2023年信息安全的论文(精选13篇)

筹备已久的运动盛宴即将开启，别错过！如何宣传运动会，吸引更多人的参与呢？小编为大家整理的运动会宣传范文，快来参考吧！

信息安全的论文篇一

信息是社会发展的重要战略资源。下面小编整理的信息安全专业认知论文，欢迎来参考！

关于网络信息安全的涵义目前有好几种说法，其中一种有代表性的观点指出：网络信息的安全即信息系统安全，是指组成信息系统的硬件、软件和数据资源受到妥善的保护，系统中的信息资源不因自然和人为因素遭到破坏、更改或泄露，信息系统能连续正常运行。总括一句话，即网络信息安全不仅指“信息的安全”，而且指“网络的安全”。

网络的无主管性、跨国界性、小设防性、缺少法律约束性等特点，在为各国带来发展机遇的同时，也带来了巨大的风险。由于网络环境下的蓄意网络攻击的来源越来越广泛，一旦造成损害，就可能快速蔓延而酿成巨祸。而且很多敏感的信息甚至是国家机密很容易成为网络黑客甚至间谍窃取的目标，因此网络安全保障已经成为国家战略防卫力量的重要组成部分，受到了各国政府的高度重视。面对众多的开发技术与工具，在系统应用的安全性方面：如何确保合法的用户访问应用程序并获得相应的权限，从而不至于将应用程序用于其他用途；如何保证私有信息或单位内部信息不受到危害或恶意篡改；如何防止恶意用户的蛮力攻击等，是目前基于网络业务安全性研究的目标与核心。因此，使系统具有强大的备灾能力和安全性，具有可靠的通信数据安全机制是系统用户的客观要求。

由于internet是面向公众，任何一个网络一旦接入就要面临很多安全威胁。网络安全威胁主要是指网络中的主机有可能受到非法入侵者的攻击，网络中的敏感数据有可能被泄露或修改，在网络中传递的信息有可能被他人或篡改等。计算机网络所面临的威胁大体可分为两种：一是对网络中信息的威胁；二是对网络中设备的威胁。影响计算机网络的因素很多，归结起来针对网络安全的威胁主要有以下几个方面：

（1）人为的无意失误：如操作员安全配置不当造成的安全漏洞，用户安全意识不强，用户口令选择不慎，用户将自己的账号随意转借他人或与别人共享等都会对网络安全带来威胁；（2）人为的恶意攻击：这是计算机网络所面对的最大威胁。敌对的攻击者和计算机犯罪就属于这一类。此类攻击又可以分为以下两种：一种是主动攻击，它以各种方式有选择地破坏信息的有效性和完整性；另一类是被动攻击，它是在不影响网络正常工作的情况下，进行截获、窃取、破译以获得重要机密信息。这两种攻击均可对计算机网络造成极大的危害，并导致机密数据的泄漏；（3）网络软件的漏洞和“后门”：网络软件不可能是百分之百的无缺陷和无漏洞的。然而，这些漏洞和缺陷恰恰是黑客进行攻击的首选目标。曾经出现过的黑客攻入网络内部的事件，这些事件的大部分就是因为安全措施不完善所招致的结果。另外，软件的“后门’都是软件公司的设计编程人员为了自己方便程序调试而设置的，一般不为外人所知，但一旦“后门”洞开，其造成的后果将不堪设想；（4）操作系统存在安全性问题：现今流行的操作系统均存在着安全漏洞；（5）网络安全设备本身的安全性存在问题：网络安全设备本身是否存在安全漏洞、安全设置是否正确需要通过实际检验；（6）来自网络内部的安全威胁：据统计造成实际损失的安全事件有70%是内部人员所为，所以内部威胁恐怕是网络面临的最严重的问题；（7）缺乏有效手段对网络系统的安全性监控。

随着信息技术的高速发展和网络应用的迅速普及，保障信息安全，维护国家安全、公共利益和社会稳定，是当前信息化

发展中迫切需要解决的重大问题。

（1）明确责任，共同保护。通过等级保护，组织和动员国家、法人和其他组织、公民共同参与信息安全保护工作；各方主体按照规范和标准分别承担相应的.、明确具体的信息安全保护责任。

（2）依照标准，自行保护。国家运用强制性的规范及标准，要求信息和信息系统按照相应的建设和管理要求，自行定、自行保护。

（3）同步建设，动态调整。信息系统在新建、改建、扩建时应当同步建设信息安全设施，保障信息安全与信息化建设相适应。因信息和信息系统的应用类型、范围等条件的变化及其他原因，安全保护等级需要变更的，应当根据等级保护的管理规范和技术标准的要求，重新确定信息系统的安全保护等级。等级保护的管理规范和技术标准应按照等级保护工作开展的实际情况适时修订。

