第 3 章

网络安全监督管理

【内容提要】

本章主要介绍信息网络安全监督管理工作的相关内容，包括互联网单位备案管理、互联网运营单位管理、互联网信息服务单位管理、联网单位管理、计算机病毒等破坏性程序防治管理等。通过学习，掌握信息网络安全监督管理工作的工作内容、工作方法、工作要求及行政处罚等方面的规定。

3.1 网络安全监督管理概述

网络安全监督管理工作，是指公安机关依照国家法律和法规，运用行政手段，对信息网络安全进行监督、检查和指导，有效预防信息网络违法犯罪，依法查处信息网络领域违法行为，维护网上公共秩序，保障社会生活正常运行的行政管理工作。信息网络安全监督管理工作是公共信息网络安全监察工作的重要内容，是国家行政管理的组成部分。

信息网络安全监督管理是由公安机关网络安全保卫部门依法公开实施的行政管理行为。《中华人民共和国人民警察法》第 6 条第 12 款规定，“公安机关的人民警察按照职责分工，依法履行监督管理计算机信息系统的安全保卫工作的职责”。公安机关网络安全保卫部门通过开展信息网络安全监督管理工作，达到维护信息网络安全的目的。

网络安全监督管理工作的对象包括互联网运营单位、互联网信息服务单位、联网单位、互联网上网服务营业场所和重要信息系统。本章重点介绍互联网运营单位、互联网信息服务单位和联网单位的监督管理工作。

3.1.1 网络安全监督管理指导思想

以维护信息网络领域安全为主要任务，依托基层基础工作，实行监督管理与技术防控相结合，依法管理、依法行政，增强网上防范控制能力，建立现代化的管理方式和长效机制，为开展网上工作、维护网络秩序、打击涉网犯罪提供重要保障。

1. 打牢基础，协调发展

信息网络安全监督管理工作是国家赋予公安机关的一项重要法定职责，是公安机关开展网上工作的重要支撑和重要基础。只有高度重视并扎实做好监督管理工作，与其他网络

安全保卫工作协调发展，齐头并进，才能为公安机关开展网上工作构建起坚实的基础支撑。

2. 群防群治，综合治理

信息网络安全监督管理工作是一项社会化综合治理工程，是全社会共同的责任，必须坚持“谁主管谁负责，谁经营谁负责，谁受益谁负责”的原则，充分调动网络运营单位、信息服务单位、联网单位和广大网民的积极性、主动性，构建全社会共同参与、群防群治的信息网络安全监督管理工作新格局，实现对信息网络安全的综合治理。

3. 积极防御，综合防范

加强对互联网安全的监督管理，落实各项安全保护管理制度和安全保护技术措施，有效遏制境内外敌对势力、敌对分子和一些别有用心的人利用境内网上各种信息传播渠道对我进行煽动、渗透和破坏活动，加强对计算机病毒和网络攻击等网络安全威胁事件的预警发现和快速处置能力，积极推进信息系统安全等级保护，确保基础信息网络和重要信息系统的安全运行。

4. 紧跟发展，掌握主动

互联网信息产业发展迅速，各种新兴业务层出不穷，公安机关网络安全保卫部门要密切关注互联网发展，对信息网络安全监督管理工作面临的形势、任务和挑战有清醒认识，对各种新兴的网络应用和服务主动介入，适时开展调查研究，坚持“正确引导、趋利避害、为我所用”的原则，加强对网络服务提供商的监督管理，明确责任、落实义务，做好各项管理制度和安全技术防范措施，牢牢把握网上控制的主动权。

5. 严格执法，热情服务

公安机关网络安全保卫部门必须依照有关法律法规的规定，及时、主动上门指导网络运营单位、联网单位落实安全保护管理制度和技术措施，做好网络安全知识宣传，建立方便、快捷的办事渠道，以热情的服务树立网络警案的形象。对“重建设，轻安全；重应用，轻管理”的单位，要采取必要的行政管理手段、法律手段强制其落实各项制度措施。

3.1.2　网络安全监督管理工作特点

信息网络安全监督管理具有不同于国家其他社会组织活动工作的特点，具体表现如下。

1. 管理对象的广泛性

(1) 互联网运营单位：包括互联网接入服务单位(Internet Service Provider，简称 ISP)、互联网数据中心(Internet Data Center，简称 IDC)等。

(2) 互联网信息服务单位(Internet Content Provider，简称 ICP)：包括网站、聊天室、论坛、搜索引擎、电子邮件、互联网娱乐平台、点对点服务、短信息、电子商务、网上视音频、声讯信息等服务单位。

(3) 联网单位。

(4) 互联网上网服务营业场所。

(5) 重要信息系统：涉及电力、民航、铁路等国家重要基础设施，也涉及金融、证券、保

险、工商、税务、海关等重点单位和重要政府部门的内部应用网络系统。

2. 管理方式的复杂多样性

管理对象的广泛性，决定了具体管理方式的多样性。尤其多个对象在现实中往往交织在一起，致使信息网络安全监督管理工作变得更加复杂。既有行政管理的一般管理方法，如指导、检查、督促和查处等，也有公安机关网络安全保卫部门所特有的特殊管理方式。另外，互联网新型服务以及新的管理对象层出不穷，也带来了新的管理方式。

3. 管理措施的强制性

监督管理工作不同于一般意义上的行政管理工作，它是以国家赋予公安机关治安强制措施作为后盾。

4. 管理活动的社会性

监督管理工作既是国家事务，也是一项社会事业。一方面，信息网络安全监督管理工作主要是面向社会公开进行的，关系到国家、集体和群众方方面面具体的利益；另一方面，信息网络安全监督管理工作的组织开展也离不开社会力量，依靠人民群众参与信息网络安全管理活动，也是维护社会治安秩序的客观需要。

3.1.3 网络安全监督管理主要任务

信息网络安全监督管理工作既包括公安机关网络安全保卫部门依法对互联网单位的监督、检查、管理工作，也包括公安机关网络安全保卫部门依法对重要信息系统的监督、指导工作。其主要任务大体分为以下几个方面。

1. 互联网安全管理

(1) 指导督促互联网单位的备案工作。

(2) 监督、检查互联网单位落实安全管理制度和安全保护技术措施。

(3) 监督管理互联网上网服务营业场所，严格进行安全审核和日常检查。

2. 监督、检查、指导重要信息系统的信息安全等级保护工作

3. 处置网上有害信息

4. 查处信息网络违法违规行为

5. 组织开展计算机病毒等破坏性程序的日常防治管理

6. 组织开展重大活动的信息安全保卫工作

7. 组织计算机安全员培训

3.1.4 网络安全监督管理主要方法

1. 开展基础调查

基础调查是公安机关网络安全保卫部门一项经常性和基础性的工作，是了解和掌握信息网络运营、服务和使用单位基本情况的重要手段，是总结经验教训、改进管理方式、提高管理水平的重要方法。

（1）建立畅通的交流和信息传输渠道。在公安机关和被管理的互联网单位之间建立纵向的信息交流和传输渠道，实行案事件报告制度、情况数据定期上报和数据变更及时上报等制度，全面掌握本地 ISP、IDC、ICP、联网单位的基本情况，熟悉网络的拓扑结构；在公安机关内部建立横向的交流渠道，实行情况通报制度，共享信息和数据。

（2）开展基础调查。按照特定时期的工作需要，组织开展基础调查专项工作，针对某一方面基础数据、基本情况进行调查和普查。

（3）对基础数据进行统计、分析。对大量数据进行统计、关联性分析研究，从中发现翔实的、有用的、规律性的基础数据，为制定管理计划和措施提供资料。

（4）建立基础数据库。通过基础调查获得的数据和掌握的情况都应建库管理，长期积累，及时更新；还要建立数据资料采集、录入的工作规范。

2. 建立信息网络安全监督管理制度

依照国家有关法律法规，结合安全管理工作实际，制定、完善和落实一整套针对性强，责、权明确的安全管理规章和制度，对重要信息系统单位、重点要害部位、上网服务场所、互联网联网单位、安全产品进行规范化管理。

3. 落实互联网安全保护技术措施

按照《互联网安全保护技术措施规定》的要求，监督管理互联网服务提供者、联网使用单位落实互联网安全保护技术措施。采取的互联网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，并保障互联网安全保护技术措施功能的正常发挥。

4. 建设社会支撑力量

“专群结合、依靠群众”是确保信息网络安全监督管理工作顺利进行的重要保障，通过发动、组织社会力量参与信息网络安全防范和管理工作，可以有效弥补公安机关警力不足，将违法犯罪行为置于群众和社会的监督之下。

（1）建立日常联络机制。

（2）安全组织和安全员的建设和管理。

（3）建立、健全网上信息安全的协管队伍。

（4）组织开展行业自律。

5. 加强宣传教育

（1）加强日常网络安全知识宣传。通过互联网站、本地主流新闻媒体，或者通过印制宣传书籍、画册的形式开展互联网日常安全的教育宣传活动，向社会宣传国家法律法规，指导开展信息网络安全防范；专项行动期间还应配合工作需要进行专题的宣传教育。

（2）通过计算机安全员培训进行集中宣传教育。

（3）管理工作中的宣传教育。网络安全保卫部门在日常管理执法工作中，有针对性地宣传法律法规，督促落实制度和技术措施，提高被管理单位和个人的安全意识；依法对违法违规行为进行处罚，起到惩戒教育的作用。

3.2 互联网单位管理

3.2.1 备案管理

备案是互联网安全管理的基础。备案制度的实施，可以增强连接互联网的单位的安全管理意识，建立健全安全管理制度，督促其依法履行社会责任；而备案工作也是公安机关网络安全保卫部门依法开展的警务工作，可以有效防止和控制危害我国国家利益的有害信息流入和涉及我国国家机密的重要信息流出。

1. 备案法律依据

1)《中华人民共和国计算机信息系统安全保护条例》(国务院147号令)

第十一条规定："进行国际联网的计算机信息系统，由计算机信息系统的使用单位报省级以上人民政府公安机关备案"。

2)《计算机信息网络国际联网安全保护管理办法》(公安部第33号令)

第十一条　用户在接入单位办理入网手续时，应当填写用户备案表。备案表由公安部监制。

第十二条　互联单位、接入单位、使用计算机信息网络国际联网的法人和其他组织(包括跨省、自治区、直辖市联网的单位和所属的分支机构)，应当自网络正式联通之日起三十日内，到所在地的省、自治区、直辖市人民政府公安机关指定的受理机关办理备案手续。

前款所列单位应当负责将接入本网络的接入单位和用户情况报当地公安机关备案，并及时报告本网络中接入单位和用户的变更情况。

第十四条　涉及国家事务、经济建设、国防建设、尖端科学技术等重要领域的单位办理备案手续时，应当出具其行政主管部门的审批证明。

前款所列单位的计算机信息网络与国际联网，应当采取相应的安全保护措施。

第十六条　公安机关计算机管理监察机构应当掌握互联单位、接入单位和用户的备案情况，建立备案档案，进行备案统计，并按照国家有关规定逐级上报。

3)《公安部关于对与国际联网的计算机信息系统进行备案工作的通知》

与国际联网的计算机信息系统的使用单位和个人，应当在网络正式联通后的三十日内，到所在地的省、自治区、直辖市人民政府公安机关指定的地(市)级或者县(市)级人民政府公安机关办理备案手续。

已经与国际联网的计算机信息系统，其使用单位和个人应当在本通知公布之日起三十日内，到所在地(市)级或者县(市)级人民政府公安机关补办备案手续。

与国际联网的计算机信息系统的使用单位和个人的联网方式变更或者终止联网时，应当在三十日内通知所在地(市)级或者县(市)级人民政府公安机关。

2. 备案对象和要求

凡中华人民共和国境内的互联网运营单位(包括ISP、IDC)、互联网信息服务单位

(ICP)、联网单位、互联网上网服务营业场所和个人联网用户均为备案对象。

注意：以上单位凡服务器托管地与维护地不在同一行政区划内的，必须同时向服务器托管地和维护地的公安机关网络安全保卫部门申请备案。

各互联网单位备案具体要求如下：

1) 互联网接入服务单位

互联网接入服务单位(Internet Service Provider，ISP)是指提供互联网接入网络运行的单位。接入网络是指通过接入互联网络进行国际联网的计算机信息网络，接入网络可以是多级连接的网络。

互联网接入服务单位办理备案需提供的资料清单如下：

(1) 中华人民共和国公安部网络安全保卫局印发的备案表一式两份(加盖备案单位公章)。

(2) 本单位的计算机信息网络安全组织成员名单，包括单位负责人、两名计算机安全员，含联系方式。

(3) 计算机安全员证书复印件。

(4) 本单位的计算机信息网络安全保护管理制度，包括互联网公用账号登记制度、互联网安全保护管理制度、互联网安全应急处置制度等。

(5) 安全保护技术措施。包括：网络安全审计、防病毒、防黑客攻击措施等。

(6) 本单位的网络拓扑图(标明内部 IP 使用情况)。

(7) 本单位的 IP 分配、使用和变更情况。

(8) 本单位的接入方式使用、新增和变更情况。

(9) 本单位的用户注册登记、使用与变更情况(包括固定 IP 用户、动态 IP 用户、托管主机用户)。

(10) 在提交上述材料的基础上，还需按照其他法律法规要求提交相关管理部门颁发的证照的复印件，如工商部门核发的营业执照副本复印件，信息产业部及各省市通信管理部门颁发的相关经营许可证等。

注意：公安机关网络安全保卫部门在受理互联网接入服务单位备案的同时，还要督促互联网接入服务单位报送接入本网络的联网用户(包括单位和个人)的情况，并及时以电子表格的形式报告本网络中接入用户的变更情况，包括用户姓名、联系电话、地址、身份证复印件、开户账号等。

除未开设个人网站、网页的个人联网用户属于上述情况之外，其他 IDC、ICP 等互联网接入服务单位的联网用户需直接到公安机关网络安全保卫部门备案。

2) 互联网数据中心

互联网数据中心(Internet Data Center，IDC)是指向企业、商户或网站服务器群提供大规范、高质量、安全可靠的专业化服务托管、虚拟空间租用、网络带宽出租等服务的单位。

