普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

教育部高等学校信息安全专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

顾问委员会主任：沈昌祥 编委会主任：肖国镇

网络侦查与电子物证系列丛书主编：秦玉海

网络安全管理

李娜 孙晓冬 主编

秦玉海 审

Information Security

http://www.tup.com.cn

根据教育部高等学校信息安全专业教学指导委员会编制的《高等学校信息安全专业指导性专业规范》组织编写

清华大学出版社

普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

网络安全管理

李娜 孙晓冬 主编

Information Security

http://www.tup.com.cn

清华大学出版社
北京

内 容 简 介

本书对实战工作中的网络安全管理问题做了详尽的解释与阐述，同时也比较全面地介绍了网络安全保卫部门实际工作执法过程中的相关规范与标准。主要内容包括网络安全管理概述、计算机信息网络国际联网安全管理、互联网用户的用网行为安全规范、互联网单位用户的安全管理、互联网上网服务营业场所安全管理、信息系统安全等级保护制度、计算机病毒防护、计算机信息系统安全专用产品安全管理。

本书适合作为高等院校信息安全、网络犯罪侦查等专业的研究生、本科生、双学位学生的授课教材或教学参考书，也可以作为网络犯罪相关执法人员的参考书。

图书在版编目(CIP)数据

网络安全管理/李娜，孙晓冬主编. --北京：清华大学出版社，2014
高等院校信息安全专业系列教材
ISBN 978-7-302-35218-1

Ⅰ. ①网… Ⅱ. ①李… ②孙… Ⅲ. ①计算机网络－安全技术－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2014)第 014326 号

责任编辑：张　民　薛　阳
封面设计：常雪影
责任校对：时翠兰
责任印制：沈　露

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：11.75　　**字　　数**：269 千字
版　　次：2014 年 7 月第 1 版　　**印　　次**：2014 年 7 月第 1 次印刷
印　　数：1～2000
定　　价：25.00 元

产品编号：056203-01

高等院校信息安全专业系列教材

编审委员会

出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定，确定了本丛书首批教材的作者，这些作者绝大多数都是既在本专业领域有深厚的学术造诣、又在教学第一线有丰富的教学经验的学者、专家。

本系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整、结构合理、内容先进。

② 适应面广：能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套：除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

为了保证出版质量，我们坚持宁缺毋滥的原则，成熟一本，出版一本，并保持不断更新，力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材，满足学生用书的基础上，还经由专

家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到本系列教材中，以进一步满足大家对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍，同时也欢迎广大读者对本系列教材提出宝贵意见，以便我们对本系列教材的组织、编写与出版工作不断改进，为我国信息安全专业的教材建设与人才培养做出更大的贡献。

“高等院校信息安全专业系列教材”已于2006年年初正式列入普通高等教育“十一五”国家级教材规划（见教高[2006]9号文件《教育部关于印发普通高等教育“十一五”国家级教材规划选题的通知》）。我们会严把出版环节，保证规划教材的编校和印刷质量，按时完成出版任务。

2007年6月，教育部高等学校信息安全类专业教学指导委员会成立大会暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办，清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展起到重要的指导和推动作用。2006年教育部给武汉大学下达了“信息安全专业指导性专业规范研制”的教学科研项目。2007年起该项目由教育部高等学校信息安全类专业教学指导委员会组织实施。在高教司和教指委的指导下，项目组团结一致，努力工作，克服困难，历时5年，制定出我国第一个信息安全专业指导性专业规范，于2012年底通过经教育部高等教育司理工科教育处授权组织的专家组评审，并且已经得到武汉大学等许多高校的实际使用。2013年，新一届“教育部高等学校信息安全专业教学指导委员会”成立。经组织审查和研究决定，2014年以“教育部高等学校信息安全专业教学指导委员会”的名义正式发布《高等学校信息安全专业指导性专业规范》（由清华大学出版社正式出版）。“高等院校信息安全专业系列教材”在教育部高等学校信息安全专业教学指导委员会的指导下，根据《高等学校信息安全专业指导性专业规范》组织编写和修订，进一步体现科学性、系统性和新颖性，及时反映教学改革和课程建设的新成果，并随着我国信息安全学科的发展不断完善。

