ISSN:2661-3719(Print); 2661-3727(Online)

移动互联网通信及信息化的维护工作

杨晏川
重庆信科设计有限公司　重庆　401121

摘　要：在信息化一日千里的发展的同时，互联网通讯技术也在高速发展，具有良好发展前景，由于网络技术自身的特点，具有不安全性，不法分子容易通过各种途径，盗取或是利用用户信息。为保障移动互联网用户的信息安全，必须加强运维管理，提升移动网络的稳定性和安全性。本文讲述了我国移动互联网通信及信息化维护工作存在的问题，及维护措施。

关键词：移动互联网；通信；信息化；维护

引言：

随着社会的发展和科技的不断进步，我国经济和科技的发展以惊人的速度在全球各国之间闯出了一片天地，这与我国的改革制度以及国家政策密切相关，除此之外，还有很多先进的网络通信技术被引进国内。因此，相关工作人员在进行工作时，一定要认识到通信工程建设的重要性，并且树立起责任意识，这样才能够促进工程建设的整体提升，促进社会的发展。

1　移动互联网通信及信息化维护工作存在的问题

1.1资金投入不足

互联网技术不断发展的过程中，很多企业得到了红利，也越来越希望能够通过互联网技术，为自身谋求更大的发展和利益。但是，这些企业或个人在利用互联网的同时，却没有投入相应的成本，也没有能力去研究和建设更新、更强大的互联网技术，进而制约了电子信息化的建设。也有一部分企业投入了大量的资金，但却没有找准方向，将资金投入到了运营方面的工作，没有重视技术的更新和维护，导致电子信息化技术水平永远都是保持在原本的水平，并没有随着时间的推移而革新，同时还会出现各种各样的技术问题。这些问题也就直接导致电子信息化建设无法前进，通信工程的建设也很难得到发展[1]。

1.2手机病毒

手机病毒是指一类具有传染性、破坏性的手机程序。可通过短信、彩信、电子邮件、网页、APP、蓝牙等多种途径在手机间进行传播，造成被感染的手机出现死机、关机、用户私人信息被盗、向外发送垃圾信息、自动拨打电话甚至SIM卡、芯片等硬件损毁等问题，导致手机无法正常使用、私人信息被盗取或话费大量消耗。比如近年来出现的“X卧底”病毒，入侵手机后不仅能识别手机用户的通话记录和短（彩）信收发记录，还能通过手机听筒实时监听用户的语音通话内容，此外还能利用GPS定位系统检测到用户出行路线和所在位置，这些都严重侵犯手机用户的隐私权。

1.3 WLAN安全运营

研究发现，现阶段我国三大运营商全国WiFi热点上百万个，三大运营商4G、5G的发展过程中，都高度重视WiFi建设。作为蜂窝网络的重要补充，WLan有着至关重要的作用，其是移动管商进行宽带市场切入点和基础，因此，我们要高度重视WLAN推广建设过程的信息安全和网络安全问题，在WLAN建设和运营过程中，存在着诸多安全问题，如，WebPortal安全问、利用DNS端口绕开计费问题以及AP钓鱼攻击风险问题等。

1.4互联网信息泄露

信息泄露可说是目前移动互联网信息化的最大难题。一项调查数据显示：45.5%的网络用户经历过即时通帐户被盗，32%的网络用户经历过游戏帐户被盗，而因为中奖、求助等网络钓鱼信息被骗取个人信息的则更是屡见不鲜；另有一份调查数据显示：在我国发生的网络信息泄密事件中，有85%属于内部泄密，即用户自己有意或者无意间造成的信息泄露，而内部泄密事件中，泄密途径前三位是信息存储介质（移动硬盘、U盘、内存卡、智能手机、平板电脑等）、信息传输介质（传真、打印、蓝牙等）和网络通道（QQ/微信等聊天软件传输、在线上传、邮件发送等）。由此可见，互联网信息泄露的原因与移动互联网通信技术的应用关系密切，加强移动互联网通信信息化的安全维护工作无可厚非[2]。

2　移动互联网通信信息化的维护有效策略

2.1日志审计技术措施

其维护互联网信息和网络安全基石，互联网日志审计措施是有关部门打击计算犯罪重要依据，因此，这就要求接入单位体统P地址、网络拓扑结构等，在防火墙，网关以及计算机主机上构建系统的较为完善的日志审计

记录。在这过程中互联网接入单位主要使用有关部门检测合格的产品，ISP单位可以研发相应产品，操作系统日志和系统时针时日志审计考虑的中的重点，具体包含了用户进行操作、用户登陆账号、系统启动时间以及关机时间等，技术人员每一次网络连接都必须要记录源IP地址、连接的时间、机器IP地址以及使用的协认等信息。