互联网数据中心办理备案需提供的资料清单如下：

(1) 中华人民共和国公安部网络安全保卫局印发的备案表一式两份(加盖备案单位公章)。

（2）本单位的计算机信息网络安全组织成员名单，包括本单位负责人、两名计算机安全员，含联系方式。

（3）计算机安全员证书复印件。

（4）本单位的计算机信息网络安全保护管理制度。包括信息发布审核制度、24 小时交互栏目信息巡查制度、互联网公用账号登记制度、互联网安全管理制度、互联网安全应急处置制度等。

（5）安全保护技术措施。包括交互式栏目必须有关键字过滤技术措施、网络安全审计、防病毒防黑客攻击等措施。

（6）本单位的网络拓扑图（标明内部 IP 使用情况）。

（7）本单位 IP 分配、使用和变更情况。

（8）本单位所有托管主机服务用户的基本情况，包括网站相关资料、负责人信息、联系方式等。

（9）在提交上述材料的基础上，还需按照其他法律法规要求提交相关管理部门颁发的证照的复印件。

注意：公安机关网络安全保卫部门在受理互联网数据中心备案的同时，还要督促互联网数据中心报送本单位虚拟空间服务用户的情况，并及时以电子表格的形式报告虚拟空间服务用户的变更情况，包括用户虚拟空间的服务器地址、用户网站信息，用户姓名、联系电话、地址等。

3）互联网信息服务单位

互联网信息服务单位（Internet Content Provider，ICP）是指以互联网为载体，提供信息发布和信息查询服务的单位或个人，包括各类网站、个人主页和提供短信内容服务、游戏服务、邮件服务以及其他互联信息服务的单位或个人。

互联网信息服务分为经营性 ICP 和非经营性 ICP。

互联网信息服务单位办理备案需提供的资料清单如下：

（1）中华人民共和国公安部网络安全保卫局印发的备案表一式两份（加盖备案单位公章）。

（2）本单位的计算机信息网络安全组织成员名单，包括本单位负责人、两名计算机安全员，含联系方式；个人网站应提交计算机安全员名单及联系方式。

（3）计算机安全员证书复印件。

（4）本单位的计算机信息网络安全保护管理制度。包括：信息发布审核制度、24 小时交互栏目信息巡查制度、互联网公用账号登记制度、互联网安全管理制度、互联网安全应急处置制度等。

（5）安全保护技术措施。包括：交互式栏目必须有关键字过滤技术措施、网络安全审计、防病毒防黑客攻击等措施。

（6）本单位的网络拓扑图（标明内部 IP 使用情况）。

（7）网站网页基本情况，网页栏目设置与变更及栏目负责人情况。

(8) 提供服务或开办栏目的种类,重点说明新闻、交互式栏目、邮件服务、搜索引擎等情况;针对各种服务类型制定的安全保护管理制度及安全保护技术措施等。

(9) 虚拟主机用户情况。

(10) 在提交上述材料的基础上,还需按照其他法律法规要求提交工商部门核发的营业执照副本复印件;经营性网站必须提供通信管理部门核发的电信与信息服务业务经营许可证,非经营性网站必须提交通信管理部门核发的备案证书;从事新闻、出版、教育、医疗保健、药品和医疗器械等互联网信息服务的单位,还需提交审核证明等相关管理部门颁发的证照复印件。

注意:公安机关网络安全保卫部门在受理互联网信息服务单位备案的同时,还要督促互联网信息服务单位报送本单位提供出租网站服务用户的情况,并及时以电子表格的形式报告出租网站服务用户的变更情况,包括用户服务器的地址,所有者姓名、联系电话、详细地址、服务内容等。

同时具备 ISP、IDC、ICP 三种业务功能中两种或两种以上的,或者在原有业务功能基础上增加新业务功能的互联网单位,必须就每一种业务功能到公安机关网络安全保卫部门依法履行备案义务。具体要求:具备两种或两种以上业务功能的,必须一次性提交相关业务功能备案材料(参照 ISP、IDC 和 ICP 备案需提交的材料),到公安机关进行综合备案;在原有业务功能基础上增加新业务功能的,必须提交新业务功能对应的备案材料,到公安机关进行变更备案。

4) 互联网联网单位

互联网联网是指中华人民共和国境内的计算机互联网络、专业计算机信息网络、企业计算机信息网络,以及其他通过专线进行国际联网的计算机信息网络同外国的计算机信息网络相连接。互联网联网单位是指通过接入网络与互联网连接的计算机信息网络用户,包括单位用户及个人用户。社区、学校、图书馆、宾馆、咖啡馆、娱乐休闲中心等向特定对象提供上网服务的场所也纳入互联网联网单位管理。

互联网联网单位办理备案需提供的资料清单如下:

(1) 中华人民共和国公安部网络安全保卫局印发的备案表一式两份(加盖备案单位公章)。

(2) 本单位的计算机信息网络安全组织成员名单,包括单位负责人、两名计算机安全员,含联系方式。

(3) 计算机安全员证书复印件。

(4) 本单位的计算机信息网络安全保护管理制度,包括互联网安全保护管理制度、互联网安全应急处置制度等。

(5) 安全保护技术措施。包括:网络安全审计、防病毒、防黑客攻击措施等。

(6) 本单位的网络拓扑图(标明内部 IP 使用情况)。

(7) 在提交上述材料的基础上,还需提供工商行政管理部门核发的营业执照副本复印件。

5) 互联网上网服务营业场所

互联网上网服务营业场所是指通过计算机等设备向公众提供互联网上网服务的网吧、

电脑休闲室等营业性场所。

互联网上网服务营业场所办理备案需提供的资料清单如下：

(1) 中华人民共和国公安部网络安全保卫局印发的备案表一式两份(加盖备案单位公章)。

(2) 本单位的计算机信息网络安全组织成员名单，包括单位负责人、两名计算机安全员，含联系方式。

(3) 计算机安全员证书复印件。

(4) 本单位的计算机信息网络安全保护管理制度。包括互联网安全保护管理制度、互联网安全应急处置制度等。

(5) 互联网上网服务营业场所安全保护管理制度，包括上网人员登记制度，对上网人员可能利用互联网络从事违法犯罪活动进行巡查、举报、制止制度等。

(6) 互联网安全保护技术措施。包括网络安全审计、防病毒、防黑客攻击措施等。

(7) 互联网上网服务营业场所技术支持单位信息，包括单位名称、地址、主要联系人、联系方式、技术支持类型等。

(8) 本单位的安全管理软件安装使用情况，包括管理软件名称、型号、销售许可证号、生产厂家、联系人等。

(9) 本单位的网络拓扑图(标明内部 IP 使用情况)。

(10) 本单位的场地结构图(标明计算机位置编号与 IP 地址对应情况)。

(11) 本单位营业场所方位图。

(12) 租房协议(房屋是自己的需提交房产证复印件)。

(13) 在提交上述材料的基础上，还需按照其他法律法规要求提交工商部门核发的营业执照，文化部门核发的网络经营许可证，消防部门核发的消防安全审核意见书等相关管理部门颁发的证照的复印件。

6) 个人联网用户

个人联网用户是指以个人使用为目的，接入互联网的用户。

个人联网用户备案须知：

(1) 个人联网用户备案工作由互联网接入服务单位协助公安机关进行。

(2) 个人联网用户备案由互联网接入服务单位负责实名登记。个人用户在开通互联网时要提供相关基本资料，包括：个人用户姓名、联系电话、地址、身份证复印件、开户电话、开户账号、IP 用途等。资料先保存在接入服务单位，由接入服务单位汇总、整理后，统一报给公安机关备案。原则上，一般个人用户不直接到公安机关办理备案手续(个人用户计划开办网站、网页等互联网信息服务的，应当在接入服务商处登记相关资料时予以说明，并在网站开办后按网站、网页备案程序进行备案)。

(3) 互联网接入服务单位按照规定时间，将个人用户备案资料汇总、整理后，按照统一数据格式，以电子数据报表形式报送公安机关网络安全保卫部门。

(4) 公安机关网络安全保卫部门指导互联网接入服务单位调整、完善个人用户备案电

子数据报表数据项。

3. 备案管辖

(1) 各地级以上(含地级)人民政府公安机关网络安全保卫部门对物理位置在本行政区划内与互联网相连接的计算机信息系统(服务器)或维护人员都具有备案管辖权。

(2) 各地级以上(含地级)人民政府公安机关网络安全保卫部门对分别落于不同地级市的与互联网相连接的计算机信息系统(服务器)所在单位或维护人员、维护权在本地的都具有备案管辖权,即共同管辖。

备案管辖以计算机信息系统服务器所在地的公安机关网络安全保卫部门为主,负有监督管理责任,必须加强管理,及时指导、督促其履行备案义务。

(3) 计算机信息系统服务器所在地的公安机关网络安全保卫部门有义务将互联网单位的有关资料在备案结束后 15 天内抄送给计算机信息系统所在单位或维护人员、维护权所在地的公安机关网络安全保卫部门。

抄送互联网单位资料的主要内容包括:互联网单位和个人的基本资料、服务器资料、网站和网上服务相关资料、维护人员基本情况等。

(4) 与互联网相连接的互联网信息系统(服务器)或维护人员所在单位或个人都必须向服务器托管地和维护地的公安机关网络安全保卫部门申请备案。

4. 备案程序

1) 互联网单位备案程序

(1) 互联网单位下载或到公安机关网络安全保卫部门领取备案相关资料与表格。

(2) 各互联网单位按照要求填写备案表,由单位领导签字盖章,在其网络正式联通之日起 30 日内与其他需提交的材料一起提交到公安机关网络安全保卫部门。

(3) 公安机关网络安全保卫部门对各互联网单位提交的备案资料进行初审(对备案材料的真实性和合法性进行审核)和复审(按照备案表填写的内容逐项实地核查),审核无误后加盖公章,统一编号建立备案档案。审核中若发现各项制度未按要求落实或提交材料不齐的,退回材料,限期整改,符合要求后,可申请再次审核。

(4) 各互联网备案单位要记录好反馈的受理编号及密码,凭受理编号及密码可以登录修改备案资料、查看审核结果。审核通过后,各互联网备案单位要领取备案回执、备案证书,下载网站的备案图标。

(5) 如果是网站备案,除了下载备案图标、报警岗亭图标和“警警察察”图标外,还要及时将备案图标、报警岗亭图标置于网站首页的下方,“警警察察”图标置于交互式栏目入口处,并按要求完成相应的链接。

2) 公安机关网络安全保卫部门受理备案材料工作流程

公安机关网络安全保卫部门受理备案材料工作流程如图 3-1 所示。

3) 公安机关网络安全保卫部门核实检查备案工作流程

公安机关网络安全保卫部门核实检查备案工作流程如图 3-2 所示。

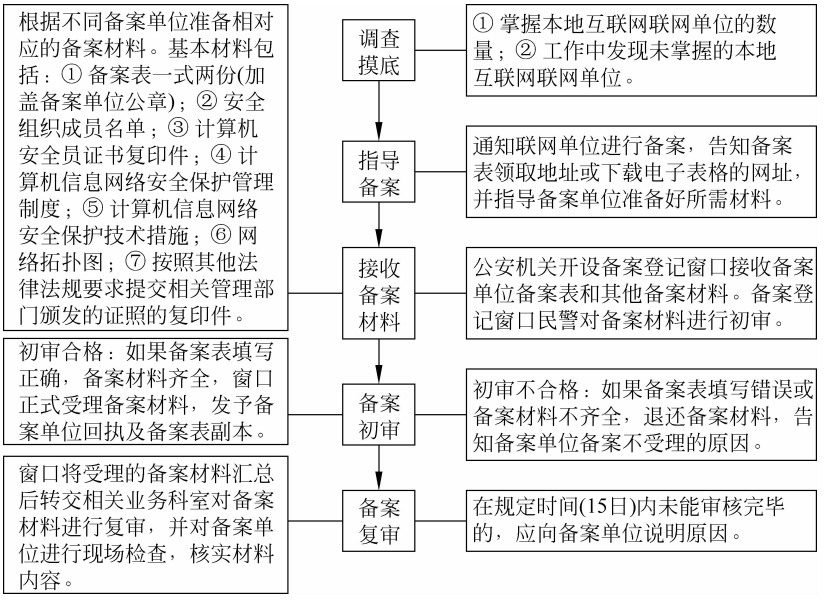

图 3-1　备案材料受理工作流程

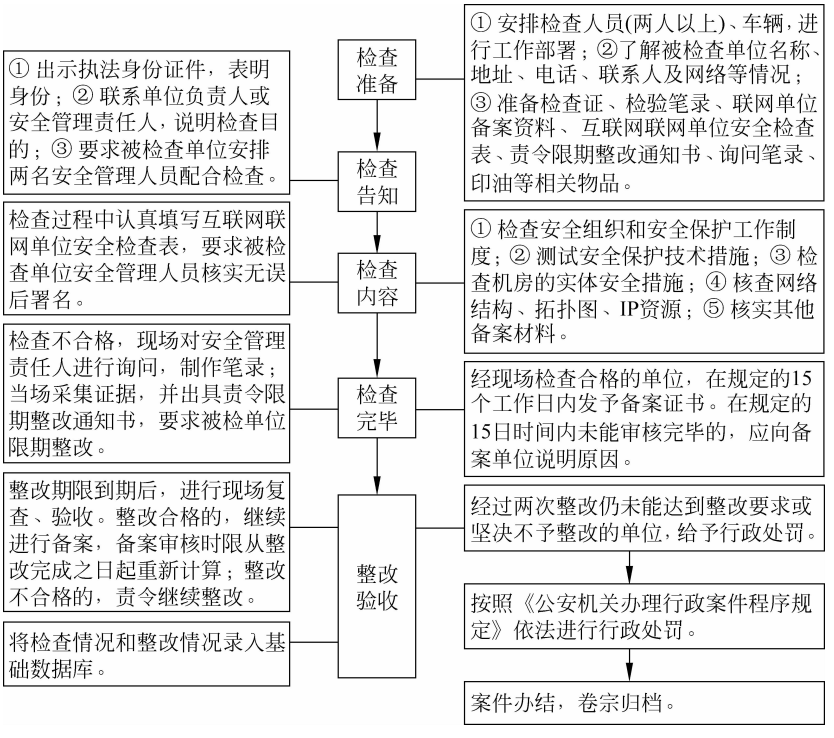

图 3-2　备案核实检查工作流程

5. 备案罚则

对不按规定履行备案义务的单位或个人，不落实安全管理制度和措施的，按照《中华人民共和国计算机信息系统安全保护条例》第二十条和《计算机信息网络国际联网安全保护管理办法》第二十三条规定，由公安机关责令限期改正，给予警告，有违法所得的，没收违法所得；在规定的限期内未改正的，对单位的主管负责人员和其他直接责任人员可以并处五千元以下的罚款，对单位可以并处一万五千元以下的罚款；情节严重的，并可以给予六个月以内的停止联网、停机整顿的处罚，必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格。