我们的E-mail地址：zhangm@tup.tsinghua.edu.cn；联系人：张民。

“高等院校信息安全专业系列教材”编审委员会

前言

随着网络技术的提高与网络的普及，人们的生活与网络也越来越紧密。同时，网络犯罪日益成为区别于传统犯罪的高发领域。网络犯罪的日趋增多，给我国广大网民的社会生活造成了严重的威胁。还网络一个净化的空间，一方面要依赖网络犯罪案件的侦办，还有一个不容忽视的方面就是网络安全的管理，可以使网络犯罪防患于未然，同时，还可以为网络犯罪案件的侦办提供良好的条件或者信息。

本书对实战工作中的安全管理问题做了详尽的解释与阐述，同时也比较全面地介绍了网络安全保卫部门实际工作执法过程中的相关规范与标准。本书适合作为公安高等院校信息安全、网络安全与执法、网络犯罪侦查等专业的研究生、本科生、二学位学生的授课教材或教学参考书，也可以作为网络犯罪相关执法人员的参考书。

本书主要内容包括网络安全管理概述、计算机信息网络国际联网安全管理、互联网用户的用网行为安全规范、互联网单位用户的安全管理、互联网上网服务营业场所安全管理、信息系统安全等级保护制度、计算机病毒防护、计算机信息系统安全专用产品安全管理。

本书由李娜和孙晓冬担任主编，负责全书的整体结构设计和内容统编。李娜编写第1、2章，第6～8章；孙晓冬编写第3～5章。秦玉海教授对全书内容进行了审阅，提出很多宝贵意见！

尽管本书作者付出了很多努力，但仍然有不足之处，敬请读者提出宝贵意见！

作　者

目录

第1章 网络安全管理概述

1.1 网络安全保卫部门的行政职能授权和执法依据

网络安全保卫部门如果想要准确、及时地执法，就必须要有法律授权与执法依据，有关网络安全保卫部门的主要法律法规是比较健全的。具体如下：

(1)《中华人民共和国警察法》，1995年2月28日第八届全国人民代表大会常务委员会第十二次会议通过，1995年2月28日中华人民共和国主席令第四十号公布施行。

本法律的制定是为了维护国家安全和社会治安秩序，保护公民的合法权益，加强人民警察的队伍建设，从严治警，提高人民警察的素质，保障人民警察依法行使职权，保障改革开放和社会主义现代化建设的顺利进行。

本法律的制定充分体现本法以公安机关的人民警察为主体，规定人民警察的职权、组织管理、义务和纪律以及执法监督等问题。其中，第六条规定：公安机关的人民警察按照职责分工，依法履行下列职责：

① 预防、制止和侦查违法犯罪活动；

② 维护社会治安秩序，制止危害社会治安秩序的行为；

③ 监督管理计算机信息系统的安全保护工作。

(2)《中华人民共和国刑法》，1979年7月1日第五届全国人民代表大会第二次会议通过，1997年3月14日第八届全国人民代表大会第五次会议修订。从1999年12月25至2011年2月25共出台8个修正案。

本法律的制定是为了惩罚犯罪，保护人民。

其中，第二百八十五条规定：违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。

第二百八十六条规定：违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。

故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

第二百八十七条规定：利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。

中华人民共和国第十一届全国人民代表大会常务委员会第七次会议于2009年2月28日通过的《中华人民共和国刑法修正案(七)》中第九条规定：在刑法第二百八十五条中增加两款作为第二款、第三款："违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。"

"提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。"

(3)《中华人民共和国刑事诉讼法》，1979年7月1日第五届全国人民代表大会第二次会议通过，根据1996年3月17日第八届全国人民代表大会第四次会议《关于修改(中华人民共和国刑事诉讼法)的决定》第一次修正。《关于修改(中华人民共和国刑事诉讼法)的决定》于1996年3月17日公布，自1997年1月1日起施行。

本法的目的是为了保证刑法的正确实施，惩罚犯罪，保护人民，保障国家安全和社会公共安全，维护社会主义社会秩序。本法的任务，是保证准确、及时地查明犯罪事实，正确应用法律，惩罚犯罪分子，保障无罪的人不受刑事追究，教育公民自觉遵守法律，积极同犯罪行为作斗争，以维护社会主义法制，保护公民的人身权利、财产权利、民主权利和其他权利，保障社会主义建设事业的顺利进行。