（4）指导监督，重点保护。国家指定信息安全监管职能部门通过备案、指导、检查、督促整改等方式，对重要信息和信息系统的信息安全保护工作进行指导监督。国家重点保护涉及国家安全、经济命脉、社会稳定的基础信息网络和重要信息系统。

自网络服务于公众起，网络安全问题就一直如影随形。滥用网络技术缺陷和漏洞的网络入侵，更让人们防不胜防。相应的网络安全技术也就出现了，如防火墙、病毒防护软件等。随着网络技术的飞速发展，新的威胁和脆弱点不断出现，从而对网络全技术提出了更高的要求。随着互联网的发展以及信息化程度的逐步提高，网络安全威胁也呈现出多元化、复杂化的趋势。依靠单一的防火墙已经很难解决现有的网络安全问题，网络安全要靠一个包括防火墙、防病毒、入侵检测、漏洞扫描器等多项技术和安全设备组成的安全体系来实现。

同时，要求我们从各个角度通过模拟预测、资源优化、协同联防等方式聚合调控各类安保资源，高效率地处理安全问题，实现网络信息空间整体安全。

信息安全的论文篇二

随着科技的高速发展，网络时代已如期而至，伴随着互联网+、大数据、云计算等新兴技术被广泛运用，人们的生活便捷性大大提高。在大数据时代，网络购物学习和交流不断进行，个人信息数据安全面临严峻的考验，信息泄露存在一定的风险，因此必须加强个人信息安全的保护工作，防止人们在网络交易过程中受到不法分子侵害。

大数据在本质上是一种电子数据，它具有自身独特的特性。首先，数据处理规模大。现今社会，全球每天产生的数据就已经达到4.5eb□这个数字仍然以惊人的速度高速增长。其次，数据信息快速化。信息产生的速度常常比数量更加重要，通过手机定位数据可以计算出一个商场当天的客流量，从而推断出该商家的当天营业额。最后，数据信息具有多样性。大数据的形态多样，包括了结构化、半结构化和非结构化数据。此外，现代互联网应用呈现出非结构化数据大幅增长的特点，来源形式多种多样，包括各种信息、应用更新、社交网络的图片、传感器读取的信息、手机的定位等，而且不少信息来源的重要方式都是新近才出现的。

1.个人隐私安全风险增大。网络的浩瀚性意味着数据来源更加宽泛和多元，监控摄像头、交互平台、移动电话、电子档案、数据库等，大量的信息堆积，必然给个人的信息安全带来影响和破坏，增大了个人信息被泄露的可能。

2.大数据成为了网络攻击的主要目标。在互联网时代，大数据能够反馈出更多、更有价值的信息，信息的含金量不断提升，带来的丰厚利润不言而喻，因此遭到攻击和盗取的概率也就越大。同时，大数据的窃取能够是不法分子获得大量相

关信息，一次获取，多重效益，必然让*客垂涎欲滴。

3.不法分子利用大数据精确攻击。大数据对于企业来说是财富是影响，对于不法分子来说同样是金钱是价值。不法分子在获取大数据的同时，也会反其道而行之，利用大数据来检索、定位，为新一轮的攻击盗取提供更加快捷的技术手段和方式。为了提升攻击的效率和质量，*客往往会尽最大可能的收集包括社交平台、微博微信、通话记录、电子邮件、消费记录等信息，并加以归档整理，方便下次调用，提高攻击的精确性和时效性。

1.加强舆论宣传，提高保护意识。国家网络相关部门要通过各种舆论宣传工具，对网络用户进行个人信息保护知识的宣传，提高公民对个人信息安全的认识和重视，树立公民保护个人信息、尊重他人个人信息的理念。个人在信息保护上是第一责任人，负有维护个人信息安全的当然义务。个人在进行网络行为时，尽量避免个人信息的泄露。同时，加强对个人电脑的安全防护，安装并及时升级杀毒软件与防火墙，提高个人上网设备的安全性能。

2.建立个人信息安全保护的法律法规。我国目前现有的法律法规对个人信息的保护虽然有所涉及，但这些规定都还只是零散地分布在各个法律之中，并未形成一个完整的个人信息安全保护的法律体系，而且没有一部明确保护个人信息的专门法律。立法保护个人信息，不仅突出了公民的信息自由权，彰显出以人为本的理念，回应了和谐社会权利有序化的诉求。同时还可保护网上消费者的个人信息安全，促使网络运营有序化，推动全国电子商务和电子政务的健康发展。

3.完善个人信息安全保护的技术措施。在互联网环境下，个人信息的泄露主要是由*客等机构外部人员获取和网络传输过程中的问题造成的，因此要加强软硬件的技术保障，从而保护用户个人信息安全。在硬件方面主要通过安装防病毒硬盘等硬件设施进行保护。在软件方面主要通过个人隐私安全平

台、加密软件、数据备份软件、自动删除个人资料软件等保护措施。针对网络上的个人信息易泄露的问题，网络营运商除了应向用户提供提示信息，还应该使用各种安全技术来保护网络用户的个人信息不被不法分子侵害。