6. 相关表格

计算机信息网络国际联网单位备案表

填表时间：年　月　日　　编号：

<table>
<tr><td>单位名称</td><td colspan="3"></td><td>单位负责人
（法人代表）</td><td colspan="3"></td></tr>
<tr><td>通信地址</td><td colspan="7"></td></tr>
<tr><td>邮政编码</td><td colspan="3"></td><td colspan="2">联系电话</td><td colspan="2"></td></tr>
<tr><td rowspan="3">备案单位
安全管理员</td><td>姓名</td><td></td><td>电话</td><td></td><td>传真</td><td colspan="2"></td></tr>
<tr><td>姓名</td><td></td><td>电话</td><td></td><td>传真</td><td colspan="2"></td></tr>
<tr><td colspan="2">E-mail 地址</td><td colspan="5"></td></tr>
<tr><td>网络名称</td><td colspan="3"></td><td colspan="3">域名注册服务商</td><td></td></tr>
<tr><td>接入网络服务商</td><td colspan="3"></td><td colspan="3">申请入网时间</td><td></td></tr>
<tr><td>所属网络</td><td colspan="7">○中国电信　○中国教育和科研计算机网　○中国网通
○中国联通　○中国铁通　○中国移动　○其他网络</td></tr>
<tr><td>服务种类</td><td colspan="7">□接入服务　□ 虚拟空间租用　□ 主机托管　□ 电子邮件服务
□个人主页　□ 论坛、留言板、BBS 服务　□ FTP 服务
□WWW 服务　□ 聊天室　□ 电子商务　□ 即时通信服务
□短信息服务　□ 宽带多媒体服务　□ 网络游戏　□ 其他</td></tr>
<tr><td>服务性质</td><td colspan="7">○ ISP　○ ICP　○ IDC　○互联网单位用户　○ 其他</td></tr>
<tr><td>安全措施</td><td colspan="7">□ 防病毒　□ 防入侵　□ 信息过滤　□ 人工巡查　□ 其他</td></tr>
<tr><td>审计方式</td><td colspan="7">□ 人工登记　□ 系统日志　□ 专用审计软件　□ 其他</td></tr>
<tr><td>网络概况</td><td colspan="7">下级网络（详情填附表）_____个，联网主机_____台</td></tr>
<tr><td>网站、网页类型</td><td colspan="7">□ 自管主机　□ 托管主机　□ 虚拟空间　□ 虚拟主机</td></tr>
<tr><td>联网单位
接入方式</td><td colspan="7">□ DDN 专线　□ 光纤　□ 城域 IP 网　□ ADSL　□ ISDN
□ 拨号　□ Cable Modem　□ 其他</td></tr>
<tr><td>IP 地址范围</td><td colspan="7"></td></tr>
<tr><td>出口路由器 IP</td><td colspan="7"></td></tr>
<tr><td>域名服务器 IP</td><td colspan="7"></td></tr>
<tr><td>邮件服务器 IP</td><td colspan="7"></td></tr>
<tr><td colspan="4">备案单位盖章

年　月　日</td><td colspan="4">公安机关盖章

年　月　日</td></tr>
</table>

附表一　下级网络、虚拟空间租用及主机托管服务备案表

编号：

类型	○下级网络　○虚拟空间租用　○主机托管		
网络名称			
单位名称			
所在省(区市)		所在地(市)	
联系人		联系电话	
通信地址			
域名			
IP 地址段			

附表二　固定 IP 地址个人用户入网备案表(ISP 提供)

编号：

姓名		性别		出生日期	
证件种类		证件编号			
职业类别	○国家公务员　○企事业单位人员　○军人 ○农民　○商业、服务业人员　○学生、教师 ○无业人员　○其他				
联系电话					
上网地址					
通信地址					
IP 地址					
申请入网时间					
IP 地址分配单位					

***** 计算机国际联网单位备案审批表**

填表时间：年　月　日　　编号：

备案单位	
网站域名	
所提交备案材料清单	❑1. 公共信息网络安全保卫部门统一印制的备案表一式两份(加盖公章)； ❑2. 经营性互联网站需提交通信管理部门核发的《电信与信息服务业务经营许可证》、工商部门核发的《营业执照》副本复印件； ❑非经营性网站需提交建立网站用途及栏目说明性文件(加盖单位公章)； ❑个人网站需提交有效身份资料证照复印件； ❑3. 单位计算机信息网络安全组织成员名单(包括本单位主管领导、两名计算机安全员，含联系方式)； ❑4. 计算机安全员证书复印件； ❑5. 单位计算机信息网络安全管理制度(包括：信息发布审核制度、24 小时交互式栏目信息巡查制度、互联网安全应急处置制度等)；

续表

备案单位			
网站域名			
所提交备案材料清单	❑6. 互联网信息网络安全技术措施解决方案(包括：交互式栏目必须有关键字过滤技术措施、日志审计、防病毒防黑客攻击措施等)； ❑7. 从事刊载新闻的网站还必须提交新闻管理部门的批准文件； ❑8. 提供虚拟主机服务的信息服务单位，除提交以上材料外，还必须提交使用本单位虚拟主机服务的所有用户的基本情况，包括 URL、负责人、联系方式； ❑9. 系统维护权落于外地，服务器托管于云南的网站，除提交以上材料外，还必须提交其系统维护权所在地主管公安机关出具的备案证明。		
受理人		受理时间	
备案编号录入			
审核民警意见			
领导审批意见			
档案接收情况		接收时间	
备注			

网站备案信息真实性核验单

网站主办者基本信息：(网站主办者填写)			
网站主办者名称		网站类型	□单位　□个人
网站域名			
网站备案信息核验内容：(接入服务单位填写)			
一、主体信息核验内容：			
核验网站主办者、网站负责人证件资质(网站类型为“个人”时只需核验个人证件资质，请在核验的对应证件下打“√”)			
单位证件资质：□组织机构代码证书　□工商营业执照　□事业法人证书　□社团法人证书　□军队代号　□其他			
个人证件资质：□身份证　□户口簿　□军官证　□港澳台胞证　□护照　□其他			
网站主办者、网站负责人证件号码报备信息是否正确　□是　□否			
是否留存网站主办者、网站负责人证件复印件　□是　□否			
是否当面采集并留存网站负责人照片　□是　□否			
二、联系方式核验内容：			
网站负责人手机号码报备信息是否正确　□是　□否			
网站负责人座机号码报备信息是否正确(网站类型为“个人”时选填)　□是　□否			
网站负责人电子邮箱报备信息是否正确　□是　□否			
网站负责人通信地址报备信息是否正确　□是　□否			
三、网站信息核验内容：			
网站名称报备信息是否规范　□是　□否		域名报备信息是否正确　□是　□否	

续表

网站服务内容/项目报备信息是否正确 □是 □否
是否有前置审批或专项审批文件(如有前置审批或专项审批文件,请在核验文件内容的对应类别下打"√") □是 □否
□新闻 □出版 □教育 □医疗保健 □药品和医疗器械 □文化 □广播电视节目 □电子公告服务 □其他
四、接入信息报备内容:
本单位是否正确报备接入信息(包括"接入服务提供者名称"、"接入方式"、"服务器放置地点"、"网站IP地址") □是 □否
五、是否留存网站备案信息书面文档 □是 □否
网站备案信息核验承诺:(接入服务单位、网站主办者签署)
本单位(接入服务单位)已仔细阅读"《网站备案信息真实性核验单》填写说明",对说明内容已全部知晓并充分了解,愿意遵守全部内容。承诺已对《网站备案信息真实性核验单》"网站备案信息核验内容"中包含的网站主办者提交主体信息、联系方式、网站信息,本单位报备的接入信息进行逐项核验;承诺以上核验记录真实有效。 核验人签字: 单位盖章(接入服务单位): 日 期: 年 月 日 - 本人(本单位)已履行网站备案信息当面核验手续,承认以上填写信息和核验记录真实有效,承诺上述备案信息一旦发生变更,将及时进行更新,并愿意承担因网站备案信息不准确或更新不及时而采取的停止网站接入服务、注销备案等相应处理措施。 网站负责人签字: 单位盖章(网站主办者): 日 期: 年 月 日

3.2.2 互联网运营单位管理

1. 管理依据

1)《中华人民共和国计算机信息系统安全保护条例》

第六条 公安部主管全国计算机信息系统安全保护工作。

2)《中华人民共和国计算机信息网络国际联网管理暂行规定》

第六条 计算机信息网络直接进行国际联网,必须使用邮电部国家公用电信网提供的国际出入口信道。

任何单位和个人不得自行建立或者使用其他信道进行国际联网。

第八条 接入网络必须通过互联网络进行国际联网。

接入单位拟从事国际联网经营活动的,应当报有权受理从事国际联网经营活动申请的

互联单位主管部门或者主管单位申请领取国际联网经营许可证；未取得国际联网经营许可证的，不得从事国际联网经营业务。

接入单位拟从事非经营活动的，应当报经有权受理从事非经营活动申请的互联单位主管部门或者主管单位审批；未经批准的，不得接入互联网络进行国际联网。

申请领取国际联网经营许可证或者办理审批手续时，应当提供其计算机信息网络的性质、应用范围和主机地址等资料。

国际联网经营许可证的格式，由国务院信息化工作领导小组统一制定。

第十条　个人、法人和其他组织（以下统称用户）使用的计算机或者计算机信息网络，需要进行国际联网的，必须通过接入网络进行国际联网。

前款规定的计算机或者计算机信息网络，需要接入网络的，应当征得接入单位的同意，并办理登记手续。

3）《计算机信息网络国际联网安全保护管理办法》

第三条　公安部计算机管理监察机构负责计算机信息网络国际联网的安全保护管理工作。公安机关计算机管理监察机构应当保护计算机信息网络国际联网的公共安全，维护从事国际联网业务的单位和个人的合法权益和公众利益。

第八条　从事国际联网业务的单位和个人应当接受公安机关的安全监督、检查和指导，如实向公安机关提供有关安全保护的信息、资料及数据文件，协助公安机关查处通过国际联网的计算机信息网络的违法犯罪行为。

第九条　国际出入口信道提供单位、互联单位的主管部门或者主管单位，应当依照法律和国家有关规定负责国际出入口信道、所属互联网络的安全保护管理工作。

第十五条　省、自治区、直辖市公安厅（局），地（市）、县（市）公安局，应当有相应机构负责国际联网的安全保护管理工作。

第十六条　公安机关计算机管理监察机构应当掌握互联单位、接入单位和用户的备案情况，建立备案档案，进行备案统计，并按照国家有关规定逐级上报。

第十七条　公安机关计算机管理监察机构应当督促互联单位、接入单位及有关用户建立健全安全保护管理制度。监督、检查网络安全保护管理以及技术措施的落实情况。

公安机关计算机管理监察机构在组织安全检查时，有关单位应当派人参加。公安机关计算机管理监察机构对安全检查发现的问题，应当提出改进意见，作出详细记录，存档备查。

2. 管理对象

互联网运营单位安全管理对象主要包括在中华人民共和国境内从事互联网接入、主机托管及租赁、空间租用、域名注册等互联网运营服务单位。

3. 管理与服务内容

（1）督促、指导互联网运营单位建立安全组织机构，落实安全管理人员，并报公安机关网络安全保卫部门备案。计算机安全组织负责指挥、组织、协调本单位的计算机信息系统安全保护工作，对本单位的计算机信息网络安全统一指导管理。安全组织要设立两名以上专

职安全员，安全员和计算机安全相关重要岗位的人员应当参加公安机关组织的安全培训，持证上岗。

（2）督促、指导互联网运营单位到公安机关网络安全保卫部门进行备案。互联网运营单位应当自网络开通之日起30日内到所在地公安机关网络安全保卫部门依法办理备案手续，并按照公安机关规定提交个人用户变更情况，协助公安机关开展个人用户的备案工作。

（3）督促、指导互联网运营单位履行告知新增的联网单位用户和开设网站、网页的联网个人用户到公安机关网络安全保卫部门进行备案的义务。

（4）督促、指导互联网运营单位完善具体网络服务项目、网络拓扑结构、上网接入方式（包括小区的接入方式及小区内的组网方式）、IP地址的分布及IP地址和用户对应等基本要求。

（5）督促、指导互联网运营单位建立健全安全保护管理制度，包括：

① 计算机机房安全保护管理制度。

② 安全管理责任人、信息审查员的任免和安全责任制度。

③ 网络安全漏洞检测和系统升级管理制度。

④ 操作权限管理制度。

⑤ 用户登记制度。

⑥ 异常情况及违法犯罪案件报告和协查制度。

⑦ 安全教育和培训制度。

⑧ 重要信息系统的系统备份及应急预案制度。

⑨ 备案制度。

（6）督促、指导互联网运营单位在实体安全、信息安全、运行安全和网络安全等方面采取必要的安全保护技术措施，包括：

① 系统时钟统一，采取核对北京时间措施。

② 系统重要部分的冗余或备份措施。

③ 计算机病毒防治措施。

④ 网络攻击防范、追踪措施。

⑤ 安全审计和预警措施。

⑥ 系统运行和用户使用日志记录保存60日以上措施。

⑦ 对使用公网动态IP地址上网的用户，上网日志应包括上网时间、下网时间、用户名、主叫电话号码、分配给用户的IP地址等信息。

⑧ 使用内部IP地址，通过网络地址转换技术（NAT）上网的用户，上网日志应包括上网时间、下网时间、用户名、网卡MAC地址、内部IP地址、内部IP地址与外部IP地址的对应关系、访问的目标IP地址等信息。

