一性、开放性的网络信息数据库和信息平台，从而为各大运营商提供统一的用户信息，避免运营商基于自身需要单独搜集用户信息，进而解决信息数据重复性搜集的问题。同时，政府部门要出台相应的法律法规和政策文件，对运营商在用户信息数据方面的共享共用提供规范性的指导，打破网络运营商间的数据信息垄断，实现信息的共同存储和使用。第二，通信网络运营商要主动对接公共网络基础设施，提高对公共网络信息数据的利用率并增强利用效果，避免过多地搜集一些无效性的信息，最终提高信息搜集和处理的能力[4]。

2.3 强化信息安全保护立法

信息化环境中，传统的信息测算方法已无法满足企业精准洞察和精准服务的需求。为此，运营商要完善数据质量管理，在挖掘利用大数据商业利益为企业提供信息服务的同时，必须承担其社会责任。比如从源头治理垃圾短信及电信诈骗工作，切实服务于客户利益。同时，运营商要高度重视信息数据安全保护工作。国家也应从法律层面制定相应的法律法规，重视信息数据安全工作。尤其要在数据挖掘、数据信息传输、和信息安全等方面进行完整立法。例如，我国出台的《国家网络空间安全战略》和《“十三五”国家信息化规划》《网络安全法》等保护信息数据的法律法规及文件，从行业、国家层面制定了保护个人网络信息的相关标准，尤其是自《网络安全法》实施以来，运营商均开始研究部署有关法规、政策的落地工作[5]。

2.4 加强设备安全管理

设备作为信息通信网络安全的重要基础和

保障，加强对设备的日常维护和管理，对整个网络安全管理有着非常重要的作用。在对信息通信网络进行应用的过程中，相关使用者应派遣专员对设备进行定期管理和维护，包括对设备所处的环境、设备运行状态等进行有效管理。还要加强对设备以及线路的巡检，做好日常参数的检测、设备的维护与保养、线路的养护等。与此同时，要建立完善的设备管理制度对整个管理工作进行约束和规范，定期对设备进行检修，及时排除其中存在的故障和隐患，保证各项设备的稳定运行。除此之外，还要定期对设备进行更新与替换，引进更多先进的设备，这样也能够在很大程度上提升整个设备的安全稳定性。

2.5 提升网络数据安全保障能力

第一，运营上应构建和完善网络系统安全保障机制。在通信网络系统构建及运营中，运营商应该在系统中加入防火墙、入侵检测和病毒查杀等技术，及时了解和把握通信网络中存在的信息安全漏洞和不足，以便能够及时采取相关措施补足漏洞，从而防范安全风险，并为大数据技术应用创造良好的系统条件支持。第二，网络运营商要加强数据处理行为的规范性。运营商在平时的通信网络建设及运营中，应创建完善的数据安全工作机制；各部门人员在平时的大数据技术操作中，高度关注网络系统的安全性；运营商对数据采集、处理和存储等关键环节的安全保障措施进行规范化的检查和监测，从而及时发现和解决网络数据中的安全漏洞，并对相关责任人员进行追责，确保数据信息管理的安全性[6]。

2.6 强化网络系统数据信息加密工作

第一，端到端加密技术，主要是在数据信息传输之前对其进行加密处理，且在数据信息传输过程中不对其进行解密，而是在接收端对数据信息进行解密，与链路加密技术以及节点加密技术相比较，端到端加密技术更加安全可靠，哪怕不法分子对网络节点进行入侵也难以得到切实有效的数据信息，再加上端到端加密技术具有较好的稳定性以及使用方法较为简便等特点，在通信网络系统安全防护工作中有着较为广泛的应用。

第二，设置访问权限和密码，在网络安全维护与管理工作中，为了防止大数据背景下数据的不慎泄露或是遭到他人的恶意盗取，管理工作者可以从内部对数据信息进行加密处理，提高网络平台数据的安全程度。这要求管理工作者在数据在网络渠道传输活动进行前，提前做好加密协调的设置工作，以二次加密的形式在网络数据平台的加密基础上强化数据传输的安全性，以此尽可能地减少数据传输过程中的泄露问题。