4. 建立健全个人信息安全保护与防范机制。个人信息安全的保护不仅要依靠法律，更需要网络主体从业人员的道德意识以及自律意识。加强网络道德建设，用道德标准约束人们在网络上的行为，要让网络道德成为人们在网络中实施行为时的一个标准。对网络运营商而言，除了要对网络从业人员进行道德教育并提高行业自律意识外。

许多网络运营企业掌握着客户大量的个人信息，如果没有很好的防范机制就很容易造成信息的丢失。无论是电信运营商、电子商务企业，还是信息安全企业都需要对外来的技术攻击加以防范。因此，企业必须加强自我约束力，提高保护客户信息的意识，同时提高技术手段，完善相关信息管理系统，并对用户个人信息安全管理制度和流程进行梳理和完善，建立健全侵犯用户个人信息的各项管理制度与规范，用户个人信息安全管理和保护机制、问题处理机制、监督机制和奖惩机制等。对侵犯用户个人信息的情况，要做到迅速和准确处理。

大数据时代的到来极大地促进整个社会的发展。大数据在各行各业中的运用，使我们精确地了解到过去通过抽样调查很难了解的许多东西，让我们更深刻地认识了这个社会，从而更进一步改善这个社会。我们不应该否认大数据带来的益处，同样我们应该使这种益处最大化。但大数据带来的对个人信息安全的威胁我们也应该有着充分的认识。保护个人信息不仅是对社会每个成员的保护，更是对国家安全以及社会长期持续健康发展的保护。

信息安全的论文篇三

1.1计算机软件的bug

计算机软件在开发、使用的过程中需要经过编程开发、编码架构形成等一系列环节，计算机编码程序上的漏洞就会给不法分子带来可乘之机，进而给用户信息带来风险。

因此软件开发需要在相应的规范化的工作标准上进行，从而防止非法人员通过不正规途径窃取信息，降低使用者信息丢失和数据受损等一系列风险。

在现阶段，随着手机app的使用越来越普及，其安全性也引起了人们的充分关注，因此在软件开发过程中，数据安全的保障范围也要扩大到手机等移动端领域上。

1.2计算机病毒的入侵

计算机网络具有多元化的特点，也就是在信息的产生、传播、利用的过程中，可能会在某一个环节受到计算机病毒的攻击，从而对计算机系统的整体性能造成一定的影响。不同的国家有不同的网络法律法规，国外不法分子往往通过翻越网络墙将网络病毒植入其他国家。

再者，由于缺乏网络监管部门的监督管理，计算机软件会受到各类病毒的侵害，严重危害网络环境。网络病毒由于其传播速度非常快，带来的影响也是很大的，产生的数据流失等一系列安全问题可能会造成严重的计算机系统应用方面的后果。

2.1电脑病毒

电脑病毒具有多样性、潜伏性、超强的传播性，因此在电脑病毒的预防和处理的过程中，要对其传播途径加以控制。其

传播途径和类型呈现多样化趋势，计算机网页、优盘等都是其传播的渠道，在其潜伏的过程中可能会对计算机系统的稳定性和安全性等造成长期的影响而不被察觉。

首先，它潜入计算机系统，然后等待机会进而破坏计算机的核心系统。严重时，甚至会导致计算机系统瘫痪，使其无法正常运行。

2.2网络环境

开放的网络环境，在给人们的生活带来极大便利的同时，带来的信息安全问题也是不容忽视的。目前保障我国网络环境安全运行的方式主要有防火墙和网闸、安全认证等，使用时需要提前设定网络运行参数，然后对信息进行控制和筛选。

但是在信息化和大数据飞速发展的今天，这种方法难以满足目前的防控需求，且容易受到外界大数据的冲击。

2.3欠缺合理的人才培养机制

信息技术和网络技术属于新兴技术，发展速度非常快，因此在人才培养方面需要紧跟时代的步伐。技术能力提升是网络信息安全工作的重点。在计算机高端人才培养方面，我国欠缺健全的人才发展体制，信息技术专业化发展也不完善，人才队伍的逐步壮大也需要相应的人才培养机制。

在网络信息安全技术发展的过程中，计算机人才发挥了十分重要的作用，面对人才流失和发展能力不足等一系列的问题也需要加大人才培养力度，完善计算机人才管理制度，从而促进其更好地发展。

3.1制定安全管理制度，实现一体化安全管理

为了保证计算机和相关网络的`安全运行，需要大力提升网络

安全运行制度的管理水平。安全管理机制工作的完善，可以使得计算机网络的运行环境得到进一步的优化。首先，政府干预和对网络运行风险的政策性控制十分重要，通过对法律法规的完善，可以使信息安全管理工作得到个人和单位的双重落实。