(4)《中华人民共和国行政处罚法》，中华人民共和国主席令第63号，1996年3月17日第八届全国人民代表大会第四次会议通过，1996年10月1日起施行。根据2012年3月14日第十一届全国人民代表大会第五次会议《关于修改〈中华人民共和国刑事诉讼法〉的决定》第二次修正。《全国人民代表大会关于修改〈中华人民共和国刑事诉讼法〉的决定》已由中华人民共和国第十一届全国人民代表大会第五次会议于2012年3月14日通过，现予公布，自2013年1月1日起施行。

本法对于规范行政处罚的设定和实施，保障和监督行政机关有效实施行政管理，维持公共利益和社会秩序，保护行政管理相对人的合法权益起了很好的促进作用。本法是为了规范行政处罚的设定和实施，保障和监督行政机关有效实施行政管理，维护公共利益和社会秩序，保护公民、法人或者其他组织的合法权益，根据宪法规定制定的法律。

本法由八章构成。其中，第一章总则；第二章行政处罚的种类和设定；第三章行政处

罚的实施机关；第四章行政处罚的管辖和适用；第五章行政处罚的决定；第六章行政处罚的执行；第七章法律责任；第八章：附则。

(5)《中华人民共和国治安管理处罚法》，主席令第 38 号，2005 年 8 月 28 日中华人民共和国第十届全国人民代表大会常务委员会第十七次会议通过，自 2006 年 3 月 1 日起施行。

本法律的目的是为了维护社会治安秩序，保障公共安全，保护公民、法人和其他组织的合法权益，规范和保障公安机关及其人民警察依法履行治安管理职责。

本法律由六章构成。其中，第一章总则；第二章处罚的种类和适用；第三章违反治安管理的行为和处罚；第四章处罚程序；第五章执法监督；第六章附则。与网上违法行为处罚相关的条款有 8 类 12 条。

其中，第二十九条规定，有下列行为之一的，处五日以下拘留；情节较重的，处五日以上十日以下拘留：

① 违反国家规定，侵入计算机信息系统，造成危害的；

② 违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行的；

③ 违反国家规定，对计算机信息系统中存储、处理、传输的数据和应用程序进行删除、修改、增加的；

④ 故意制作、传播计算机病毒等破坏性程序，影响计算机信息系统正常运行的。

(6)《中华人民共和国计算机信息系统安全保护条例》，第 147 号中华人民共和国国务院令(147 号)，1994 年 2 月 18 日发布，自发布之日起施行。

本行政法规是关于计算机安全方面最早的法规，起到提纲挈领性的作用，对以后的计算机安全工作有很重要的指导意义，但是可执行性一般。之后根据这个行政法规出台了一系列的保护计算机信息系统安全的行政法规和部门规章。例如，对于计算机信息系统等级保护工作这部分内容，本行政法规中只是在第九条提到："计算机信息系统实行安全等级保护。安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定。"根据这一条，后来出台了一系列的规章和国家标准，直到今天有关等级保护的标准就已经出台了五十多个。

本行政法规的目的是为了保护计算机信息系统的安全，促进计算机的应用和发展，保障社会主义现代化建设的顺利进行。这个条例制定的时候我国计算机信息网络还未正式接入国际联网，正式接入的时间是 1994 年 5 月，在当时还缺乏经验，对信息网络要面临的问题的认识也不够，其中所指的网络主要是指局域网。保护的对象主要是国家事务、经济建设、国防建设、尖端科学技术等重要领域的计算机信息系统的安全。授权执法的政府部门是公安部，公安部主管全国计算机信息系统安全保护工作。

本行政法规的主要内容有：准确标明了安全保护工作的性质；科学界定了"计算机信息系统"的概念；系统设置了安全保护的制度；明确确定了安全监督的职权；全面规定了违法者的法律责任；定义了计算机病毒及专用安全产品。

其中，第十七条规定了公安机关对计算机信息系统保护工作行使下列监督职权：

① 监督、检查、指导计算机信息系统安全保护工作；

② 查处危害计算机信息系统安全的违法犯罪案件；

③ 履行计算机信息系统安全保护工作的其他监督职责。

(7)《全国人大常委会关于维护互联网安全的决定》,2000 年 12 月 28 日第九届全国人民代表大会常务委员会第十九次会议通过。

本决定是为了保障互联网的运行安全和信息安全问题。其中,分别在促进我国互联网的健康发展,维护国家安全和社会稳定,维护社会主义市场经济秩序和社会管理秩序,保护个人、法人和其他组织的合法权益方面做了规定。

