最新安全防护文明施工措施费用投入计划表 安全防护措施(精选5篇)

计划是指为了实现特定目标而制定的一系列有条理的行动步骤。大家想知道怎么样才能写一篇比较优质的计划吗？以下是小编为大家收集的计划范文，仅供参考，大家一起来看看吧。

安全防护文明施工措施费用投入计划表篇一

1.1控制设备类型单一化

以硬件为基础的相关安全增强技术在适用性方面表现出了一定的不足，且安全功能单一，无法升级。软件方面，一些功能强大且针对性较强的安全技术，不仅实现了控制粒度的进一步细化，而且具备了多项安全功能，其不足之外在于，局限于特定设备的存储安全问题，如对信息的正确性进行检查，对数据进行恢复等，没有充分考虑信息传输的严格监控问题。另外，由于针对性太强，当需要对多种存储设备进行控制时，往往需要设计不同的控制程序，如此一来，关于全局外围存储设备的策略部署问题便会变得相当复杂，很难实现对外围设备的统一监管。

1.2没有详细的安全使用视图

许多现有技术过于简单，往往只做一些相对简单的控制，绝大部分没能提供审计功能以实现对存储设备安全使用的跟踪处理。如果需要进行细粒度的控制，则应该提供更为具体的外围存储设备的使用状况，以了解外围存储设备的整个使用现状，来提高进一步改进、改正策略部署，进一步改进系统的有用信息。

2.1对信息数据网络传输进行强制加密

计算机通信协议是一个完全开放的协议，在本身设计上没有关于安全性的考虑，所以，数据在网络传输过程中有被截获的风险。在解决内部网络信息安全问题时，应该具体到解决系统中任意两台计算机之间数据传输的安全性问题。为实现这一效果，应对信息数据网络传输进行强制加密，保证任意两台机器均具有不同的通信密钥，如此一来，便能最大程度杜绝侦听软件在内部网络的恶意侦听行为。加密之后，即使通过modem□adsl拨号以及双网卡等多种方式实现了对外的非法外联，也没有办法进行信息的互通，因为网络数据封装格式已经发生了改变，这样便大大降低了非法外联所带了威胁[2]。

2.2对本地硬盘进行强制加密

通过强加密算法来完成对所有本地磁盘数据的强制加密（除了系统盘之外），当确认内网安全产品完全启动且正常运行的条件下，才能正常打开本地磁盘，展开相关操作。为避免有人通过系统盘来窃取数据信息，一方面要严格禁止任何数据的写入，另一方面禁止私自安装任何一款新的应用程序；将那些写入系统盘的相关数据，全部缓存到指定的区域，当计算机系统被关闭后，那些缓存数据也随之被彻底清除。进行加解密时，应采用透明的方式进行，除此之外，还应充分考虑计算机用户的使用习惯。只要是本地磁盘中的文件，都将被计算机系统采用自动强制加密的方式保存到磁盘中。如此一来，磁盘不管是丢失，还是被盗用都不会导致信息泄密的问题。透明加密技术除了提高内部网络信息安全之外，还具有以下两点优势，一是不会对计算机中的应用程序造成不良影响，二是不会对计算机用户的使用习惯造成不良的影响。总之，对本地硬盘进行强制加密，能够有效避免硬盘丢失、多系统操作以及光盘启动等各种因素导致的内网数据泄密的发生。

2.3强化移动存储设备安全措施

只有得到管理员授权后，才允许在设定的范围内遵循既定的读写策略进行使用，从而实现对移动存储设备的严格管理，包括软盘□u盘以及移动硬盘等。在使用移动存储设备的过程中，如果被执行加密读写策略，那么转入该设备的全部数据信息将会被强制加密，仅能在管理员事先设定的一定范围内使用，如果将这些数据信息带离这个范围，那么它们将变成一些无法识别的加密数据，不能正常读写。上述方式对数据的可用范围进行了严格的限定。对于计算机用户而言，一方面可以享受移动存储设备所带来的便利性，另一方面又可满足对数据共享范围进行有效管理的要求。