其次，对于病毒入侵工作的重点防御，主要是通过完善安全监测、应急管理制度等工作，及时进行有效的控制，来减少安全威胁，保障日常工作的正常开展。最后，加强网络监督管理工作，以及监护系统的日常更新工作可以使计算机系统的运行效率得到大幅提升。

3.2防病毒技术在计算机中的应用

防病毒技术在计算机硬件的防护方面发挥了十分积极的作用，主要包括：病毒的预防技术、检测技术以及清除技术。

在工作中可以及时对病毒进行处理，使互联网、计算机的使用更加安全。预防病毒工作主要是利用技术手段阻隔病毒传播，而在病毒的检测工作中，会对病毒进行检测和针对性的处理，防止其对软件和计算机中的信息进行破坏。同时加强防火墙的使用，滤防火墙主要是对计算机系统从经由路由器获取的数据进行过滤。

3.3加强身份验证

目前，软件登录或人工出行安全检查都需要经过严格的认证，这是对自己和他人安全的保障。加密工作是在充分考虑业务需求和设备安全的基础上隔离相关网络。在重要数据的传输过程中选择局域网络和加密通道进行传输，并且对移动终端的接入更好地执行筛选工作，从而实现安全可靠的移动终端的接入工作。另外，实体认证工作非常重要。

进一步开展无线接入网与移动终端设备之间的身份认证，提

高用户的身份认证和信息传输能力，也是系统稳定的保障。除此之外，数字认证工作，也是提升数据安全性的另一种方式。利用端口访问控制以及物理地址过滤等安全性防护技术，为后台工作的稳步运行及监察监测系统工作的开展奠定了技术基础。监察监测系统需要对异常操作行为进行实时记录、监控，及时发现安全隐患，并对造成安全隐患的相关数据进行安全过滤以及筛查等，以提升系统的敏感度，确保后续工作的开展。

3.4加大计算机尖端人才的培养力度

网络信息安全的重要性是不言而喻的，同通讯安全、军事领域安全都有着密切的关系，尖端计算机人才的培养是十分重要的。从事网络信息安全的工作人员的能力、素质的提升，是网络运行防护系统能够稳定发展的前提。在技术层面上，可以对内部进行技能培训，强化学习计算机专业技术的相关知识点，培训之后还可以开展考核评估工作，考核的过程中可以进一步加强学习。其优势非常明显，一方面通过考核制度增强工作人员的学习热情。

与上岗作业环节相衔接的考核，在很大程度对技术人员的学习起到促进作用。培训考核合格方能上岗工作，考核不合格的人员将面临着重复的培训，甚至是辞退的风险。另一方面将考核制度与员工的绩效工资制度挂钩，提高了员工自主学习的积极性。通过再学习，可以提升员工的技术水平、安全管理和安全忧患意识，进而高质量完成各项工作。思想层面的提升可以更好地对电力系统的稳定性做出贡献，在和网络信息安全设备生产厂家的交流合作过程中，可以使工作人员对设备的工作原理、运行维护、检查检修等更加的明晰，有助于提高工作质量。

综上所述，网络在人们的生活中发挥了越来越重要的作用，为人们的生活增加便利的同时也给人们带来了网络安全方面的问题。在处理网络安全方面的问题的过程中，重视网络信

息安全问题，加强网络安全管理工作，可以更加科学的使用计算机，进而提高网络信息技术的应用能力。

[1]王民川。基于网络信息安全技术管理的计算机应用[j]□煤炭技术，2018.32(7)：36—37.

[2]邹小琴。基于网络的管理信息系统研究[j]□计算机应用研究，2017.19(1)：25—27.

[3]罗荣燊。计算机病毒防护技术在网络安全中的应用[j]□信息与电脑(理论版)，2018(07)：191—192.

[4]胡锐。计算机网络安全问题中的病毒辐射攻防[j]□电脑知识与技术，2018.14(07)：31—32.

信息安全的论文篇四

大数据在商业、政府管理和公民个人生活中均有应用。在普通服务业、电子商务业以及金融信息业等领域，大数据的使用可以帮助分析消费者需求，便于商家进行更精准的广告推介，开展便捷服务。

目前的电子商务平台所收集到的用户信息具有真实性、确定性和对应性，通过对这些数据进行分析，能够进一步了解客户的购物习惯、兴趣爱好和购买意愿，实现个性化服务。不光是商业，大数据对政府提高治理效率也提供了新的思路，起到不可小觑的作用。

政府是一国最具有公信力的社会管理机构，也是是最大的信息制作和使用者，它能够系统的管理和利用公民的个人信息，大数据时代的到来对政府管理社会秩序可以起到很大的帮助。除去户籍管理等这些基本数据应用，公安部门甚至可以结合个人用户使用水和电的数据判断哪些住宅是传销聚集地，因为传销几十个人挤在一个小房子里，用水用电量是超过正常