⑨ 身份登记和识别确认措施。

⑩ 使用有关国家规定的安全管理产品（硬件和软件）。

(7) 督促、指导互联网运营单位制定突发安全事件和事故的应急处置方案。

(8) 督促、指导互联网运营单位通过互联网络进行国际联网，不得以其他方式进入国际联网。

(9) 督促、指导互联网运营单位落实计算机有害数据过滤、报告制度。

(10) 督促、指导互联网运营单位提供安全保护管理所需信息、资料及数据文件，主要包括：

① 用户注册登记、使用与变更情况(含用户账号、IP 地址及用户个人备案资料等)。

② IP 地址分配、使用及变更情况。

③ 用户网络服务功能设置及变更情况。

④ 与安全保护工作相关的其他信息。

4. 工作方法和要求

(1) 全面掌握本地所有互联网运营单位的基本情况，积极发展安全组织机构和安全员，加强对安全负责人、安全联络员、安全专管员及相关技术人员的管理，建立安全组织人员资料库，及时掌握运营单位的运行情况。

(2) 全面掌握互联网运营单位网络拓扑结构的基本情况，要求运营单位向公安机关网络安全保卫部门提供本单位网络拓扑结构的三级网络示意图。

(3) 全面掌握互联网运营单位 IP 资源和 IP 资源的分配接入方式(包括小区的接入方式、小区内的组网方式、IP 地址的分配和使用情况)，将 IP 资源情况录入基础数据库。

(4) 全面掌握互联网运营单位网络出口情况，重点发现互联网运营单位私自接入互联网或使用异地网络出口的情况，有效避免出现监管漏洞。

(5) 加强安全保护技术措施的检查，重点检查安全审计技术措施落实情况，对提供拨号上网、无线上网或小区接入的单位，着重要求采取必要的技术措施实现上网 IP、上网时间与上网用户的一一对应关系；特别是针对采用 NAT 方式为用户提供上网服务的单位，务必要求其记录 NAT 转换记录(包括内网 IP、转换出口的公网 IP、时间、访问的目的地址等)。

(6) 督促互联网运营单位依法履行备案义务和通知其提供服务的联网用户办理备案手续，并按照要求做好定期数据报送。在规定期间向公安机关网络安全保卫部门报送本月新增和变更的用户资料以及本单位 IP 地址使用情况，及时将报送数据整理录入基础数据库。

(7) 统一向互联网运营单位提供固定的报送接口和报送格式，不得随意改变报送接口和报送格式。

(8) 定期走访运营单位，每半年至少到各个单位走访调研一次，及时了解各单位发展情况和业务发展计划。

(9) 对未落实安全保护管理制度，经常发生违法行为，或未落实案件协查制度，案件倒查准确率不足 95%的，经屡次教育坚决不予改正的互联网运营单位严格依法查处。

5. 行政处罚

(1)《计算机信息网络国际联网安全保护管理办法》。

第二十一条　有下列行为之一的,由公安机关责令限期改正,给予警告,有违法所得的,没收违法所得;在规定的限期内未改正的,对单位的主管负责人员和其他直接责任人员可以并处五千元以下的罚款,对单位可以并处一万五千元以下的罚款;情节严重的,并可以给予六个月以内的停止联网、停机整顿的处罚,必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格。

① 未建立安全保护管理制度的。

② 未采取安全技术保护措施的。

③ 未对网络用户进行安全教育和培训的。

④ 未提供安全保护管理所需信息、资料及数据文件,或者所提供内容不真实的。

⑤ 对委托其发布的信息内容未进行审核或者对委托单位和个人未进行登记的。

⑥ 未建立电子公告系统的用户登记和信息管理制度的。

⑦ 未按照国家有关规定,删除网络地址、目录或者关闭服务器的。

⑧ 未建立公用账号使用登记制度的。

⑨ 转借、转让用户账号的。

(2) 不履行备案职责的,根据《计算机信息网络国际联网安全保护管理办法》第二十三条规定,由公安机关给予警告或者停机整顿不超过六个月的处罚。

(3) 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实施办法》第二十二条规定,对未使用邮电部国家公用电信网提供的国际出入口信道,或自行建立或者使用其他信道进行国际联网的,由公安机关责令停止联网,可以并处一万五千元以下罚款;有违法所得的,没收违法所得。对接入单位未领取国际联网经营许可证从事国际联网经营活动的,由公安机关给予警告,限期办理经营许可证;在限期内不办理经营许可证的,责令停止联网;有违法所得的,没收违法所得。对个人、法人和其他组织用户未通过接入网络进行国际联网的,对个人由公安机关处五千元以下的罚款;对法人和其他组织用户由公安机关给予警告,可以并处一万五千元以下的罚款。对进行国际联网的专业计算机信息网络经营国际互联网络业务的,由公安机关给予警告,可以并处一万五千元以下的罚款;有违法所得的,没收违法所得。企业计算机信息网络和其他通过专线进行国际联网的计算机信息网络违反只限于内部使用规定的,由公安机关给予警告,可以并处一万五千元以下的罚款;有违法所得的,没收违法所得。

6. 工作流程

1) 日常管理工作流程

互联网运营单位日常管理工作流程如图 3-3 所示。

2) 日常检查工作流程

互联网运营单位日常检查工作流程如图 3-4 所示。

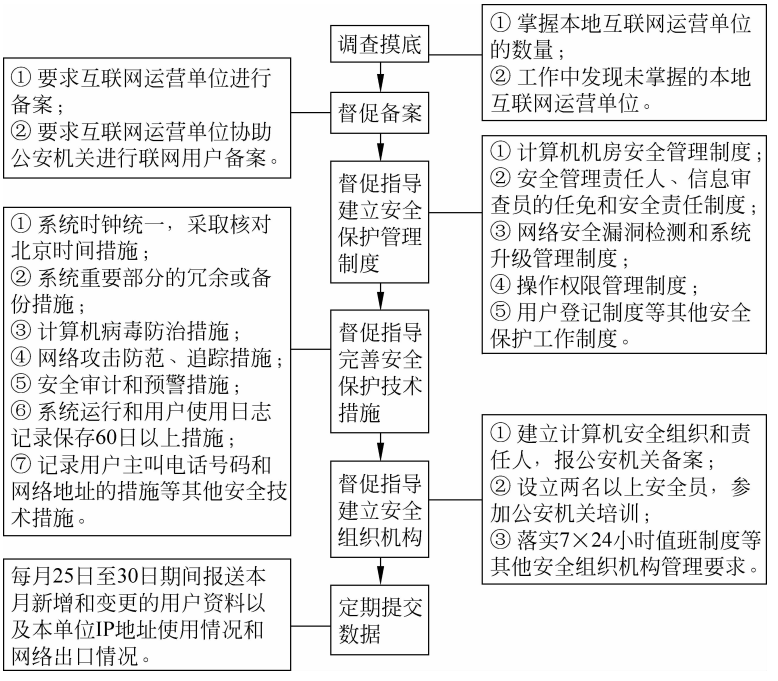

图 3-3　互联网运营单位日常管理工作流程

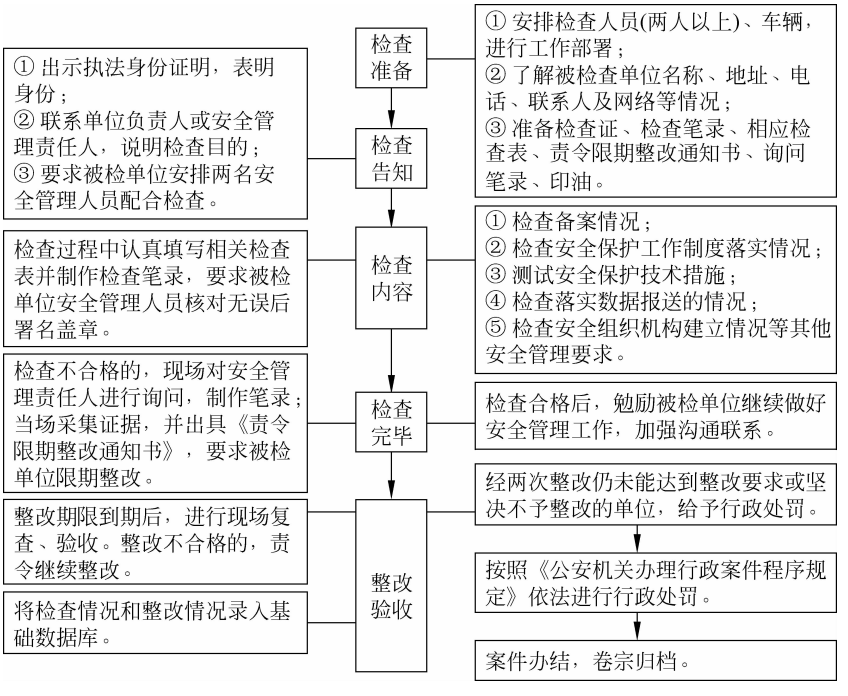

图 3-4　互联网运营单位日常检查工作流程

7. 相关表格

××市公共信息网络运营单位安全检查表

检查单位：××市公安局公共信息网络安全保卫部门

时间： 年 月 日

被检查单位		经营业务范围		
单位地址		邮政编码		
单位负责人		联系电话		
安全员		联系电话		
安全管理制度	1. 有无建立计算机机房安全保护管理制度			有□无□
	2. 有无建立安全管理责任人、信息审查员的任免和安全责任制度			有□无□
	3. 有无建立网络安全漏洞检测和系统升级管理制度			有□无□
	4. 有无建立操作权限管理制度			有□无□
	5. 有无建立用户登记制度			有□无□
	6. 有无建立病毒检测和网络安全漏洞检测制度			有□无□
	7. 有无建立违法案件报告协助查处制度			有□无□
	8. 有无建立账号使用登记和操作权限管理制度			有□无□
	9. 有无建立安全教育培训制度			有□无□
	10. 有无依法办理备案			有□无□
安全保护技术措施	11. 有无建立系统重要部分的冗余或备份措施			有□无□
	12. 有无建立计算机病毒防治措施，使用何种计算机防病毒软件			有□无□
	13. 有无建立网络攻击防范、追踪措施			有□无□
	14. 有无建立安全审计和预警措施			有□无□
	15. 系统各部位时钟是否以北京时间为标准统一			是□否□
	16. 有无系统运行和用户使用日志记录			有□无□
	17. 系统运行和用户使用日志记录有无保存 60 日以上			有□无□
	18. 有无记录用户主叫电话号码和网络地址的措施			有□无□
	19. 有无身份登记和识别确认措施			有□无□
	20. 是否使用国家规定的安全管理产品(硬件和软件)			有□无□
	21. 有无制定应急方案			有□无□
	22. 有无措施定期进行计算机信息网络风险评估，及时发现信息系统安全隐患并采取整改			有□无□
	23. 有无记录 ISDN、ADSL 等各类拨号上网用户的主叫号码、网络地址			有□无□
	24. 有无记录发生案件、事故和发现计算机有害数据的情况			有□无□
安全责任书	有无与公安机关签订有关网络与信息安全责任书，落实“谁主管、谁负责”的安全责任制度			有□无□
IP 地址段范围				

续表

提供安全保护管理所需信息、资料及数据文件情况	用户注册登记、使用与变更情况（含用户账号、IP 与 E-mail 地址等）	
	IP 地址分配、使用及变更情况	
	网络服务功能设置情况	
	与安全保护工作相关的其他信息	
用户备案情况		
计算机信息网络安全事件、事故报告制度落实情况		
安全领导小组和安全员名单及联系电话		

检查民警：　　联系电话：

被检查单位负责人：

安全员或技术员：

（盖章）

检查日期：　年　月　日

互联网信息安全责任书

管理监察单位：××市公安局公共信息网络安全保卫支队

责任单位：

为了明确各互联网数据中心（IDC）和开展虚拟主机业务的单位所应履行的安全管理责任，进一步规范互联网数据中心（IDC）和开展虚拟主机业务的单位的经营行为，确保互联网络与信息安全，同时也为客户营造一个安全洁净的网络环境，根据《计算机信息网络国际联网安全保护管理办法》等有关法律法规的规定，责任单位将认真落实如下责任：

一、自觉遵守法律、行政法规和其他有关规定，接受公安机关的安全监督、检查和指导，如实向公安机关提供有关安全保护的信息、资料及数据文件，协助公安机关查处通过国际联网的计算机信息网络的违法犯罪行为。

二、不利用国际联网危害国家安全，泄露国家秘密，不侵犯国家的、社会的、集体的利益和公民的合法权益，不从事违法犯罪活动。

三、不利用国际联网制作、复制、查阅和传播下列信息：

（一）煽动抗拒、破坏宪法和法律、行政法规实施的；

（二）煽动颠覆国家政权，推翻社会主义制度；

（三）煽动分裂国家、破坏国家统一；

（四）煽动民族仇恨、民族歧视，破坏民族团结；

（五）捏造或歪曲事实，散布谣言，扰乱社会秩序；

（六）宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪的；

（七）公然侮辱他人或者捏造事实诽谤他人的；

（八）损害国家机关信誉的；

（九）其他违反宪法和法律、行政法规的。

四、不从事下列危害计算机信息网络安全的活动：

（一）未经允许，进入计算机信息网络或者使用计算机信息网络资源的；

（二）未经允许，对计算机信息网络功能进行删除、修改或者增加的；

（三）未经允许，对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的；

（四）故意制作、传播计算机病毒等破坏性程序的；

（五）其他危害计算机信息网络安全的。

五、建立安全保护管理制度，落实各项安全保护技术措施，保障本单位网络运行安全和信息安全。

六、严格按照国家相关的法律法规做好本单位网络的信息安全管理工作，设立信息安全责任人和信息安全审查员，信息安全责任人和信息安全审查员在参加××市公安局网安支队认可的安全技术培训后，持证上岗。每月由信息安全审查员定期对本单位的接入用户及主机托管用户、主机租用用户、虚拟主机用户的安全审计日志及信息发布内容进行检查，发现有以上二、三、四点所列情形之一的，应当保留有关原始记录，并在 24 小时内向公安网络安全保卫部门报告。