2.4完善的身份认证授权体系

身份认证授权体系应该是一个完全独立的体系，区别于计算机原有的认证体系。对身份认证授权体系进行设计时，通常将软件认证体系和硬件认证体系进行有机结合，从而建立一个多重认证体系，以提高其安全性及可靠性，可以支持各类标准的ca服务器，应用起来十分方便，不会对原内部网络体系造成太大影响。同时，可实现对全部外设□i/o端口以及相关操作的授权管理，授权人仅可进入授权的区域并进行相关的授权操作，如此一来，为内部网络信息安全奠定了坚实的基础。

针对内部网络信息安全制定防护措施时，应本着方便、有效、先进的原则，重点解决信息数据网络传输问题、本地硬盘保密问题、移动存储设备保密问题、计算机用户身份认证问题，以实现外部无法入侵、内部无法窃取、拿走也看不懂的效果，从而有效避免重要信息泄漏的问题，构建一个安全、稳定、可控的内部网络，为企事业单位的正常运转提供便利。

安全防护文明施工措施费用投入计划表篇二

现在全世界都步入了信息时代，现在的计算机作为现在信息时代的产物，已经成为了人们生活学习以及各个领域处理信

息的物品，现在甚至有很多的人在离开了计算机以后，有很多人无法正常的工作与学习，可见现在计算机在人们生活当中是多么重要的。虽然现在计算机在使用的时候相当方便，但是现在计算机信息安全问题是一个比较常见的问题，也是困扰现在使用计算机的人的主要问题，如何有效的解决计算机信息安全问题是现在我们需要研究的问题。

现在有很多人，甚至企业国家，都有很多的信息存在于计算机当中，所以这些信息一旦泄露了出去，那么一定会给相关的企业与国家带来巨大的损失，会给企业与国家造成很多的经济损失，尤其一些国家的军事信息，财务资料，这些信息一旦泄露了出去，那么一定会造成很大的威胁。以下就是计算机信息安全所存在的一些问题。

2.1缺少计算机信息安全的关键技术

随着现在各个国家的发展，现在很多国家的计算机信息安全关键技术已经成为世界先進，跟这些国家相比较，现在我国的计算机信息安全的关键技术还比较落后，现在我国还有很多的计算机零件需要从其他国家进口，从其他国家进口的零件并不能保证我国相关计算机信息的安全，甚至在使用了这些零件以后，整个计算机的网络都存在被监听监视的状态，这是现在我国缺少计算机信息安全关键技术的问题之一。

2.2现在计算机存在很多病毒入侵

随着计算机的不断发展，现在有很多的计算机存在病毒，而且现在病毒的种类也在不断的增加，虽然现在有很多防止病毒入侵的软件，但是病毒也在根据这些软件更新，病毒常常能够利用人们打开网页的时机，进入到计算机当中，这些病毒能够给计算机系统带来很严重的危害，能够很严重的威胁计算机信息安全。

2.3信息传递时缺乏保障

现在是一个信息化的时代，现在人们也在用信息交流，在交流的过程当中，常常这些交流的信息就被有机可乘，在很多信息在发送过程当中，有些信息就会被盗取，这是由于信息在传递的过程当中缺乏一个保障的体系，有的信息甚至在传递的过程当中，并不能准确的到达另一台计算机当中。现在信息传递的时候确实缺乏一个完整的保障体系，并不能保证信息能够及时的传递。

2.4管理计算机信息不严密

现在计算机已经成为生活当中必不可少的一个工具之一，所以现在计算机需要一套完整的信息管理体制，但是现在存在的问题是，现在即使有一套完整的计算机信息管理体制，但是现在很多的相关计算机信息管理人员并不能够有效的管理，有很多的管理人员由于疏忽，有很多的管理人员甚至认为没有必要去管理，导致了现在有很多的信息都是由于这个原因而丢失的，在管理计算机的人员方面，现在有很多的人员由于并没有对于计算机使用相应的管理手段，很多人认为他们的计算机很安全，不用这些管理手段，计算机照样不会受到影响，但事实是，由于管理人员没有一个具体的管理体制，而导致了很多的计算机安全信息遭到了泄漏。这是现在比较常见的现象。