住户范围的。

这样对公安部门维护社会稳定起到积极作用。大数据的运用还渗透于公民个人的日常生活之中，公民可以根据他人在网络平台的相关信息，分析出对方的性格和喜好，对于个人社交起到很大的帮助作用。大数据对于公民日常的上网时间、消费状况、理财情况也能有一个系统的统计，便于公民个人自我了解，自我规划。

信息安全的论文篇五

编码重排这种较为常见的方式容易被人破解，进而对数据信息产生威胁，甚至造成不必要的经济损失等。当前我们有两种主要的加密方式：对称数据加密和非对称数据加密。对称数据加密算法是应用较早并且技术成熟的加密算法。在对称加密算法中，使用的密钥只有一个，发收信双方都使用这个密钥对数据进行加密和解密，这就要求解密方必须事先知道加密密钥。通过这些严谨并且成熟、高级的加密程序能够保证信息安全性，使得信息不被第三方所知。

信息安全的论文篇六

目前我国在收集公民个人信息缺乏规范的准入规则。在公民的日常生活中，存在着无权收集、过度收集，非法收集的现象。除了一些政府部门和商家之外，还有未经过批准的企业和个人进行着非法采集公民个人信息的活动，甚至有胆大包天的民间调查机构，私自成立调查公司，公然兜售公民的个人信息。

而有权收集个人信息者，则大多数存在着过度收集的问题，他们私自存储着大量的与自己业务无关的他人信息，掌控着本不需要存储的数据资源。而在实际操作中，政府部门也大量收集了覆盖公民生活方方面面的详细的个人信息。

像银行、电信、铁路、民航等部门就更不用说了，它们往往先准备好格式条款合同来要求用户填写，强制性收集他们的个人信息，比如家庭背景、手机号码、电子邮箱等，这些信息有时与这些机构的业务并无关系，但有时候公民却会因为预留了这些信息而遭到这些机构的电话骚扰。

信息安全的论文篇七

当前我国公民的信息安全规范化保护缺乏完善的法律支撑，应当建立单独的统一的针对个人信息保护方面的法规与制度，健全公民个人信息保护的处罚机制，包括宪法、刑事、民事和行政保护。依法追究违法违规人员的法律责任，促进个人信息的使用者自律，国家应为保护公民个人信息安全创建一个良好的法治环境，为大数据应用与个人信息安全的结合梳理出更为清晰的制度规范，建构符合我国国情的个人数据安全模式。

对于违反相关信息保护规定的，相关政府主管部门应加大惩处力度，加强对其在个人信息保护方面的问责。可责令其限期整改，对违规人员采取警告、罚款、没收违法所得、吊销许可证禁止有关责任人员从事网络服务业务等行政处罚，同时可将违法记录记入社会诚信档案。

随着实践中不断出现的个人信息被泄露的问题，我国在公民个人信息保护方面也加大了立法保护和司法、执法方面的保护力度，相关的法律、法规、规章和司法解释在不断的完善，法治层面的保障是提升公民信息安全的最有力的保证。

信息安全的论文篇八

在使用安全防御系统的过程中，未能合理应用现代化的数据防护技术方式，不能保证操作系统的安全性与可靠性，严重影响整体结构的使用效果。而在整体结构中，操作系统处于核心发展地位，成为恶意攻击的目标，导致操作系统的运行

与使用受到威胁。

信息安全的论文篇九

通过良好的信息安全治理， 可以保护企业的信息资产，避免遭受各种威胁，降低对企业之伤害，确保企业的永续经营，以及提升企业投资回报率及竞争优势。

通过长期的.实践经验以及结合cobit标准和gb/t 22080-信息安全管理体系要求，总结出信息安全治理的框架主要由四部分组成，如图1所示。

(1)信息安全战略：结合企业的整体信息技术战略规划和信息安全治理现状，制定信息安全战略。

(2)信息安全组织架构：根据企业层面在决策、管理和执行机制对组织结构的要求，建立信息安全治理框架和决策沟通机制，明确公司各级管理层及相关部门在信息安全组织架构中的工作职责与角色定位。

(3)信息安全职责：根据公司信息安全组织架构，进一步明确信息安全相关岗位的工作职责、分工界面和汇报路径等。

(4)信息安全管理制度：信息安全管理制度通过建立一个层次化的制度体系，针对不同的需求方(管理者、执行者、检查者等)从政策、制度、流程、规范和记录等方面进行信息安全活动相关的规定，实现信息安全的功能和管理目标。

6 信息安全治理评估

企业信息安全治理评估有助于提高信息安全治理投资的效益和效果。

企业的最高管理层和管理执行层可以使用信息安全治理成熟

度模型建立企业的安全治理级别。

该模型，如表2所示，被应用为几个方面。

(1)在市场环境中，相对于国际信息安全治理标准、行业最佳实践，以及直接竞争对手，了解企业在信息安全治理上的级别。

(2)进行差距分析，为改进措施提供明确的路径。

(3)了解企业的竞争优势和劣势。

(4)有利于对信息安全治理进行绩效评估。

7 结束语

本文从企业信息安全治理的实践出发，概述了目前企业信息安全治理存在的问题和困惑，总结了企业实现有效的信息治理的关注领域和实施内容，为企业建立良好的信息安全治理提供了基本框架。