七、按照国家有关规定，删除本单位网络中含有以上第三点内容地址、目录或关闭服务器。

八、与本单位所属接入用户及主机租用、托管用户和虚拟主机用户签订互联网信息安全承诺书，明确其责任、规范其管理维护行为。

九、对本单位接入用户及主机托管、主机租用和虚拟主机的用户应采用实名登记，并将用户变更情况于每月 25 日前报送公安网安部门。

十、变更名称、住所、法定代表人或者主要负责人、网络资源或者终止经营活动，到公安机关办理有关手续或者备案。

十一、本责任书自签署之日起生效。

责任单位（盖章）：

法人代表（签字）：

年　月　日

互联网信息安全承诺书

一、本单位(或个人)因为("□"为选项):

□使用_____的互联网络资源;

□与_____开展其他互联网合作项目。

郑重承诺遵守本承诺书的有关条款,如有违反本承诺书有关条款的行为,由本单位(或个人)承担由此带来的一切民事、行政和刑事责任。

二、本单位(或个人)承诺遵守《中华人民共和国计算机信息系统安全保护条例》和《计算机信息网络国际联网安全保护管理办法》等国家的有关法律、法规和行政规章制度。

本单位(或个人)开设的网站,在开通联网的 30 天内到××市公安局网安部门履行备案手续,并将接受××市公安局网安部门的监督和检查,如实主动提供有关安全保护的信息、资料及数据文件,积极协助查处通过国际联网的计算机信息网络违法犯罪行为。

三、本单位(或个人)保证不利用国际互联网危害国家安全、泄露国家秘密,不侵犯国家的、社会的、集体的利益和公民的合法权益,不从事违法犯罪活动。

四、本单位(或个人)承诺严格按照国家相关的法律法规做好网站的信息安全管理工作,设立信息安全责任人和信息安全审查员,信息安全责任人和信息安全审查员在参加××市公安局网络安全保卫部门认可的安全技术培训后,持证上岗。

本单位(或个人)承诺健全各项互联网安全保护管理制度和落实各项安全保护技术措施。

五、本单位(或个人)承诺不制作、复制、查阅和传播不列信息:

(一) 反对宪法所确定的基本原则的;

(二) 危害国家安全,泄露国家秘密,颠覆国家政权,破坏国家统一的;

(三) 损害国家荣誉和利益的;

(四) 煽动民族仇恨、民族歧视,破坏民族团结的;

(五) 破坏国家宗教政策,宣扬邪教和封建迷信的;

(六) 散布谣言,扰乱社会秩序,破坏社会稳定的;

(七) 散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的;

(八) 侮辱或者诽谤他人,侵害他人合法权益的;

(九) 含有法律、行政法规禁止的其他内容的。

六、本单位(或个人)承诺不从事下列危害计算机信息网络安全的活动:

(一) 未经允许,进入计算机信息网络或者使用计算机信息网络资源的;

(二) 未经允许,对计算机信息网络功能进行删除、修改或者增加的;

(三) 未经允许,对计算机信息网络中存储或者传输的数据和应用程序进行删除、修改或者增加的;

(四) 故意制作、传播计算机病毒等破坏性程序的;

(五) 其他危害计算机信息网络安全的。

七、本单位(或个人)承诺当计算机信息系统发生重大安全事故时,立即采取应急措施,保留有关原始记录,并在24小时内向××市公安局网络安全保卫部门报告。

八、若违反本承诺书有关条款和国家相关法律法规的,本单位(或个人)直接承担相应法律责任;造成第三方财产损失的,本单位(或个人)将在国家有关机关确认的责任范围内直接赔偿。

九、本承诺书自签署之日起施行。

责任单位(或个人):

法人代表(或授权代表):

二〇　年　月

3.2.3 互联网信息服务单位管理

1. 管理依据

1)《计算机信息网络国际联网安全保护管理办法》

第五条　任何单位和个人不得利用国际联网制作、复制、查阅和传播下列信息:

① 煽动抗拒、破坏宪法和法律、行政法规实施的;

② 煽动颠覆国家政权,推翻社会主义制度的;

③ 煽动分裂国家、破坏国家统一的;

④ 煽动民族仇恨、民族歧视,破坏民族团结的;

⑤ 捏造或者歪曲事实,散布谣言,扰乱社会秩序的;

⑥ 宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖,教唆犯罪的;

⑦ 公然侮辱他人或者捏造事实诽谤他人的;

⑧ 损害国家机关信誉的;

⑨ 其他违反宪法和法律、行政法规的。

第六条　任何单位和个人不得从事下列危害计算机信息网络安全的活动:

① 未经允许,进入计算机信息网络或者使用计算机信息网络资源的;

② 未经允许,对计算机信息网络功能进行删除、修改或者增加的;

③ 未经允许,对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的;

④ 故意制作、传播计算机病毒等破坏性程序的;

⑤ 其他危害计算机信息网络安全的。

第七条　用户的通信自由和通信秘密受法律保护。任何单位和个人不得违反法律规定,利用国际联网侵犯用户的通信自由和通信秘密。

第十条　互联单位、接入单位及使用计算机信息网络国际联网的法人和其他组织应当履行下列安全保护职责:

① 负责本网络的安全保护管理工作,建立健全安全保护管理制度;

② 落实安全保护技术措施，保障本网络的运行安全和信息安全；

③ 负责对本网络用户的安全教育和培训；

④ 对委托发布信息的单位和个人进行登记，并对所提供的信息内容按照本办法第五条进行审核；

⑤ 建立计算机信息网络电子公告系统的用户登记和信息管理制度；

⑥ 发现有本办法第四条、第五条、第六条、第七条所列情形之一的，应当保留有关原始记录，并在二十四小时内向当地公安机关报告；

⑦ 按照国家有关规定，删除本网络中含有本办法第五条内容的地址、目录或者关闭服务器。

第十二条　互联单位、接入单位、使用计算机信息网络国际联网的法人和其他组织（包括跨省、自治区、直辖市联网的单位和所属的分支机构），应当自网络正式联通之日起三十日内，到所在地的省、自治区、直辖市人民政府公安机关指定的受理机关办理备案手续。

前款所列单位应当负责将接入本网络的接入单位和用户情况报当地公安机关备案，并及时报告本网络中接入单位和用户的变更情况。

第十七条　公安机关计算机管理监察机构应当督促互联单位、接入单位及有关用户建立健全安全保护管理制度。监督、检查网络安全保护管理以及技术措施的落实情况。

公安机关计算机管理监察机构在组织安全检查时，有关单位应当派人参加。公安机关计算机管理监察机构对安全检查发现的问题，应当提出改进意见，作出详细记录，存档备查。

2）《互联网信息服务管理办法》

第十四条　从事新闻、出版以及电子公告等服务项目的互联网信息服务提供者，应当记录提供的信息内容及其发布时间、互联网地址或者域名；互联网接入服务提供者应当记录上网用户的上网时间、用户账号、互联网地址或者域名、主叫电话号码等信息。

互联网信息服务提供者和互联网接入服务提供者的记录备份应当保存 60 日，并在国家有关机关依法查询时，予以提供。

第十五条　互联网信息服务提供者不得制作、复制、发布、传播含有下列内容的信息：

① 对宪法所确定的基本原则的；

② 危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

③ 损害国家荣誉和利益的；

④ 煽动民族仇恨、民族歧视，破坏民族团结的；

⑤ 破坏国家宗教政策，宣扬邪教和封建迷信的；

⑥ 散布谣言，扰乱社会秩序，破坏社会稳定的；

⑦ 散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

⑧ 侮辱或者诽谤他人，侵害他人合法权益的；

⑨ 含有法律、行政法规禁止的其他内容的。

第十六条　互联网信息服务提供者发现其网站传输的信息明显属于本办法第十五条所列内容之一的，应当立即停止传输，保存有关记录，并向国家有关机关报告。

2. 管理种类

互联网信息服务单位管理包括网站、电子邮件服务单位、互联网娱乐平台服务单位、点对点信息服务单位、网上短消息服务单位及网上公共信息场所等单位的管理。

互联网信息服务分为经营性和非经营性两类。非经营性互联网信息服务单位是指通过互联网向用户无偿提供具有公开性、共享性信息服务活动。主要是指各级政府部门的网站、新闻机构的电子版报刊，企事业单位、教育科研机构的各类公益性网站和对本单位产品或业务作自我宣传的网站。经营性互联网信息服务单位是指通过互联网，向上网用户有偿提供信息或者网页制作等服务活动。经营的内容主要是网上广告、代制作网页、服务器内存空间出租、有偿提供特定信息内容、电子商务及其他网上应用服务。国家对经营性互联网信息服务单位实行经营许可证制度，对非经营性 ICP 实行备案制度。

3. 管理对象

(1) 网站安全管理对象包括中华人民共和国境内的网站开设单位。

(2) 电子邮件安全管理对象包括中华人民共和国境内的电子邮件服务单位。

(3) 互联网娱乐平台安全管理对象是中华人民共和国境内以公共信息网络为平台，发行、运营互联网网络游戏的单位和互联网网络游戏开发、代理、运营单位。

(4) 点对点信息安全管理对象是中华人民共和国境内，以点对点共享网络为平台进行点对点文件共享和数据交互以及其他点对点信息应用的单位。

(5) 互联网短信息服务安全管理对象是中华人民共和国境内以移动通信运营商和互联网信息服务单位提供的信息交换平台，进行文字、图片等短信息交流的单位。

(6) 网上公共信息场所管理对象是指通过互联网向上网用户提供信息或者电子公告、BBS、论坛、网络聊天室、网页制作、即时通信等交互形式，为上网用户提供信息发布条件，为市民提供信息公共场所的单位。

4. 管理和服务的内容

(1) 督促、指导互联网信息服务单位建立安全组织机构，落实安全管理人员。

(2) 督促、指导互联网信息服务单位到公安机关网络安全保卫部门依法履行备案义务。

(3) 督促、指导互联网信息服务单位建立健全安全保护管理制度。

(4) 督促、指导互联网信息服务单位完善落实安全保护技术措施。

(5) 督促、指导电子邮件服务单位建立健全邮件服务工作规范。

(6) 督促、指导网络娱乐平台服务单位、点对点信息服务运营单位与公安机关信息网络安全报警处置系统连接，实现用户账号等报警特征条件和有害信息过滤关键词远程更新，用户信息和留存信息远程查询。

(7) 督促、指导点对点信息服务运营单位关闭或删除含有有害信息的地址、目录或者服务器；对传播有害信息的用户基于用户账号、网络地址进行屏蔽。

(8) 督促、指导点对点信息服务运营单位与公安机关网络安全保卫部门建立网上违法犯罪案件协助配合调查的工作程序。

5. 工作方法和要求

(1) 全面掌握基本情况。

(2) 加强安全检查和指导。

(3) 建立日常应急联络机制。

(4) 逐步落实实名制。

(5) 督促、指导网站落实信息先审后发制度。

(6) 督促、指导电子邮件服务单位落实关键字技术措施；推动电子邮件服务单位履行行业规范；建立案件协查机制；建立有害信息的应急处置机制。

(7) 加强对互联网娱乐平台开设的新业务、新栏目指导监管，防止涉及黄赌毒内容的业务进入互联网娱乐平台；落实重点网络游戏用户虚拟财产保护工作；加强对互联网娱乐平台的公示牌聊天功能等交互式空间内容的管理。

(8) 建立紧急突发事件预警通报机制。

6. 行政处罚

(1) 根据《计算机信息网络国际联网安全保护管理办法》第二十条规定，利用国际联网制作、复制、查阅和传播有害信息或者从事危害计算机信息网络安全活动的，由公安机关给予警告，有违法所得的，没收违法所得，对个人可以并处五千元以下的罚款，对单位可以并处一万五千元以下的罚款；情节严重的，并可以给予六个月以内停止联网、停机整顿的处罚，必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格；构成违反治安管理行为的，依照治安管理处罚条例的规定处罚；构成犯罪的，依法追究刑事责任。

(2) 根据《计算机信息网络国际联网安全保护管理办法》第二十一条规定，有下列行为之一的，由公安机关责令限期改正，给予警告，有违法所得的，没收违法所得；在规定的限期内未改正的，对单位的主管负责人员和其他直接责任人员可以并处五千元以下的罚款，对单位可以并处一万五千元以下的罚款；情节严重的，并可以给予六个月以内的停止联网、停机整顿的处罚，必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格。

① 未建立安全保护管理制度的。

② 未采取安全技术保护措施的。

③ 未对网络用户进行安全教育和培训的。

④ 未提供安全保护管理所需信息、资料及数据文件，或者所提供内容不真实的。

⑤ 对委托其发布的信息内容未进行审核或者对委托单位和个人未进行登记的。

⑥ 未建立电子公告系统的用户登记和信息管理制度的。

⑦ 未按照国家有关规定，删除网络地址、目录或者关闭服务器的。

⑧ 未建立公用账号使用登记制度的。

⑨ 转借、转让用户账号的。

(3) 根据《计算机信息网络国际联网安全保护管理办法》第二十三条规定，不履行备案职责的，由公安机关给予警告或者停机整顿不超过六个月的处罚。

（4）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实施办法》第二十二条规定，对未使用邮电部国家公用电信网提供的国际出入口信道，或自行建立或者使用其他信道进行国际联网的，由公安机关责令停止联网，可以并处一万五千元以下罚款；有违法所得的，没收违法所得。对接入单位未领取国际联网经营许可证从事国际联网经营活动的，由公安机关给予警告，限期办理经营许可证；在限期内不办理经营许可证的，责令停止联网；有违法所得的，没收违法所得。对个人、法人和其他组织用户未通过接入网络进行国际联网的，对个人由公安机关处五千元以下的罚款；对法人和其他组织用户由公安机关给予警告，可以并处一万五千元以下的罚款。对进行国际联网的专业计算机信息网络经营国际互联网络业务的，由公安机关给予警告，可以并处一万五千元以下的罚款；有违法所得的，没收违法所得。企业计算机信息网络和其他通过专线进行国际联网的计算机信息网络违反只限于内部使用规定的，由公安机关给予警告，可以并处一万五千元以下的罚款；有违法所得的，没收违法所得。