2.5对于计算机信息安全缺乏意识

现在很多使用计算机的人有关于间算计的。信息安全知识比较的缺乏，对于计算机信息安全意识并不强烈，现在网上管理并没有很大的资金投入，导致了现在很多人对于网上的信息安全有误解，也有很多的人并不了解现在网上的信息安全事故，人们认为只要平时在使用计算机的时候多加注意就能防止计算机信息的泄漏，其实并不是这样的，有很多网络现在其实并不安全，一旦出现了计算机信息安全泄漏的事故，人们就会不知所措，不知道该怎么办。

2.6在计算机信息安全遭到威胁以后不能及时的应急

计算机的系统在建设的时候是相当复杂的，网络的系统也是相当复杂的。在系统当中任何的一个地方出现了问题，那么一定会威胁到整个计算机信息的安全，往往在这个过程当中，我们很多人并没有一个合理的方式去拯救，去应急，所以现在有很多的信息泄露人们都是无能为力，面对各种的突发情况，没有一个紧急的预案来把问题解决，是现在的主要问题。

3计算机信息安全问题的有效防护措施

3.1加强计算机的技术控制

为了能够有效的防止计算机信息安全的隐患，首先一定要从计算机信息技术控制来处理，技术一定要改进，这样才能加强对于计算机信息安全的管理，在人们使用计算机的时候，运用相应的软件是很重要的，就比如现在的很多杀毒软件，在使用的过程当中一定要运用充分，杀毒软件能够确保第一时间的发现病毒并且清除，在使用计算机的时候，还一定要及时的更新杀毒软件，因为现在病毒的更新速度相当的快，所以杀毒软件也要时常更新，防火墙对于一个计算机来说是很重要的，防火墙的建设能够知道访问者的来源以及技术，能够及时的发现问题；除了这些以外，还要在计算机上装上一些对于软件的检测系统，实时的检测每一个软件的动态，这样在发现病毒的时候能够及时的去处理。

3.2完善计算机的管理体制

现在很多计算机发生问题，都是由于计算机本身的管理体制有问题，所以在建设计算机系统的时候，一定要建立并且完善一套完整的管理体系，这些管理的体系不仅包括了对于计算机信息安全的管理，还要对于计算机信息做好备份，防止在信息丢失了以后，没有一个处理办法，在使用计算机的时候，常常会碰到一些自然或者人为的灾害，就比如说雷电灾

害、停电、或者火灾，在这些问题出现了以后，计算机往往会出现问题，有的会直接关机，如果你在处理信息的时候，突然断电了，并且相关信息没有保存，就会给相关使用计算机的人带来一定的不便。

3.3管理电脑的人员一定要有计算机信息安全的意识

现在由于很多的管理电脑人员缺乏相应的安全意识，所以导致了现在很多计算机的信息安全出现泄漏，为了预防这方面的问题，在平时一定要给计算机用于普及相关计算机信息安全的严重性，让相关计算机用户了解威胁计算机信息安全的威胁，还要让相关计算机用户学习防止计算机信息安全泄漏的方法，让计算机用户能够有效的利用计算机的杀毒软件等，让相关计算机用户提高相关计算机安全知识，还要培养计算机用户安全意识。这是有效提升计算机信息安全的途径之一。

现在计算机在日常生活工作学习当中很普遍，也很常见，计算机信息安全问题是一个相当复杂，而且涉及相当广泛的问题，相关的工作人员以及用户一定要对于计算机的信息安全给予足够的重视，还有有一定的监管制度，这样才能够有效的保证计算机信息安全。

[1]谭国锐。个人计算机信息安全与防护措施[j].科技信息□20xx□11□.

[2]李桂岩。计算机信息安全问题及对策[j].科技风□20xx□1□.

[3]王晓蕾。网络环境下计算机信息安全防护措施[j].计算机光盘软件与应用□20xx□5□.