参考文献

信息安全的论文篇十

摘要

关于网络信息安全的涵义目前有好几种说法，其中一种有代表性的观点指出：网络信息的安全即信息系统安全，是指组成信息系统的硬件、软件和数据资源受到妥善的保护，系统中的信息资源不因自然和人为因素遭到破坏、更改或泄露，信息系统能连续正常运行。总括一句话，即网络信息安全不仅指“信息的安全”，而且指“网络的安全”。

关键词网络信息安全认知思考

网络的无主管性、跨国界性、小设防性、缺少法律约束性等特点，在为各国带来发展机遇的同时，也带来了巨大的风险。由于网络环境下的蓄意网络攻击的来源越来越广泛，一旦造成损害，就可能快速蔓延而酿成巨祸。而且很多敏感的信息甚至是国家机密很容易成为网络黑客甚至间谍窃取的目标，因此网络安全保障已经成为国家战略防卫力量的重要组成部分，受到了各国政府的高度重视。面对众多的开发技术与工具，在系统应用的安全性方面：如何确保合法的用户访问应用程序并获得相应的权限，从而不至于将应用程序用于其他用途；如何保证私有信息或单位内部信息不受到危害或恶意篡改；如何防止恶意用户的蛮力攻击等，是目前基于网络业务安全性研究的目标与核心。因此，使系统具有强大的'备灾能力和安全性，具有可靠的通信数据安全机制是系统用户的客观要求。

1网络信息安全面临的主要威胁

由于internet是面向公众，任何一个网络一旦接入就要面临很多安全威胁。网络安全威胁主要是指网络中的主机有可能受到非法入侵者的攻击，网络中的敏感数据有可能被泄露或修改，在网络中传递的信息有可能被他人或篡改等。计算机网络所面临的威胁大体可分为两种：一是对网络中信息的威胁；二是对网络中设备的威胁。影响计算机网络的因素很多，归结起来针对网络安全的威胁主要有以下几个方面：

（1）人为的无意失误：如操作员安全配置不当造成的安全漏洞，用户安全意识不强，用户口令选择不慎，用户将自己的账号随意转借他人或与别人共享等都会对网络安全带来威胁；
（2）人为的恶意攻击：这是计算机网络所面对的最大威胁。敌对的攻击者和计算机犯罪就属于这一类。此类攻击又可以分为以下两种：一种是主动攻击，它以各种方式有选择地破坏信息的有效性和完整性；另一类是被动攻击，它是在不影

响网络正常工作的情况下，进行截获、窃取、破译以获得重要机密信息。这两种攻击均可对计算机网络造成极大的危害，并导致机密数据的泄漏；（3）网络软件的漏洞和“后门”：网络软件不可能是百分之百的无缺陷和无漏洞的。然而，这些漏洞和缺陷恰恰是黑客进行攻击的首选目标。曾经出现过的黑客攻入网络内部的事件，这些事件的大部分就是因为安全措施不完善所招致的结果。另外，软件的“后门’都是软件公司的设计编程人员为了自己方便程序调试而设置的，一般不为外人所知，但一旦“后门”洞开，其造成的后果将不堪设想；（4）操作系统存在安全性问题：现今流行的操作系统均存在着安全漏洞；（5）网络安全设备本身的安全性存在问题：网络安全设备本身是否存在安全漏洞、安全设置是否正确需要通过实际检验；（6）来自网络内部的安全威胁：据统计造成实际损失的安全事件有70%是内部人员所为，所以内部威胁恐怕是网络面临的最严重的问题；（7）缺乏有效手段对网络系统的安全性监控。

2浅谈主要应对措施

随着信息技术的高速发展和网络应用的迅速普及，保障信息安全，维护国家安全、公共利益和社会稳定，是当前信息化发展中迫切需要解决的重大问题。

（1）明确责任，共同保护。通过等级保护，组织和动员国家、法人和其他组织、公民共同参与信息安全保护工作；各方主体按照规范和标准分别承担相应的、明确具体的信息安全保护责任。

（2）依照标准，自行保护。国家运用强制性的规范及标准，要求信息和信息系统按照相应的建设和管理要求，自行定、自行保护。

（3）同步建设，动态调整。信息系统在新建、改建、扩建时应当同步建设信息安全设施，保障信息安全与信息化建设相

适应。因信息和信息系统的应用类型、范围等条件的变化及其他原因，安全保护等级需要变更的，应当根据等级保护的管理规范和技术标准的要求，重新确定信息系统的安全保护等级。等级保护的管理规范和技术标准应按照等级保护工作开展的实际情况适时修订。