(8)《中华人民共和国计算机信息网络国际联网管理暂行规定》,中华人民共和国国务院令第 195 号,1996 年 2 月 1 日发布,根据 1997 年 5 月 20 日《国务院关于修改<中华人民共和国计算机信息网络国际联网管理暂行规定>的决定》修正。

本规定的目的是为了加强对计算机信息网络国际联网的管理,保障国际计算机信息交流的健康发展。计算机信息网络的国际联网,关系到国家的网络安全,关系到国家主权和国防利益,对一个国家有至关重要的意义。

本规定对计算机信息网络国际联网的一些基本概念进行规定,例如互联单位、接入单位等,同时对通过什么来联网、联网的方式是什么,都有明确规定。也就是说不是用户想怎么接入都可以,而是有明确规定。

(9)《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》,1997 年 12 月 8 日国务院信息化工作领导小组审定。

本办法是为了加强对计算机信息网络国际联网的管理,保障国际计算机信息交流的健康发展,根据《中华人民共和国计算机信息网络国际联网管理暂行规定》而制定。

本办法的颁布主要是有利于暂行规定更有效地实施。同时也细化了对国际联网进行管理的规定与罚则。

(10)《计算机信息网络国际联网安全保护管理办法》,公安部令第 33 号,1997 年 12 月 11 日国务院批准,1997 年 12 月 30 日公安部发布。本办法是根据《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》和其他法律、行政法规的规定制定的。国务院第 147 号令主要的目的是保护计算机信息系统自身的安全,国务院第 195 号令是为了加强对计算机信息网络国际联网的管理,而本办法是为了加强对计算机信息网络国际联网的安全保护,维护公共秩序和社会稳定。

网络安全保卫部门对网络安全进行监督管理时,在行政法规中,本办法是最常用的部门规章之一,可操作性比较强,各地网监部门在行政管理方面的工作,很大程度上依据本办法。对于某些行为不能依据《刑法》285 条、第 286 条、第 287 条或者《治安管理处罚法》第 29 条中的规定进行处罚时,可以根据本办法进行处罚。本规章涉及的公共生活的内容比较多,管的比较多,管的比较细,甚至深圳的一名律师说本办法屡屡强奸民意。在实际工作中,网络安全保卫部门在日常工作中涉及的案件能够依据《刑法》或《治安管理处罚法》进行处罚的不是很多,很大程度上要依据本办法,可操作性很好。

(11)《计算机病毒防治管理办法》,2000 年 3 月 30 日公安部部长办公会议通过,2000 年 4 月 26 日发布施行。

本办法的目的是为了加强对计算机病毒的预防和治理,保护计算机信息系统安全,保

障计算机的应用与发展，根据《中华人民共和国计算机信息系统安全保护条例》的规定而制定。本办法的适用范围是中华人民共和国境内的计算机信息系统以及未联网计算机的计算机病毒防治管理工作。同时，规定执法部门是公安部公共信息网络安全监察部门，主管全国的计算机病毒防治管理工作。地方各级公安机关具体负责本行政区域内的计算机病毒防治管理工作。

本办法规定了计算机病毒的定义，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

(12)《互联网上网服务营业场所管理条例》，国务院令第363号，2002年8月14日国务院第62次常务会议通过，2002年11月15日施行。其前身是2001年4月3日信息产业部、公安部、文化部、国家工商行政管理局发布的《互联网上网服务营业场所管理办法》。

本条例的前身是办法，有一个事件促成了此条例在很短的时间内颁布。2002年6月16日凌晨，北京海淀区“蓝极速”网吧发生火灾，造成24人死亡，13人受伤。这个网吧的状况是这样的：网吧里铺着地毯，网吧里有煤气罐，可以为上网的人做饭，服务员也是自己做饭。网吧所在二层楼窗户被铁栅栏封起来。平常1小时3元，晚上12时至第二天早8时连续上网只需要12元。当时网吧管理混乱、经营无序、事故不断、良莠不齐。当时，有很多黑网吧就开在居民楼里，在巴掌大的地方摆几台计算机就是网吧了。有的网吧还设有单间，里面不仅有计算机，还有床和卫生间，甚至存在色情包间。网吧里会经常有赌博、色情、盗窃等治安及刑事案件发生。此条例加大了对网吧的管理力度，防止网吧过多过滥、接纳未成年人等违法违规经营，取缔黑网吧。