安全防护文明施工措施费用投入计划表篇三

第一条为贯彻"安全第一、预防为主"的方针，确保在施工现场生产过程中的人身和财产安全，减少事故的发生，加强施

工现场危险作业环境及作业过程中安全防护设施的有效使用和管理，制订本制度。

第二条本制度适用于本公司承接的所有施工现场全过程的 安全设施管理和控制。

则各承包单位按承包工程的规模、特点，建立相应的安全设施保证体系。

第四条工程项目部作为工程施工安全管理的责任主体，应按国家有关规定落实施工现场安全设施所需费用，并专款专用。

第二章安全设施的内容、范围

第五条安全设施的内容、范围：

1)为安全而重新布置或改装的机械和设备；

2)电器设备安装的防护性接地或接中性线的装置，以及其他防止触电的设施；

3)为安全而设低电压照明设备；

7)在施工生产区域内危险处装置的标志、信号和防护设施；

8)在施工人员可能到达的洞、坑、沟、升降口、漏斗等处安设的临时防护装置；

9)在施工生产区域内，施工人员经常往来的地点，为安全而设置的通道及便桥；

10)在高处作业时，为避免物料坠落伤人而设置的工具箱以及防止人员坠落的防

护网、绳；

11)在脚手架、井架（龙门架）外围封闭的。防护网；

12)为防止塌方采取的支护措施；

13)高处作业的上下通道及防护措施；

14)立体交叉施工作业区域的隔离措施；

15)在建工程与周围人行通道及民房的防护隔离设施；

16)在建工程的外边缘与外电架空线路的隔离防护设施；

17)防火、防毒、防爆、防雷等安全设施。

第三章安全设施策划

第六条根据工程项目的结构、环境、技术含量和施工风险程度等因素，由项目经理牵头，汇同工程技术负责人、安全专业管理人员、施工负责人实施安全设施策划，策划内容如下：

1)确定整个施工过程中应执行的安全技术标准、规范。

第七条根据安全设施策划结果编制安全技术措施计划，对所须安全设施的结构形式、材料、设置要求等可在施工方案中完整独立体现。

第八条工程项目施工前，安全措施计划须报经公司安全主管部门审核确认。

第四章采购（安全设施所需的材料、设备及防护用品）

第九条工程项目部将施工安全设施所需的材料、设备及防护用品列出计划清单，交由公司物资供应站统一采购管理。

第十条公司物资供应站应向工程项目部提供的安全设施所需

的材料、设备及防护用品检验合格的相关资料，否则工程项目部不得投入使用。

第十一条工程项目部对分包方自行采购的安全设施所需的材料、设备及防护用品应实行控制。

第十二条公司物资供应站应对供应商进行评价。

1、根据能否满足安全设施所需的材料、设备及防护用品要求的能力选择供应商。

2、根据采购的安全设施所需的材料、设备及防护用品的重要性，从以下几方面对供应商进行评价：

1)对供应商所生产的安全设施所需的材料、设备及防护用品，验证是否取得生产许可证；

第十三条工程项目部对安全设施所需的材料、设备及防护用品，应与公司物资供应站签订供货合同，合同中明确规定供货和检验方式。

第五章过程检验

第十四条现场安全设施由工程项目部统筹规划，各分包单位根据施工方案中的安全措施计划负责建立、管理。

第十五条按安全措施计划的要求，对施工现场的安全设施、设备进行检验，只有通过检验的设施、设备才能安装和使用。

第十六条工程项目部安全专业管理人员应依据各分包单位编制的安全措施计划，组织相关管理人员及分包单位负责人对下列内容检查、验收：

1)对施工过程中所需的安全设施及防护用品的验证；

4)对施工过程中的安全设施，如通道防护棚；电梯井内隔离排或安全网；脚手架外围封闭、上下通道、上层施工通道；″四口″、″五临边″的防护设施；悬挑钢平台；高处作业的上下通道、人员行走防护设施、作业点的防护措施；外挑安全网等搭设、组装完毕后须进行检查验收。

5)对专项编制的安全技术措施落实检查；

第十八条工程项目部设备负责人应根据施工组织设计（施工方案），组织相关人员及分包单位负责人对下列内容检查验收：

第十九条上述各类检查和检验完毕后工程项目部须填写验收记录。

第六章施工过程的控制

第二十二条搭设或拆除安全防护设施、脚手架、起重机械或其它设施、设备，必须经工程项目部确认同意。如当天未能完成时，应做好局部收尾，并设置临时安全措施。

第二十三条工程项目部应根据安全措施计划中确定的危险部位和过程，责成分包单位落实监控人员，确定监控措施和方式，实施重点监控，必要时应连续监控。

2、各分包单位在拆除现场安全防护设施前应通知工程项目部，由其确认可拆除时，方可拆除。因拆除后影响该区域或后工序的施工安全，应服从安排，予以保留，不得以任何理由拒不执行。