（4）指导监督，重点保护。国家指定信息安全监管职能部门通过备案、指导、检查、督促整改等方式，对重要信息和信息系统的信息安全保护工作进行指导监督。国家重点保护涉及国家安全、经济命脉、社会稳定的基础信息网络和重要信息系统。

3结论

自网络服务于公众起，网络安全问题就一直如影随形。滥用网络技术缺陷和漏洞的网络入侵，更让人们防不胜防。相应的网络安全技术也就出现了，如防火墙、病毒防护软件等。随着网络技术的飞速发展，新的威胁和脆弱点不断出现，从而对网络全技术提出了更高的要求。随着互联网的发展以及信息化程度的逐步提高，网络安全威胁也呈现出多元化、复杂化的趋势。依靠单一的防火墙已经很难解决现有的网络安全问题，网络安全要靠一个包括防火墙、防病毒、入侵检测、漏洞扫描器等多项技术和安全设备组成的安全体系来实现。同时，要求我们从各个角度通过模拟预测、资源优化、协同联防等方式聚合调控各类安保资源，高效率地处理安全问题，实现网络信息空间整体安全。

信息安全的论文篇十一

信息安全专业，根据教育部《普通高等学校本科专业目录》，专业代码为080904k□属于计算机类(0809)。具有全面的信息安全专业知识，使得学生有较宽的知识面和进一步发展的基本能力;加强学科所要求的基本修养，使学生具有本学科科学研究所需的基本素质，为学生今后的发展、创新打下良好的

基础;使学生具有较强的应用能力，具有应用已掌握的基本知识解决实际应用问题的能力，不断增强系统的应用、开发以及不断获取新知识的能力。努力使学生既有扎实的理论基础，又有较强的应用能力;既可以承担实际系统的开发，又可进行科学研究。

信息安全专业的大学排名情况如何?

1、北京航空航天大学

2、哈尔滨工业大学

3、电子科技大学

4、西安电子科技大学

5、华中科技大学

6、华南理工大学

7、北京邮电大学

8、山东大学

9、南京邮电大学

10、武汉大学

11、上海交通大学

12、中国科学技术大学

13、海南大学

14、中国矿业大学(北京)

15、华北电力大学(保定)

16、北京交通大学

17、中国地质大学(北京)

18、东北大学

19、暨南大学

20、南开大学

信息安全的论文篇十二

进入21世纪以来，信息安全问题也日显突出，迫切需要加强信息安全教育立法工作。信息安全教育立法不仅具有必要性，还具有可行性。

信息安全;教育立法;安全教育

(一)信息安全教育立法是我国现阶段信息安全教育事业发展的需要

纵观信息安全工作发展历程，特别是改革开放以来，我国信息安全教育取得了显著的成绩，得到长足发展。随着社会信息化进程的不断深入，信息安全教育立法一直落后于全国教育的总体发展水平，已远远不能满足信息安全教育发展的需求。究其因，归纳起来，有社会、经济以及认识等诸方面的问题，不能起到保障和促进信息安全教育的作用。我国现阶段信息安全教育事业的发展迫切需要加强信息安全教育立法工作。

(二)信息安全教育立法是全面依法治国的需要

依法治国，建设社会主义法治国家作为新时期治国的重要方针。依法治国的一个根本前提，是有法可依。新世纪以来，我国法治建设对于推动经济持续健康发展和社会发展，保障国家经济社会发展，发挥了不可替代的作用。信息安全教育作为我国信息安全工作的一个重要组成部分和社会生活的一个重要领域，它在一定程度上影响着国家管理的法制化进程和信息社会化水平。

(三)信息安全教育立法是信息安全工作发展的需要

我国信息安全立法虽取得了一定的成绩，同时，在信息安全教育立法方面也存在诸多问题。要改变这种状况，就必须推进信息安全教育立法工作。只有这样，才能以法的形式把信息安全教育发展所要求的各种社会条件以及基本社会关系固化下来，从而保证信息安全以及教育工作稳定发展。

(一)教育优先发展战略地位的确立，为信息安全教育立法创造了有利的氛围

我国党和政府十分重视教育的发展，把科教兴国列为国家社会发展的战略重点，并颁布一系列法律法规为其发展提供了强有力的保障。这对于切实落实优先发展教育的战略地位，提高人们的思想认识，具有巨大的指导作用和十分深远的意义，从而也为信息安全教育立法创造了有利的外部环境。

(二)我国信息安全立法的实践与理论研究，为信息安全教育立法提供了经验和理论基础

改革开放，特别是新世纪以来，我国信息安全立法实践从国家和行业两个方面都取得了相当的进展，为信息安全教育立法提供了丰富的实践经验与广泛的内容范畴。随着信息安全立法以及教育立法的理论问题日益引起人们的重视与关注，许多信息安全工作者和法学工作者，将理论研究不断引向深入，探讨实际工作中的热点与难点问题，纷纷撰文或著书，