7. 工作流程

1）日常管理工作流程

互联网信息服务单位日常管理工作流程如图 3-5 所示。

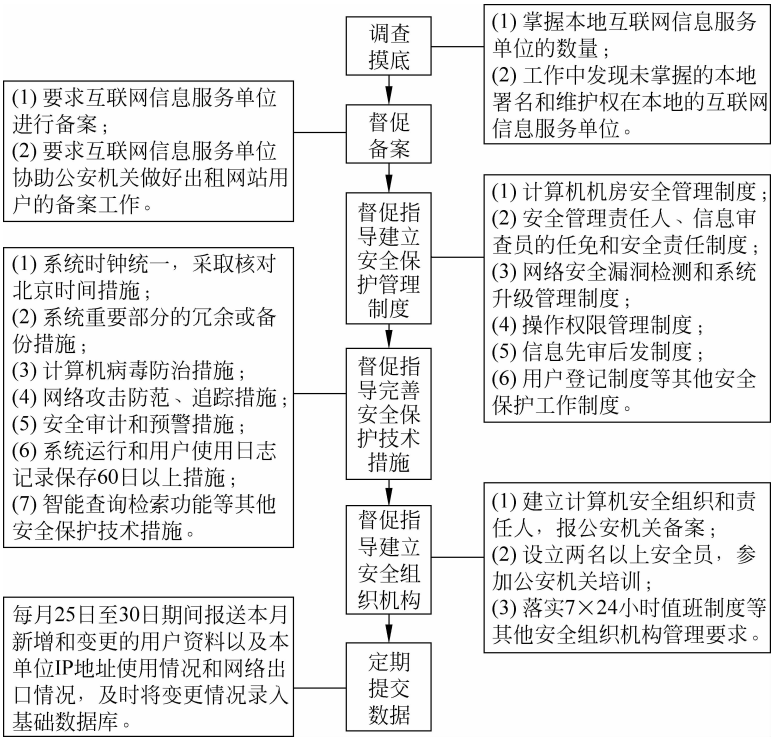

图 3-5　互联网信息服务单位日常管理工作流程

2）日常检查工作流程

互联网信息服务单位日常检查工作流程参见如图 3-4 所示的互联网运营单位日常检查工作流程。

8. 相关表格

××市信息网络应用单位网络安全检查表

检查单位：××市公安局公共信息网络安全保卫支队　　时间：　年　月　日

<table>
<tr><td>被检查单位名称</td><td colspan="3"></td></tr>
<tr><td>单位地址</td><td colspan="3"></td></tr>
<tr><td>负责人</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>联网情况</td><td colspan="2">接入方式(服务商)_____
账号(电话)_____
联网主机数_____
IP 地址_____
服务内容_____
联网用途_____</td><td>网络拓扑图</td></tr>
<tr><td rowspan="4">组织制度</td><td colspan="2">单位成立网络安全小组，确立安全小组责任人(单位领导任组长)，确立组长责任制</td><td>有□　无□</td></tr>
<tr><td colspan="2">组长落实小组人员岗位工作职责</td><td>有□　无□</td></tr>
<tr><td colspan="2">配备 2～4 名计算机安全员，须持证上岗</td><td>有□　无□</td></tr>
<tr><td colspan="2">制定网络安全事故处置措施</td><td>有□　无□</td></tr>
<tr><td rowspan="8">安全保护管理制度</td><td colspan="2">计算机机房安全保护管理制度</td><td>有□　无□</td></tr>
<tr><td colspan="2">用户登记制度和操作权限管理制度</td><td>有□　无□</td></tr>
<tr><td colspan="2">网络安全漏洞检测和系统升级管理制度</td><td>有□　无□</td></tr>
<tr><td colspan="2">交互式栏目 24 小时巡查制度</td><td>有□　无□</td></tr>
<tr><td colspan="2">电子公告系统用户登记制度</td><td>有□　无□</td></tr>
<tr><td colspan="2">信息发布审核、登记、保存、清除和备份制度，信息群发服务管理制度</td><td>有□　无□</td></tr>
<tr><td colspan="2">违法案件报告和协查制度</td><td>有□　无□</td></tr>
<tr><td colspan="2">备案制度</td><td>有□　无□</td></tr>
<tr><td rowspan="8">安全保护技术措施</td><td colspan="2">具有保存 3 个月以上系统网络运行日志和用户使用日志记录功能，内容包括 IP 地址分配及使用情况，交互式信息发布者、主页维护者、邮箱使用者和拨号用户上网的起止时间和对应 IP 地址，交互式栏目的信息等</td><td>有□　无□</td></tr>
<tr><td colspan="2">安全审计及预警措施</td><td>有□　无□</td></tr>
<tr><td colspan="2">网络攻击防范、追踪措施</td><td>有□　无□</td></tr>
<tr><td colspan="2">计算机病毒防治措施</td><td>有□　无□</td></tr>
<tr><td colspan="2">身份登记和识别确认措施</td><td>有□　无□</td></tr>
<tr><td colspan="2">交互式栏目具有关键字过滤技术措施</td><td>有□　无□</td></tr>
<tr><td colspan="2">开设短信息服务的具有短信群发限制、过滤和删除等技术措施</td><td>有□　无□</td></tr>
<tr><td colspan="2">开设邮件服务的，是否具有垃圾邮件的清理功能</td><td>是□　否□</td></tr>
<tr><td colspan="4">检查意见：</td></tr>
</table>

检查民警：　　被检查单位负责人：

××市互联网电子邮件服务安全检查表

检查单位：××市公安局公共信息网络安全保卫支队　　时间：　年　月　日

<table>
<tr><td>单位名称</td><td></td><td>负责人</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>单位地址</td><td></td><td>邮件服务管理人</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>联网方式</td><td colspan="3">□ADSL　□ISDN　□DDN
□微波　□HFC　□光纤</td><td colspan="2">有(　　)个接入 IP</td></tr>
<tr><td>(固定 IP)互联网接入 IP 地址</td><td colspan="2"></td><td>所属 ISP</td><td colspan="2"></td></tr>
<tr><td>(动态 IP)互联网接入账号</td><td colspan="2"></td><td>上网电话</td><td colspan="2"></td></tr>
<tr><td>网站名称</td><td colspan="2"></td><td>网站 URL</td><td colspan="2"></td></tr>
<tr><td>电子邮件服务器 IP 地址</td><td></td><td rowspan="2">用户数量</td><td colspan="3">外：</td></tr>
<tr><td>使用的电子邮件服务软件</td><td></td><td colspan="3">内：</td></tr>
<tr><td rowspan="6">安全管理制度</td><td colspan="4">是否到公安机关履行备案手续</td><td>是□　否□</td></tr>
<tr><td colspan="4">有无设立有害垃圾电子邮件举报、投诉信箱</td><td>有□　无□</td></tr>
<tr><td colspan="4">有无建立用户举报、投诉处理制度</td><td>有□　无□</td></tr>
<tr><td colspan="4">有无设立反有害垃圾邮件公告信息</td><td>有□　无□</td></tr>
<tr><td colspan="4">有无建立与公安机关联系、报告制度</td><td>有□　无□</td></tr>
<tr><td colspan="4">有无保留备份有害垃圾电子邮件地址和相关记录</td><td>有□　无□</td></tr>
<tr><td rowspan="13">技术防范措施</td><td colspan="4">是否限制本地电子邮件用户一次性发送 25 封以上电子邮件(除特定用户外)</td><td>是□　否□</td></tr>
<tr><td colspan="4">有无本地邮件服务器电子邮件用户账号认证功能</td><td>有□　无□</td></tr>
<tr><td colspan="4">是否限制邮件服务器自动转发功能(除特定电子邮件外)</td><td></td></tr>
<tr><td colspan="4">有无保留电子邮箱用户登录、退出等日志记录 60 天</td><td>有□　无□</td></tr>
<tr><td colspan="4">是否能够对发送电子邮件的特定 IP 地址进行阻断</td><td>是□　否□</td></tr>
<tr><td colspan="4">是否能够限制来自相同客户端 IP 的最大同时连接数量、最大连接频率</td><td>是□　否□</td></tr>
<tr><td colspan="4">是否能够对电子邮件信头主题、收发件人、抄送人等内容进行基于特征字符串的过滤</td><td>是□　否□</td></tr>
<tr><td colspan="4">是否能够对电子邮件信体内容进行基于特征字符串的过滤</td><td>是□　否□</td></tr>
<tr><td colspan="4">是否能够对电子邮件附件标题、文件类型和长度进行基于特征字符串的过滤</td><td>是□　否□</td></tr>
<tr><td colspan="4">有无对符合过滤规则的电子邮件可以采用弹回、丢弃、转发、投递、等待、延时等动作</td><td>有□　无□</td></tr>
<tr><td colspan="4">是否支持过滤规则动态导入和维护，并立即生效</td><td>是□　否□</td></tr>
<tr><td colspan="4">是否对电子邮件信头、信体进行扫面之前，支持 BASE64 和 QuotedPrintable 等解码</td><td>是□　否□</td></tr>
<tr><td colspan="4">有无对有害垃圾电子邮件过滤和阻断数量进行统计的功能</td><td>有□　无□</td></tr>
<tr><td colspan="4">对公安机关所要求过滤的有害信息是否可以向公安机关远程传送</td><td>是□　否□</td></tr>
<tr><td colspan="6">检查结果：</td></tr>
</table>

检查民警：　　被检查单位负责人：

××市网络游戏运营单位安全检查表

检查单位：××市公安局公共信息网络安全保卫支队　　时间：　年　月　日

单位名称		负责人		联系电话	
单位地址		游戏运营管理人		联系电话	
公司业务					
网站名称			网站 URL		
游戏网站及服务器接入 IP 地址				所属 ISP	
游戏网站及服务器分布情况					
安全管理制度	是否到公安机关履行备案手续				是□　否□
	有无建立与公安机关联系、报告制度				有□　无□
	有无建立违法案件报告和协查制度				有□　无□
	有无设立安全组织				有□　无□
	有无建立安全管理人员岗位工作职责				有□　无□
	有无安全教育和培训制度				有□　无□
	有无建立突发事件应急计划				有□　无□
	有无制定信息发布审核、登记制度				有□　无□
	有无落实病毒检测和网络安全漏洞检测制度				有□　无□
技术防范措施	有无保存系统网络运行日志和用户使用日志记录 60 天以上				有□　无□
	有无保存游戏用户注册登记、使用与变更情况				有□　无□
	有无记录、保存游戏用户注册 IP 地址与登录 IP 地址				有□　无□
	有无落实游戏用户身份审计和在线监控措施				有□　无□
	有无对在线聊天采取关键字过滤技术				有□　无□
其他安全管理制度和技术措施					
网络游戏运营情况	网络游戏种类		游戏名称		用户数量
检查结果：					

检查民警：　　被检查单位负责人：

××市互联网信息服务单位安全检查表

检查单位：××市公安局公共信息网络安全保卫支队　　时间：　年　月　日

被检查单位			经营业务范围		
单位地址			邮政编码		
单位负责人		联系电话			
安全员		联系电话			
网站中文名		IP 地址			
网址					
设置的网络服务栏目	论坛□　留言板□　聊天室□　即时通信□　电子邮件□　网页制作□　P2P□ 短信息□　新闻□　短信息□　网络游戏□　电子商务□ 空间出租□　域名服务□　搜索引擎□				
安全管理制度	1. 网站是否在公安部门备案			有□	无□
	2. 有无建立本单位网络安全管理负责人和安全领导小组负责制度			有□	无□
	3. 安全员、信息员是否经过培训持公安部门合格证上岗			有□	无□
	4. 新闻网站和具有新闻登载资格的非新闻单位网站对新闻栏目有无实行先审后发制度			有□	无□
	5. 有无对 BBS 栏目实行先审后发制度			有□	无□
	6. 有无对新闻编辑人员实行资格认证和岗位责任制			有□	无□
	7. 有无建立链接网站和聊天室等有害信息的检查管理制度			有□	无□
	8. 有无建立电子公告服务、个人主页等栏目的信息审核、登记制度			有□	无□
	9. 有无建立信息监视制度			有□	无□
	10. 有无建立信息的保存、清除和备份制度			有□	无□
	11. 有无建立病毒检测和网络安全漏洞检测制度			有□	无□
	12. 有无建立违法案件报告和协助查处制度			有□	无□
	13. 有无建立账号使用登记和操作权限管理制度			有□	无□
	14. 有无落实安全管理人员岗位工作职责			有□	无□
	15. 有无建立信息审查人员和用户的内部安全教育培训制度			有□	无□
	16. 有无建立值班制度			有□	无□
	17. 是否有个人主页上传信息管理制度			是□	否□
	18. 是否有搜索引擎安全保护管理制度			是□	否□
	19. 有无其他与安全保护相关的管理制度			是□	否□
	20. 有无根据公安机关要求，提供有关安全管理和安全保护的技术资料和信息			有□	无□