第二十四条在工序交接中，应由项目部施工技术负责人和安全专业管理人员组织交接双方负责人，对现场的安全设施进行验收、确认。

第七章事故隐患的控制

第二十五条工程项目部应对存在隐患的安全设施、过程和行为进行控制，确保不合格设施不使用、不合格过程不通过、不安全行为不放过。

第二十六条对事故隐患应由项目部安全专业管理人员汇同项目部相关人员进行处理。

处理方式：

1、停止使用、封存；

2、指定专人进行整改以达到规定要求；

3、进行返工，以达到规定要求；

4、对有不安全行为的人员进行教育或处罚；

5、对不安全生产的过程重新组织。

安全防护文明施工措施费用投入计划表篇四

安全防护措施是保证生产安全的重要手段与保障，搞好安全防护措施的管理，有利于安全、文明生产，减少或避免事故的发生。为了保证安全生产，降低生产安全隐患，进一步加强对安全防护措施的管理，特制定本制度。

1、安全生产管理制度的建立，健全各级各部门的安全生产责任制度，责任落实到人。各项生产任务都必须有明确的安全指标等保证措施。

2、新进公司员工上岗都须进行安全知识培训。员工变换工种，须进行新工种的安全技术教育。工人应掌握本工种操作技能，

熟悉本工种安全技术操作规程。

3、施工组织设计施工方案时，应有针对性的安全技术措施，经技术负责人审查批准。

4、分部分项工程安全技术交底要进行全面的`针对性的安全技术交底。

5、特种作业持证上岗特种作业人员必须经培训考试合格持证上岗，操作证必须按期复审，不得超期使用。

6、各生产队每天做好班前安全检查，各负责人进行安全记录交接。

7、遵章守纪、佩戴标记，严禁违章指挥、违章作业。

8、安全事故处理要建立安全事故档案，按调查分析规则、规定进行处理报告。

施工现场的防护范围有建筑物周边防护；建筑物五临边防护；现场施工用电安全防护；现场机械设备安全防护；施工人员安全防护；现场防火、防风等措施。

一、“三宝”“四口”安全保护措施

1、安全帽

（1）安全帽须经有关部门检验合格后方能使用。

（2）正确使用安全安全帽并扣好帽带。

（3）不准把安全帽抛、扔或坐、垫。

（4）不准使用缺衬、缺带及破损安全帽。

2、安全带

（1）安全带须经有关部门检验合格后方能使用。

（2）安全带使用两年后，必须按规定抽检不合格的，必须更换安全绳后才能使用。

（3）安全带应储存在干燥、通风的仓库内，不准接触高温、明火、强碱酸或尖锐的坚硬物体。

（4）安全带应高挂抵用，不准将绳打结使用。

（5）安全带上的各种部件不得任意拆除。更换新绳时要注意加绳套。

3、安全网

（1）网绳不破损并生根牢固、绷紧、圈牢，拼接严密。

（2）网宽不小于2□6m□里口离墙不得大于15cm□外高内低，每隔3m设支撑。

二、施工用电安全防护制度

1、支线架设

（1）配电箱的电缆线应有套管，电线进出不混乱。

（2）支线绝缘好，无老化、破损和漏电。

（3）支线应沿墙或电杆架空敷设，并用绝缘子固定。

（4）过道电线可采用硬质护套管埋地并作标记。

（5）室外支线应用橡皮线架空，接头不受拉力并符合绝缘要

求。

2、现场照明

（1）一般场所采用220v电压。

（2）照明导线应用绝缘子固定。

（3）照明灯具的金属外壳必须接地或接零。

（4）室外照明灯具距地面不得低于3m□室内距地面不得低于2□4m□

3、电箱（配电箱、开关箱）

（1）电箱应有门、锁、色标和统一编号。

（2）电箱内开关电器必须完整无损，接线正确。各类接线装置灵敏可靠，绝缘良好。无积灰、杂物，箱体不得歪斜。

（3）电箱安装高度和绝缘材料等均应符合规定。

（4）电箱内应设置漏电保护器，选用合理的额定漏电动作电流进行分级配合。

（5）配电箱应设总熔丝、分熔丝、分开关。零排地排齐全。动力和照明分别设置。

（6）配电箱的开关电器应与配电线或开关箱一一对应配合，作分路设置，以确保转录专控；总开关电器与分路来管电器的额定值、动作整定值相适应。熔丝应和用电设备的实际负荷相匹配。