从而为探索和完善我国信息安全教育立法工作提供了坚实的理论基础。

(三)境内外信息安全教育立法的成果以及经验，为我国信息安全教育立法提供了有益提示

从世界各国信息安全立法的情况看，尽管出发点不完全相同，目的各异，甚至侧重点也不一样，不同国家的信息安全教育立法在以下三点基本上是相同的：一是都非常重视信息安全及教育立法，把立法工作摆在相当重要的地位;二是信息安全教育法规操作性强，内容明确;三是信息安全教育法规制约机制严明。对于境内外十分丰富的信息安全教育立法的经验，我们可以从中找到许多带有普遍规律性的问题，在我国的信息安全教育立法中认真加以研究和借鉴。

要根本改变信息安全教育事业的滞后状况，我们必须采取切实有效且行之有效的举措，切实加强信息安全教育的立法，从而起到保障和促进信息安全教育事业的作用。

(一)加强信息安全教育立法工作的宣传

首先，我们自身必须深刻认识我国发展信息安全教育的艰巨性和紧迫性，切实了解信息安全教育的特有规律及在推进我国社会信息化进程中的重要地位。其次要充分利用新媒体，让全社会熟悉、了解信息安全教育及立法的基本知识、基本理论。总之，我们要深刻认识信息安全教育立法现状的不适应性，明确信息安全教育立法对改变当前信息安全教育的落后状况以及推进我国信息安全工作的重要现实意义，从而树立和坚定信息安全教育必须立法的思想。

(二)切实加强信息安全教育立法的理论研究

紧密围绕信息安全工作实际，我们应在我国教育立法、信息安全立法一般理论的指导下，对信息安全教育立法的基本理

论问题进行深入的研究。要通过研究，掌握信息安全教育立法的基本原理，信息安全教育立法与一般教育立法、信息安全立法的区别以及联系等等。为此，当前，一方面我们可以设立信息安全教育立法研究会，通过举办学术研讨会、论坛等多种形式，推进相关热点、难点问题探讨的不断深入，从而在国家有关部门制定信息安全教育法律法规中发挥相应作用;另一方面可以设立专项研究基金，组织相关方面的专家、学者协同攻关。总之，信息安全教育立法的理论研究工作要在加强基础性的同时突出其应用性研究，要围绕信息安全教育领域基础性的、急需的内容，加强研究工作，以促成相关法规的制定。

(三)加快制定

《信息安全教育条例》等相关信息安全教育法律法规要从根本上改变信息安全教育立法的薄弱状况，就必须尽早建立和完善信息安全教育法规体系。健全信息安全教育法律制度，使得制定《信息安全教育条例》等一些基本的法律法规成为时代的必然。《信息安全教育条例》等的相关信息安全教育法律法制定与颁布，将极大地推进我国信息安全以及教育立法工作的进程，开辟我国信息安全事业和信息安全教育事业的新纪元。

[1]陈立鹏.民族教育立法与民族教育的跨越式发展[j].黑龙江民族丛刊，2019(6).

[2]杨清.新疆少数民族教育立法探析[j].新疆大学学报(哲学人文社会科学版)，2019(5).

[3]柳卫民.警察教育法学学科构建浅探[j].中国电力教育，2019(1).

信息安全的论文篇十三

尊敬的领导：

您好！

我的名字叫xxx□我是一名即将毕业的网络工程系信息安全技术专业的学生。我怀着一颗赤诚的心和对事业的.执著追求，真诚地向你推荐自己，并乐意为贵公司的发展壮大尽绵薄之力。

经过大学三年的学习，我丰富了知识、磨练了意志、提高了修养、培养了能力。在良师益友的教导和帮助及我个人的努力下，我掌握了专业知识，具有扎实的专业基础知识。掌握了计算机基础、计算机网络、计算机专业英语、数库原理及应用□sql数据库管理与设计、局域网□windowsserver□网页设计与制作□css+div□黑客攻防等课程。学习成绩一直名列前茅，并获得了国家励志奖学金。在学好专业知识的同时，培养了较强的自学能力和独立思考、解决问题的能力。能熟练操作计算机办公相关软件。在课余时间，广泛地阅读了大量书籍，不但充实了自己，也培养了多方面的技能。

我深知过去已经成为历史，面前的挑战却是空前的。如何从校园步入社会、走向工作实践?严峻的挑战将激发我更好的发挥潜在的能力。

第一、自信是我做任何事情的必备心态，所谓初生牛犊不怕虎，困难和挑战是我前进的无穷动力！

第二、诚信是我为人处事的道德基准，从自己做起，缔造诚信社会是我真诚的意愿和目标。

第三、良好的适应能力和学习能力，使我相信世上无难事只怕有心人，没有解决不了的问题！

收笔之际，郑重地提一个小小的要求：无论您是否选择我，尊敬的领导，希望您能够接受我诚恳的谢意！

祝愿贵单位事业蒸蒸日上！

此致

敬礼！

xxx

20xx年x月x日