续表

安全技术措施	检查上网用户日志记录留存制度情况	21. 系统网络运行日志和用户使用日志记录有无保存 60 日以上	有□　无□
		22. 有无记录 IP 地址分配及使用情况	有□　无□
		23. 有无记录交互式信息发布者、主页维护者、邮箱使用者和拨号用户上网的起止时间和对应 IP 地址、交互式栏目的信息等	有□　无□
	24. 是否具有安全审计或预警功能		是□　否□
	25. 有无采取计算机防黑客入侵和病毒防护功能		有□　无□
	26. 使用何种计算机防病毒软件		
	27. 有无重要数据库和系统主要设备的冗灾备份措施		有□　无□
	28. 有无发送控制和有害信息过滤封堵技术措施		有□　无□
	29. 没有取得新闻登载资格的网站，有无登载时政、社会、文化（不包括娱乐）三类新闻		有□　无□
	30. 网站有无链接境外媒体网站和港澳台网站		有□　无□
	31. 有无建立措施配合公安机关追查有害信息的来源，协助做好取证工作		有□　无□
	32. 有无与公安机关建立二十四小时联络员工作关系		有□　无□
	33. 在紧急的情况下（包括非上班时间和节假日），联络员是否可以按公安机关的要求及时查询资料（如 IP 等）？是否可以按公安机关的要求和指令删除有害信息		是□　否□
	34. 有无其他保护信息和系统网络安全的技术措施		有□　无□
邮件服务器安全技术保护措施	35. 是否具有邮件服务身份登记和识别确认功能		是□　否□
	36. 有无将过滤的有害信息进行整理分类，其中，有无将存在反动邮件的原始数据通过存储介质或专门的传输通道 24 小时内报送公安机关网络安全保卫部门		有□　无□
	37. 有无措施限制本地电子邮件用户一次性发送 25 封以上电子邮件		有□　无□
	38. 是否具有本地邮件服务器发送电子邮件账号核实功能，停止匿名转信服务		是□　否□
	39. 有无对邮件信头、内容和附件采取基于地址和特征字符串的过滤措施		有□　无□
	40. 缺省安装电子邮件服务软件的单位是否已关闭有关端口		是□　否□
	41. 是否安装公安机关推荐使用的反垃圾电子邮件系统		是□　否□
	42. 有无与公安机关签订有关网络与信息安全责任书，落实“谁主管，谁负责”的安全责任制度		有□　无□
安全领导小组和安全员名单及联系电话			

检查民警：　　联系电话：

被检查单位负责人：　　安全员或技术员：

3.2.4 联网单位管理

1. 管理依据

《计算机信息网络国际联网安全保护管理办法》相关规定如下：

第三条　公安部计算机管理监察机构负责计算机信息网络国际联网的安全保护管理工作。

公安机关计算机管理监察机构应当保护计算机信息网络国际联网的公共安全，维护从事国际联网业务的单位和个人的合法权益和公众利益。

第十条　互联单位、接入单位及使用计算机信息网络国际联网的法人和其他组织应当履行下列安全保护职责：

① 负责本网络的安全保护管理工作，建立健全安全保护管理制度；

② 落实安全保护技术措施，保障本网络的运行安全和信息安全；

③ 负责对本网络用户的安全教育和培训；

④ 对委托发布信息的单位和个人进行登记，并对所提供的信息内容按照本办法第五条进行审核；

⑤ 建立计算机信息网络电子公告系统的用户登记和信息管理制度；

⑥ 发现有本办法第四条、第五条、第六条、第七条所列情形之一的，应当保留有关原始记录，并在二十四小时内向当地公安机关报告；

⑦ 按照国家有关规定，删除本网络中含有本办法第五条内容的地址、目录或者关闭服务器。

第十二条　互联单位、接入单位、使用计算机信息网络国际联网的法人和其他组织（包括跨省、自治区、直辖市联网的单位和所属的分支机构），应当自网络正式联通之日起三十日内，到所在地的省、自治区、直辖市人民政府公安机关指定的受理机关办理备案手续。

前款所列单位应当负责将接入本网络的接入单位和用户情况报当地公安机关备案，并及时报告本网络中接入单位和用户的变更情况。

第十五条　省、自治区、直辖市公安厅（局），地（市）、县（市）公安局，应当有相应机构负责国际联网的安全保护管理工作。

第十七条　公安机关计算机管理监察机构应当督促互联单位、接入单位及有关用户建立健全安全保护管理制度。监督、检查网络安全保护管理以及技术措施的落实情况。

公安机关计算机管理监察机构在组织安全检查时，有关单位应当派人参加。公安机关计算机管理监察机构对安全检查发现的问题，应当提出改进意见，作出详细记录，存档备查。

2. 管理对象

互联网联网单位管理对象是通过接入网络与互联网连接的计算机信息网络用户，包括单位用户及个人用户。

社区、学校、图书馆、宾馆、咖啡馆、娱乐休闲中心等向特定对象提供上网服务的场所也纳入互联网联网单位管理中。

3. 管理和服务内容

(1) 督促联网单位建立信息网络安全组织机构。

(2) 督促、指导联网单位依法履行备案义务。

(3) 督促、指导联网单位建立安全管理制度。

(4) 督促、指导联网单位完善安全保护技术措施。

(5) 督促、指导联网单位定期向公安机关提交有关安全保护的信息、资料及数据文件，协助公安机关查处通过国际联网的计算机信息网络的违法犯罪行为。

4. 工作方法和要求

1) 全面掌握联网单位基本情况

掌握联网单位基本情况的方法包括：及时收集本行政区划内互联网运营单位(ISP、IDC)报送的联网单位情况；通过备案及时掌握联网单位的情况；通过日常管理和监控工作发现联网单位的情况。

应掌握的基本情况包括：本行政区划内联网单位的底数、服务内容、用户规模以及单位的相关情况。掌握联网单位的备案率应达到 90%。

2) 加强安全检查和指导

要求各联网单位落实安全保护管理制度和安全保护技术措施，重点检查重要网络系统的系统备份、安全审计日志记录留存以及突发性事件的应急处置措施的落实情况。具有保存 60 天以上系统运行日志和内部用户使用日志记录功能。上网日志应包括上网时间、下网时间、用户名、网卡 MAC 地址、内部 IP 地址、内部 IP 与外部 IP 地址的对应关系、访问的目标 IP 地址等信息。落实安全技术保护措施的联网单位必须达到 95%。

3) 分层次、分类型指导联网单位落实安全保护管理制度

(1) 分层次管理。

① 普通联网单位。对于用户规模在 100 个以下的联网单位，纳入普通联网单位管理，指导落实安全保护管理制度。一是依法通过正规途径接入互联网，不得私自接入，并依法履行备案义务；二是安全审计产品必须使用相应带宽的硬件产品，防止低带宽产品审计高带宽出口造成丢包。

② 大型联网单位。对于用户规模在 100～500 个之间的联网单位，纳入大型联网单位重点管理。在普通联网单位管理的基础上，还要求单位服务器必须采用专用机房统一管理。

③ 特大型联网单位。对于用户规模达到 500 个以上的联网单位，纳入特大型联网单位重点管理。在大型联网单位管理的基础上，还要求把特大型联网单位纳入互联网运营单位管理对象中，采用互联网运营单位管理模式进行管理。

(2) 分类型管理。

① 党政机关联网单位。指导建立安全保护管理制度，重点落实重要信息系统的系统备份及应急预案制度、操作权限管理制度和用户登记制度；系统重要部分的冗余或备份措施、计算机病毒防治措施以及网络攻击防范、追踪措施；对使用公网动态 IP 地址上网的用户，

上网日志应包括上网时间、下网时间、用户名、主叫电话号码、分配给用户的IP地址等信息。

② 宾馆旅业。指导建立安全保护管理制度，重点落实操作权限管理制度；用户登记制度、异常情况及违法犯罪案件报告和协查制度；系统运行和用户使用日志记录措施，其中对使用内部IP地址，通过网络地址转换技术(NAT、PAT)上网的用户，上网日志应包括上网时间、下网时间、用户名、网卡MAC地址、内部IP地址、内部IP与外部IP地址的对应关系、访问的目标IP地址等信息。

③ 非经营性公共上网服务场所。指导建立安全保护管理制度，重点落实操作权限管理制度、用户登记制度和备案制度，以及系统运行和用户使用日志记录保存60日以上措施、身份登记和识别确认措施。

④ 重点联网用户。指导建立安全保护管理制度，严格上网管理，禁止一机两用。

5. 行政处罚

(1) 根据《计算机信息网络国际联网安全保护管理办法》第二十条规定，利用国际联网制作、复制、查阅和传播有害信息或者从事危害计算机信息网络安全活动的，由公安机关给予警告，有违法所得的，没收违法所得，对个人可以并处五千元以下的罚款，对单位可以并处一万五千元以下的罚款；情节严重的，并可以给予六个月以内停止联网、停机整顿的处罚，必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格；构成违反治安管理行为的，依照治安管理处罚条例的规定处罚；构成犯罪的，依法追究刑事责任。

(2) 根据《计算机信息网络国际联网安全保护管理办法》第二十一条规定，有下列行为之一的，由公安机关责令限期改正，给予警告，有违法所得的，没收违法所得；在规定的限期内未改正的，对单位的主管负责人员和其他直接责任人员可以并处五千元以下的罚款，对单位可以并处一万五千元以下的罚款；情节严重的，并可以给予六个月以内的停止联网、停机整顿的处罚，必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格。

① 未建立安全保护管理制度的；

② 未采取安全技术保护措施的；

③ 未对网络用户进行安全教育和培训的；

④ 未提供安全保护管理所需信息、资料及数据文件，或者所提供内容不真实的；

⑤ 对委托其发布的信息内容未进行审核或者对委托单位和个人未进行登记的；

⑥ 未建立电子公告系统的用户登记和信息管理制度的；

⑦ 未按照国家有关规定，删除网络地址、目录或者关闭服务器的；

⑧ 未建立公用账号使用登记制度的；

⑨ 转借、转让用户账号的。

(3) 根据《计算机信息网络国际联网安全保护管理办法》第二十三条规定，不履行备案职责的，由公安机关给予警告或者停机整顿不超过六个月的处罚。

6. 工作流程

1) 日常管理工作流程

互联网联网单位日常管理工作流程如图3-6所示。

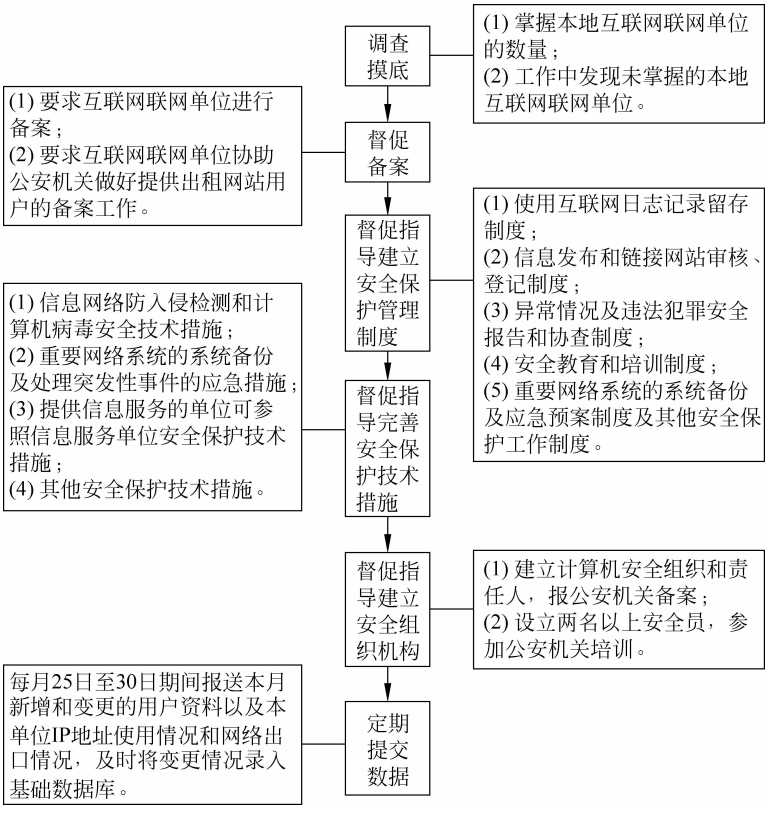

图 3-6　互联网联网单位日常管理工作流程

2）日常检查工作流程

互联网联网单位日常检查工作流程参见图 3-4 所示的互联网运营单位日常检查工作流程。

7. 相关表格

××市联网单位安全检查表

检查单位：××市公安局公共信息网络安全保卫支队　　时间：　年　月　日

被检查单位名称						
单位地址						
法人代表		联系电话				E-mail
安全负责人		联系电话				E-mail
单位基本情况	行业性质			服务性质		
	接入服务商		接入方式		介质类型	
	IP 地址					
	单位规模			可联网信息点数		
	历史整改数			完成情况		

续表

安全员信息	安全员姓名		联系电话		安全员证书号码	
	安全员姓名		联系电话		安全员证书号码	
安全产品信息	产品名称		产品类型			
	产品型号		应用范围			
	计算机信息系统安全专用产品检测合格证号					
	计算机信息系统安全专用产品销售许可证号					
	安装时间		安装单位			
落实安全保护管理制度情况	有无建立网络安全领导小组、确立小组负责人					有□ 无□
	有无落实组长、小组人员岗位工作职责					有□ 无□
	有无建立计算机机房安全管理制度					有□ 无□
	有无建立用户登记制度和操作权限管理制度					有□ 无□
	有无建立网络安全漏洞检测和系统升级管理制度					有□ 无□
	有无建立电子公告系统用户登记制度					有□ 无□
	有无建立交互栏目 24 小时巡查制度					有□ 无□
	有无建立信息发布审核、登记、保存、清除和备份制度，信息群发服务管理制度					有□ 无□
	有无制定网络安全事故处置措施					有□ 无□
	有无配备 2～4 名计算机安全员，须持证上岗					有□ 无□
	有无建立安全教育培训制度					有□ 无□
	有无落实备案制度					有□ 无□
	有无建立违法案件报告和协助查处制度					有□ 无□
落实安全保护技术措施情况	有无建立包括 IP 地址分配及使用情况，交互式信息发布者、主页维护者、邮箱使用者和拨号用户上网的起止时间和对应 IP 地址，交互式栏目信息等内容的系统网络运行日志和用户使用日志记录功能。					有□ 无□
	有无建立安全审计及预警措施					有□ 无□
	有无建立网络攻击防范、追踪措施					有□ 无□
	有无建立计算机病毒防治措施					有□ 无□
	有无建立身份登记和识别确认措施					有□ 无□
	有无系统运行和用户使用日志记录					有□ 无□
	系统网络运行日志和用户使用日志记录有无保存 60 日以上					有□ 无□
	有无记录发生案件、事故和发现计算机有害数据的情况					有□ 无□
安全保护技术措施检测情况	产品运行情况					
	有无日志记录信息					有□ 无□
	日志记录是否完整					是□ 否□
	日志格式是否规范					是□ 否□
检查意见						

检查民警：　　被检查单位负责人：

3.3　计算机病毒等破坏性程序防治管理

1994 年 2 月 18 日《中华人民共和国计算机信息系统安全保护条例》第二十八条给计算机病毒所下的定义是："计算机病毒，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。"