（7）金属外壳电箱应作接地或接零保护。

（8）开关箱与用电设备实行一机一闸以保险。

（9）同一移动开关箱严禁配有380v和220v两种电压等级。

4、接地接零

（1）接地体可用角钢、圆钢或钢管，但不得用螺纹钢，其截面不小于48mm一组2根，接地体之间间距不小于2□5m□入土深度不小于2m□接地电阻应符合规定。

（2）橡皮线中黑色或绿/黄双色线作为接地线。与电气设备相连接的接地或接零线截面最小不能低于2□5mm2多股铜芯线；手持式民用电设备应采用不小于1□5mm2多股铜芯线。

（3）电杆转角杆、终端杆及总箱、分配电箱必须有重复接地。

（4）高层配电箱重设接地，必须从地下引入。

三、机具安全使用措施

1、电焊机

（1）有可靠的防雨措施。

（2）一、二次线（电源、龙头）接线处应有齐全的防护罩，二次线应使用线鼻子。

（3）有良好的接地或接零保护。

（4）配线不得乱拉乱搭，焊把绝缘良好。

四、防火安全措施

1、施工地建立防火责任制，职责明确。按规定设专职防火负

责人。

2、建立动用明火审批制，按规定划分级别，明确审批手续，并有监护措施。

3、一般建筑各楼层、非重点仓库及宿舍，明确用火审批手续，并有监护措施。

4、焊割作业应严格执行“十不烧”及压力容器使用规定。

安全防护文明施工措施费用投入计划表篇五

:随着信息技术的发展，网络日益成为人们工作生活中不可或缺的重要组成部分，在给人们方便的同时也存在网络数据被盗、网络非法入侵及病毒等很多网络安全威胁，而最严重的就是采取解决上述威胁网络安全的方法。为有效避免网络安全威胁，提供网络安全，很多复杂的软件处理技术广泛应用于计算机中，但没有在本质上解决网络安全问题。本研究针对网络信息安全及其防护措施进行了较深入地分析，对于确保计算机系统安全稳定的运行具有比较重要的作用。

:信息技术；网络安全；防护措施

互联网技术近年来的发展十分迅速，网络在各行各业中已得到比较广泛的渗透，为人们的工作生活提供了极大的便利。互联网中为使需要的信息及时有效的获取，享受信息化的便捷及文化内涵。但也应清醒地认识，在网络上若个人重要信息被泄露，将导致难以估量的重大损失，基于网络安全中存在的常见问题有效针对性地提出了网络信息安全防护措施，对于确保计算机系统安全稳定的运行具有比较重要的作用。

2.1自然灾害

计算机信息系统在本质上就是智能机器，在运行及操作中，

容易受到温湿度、振动等自然灾害及不同环境因素的影响，在一定程度上这些因素应对计算机系统正常运行具有十分不利的影响。近年来我国很多计算机空间中对防振、防火、防潮、防雷等措施尚未做好，对于在设置计算机接地系统方面，考虑也不够细致周到，难免降低计算机对自然灾害及事故的应对能力的抵御。

2.2脆弱性的网络系统

互联网技术因其开放性特征比较明显，逐渐成为人们工作生活中不可或缺的重要组成部分，而其开放性也造成计算机存在易受网络入侵攻击的不足。另外，互联网并非独立运行，离不开tcp/ip等网络协议的支持，这些协议不具有较高的安全性，在对网络系统运行过程中，难免产生如拒绝服务、欺骗攻击及数据信息被非法盗取等很多安全问题。