2.2 政府需加强对安全事件响应能力

我国如今对网络通信技术的发展非常看重，关于网络通信安全问题，政府应加强管理，采取正确的措施，积极传播正能量宣传，号召人们加强网络通信安全意识。随着信息化建设的发展和网络通信的普及，有些不法分子利用漏洞进行犯罪，对网络通信安全问题造成了一定的威胁，国家应对这种不法行为进行彻底查处并给予一定的惩罚、严厉打击，为建设良好的网络通信安全管理工作奠定基础。国家可以通过鼓励人们积极参与网络通信安全演习，以此提高网络通信安全意识。

2.3 加大网络通信安全研发创新力度

创新精神是国家和民族发展必须拥有的科学精神，要想解决网络通信安全问题，创新精神必不可少。除此之外，也要有强大的应变能力，在危险到来时，可以理智地做出正确的判断，这些能力都是我们要必备的，对加强网络通信安全问题具有促进作用。在对网络通信安全保护程序设计以及工作上也要加大力度，从根本上加强保护工作[3]。

2.4 加大资金投入

对于通信企业而言，在发展过程当中投入更多的技术和资金是非常有必要的。资金的投入，意味着相关的工作人员可以开展更多的工作，研究更新、更强的技术，带动整个企业甚至行业的发展。因此，在进行互联网背景下的电子信息化通信工程建设时，企业的领导者一定要树立起创新的意识，认识到电子信息化和互联网技术的重要性，并且敢于冒险，对通信工程投入更多的资金，促进整体水平的提升。通过资金的投入，相关工作人员可以更多的去研究新技术，同时也可以对整个工程进行良好的运营和维护，及时解决出现的的问题，并且保障整体工程建设的水平。这对于企业而言是一个非常重要的举措，不仅能够提升自身技术水平，带动企业发展。同时，还能够保障整个工程建设的质量，为企业和工作人员带来强大的后勤保障。企业和领导者也要足够重视后期维护工作，稳步的提供相应的资金，带动相关工作的顺利进行。

2.5 防黑客、防病毒防范

移动互联网信息被恶意破坏、盗取，最有效的措施就是做好防黑客、防病毒工作。一方面，移动网络终端应通过正规渠道安装通过有关部门检测的防病毒软件，清除手机、电脑中的病毒，并定期对软件进行升级，更新病毒谱；另一方面，技术人员应采用专业技术手段保护物理网络安全，安装防火墙、入侵检测系统（IDS），预防物理介质、信号辐射等引发的信息安全隐患，用漏洞扫描软件查找系统中可能存在的漏洞，关闭那些不必要的服务端口；另外，为防范系统口令泄露或被暴力破解，还可制订口令管理制度，进一步提升网络信息的安全。

2.6 过滤、关键字检查技术措施

过滤技术措施指计算机隔离系统外网、内网单元根据计算机当中一些存在安全隐患的文件类型记录日志告警、删除或是做过滤处理。关键字检查要是指计算机隔离系统外网、内网单元可以根据技术人员设定过滤不健康或是涉密信息，同时并将过滤到关键字的信息进行日志告警或是做摈弃处理[4]。

2.7 提升WLAN保密性

无线移动通信系统安全应由独立的安全中心和专业技术人员负责，安全中心向外提供一个接入口，系统其它模块通过此接入口完成鉴权、授权及其它安全功能，其余人员不必掌握加密、解密算法，这样可在一定程度上提升信息的安全性；另外，还应向无线移动通信系统用户推广网络信息安全理念，讲解无线移动通信与有限移动通信的区别，帮助用户设置安全性较强的接入密码，对接入者进行严格审核，谨慎授权，防止病毒通过WLAN感染终端设备以致私密信息受到侵害。

3 结束语

由于移动互联网通信具有一定的动态性、开放性，如何做好移动网络信息化维护工作，保障用户信息安全已成为当下移动通信行业的热点和难点。但是随着网络通信技术的发展，安全问题也越来越受到人们的重视，所以作为一名合格的公民，应具备良好的网络通信安全意识，以维持正常的网络通信。国家也应加强对网络通信安全管理，为以后的发展做好基础。

参考文献：

[1] 朱春霞.信息化通信工程建设研究[J].计算机产品与流通，2020（05）：69.

[2] 郑煌华.“互联网+”背景下信息化通信工程建设的研究[J].通信电源技术，2019，36（11）：167-168.

[3] 刘二岗.移动互联网通信及信息化的维护工作探析[J].中国新通信，2019，21（09）：6.

[4] 闵小翠，李鹏，吴楚民.无线移动通信系统中的安全问题及解决方案[J].网络安全技术与应用，2019，215（11）：65-66.