本条例的目的是为了加强对互联网上网服务营业场所的管理，规范经营者的经营行为，维护公众和经营者的合法权益，保障互联网上网服务经营活动健康发展，促进社会主义精神文明建设。

(13)《互联网安全保护技术措施规定》，公安部令第82号，2005年11月24日公安部部长办公会审议通过，于2005年12月13日正式颁布，并于2006年3月1日起实施。

本规定是与《计算机信息网络国际联网安全保护管理办法》配套的一部部门规章。本规定从保障和促进我国互联网发展出发，根据《计算机信息网络国际联网安全保护管理办法》的有关规定，对互联网服务单位和联网单位落实安全保护技术措施提出了明确、具体和可操作性的要求，保证了安全保护技术措施的科学、合理和有效地实施，有利于加强和规范互联网安全保护工作，提高互联网服务单位和联网单位的安全防范能力和水平，预防和制止网上违法犯罪活动。本规定的颁布对于保障我国互联网安全起到促进作用。

本规定是为加强和规范互联网安全技术防范工作，保障互联网网络安全和信息安全，促进互联网健康、有序发展，维护国家安全、社会秩序和公共利益，根据《计算机信息网络国际联网安全保护管理办法》而制定的。

本规定包括立法宗旨、适用范围、互联网服务单位和联网使用单位及公安机关的法律责任、安全保护技术措施要求、措施落实与监督、名词术语解释等6个方面的内容，共19条两千余字。主要内容如下：

① 明确了互联网安全保护技术措施是指保障互联网安全和信息安全、防范违法犯罪的技术设施和技术手段，并且规定了互联网安全保护技术措施负责落实的责任主体是互

联网服务提供者和联网使用单位，负责实施监督管理工作的责任主体是各级公安机关公共信息网络安全监察部门。

② 强调了互联网服务单位和联网使用单位要建立安全保护措施管理制度，保障安全保护技术措施的实施不得侵犯用户的通信自由和通信秘密，除法律和行政法规规定外，任何单位和个人未经用户同意不得泄露和公开用户注册信息。

③ 规定了互联网服务单位和联网使用单位应当落实的基本安全保护技术措施。安全保护技术措施主要包括防范计算机病毒、防范网络入侵攻击和防范有害垃圾信息传播，以及系统运行和用户上网登录时间和网络地址记录留存等技术措施要求。

④ 为了保证安全保护技术措施的科学合理和统一规范，规定安全保护技术措施应当符合国家标准或公共安全行业标准。为了防范网上计算机病毒、网络攻击和有害信息传播，规定了安全保护技术措施应当具有符合公共安全行业技术标准的联网接口。

⑤ 为保证安全保护技术措施的正常运行，明确了互联网服务单位和联网单位不得实施故意破坏安全保护技术措施、擅自改变措施功能和擅自删除、篡改措施运行记录等行为。

⑥ 明确了公安机关监督管理责任和规范了公安机关监督检查行为。《互联网安全保护技术措施规定》明确了公安机关应当依法对辖区内互联网服务单位和联网使用单位安全保护技术措施落实情况进行指导、监督和检查。

1.2 网络安全保卫部门业务类别

1.2.1 网络安全保卫部门职能介绍

网络安全保卫部门的职能是指导并组织实施公共信息网络和国际互联网的安全保护工作；指导并组织实施信息网络安全监察工作；负责互联网上网服务营业场所的审批、管理；参与研究拟定信息安全政策和技术规范；监控信息网络违法犯罪动态，提供犯罪案件证据，依法查处在计算机网络中制作、复制、查阅、传播有害信息和计算机违法犯罪案件；防范计算机信息泄密、计算机病毒及其他计算机灾害事故的发生等。具体职责如下。

(1) 组织、协调、指导和参与对计算机及互联网违法犯罪案件的侦察、查处工作，收集犯罪证据，对犯罪案件的证据进行技术鉴定；

(2) 负责指导、组织实施公共信息网络和国际互联网的安全管理、监察和保护等工作；

(3) 负责组织、指导和参与对计算机信息泄露、计算机病毒传播及其他计算机灾害事故的防范、处置工作；

(4) 负责计算机信息系统安全专用产品销售的监督管理等工作；

(5) 负责互联网用户的备案工作；

(6) 负责互联网上网服务营业场所(网吧等)的计算机安全保护和管理工作；

(7) 监督、指导和检查重点计算机信息单位的安全保护工作；