浅析网络通信中信息安全的保障措施

张　婧

（哈尔滨自然资源综合调查中心，黑龙江 哈尔滨 150932）

摘　要　本文主要以网络通信中信息安全的保证措施作为研究的课题，笔者在研究的过程当中，运用了文献分析法对专家学者的文献资料进行了细致化的收集和整理，并在研究过程当中融入了自身创新性的看法和见解。文章首先对网络通信信息安全的重要性进行了阐述；其次，对于网络通信中信息安全存在的不足进行了分析；最后，则是提出了网络通信中信息安全的保障措施，以期通过本文的研究能够丰富这一内容的理论研究，并且还可以为网络通信中信息安全的有效保障提供一定的帮助和借鉴。

关键词　网络通信　信息安全　通信软件

中图分类号：TN91；D920.4　　**文献标识码**：A　　**文章编号**：1007-0745(2021)10-0006-02

伴随着信息化社会的进一步推进，信息安全也成为了较为凸显问题，其已经融入到了国家安全的各个领域当中，这也为国家的经济社会以及政治等各个方面带来了一定程度的影响，成为了制约国家安全的主要因素之一，立足于信息安全对国家安全形成的重大影响这一角度进行分析，需要精确信息安全基础性的问题以及信息安全的表现模式，掌握信息安全要依赖信息网络化这一种规律，想要保障网络通信安全当中的信息安全，就应该结合网络通信安全的特点，建立相关的安全措施，使信息在网络环境当中能够保障其安全性以及整体性。

1 网络通信信息安全的重要性

网络通信的方式十分灵活，具备便捷性以及开放性等等特征，可以满足现如今网络时代背景之下人们学习、生活、工作的各种需求，在现阶段社会背景之下，网络通信的信息更是达成了范围的拓展，交往的加深以及合作的提升。伴随着网络通信的发展，各种安全问题也随之形成，网络当中不合理的架构，系统当中严重的漏洞等等都有可能成为黑客以及病毒侵入网络通信系统的机会。这也给网络通信系统带来了一定程度的影响，导致出现网络通信的安全问题，致使网络通信信息出现错误，因此需要为社会以及用户提供安全的网络通信信息。[1] 所以社会以及各个行业提出了网络通信信息安全的主要目标，并且将信息安全作为一项最为主要的任务实施不断的优化与完善，通过保障网络通信当中的信息安全，从而提升通信的质量。

2 网络通信中信息安全存在的问题

2.1 网络通信架构问题

网络通信技术当中的数据传播以及交换需要国际网络技术作为帮助，用户要获取查看信息的权利以及登录网站等授权，就必须要在网络当中进行用户名的注册，这一种注册需要参考网络当中 tcp /ip 的协议才能够顺利的完成，但是一旦在协议自身内部存在着一定的漏洞和不足，那么必然会形成网络黑洞，这一种网络黑洞会存在于协议树状架构当中，黑客以及网络病毒对此就可以进行入侵以及攻击，窃取用户以及企业等相关隐私信息，给个人以及企业合法权益带来一定的影响。

2.2 网络通信软件问题

在现阶段用户使用的通讯设备当中必然会安装一些软件，而安装的这一些软件，自身就存在着一定的安全性，所以客户在使用通讯设备的过程当中，通常会接收到优化和更新软件的信息。而形成这一种问题的主要因素就是因为现如今使用的软件具备一定的公开性，用户在下载安装之后就可以正常的使用，那一旦提供源代码，就可以对这一款软件进行任意的修改，软件在长时间的使用当中形容出现漏洞，没有获得优化和完善的问题，黑客就会在这一时间段运用病毒对这一漏洞进行攻击，导致信息的丢失和损坏。

2.3 网络病毒入侵

网络病毒是计算机当中传输的一种病毒，从整体上进行分析，网络病毒在传播的过程当中具备着速度快、范围广等特征，这一些病毒也具备着多元化的传播模式，通常状况下，网络病毒不只会对局域网当中的通信设备带来影响，还可以影响到远程工作站，这是因为病毒自身传播速度快以及传播方式复杂的特征，所以网络病毒很难被彻底的清除，这一些病毒就可以对用户的信息进行窃取，致使通讯设备的系统瘫痪。

2.4 用户缺乏网络安全的意识

用户在对网络通信技术方面缺乏足够的认知和了解，在下载安装软件过程时，容易受到不法分子的欺骗安装病毒软件，亦或是用户在使用软件当中因为兼容问题关闭防火墙，网络抵御能力大大降低。除此之外，用户在使用通信设施时，连接免费的 wifi 实施网上购物以及玩游戏，都会在无意间透露自身重要的信息，致使自身财产受到损失。

3 网络通信中信息安全的保障措施

3.1 强化通信协议 TCP/IP 的安全

通常情况下，病毒以及黑客在对网络系统实施入侵和

攻击时，都需要获得用户的 IP 地址，从而获得用户的隐私信息，对信息进行窃取。对于这一种问题，务必要做好 IP 的保护工作，需要用户对自身 IP 地址进行保护，在 tcp/ip 的架构当中，第二层是交换机，这是信息传播的必经之处，简单来讲其就是保证信息正常传播的主要方面。所以，一旦想要保护自身 IP 地址，那么就务必要加强对交换机的严谨性的掌控。除此之外，还可以运用隔离把控路由器的模式，对用户 IP 地址进行有效的保护，监管所有来访的 IP 地址，及时快速的发现可疑的状况并进行处理，从而避免黑客以及病毒的非法入侵，在一定程度上保障 IP 地址的安全性。