计算机病毒具有隐蔽性强、潜伏期长、传播范围大、危害结果严重等特点，是计算机安全的头号杀手。其实，计算机病毒只是破坏性程序的一种主要表现形式，破坏性程序还包括"设备炸弹"、"逻辑炸弹"、"野兔"、"特洛伊木马"、"蠕虫"等其他多种形式。

计算机病毒传播的途径主要集中在通过网页下载，其次是电子邮件，再次是局域网，而通过光盘或者磁盘感染的比例最低。目前，计算机病毒越来越多是以窃取银行账号、信息卡密码、游戏账号、邮箱账号、机密文件等偷窃个人或企事业核心信息为主要目的。

3.3.1　管理依据

1.《中华人民共和国计算机信息系统安全保护条例》(国务院令 147 号，1994 年 2 月 18 日)

第十五条　对计算机病毒和危害社会公共安全的其他有害数据的防治研究工作，由公安部归口管理。

2.《计算机病毒防治管理办法》(公安部第 51 号令，2000 年 4 月 26 日)

第四条　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。

3.3.2　管理对象

(1) 制作、传播计算机病毒的行为。

(2) 发布虚假的计算机病毒疫情的行为。

(3) 从事计算机病毒防治产品生产的单位。

(4) 从事计算机设备或者媒体生产、销售、出租、维修行业的单位和个人。

《计算机病毒防治管理办法》中第二十一条规定了关于计算机病毒疫情的定义，是指某种计算机病毒爆发、流行的时间、范围、破坏特点、破坏后果等情况的报告或者预报。

3.3.3　管理职责

(1) 监督、检查、指导信息系统运营、使用单位建立、落实下列计算机病毒等破坏性程序防治管理制度和安全保护技术措施：

① 制定计算机病毒防治管理制度和技术规程。

② 采取计算机病毒安全技术防治措施。

③ 对计算机信息系统应用和使用人员进行计算机病毒防治教育和培训。

④ 建设计算机病毒防治系统，通过控制信息的出入口，防止病毒入侵，并对已经入侵的病毒及时进行检测和清除，并做好检测、清除的记录。

⑤ 购置和使用具有计算机信息系统安全专用产品销售许可证的计算机病毒防治产品。

⑥ 对因计算机病毒引起的计算机信息系统瘫痪、程序和数据严重破坏等重大事故及时向公安机关报告，并保护现场。

⑦ 向公安机关报告发现的计算机病毒，并协助公安机关追查计算机病毒的来源。

(2) 督促从事计算机设备或者媒体生产、销售、出租、维修行业的单位及个人做好计算机设备或者媒体的病毒检测、清除工作。

(3) 开展本地计算机病毒疫情调查，并举办各种计算机病毒等破坏性程序防范的宣传活动。

(4) 只有取得从事计算机病毒防治产品生产资格的单位才能允许存储计算机病毒，并且要到公安机关网络安全保卫部门进行审批、备案；

(5) 督促计算机病毒防治产品研制、生产、销售单位，安全服务机构和用户对发现的计算机病毒提取样本，报送公安机关网络安全保卫部门。

(6) 建设大型的网络安全监控系统。在骨干网、支网、用户网等不同层次上建设网络安全监控系统，实时检测网络病毒传播情况，及时发现新病毒预警，及时发现病毒源。

(7) 将接收的计算机病毒样本上报上级公安机关网络安全保卫部门。

(8) 指导、组织社会技术支撑力量对发现的计算机病毒及时进行处置，对用户级的计算机病毒控制与处置工作提供技术支持。包括提取计算机病毒样本，交付指定计算机病毒防治机构进行解剖、分析后，形成计算机病毒疫情分析报告和解决方案。

(9) 加强对计算机病毒防治产品的监管。任何单位和个人销售、附赠的计算机病毒防治产品，应当具有计算机信息系统安全专用产品销售许可证，并贴有“销售许可”标记。

(10) 利用行政管理手段，严格控制病毒传播源，严厉处罚各类病毒传播行为和传播人。

3.3.4 工作要求

(1) 全面掌握病毒信息，建立病毒预警机制。一是及时收集本行政区划计算机病毒研究机构和各种社会技术支撑力量报送的情况，及时掌握计算机病毒信息；二是通过备案及时掌握相关服务单位的情况；三是通过日常管理和监控工作发现计算机病毒信息；四是通过上级有关部门和各地网络安全保卫部门的通报，掌握计算机病毒信息；五是通过技术措施发现计算机病毒信息。

(2) 建立病毒快速反应机制。通过各种渠道及时发现新爆发的严重计算机病毒疫情，积极组织计算机病毒防治机构进行解剖、分析，出具计算机病毒疫情分析报告和解决方案；同时，通过新闻媒体发布计算机病毒疫情信息，通知社会各界做好防治工作。

(3) 加强计算机病毒防治知识宣传、教育和培训。一是每半年举行一次计算机病毒等破坏性程序防范的宣传活动；二是在本地政府网站上设立计算机病毒防治专栏；三是对信息系统运营、使用单位的安全员定期组织计算机病毒防治技术培训；四是开设计算机病毒报警电话，接受群众报警和咨询。

(4) 全面掌握计算机病毒防治产品研发机构的情况。重点掌握研发机构基本情况、服务内容和生产产品情况，督促研发机构就其本身及所生产销售的产品依法履行备案义务，指导其将计算机病毒防治产品送公安机关进行检测。

3.3.5　行政处罚

1.《刑法》规定

第二百八十六条　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。

2.《中华人民共和国治安管理处罚法》规定

第二十九条　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。

3.《中华人民共和国计算机信息系统安全保护条例》规定

第二十三条　故意输入计算机病毒以及其他有害数据危害计算机信息系统安全的，或者未经许可出售计算机信息系统安全专用产品的，由公安机关处以警告或者对个人处以五千元以下的罚款、对单位处以一万五千元以下的罚款；有违法所得的，除予以没收外，可以处以违法所得 1 至 3 倍的罚款。

4.《计算机信息网络国际联网安全保护管理办法》规定

第六条　任何单位和个人不得从事下列危害计算机信息网络安全的活动：

(1) 未经允许，进入计算机信息网络或者使用计算机信息网络资源的；

(2) 未经允许，对计算机信息网络功能进行删除、修改或者增加的；

(3) 未经允许，对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、

修改或者增加的；

（4）故意制作、传播计算机病毒等破坏性程序的；

（5）其他危害计算机信息网络安全的。

第二十条　违反法律、行政法规，有本办法第五条、第六条所列行为之一的，由公安机关给予警告，有违法所得的，没收违法所得，对个人可以并处五千元以下的罚款，对单位可以并处一万五千元以下的罚款；情节严重的，并可以给予六个月以内停止联网、停机整顿的处罚，必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格；构成违反治安管理行为的，依照治安管理处罚条例的规定处罚；构成犯罪的，依法追究刑事责任。

5.《计算机病毒防治管理办法》规定

（1）在非经营活动中有违反下列行为之一的，由公安机关处以一千元以下罚款；在经营活动中有违反下列行为之一，没有违法所得的，由公安机关对单位处以一万元以下罚款，对个人处以五千元以下罚款；有违法所得的，处以违法所得三倍以下罚款，但是最高不得超过三万元。

① 任何单位和个人不得制作计算机病毒；

② 向他人提供含有计算机病毒的文件、软件、媒体；

③ 销售、出租、附赠含有计算机病毒的媒体；

④ 其他传播计算机病毒的行为。

（2）违反下列行为之一的，由公安机关对单位处以一千元以下罚款，对单位直接负责的主管人员和直接责任人员处以五百元以下罚款；对个人处以五百元以下罚款。

① 任何单位和个人不得向社会发布虚假的计算机病毒疫情；

② 从事计算机病毒防治产品生产的单位，应当及时向公安部公共信息网络安全监察部门批准的计算机病毒防治产品检测机构提交病毒样本。

（3）计算机病毒防治产品检测机构应当对提交的病毒样本及时进行分析、确认，并将确认结果上报公安部公共信息网络安全监察部门。违反此规定的，由公安机关处以警告，并责令其限期改正；逾期不改正的，取消其计算机病毒防治产品检测机构的检测资格。

（4）计算机信息系统的使用单位有下列行为之一的，由公安机关处以警告，并根据情况责令其限期改正；逾期不改正的，对单位处以一千元以下罚款，对单位直接负责的主管人员和直接责任人员处以五百元以下罚款：

① 未建立本单位计算机病毒防治管理制度的；

② 未采取计算机病毒安全技术防治措施的；

③ 未对本单位计算机信息系统使用人员进行计算机病毒防治教育和培训的；

④ 未及时检测、清除计算机信息系统中的计算机病毒，对计算机信息系统造成危害的；

⑤ 未使用具有计算机信息系统安全专用产品销售许可证的计算机病毒防治产品，对计算机信息系统造成危害的。

（5）从事计算机设备或者媒体生产、销售、出租、维修行业的单位和个人，应当对计算机

设备或者媒体进行计算机病毒检测、清除工作，并备有检测、清除的记录。违反此规定的，没有违法所得的，由公安机关对单位处以一万元以下罚款，对个人处以五千元以下罚款；有违法所得的，处以违法所得三倍以下罚款，但是最高不得超过三万元。

3.4　计算机安全员培训及管理

1999 年 4 月，公安部、人事部发出《关于开展计算机安全员培训工作的通知》，对培训对象、培训内容、培训方式步骤、培训考试、培训工作的组织和管理都做了明确规定；2006 年 5 月，公安部办公厅、人事部办公厅联合发布《关于开展信息网络安全专业技术人员继续教育工作的通知》，将信息网络安全专业技术人员继续教育工作作为一项长期工作，纳入公安机关信息网络安全监督管理工作之中，逐步建立一支与公安机关密切配合、维护信息网络安全的社会力量。

3.4.1　培训目的

培训计算机安全员的目的，在于提高相关知识水平，从而提高各单位自身的网络安全防范能力，防范和制止计算机犯罪、安全事故的发生。同时通过培训和日常的沟通联络，组建一支以计算机安全员为主的社会辅助力量，协助公安机关网络安全保卫部门开展网上重大突发事件的应急处置工作以及信息网络安全的群防群治工作。

3.4.2　培训对象

计算机安全员培训对象包括：

(1) 负责计算机安全监察工作的各级公安机关民警和保卫部门的保卫干部。

(2) 计算机信息系统使用单位安全管理责任人、信息审查员。

(3) 重点安全保护单位计算机信息系统维护和管理人员。

(4) 计算机信息网络国际联网的互联单位和接入单位的有关人员。

(5) 安全服务机构专业技术人员、安全服务管理人员。

(6) 互联网上网服务营业场所的安全管理人员、经营管理人员、专业技术人员。

(7) 从事计算机安全工程和安全产品开发、生产单位的技术人员。

3.4.3　培训内容

计算机安全员培训内容有：

(1) 计算机网络安全：网络的基本安全对策，常见的网络信息安全问题，网络安全隐患，信息系统安全风险管理的方法，计算机信息系统安全事故的查处和管理，计算机犯罪的防范、打击和案件报告制度等其他计算机安全保护的相关内容。

(2) 计算机病毒及防治：常见的计算机病毒及黑客程序的检测、清除和防范。

(3) 计算机安全专用产品销售许可管理制度。

(4) 计算机信息系统安全保护法律、法规。

3.4.4 培训方式及要求

计算机安全员培训原则上采取脱产培训方式,培训时间不少于 40 学时,使用全国统编教材和统编大纲。

培训机构需经过省级以上公安机关考核、审查和资格认证,培训教员要持证上岗。同时,培训机构要具备社会办学许可证照,具有较强网络安全师资力量,要到所在地地级以上(含地级)公安机关网络安全保卫部门备案。

学员培训后参加由公安、人事部门联合组织的统一考试。考试合格者,由公安、人事部门认定其计算机安全员培训合格,并在合格证明材料上加盖省、自治区、直辖市计算机安全员培训考试专用章。党政机关、金融财税系统、国家重要经济部门等重要领域的计算机安全管理人员、工程技术人员和重要岗位上的计算机技术人员、操作人员必须持证上岗。凡未取得考试合格证者,不得从事相关工作。

3.4.5 计算机安全员的管理

培训机构对取得计算机安全员合格证书的培训人员的相关资料建档管理,并定期报送公安机关网络安全保卫部门。合格证书有效期满后,应由培训机构对持证人重新进行资格培训。

计算机安全员应履行的职责包括:

(1) 依据国家有关法规政策,从事本单位的信息网络安全保护工作,确保网络安全运行。

(2) 执行本单位计算机信息网络安全管理的各项规章制度。

(3) 在公安机关网络安全保卫部门的监督、指导下进行信息网络安全检查和安全宣传工作。

(4) 向公安机关及时报告发生在本单位网上的有害信息、安全事故和违法犯罪案件,并协助公安机关做好现场保护和技术取证工作,配合公安机关开展案件调查工作。

(5) 发现有关危害信息网络安全的计算机病毒、黑客等方面的情报应及时向公安机关报告。

(6) 应保持与公安机关联系渠道的畅通,保证各项信息网络安全政策、法规在本单位的落实,积极接受公安机关网络安全保卫部门的业务监督检查。

(7) 在发生网络重大突发性事件时,应随时响应,接受公安机关网络安全保卫部门调遣,承担处置任务。

(8) 向本单位的负责人提出改进计算机信息网络安全工作的意见和建议。

(9) 与信息网络安全保护有关的其他工作。

各单位网络安全组织的安全责任人及安全技术人员应切实履行各项安全职责,对不依法履行职责,造成安全事故和重大损害的,由公安机关予以警告,并建议其所在单位给予纪律或经济处理,情节严重的,依法追究其刑事责任。

习　　题

1. 如何正确理解信息网络安全监督管理的指导思想？
2. 信息网络安全监督管理工作的主要任务是什么？
3. 公安机关网络安全保卫部门的备案对象包括哪些？
4. 互联网单位包括哪些？它们都有哪些具体的管理内容？
5. 违反计算机病毒等破坏性程序防治管理的行政处罚有哪些？
6. 计算机安全员培训的内容是什么？