第三，节点加密技术，是一种与链路加密技术非常相似的技术手段，都是在线上对数据信息进行加密，但二者的不同之处在于，节点加密技术主要是在网络节点的安全模块中进行数据信息的解密和加密处理，使得数据信息不会以明文的形式经过网络节点，进一步提升了数据信息传输安全性。

2.7 及时排查和修补网络系统漏洞

系统漏洞是造成信息通信网络安全问题的主要原因之一，因此在网络安全监管工作中切实做好漏洞的排查与修补工作同样是安全管理人员重要的工作内容之一。在大数据技术的应用模式下，管理工作者能够对漏洞相关数据进行进一步的整合，并以构建数据库的形式，将网络安全管理模型进行共享，以此为大范围的网络安全防护工作奠定重要的数据基础。同时，在通信网络安全管理工作中，管理人员还应该合理地利用大数据的检测与云计算功能对系统进行更大范围的防护排查工作，以此通过强化扫描通信设备与计算机系统的方式实现安全检测实践，以此做到及时发现漏洞并第一时间完成漏洞的修补工作，最终实现预防病毒入侵的目的。

2.8 积极应用防火墙技术与入侵检测技术

防火墙技术可以被当作“门卫”，在获得其准许后，相关数据可以通过，在并未获得其准许后，相关数据无法被传输，因此，该技术可以对部分潜在性威胁进行防控。一般防火墙技术共

包括四大构成，依次是包过滤、应用网关、服务访问规则、验证工具。而防火墙技术共包括三大种类，依次是状态检测防火墙、分组过滤防火墙、应用代理防火墙。防火墙技术在计算机网络系统中是“首要防线”。对于入侵检测技术，其也是十分关键的网络系统防控技术，是“二道防线”。若系统被外部所入侵、攻击，或是部分非法信息借助防火墙而进入至系统，入侵检测技术就可以马上对其进行检测，以检出各类不法的信息，并报警，或是马上对其进入行为加以阻隔，以保护好系统的稳定性、安全性。

2.9 完善通信网络安全运行评估系统

建立完整的电力系统信息通信网络安全运行评估系统意味着对电力系统通信网络管理力度增强，能根据评估结果有效优化电力系统网络运行流程、环节、内容。建立完整的电力系统信息通信网络安全运行评估系统，需要打造一支专业的电力系统信息通信网络管理团队。专业的管理团队能够加强电力安全防护系统的各项管理工作，一旦出现遗漏或纰漏能够立即用专业知识进行修补。网络安全评估系统管理人员在工作中一定要注意操作规范性，加强电力系统的网络配置，能帮助工作人员准确定位与确定电力系统运行中的故障位置和故障原因，提高管理效果。专业人员运行电力系统通信网络，还能减少黑客入侵风险。

3 结语

在当前的信息通信网络安全工作中，主要面临两大方面的安全威胁：一方面是软硬件设施安全问题，另一方面是数据信息存储安全问题。如果在这两方面受到了安全威胁，那么就会导致整个信息通信受到严重的影响。对此，需要应用计算机防御以控制好网络入侵、攻击，对计算机网络通信所出现的各类安全威胁进行分析、研究，进而应用更具针对性的防控对策，最终保障计算机网络通信能够更为安全、更为牢靠。

参考文献

[1] 刘素华.大数据时代保障公民数据信息安全的网络治理[J].理论视野,2016(11):45–49,59.
[2] 刘一平.张第.裴培.王爽.潘思宇.运营商数字化转型的思考与建议[J].信息通信技术,2021(2):17–23.
[3] 薛兴华.强化网络运营商数字化转型依法合规管理[J].互联网天地,2021(1):38–43.
[4] 符安文.计算机网络通信安全中数据加密技术的应用[J].电脑知识与技术,2020,16(31):62–63,8.
[5] 李鹏举.简析大数据背景下信息通信网络安全管理策略[J].IT经理世界，2021,39(5):184–186.
[6] 王文静.大数据背景下信息通信网络安全管理策略研究[J].广播电视网络,2021,28(4):59–60.