2.3用户失误操作及网络非法入侵

我国计算机系统的应用群体日渐增大并屡创新高，但很多用户都存在着安全意识不强的普遍问题。用户在对有关口令设置时比较随意，其认为这种口令设置并非必要，一些用户甚至向他人随意泄露个人账号及密码等重要信息。人为网络入侵是存在于计算机网络操作中另一个比较严重的问题，也是目前威胁计算机网络信息安全的最大问题，主要有主动及被动两种攻击方式，通常黑*利用非法入侵等手段将他人信息截取或进行破坏或修改，对国家、社会及个人造成比较严重的损失。

3.1提高网络信息安全防护意识

在计算机网络信息系统的正常使用过程中，难免会遇到网银、支付宝□e-mail及qq等不同账号，而黑*对个人电脑的非法攻击目标就是要将用户合法的账号及密码非法获取。若黑*非法入侵得逞，容易使用户产生十分严重的损失。这需要计算机

用户在设置有关系统登录账号时应采用的密码足够复杂。另外，在对系统用户密码设置过程中，避免对密码进行相同或相似的设置，密码设置方法最好采用数字组合特殊字母的形式，最关键的是对长密码应重要的是定期进行更换，才能对账号使用的安全性进行保护，进而避免受到黑*的非法攻击。

3.2防火墙及杀毒软件的安装

网络防火墙技术应用在计算机网络中主要是特殊的一种网络互联设备，该技术的应用最主要作用是使网络之间实现控制访问的作用。另外，还可有效避免利用非法手段的外网用户进入内网，进而实现对内网操作环境的保护，提高网络信息安全性。个人计算机在防火墙应用方面，主要采用软件防火墙，在安装防火墙软件中，一般都是与杀毒软件配套安装使用。近年来，杀毒软件是应用最多的一种计算机信息安全技术，该技术不仅能够对病毒进行查杀，还能对木马及入侵的其它黑*程序进行有效防御，特别要注意在杀毒软件应用过程中，一定要对防火墙软件及时升级，只有防火墙软件升级到最新版本才能达到防范计算机病毒的作用。

3.3数字签名及文件加密技术

在目前为实现计算机信息系统及数据的安全保密，有效避免个人数据信息被非法盗取，就需要充分利用文件加密及数字签名技术。按照不同作用，文字加密和数字签名技术一般有三种：

（1）数据传输。主要加密传输过程中的。数据流，一般分为线路和端对端两种加密方法；

（2）数据存储。加密处理数据存储，主要目标是在存储过程中避免数据新发生失密情况；

（3）数据完整性。有利于对传送、存取及处理介入信息过程

中的有效验证，可实现信息保密的作用。目前，数字签名是对网络通信中存在的特有安全问题进行妥善解决的一种应用最广泛的方法。具体操作过程中，能够使电子文档实现辨认和验证，确保数据完整性。在实际应用中，有dss□rsa及hash等很多数字签名算法。

由此可见，我国计算机网络信息安全中还存在自然灾害、计算机病毒、脆弱性、失误操作及网络入侵等很多问题，为使上述问题得到妥善解决，有关技术人员开展了较深入地研究工作并获得了明显效果。本研究基于实践及深入调研，有针对性地提出计算机网络信息安全中的常用防护措施，主要应加强网络信息安全防护意识，将防火墙及杀毒软件安装在计算机中，防患于未然。最关键的是对有关软件采取文件加密与数字签名技术处理措施，切实提高网络信息的安全性。

[1]彭珺，高珺。计算机网络信息安全及防护策略研究[j]□计算机与数字工程□20xx(11)□

[2]阿曼江阿不都外力。计算机网络信息安全及其防护措施[j]□新疆职业大学学报□20xx(04)□

[3]陈卓。计算机网络信息安全及其防护对策[j]□中国卫生信息管理杂志□20xx(04)□

[4]彭珺，高珺。计算机网络信息安全及防护策略研究[j]□计算机与数字工程□20xx(02)□

[5]曹立明。计算机网络信息和网络安全及其防护策略[j]□三江学院学报□20xx(10)□

[6]刘莉，苗慧珠。计算机网络安全分析[j]□青岛建筑工程学院学报□20xx(08)□