3.2 运用用户识别技术加强计算机通信系统安全

身份认证也可以称之为身份验证以及身份的识别，其指的是在网络通信系统当中，精确用户是否具备对一定资源的访问和使用的权限，从而使网络通信系统访问策略可以更加有效且可靠的实施防止入侵者冒用用户的账户名和密码获取资源的访问权限，保障系统以及数据信息的安全性。[2] 在现如今对于用户身份识别以及认证还采取较为传统的方式，也就是用户名加密码的模式，二者在同时输入之后才能够登陆并获取访问权限，因此这一种方式也具备着一定的安全性和保密性。其次，在现如今还会使用短信加验证码的形式，用户在想要登录网站时，手机会接收到四位至六位的动态密码，用户在登陆以及交易的前期，就会输入这一条验证码当中的内容。

动态口令也是一种较为基础的身份鉴别模式，主要是由数字、字母、特殊字符等内容组成，动态口令的形成和运用有着一定的随机性，因此这一种模式的安全系数和其他两种模式相比较高，可是在使用的过程当中，用户极容易忘记口令，致使用户无法及时的登录。双因素身份认证在现阶段已然使用在了网络通信信息安全保护当中，这一种认证模式在保密性方面获得了进一步的拓展，双因素可以说是将两种认证模式进行有效的融合，在现阶段最为广泛使用的双因素的验证模式主要有动态口令牌加静态密码、二层静态密码等等。[3]

3.3 完善防火墙系统

防火墙系统主要指的是在设定可信任的企业内部网以及安全区内部的一种部件的组合，其能够有效的监控、限制，甚至更改企图穿越防火墙的数据，其最大限度的对外部信息进行屏蔽，掌控信息的运行状况，以此来达成网络的安全保护，所以简单的进行分析，防火墙不仅仅是一个分离器，也是一个限制器以及分析器，其能够及时快速的掌控内部网络和 Internet 之间的网络数据流动，保证内部数据信息的安全性，从而来保障用户的个人信息。可是在使用网络防火墙的过程当中还应该强化扫描病毒的插件，只有这样才能够防止一些恶意病毒软件的入侵，一旦安装的扫描病毒插件无法应对病毒的入侵，那么就应该创设更加完善且高效的防火墙系统，在每一次使用网络时，都应该对反病毒软件实施数据的更新，只有这样才能够有效的保障网络通信安全当中的信息安全。

3.4 提升用户网络安全的认知

在现如今导致通信安全当中信息安全不稳定最为主要的因素就是黑客运用病毒对系统实施入侵和攻击，只要电脑或者手机存在一定程度的漏洞，黑客就能够对电脑或手机实施入侵，获取用户的隐私信息，达成非法获得经济利益的主要目的。[4] 伴随着时代的进步，科学技术也在持续不断的发展，病毒也随之变异，逐渐由单一向着复杂化进行演变，危害程度更是在持续不断地加深。对此，就需要用户提升自身对于病毒防范的警惕性，强化自身对通信网络中信息安全重要性的认知，对于有争议的信息以及链接，应该始终保持着警惕的态度。[5] 对此，用户可以在电脑以及手机当中安装服务软件，例如金山毒霸以及 360 等等，应定期对手机以及计算机等通讯设备进行病毒的查杀，及时的修复通讯设施当中存在的漏洞，以此来提升通信设备的安全性，保障通信信息的安全。

4 结语

综上所述，伴随着科学技术的发展，尤其是网络通信技术的进一步拓展，其为人们的工作、学习以及生活带来便利的同时，也形成了一定的问题，网络作为虚拟的空间，在发展的同时期出现的问题需要用户的关注和重视，并运用良好的措施对其进行解决，能够保障用户的信息获得保护。例如基本的个人信息、企业的商业信息等都属于机密信息，一旦对这些数据没有进行有效的管理，信息的泄露就会对企业、个人以及国家形成了十分严重的影响和损失。因此，本文对通信网络中信息安全的保障措施进行研究，分析现阶段存在的不足，针对不足提出有效的措施，整体性的保障信息安全，从而创设更加良好和谐的信息化社会。

参考文献：

[1] 杨栋 . 网络通信中信息安全的保障措施研究 [J]. 中国新通信 ,2021,23(12):3-4.
[2] 杨志贞 . 网络通信中的数据信息安全保障技术研究 [J]. 电子测试 ,2021(11):137-138.
[3] 窦怀振 . 网络通信中的数据信息安全保障技术研究 [J]. 电脑知识与技术 ,2021,17(11):43-44,53.
[4] 燕雯霞 , 刘会芳 , 张瑾 . 网络通信中信息安全的保障措施研究 [J]. 数字通信世界 ,2021(03):152-153.
[5] 郭丰 . 网络通信中的数据信息安全保障技术分析 [J]. 中国新通信 ,2021,23(04):155-156.