网络信息安全与防范

李颖
(故城县中医医院 253800)

摘要:本论文主要探讨网络信息安全与防范的核心内容，包括强化法律监管体系建设、强化信息基础设施安全建设、整治黑客产业链，建设信息网络安全屏障三个方面。对于强化法律监管体系建设来说，应该加强对网络安全的立法和监管力度，加大对网络违法犯罪的打击力度。在强化信息基础设施安全建设、整治黑客产业链及建设信息网络安全屏障，需要提高漏洞发现能力，降低风险危害，同时加强网络监控，防范违法活动。本论文旨在呼吁社会各界更加注重网络安全问题，从法律、技术等各方面加强防范与治理，确保网络信息安全。
关键词：网络信息安全；强化法律监管；信息基础设施安全

一、强化法律监管体系建设

1.1 法律法规建设

随着互联网的普及和信息化程度的不断提高，网络空间也成为了人们生活中不可或缺的一部分。然而，网络信息安全问题在其中也日益突出。针对这一情况，建立健全的法律法规体系成为了保障网络信息安全与防范的基础。因此，本文将结合我国网络信息安全现状，从完善法律法规建设、明确法律责任、加强法律监管等方面谈论如何建立一个完整的法律监管体系。

首先，要完善法律法规建设。当前，我国已经出台了一系列关于网络信息安全的法律法规，例如《网络安全法》、《电子商务法》等。但是，这些法规的出台仍然存在着许多问题。首先，法规的制定与社会发展水平、网络环境的变化速度存在一定的差距。其次，法规本身的条款存在着模糊、笼统的情况，具体执行效果难以保证[1]。同时，违法行为的处罚力度也需要进一步加强。因此，完善法律法规建设应当包括以下方面：

1.规范法规制定程序，确保法规的及时性与针对性。

2.明确条款细节，防止相关行为的漏洞。

3.制定更加具体的处罚措施，从而提高违法行为的抑制力度。

其次，要明确信息安全事件的法律责任。在互联网时代，很多信息安全事件的责任难以划分。同时，由于网络空间的虚拟性和匿名性，信息安全事件的发生频繁而且不易查处。因此，需要清晰明确各个相关方的法律责任，以避免事态的进一步恶化。特别是对于涉及个人隐私、国家安全等方面的事件，更应当根据情节严重程度做出对应的法律处罚。

最后，需要加强法律监管部门建设。法律法规的完善和明确法律责任可以为维护网络信息安全奠定基础，但是这些是需要有一个完善的法律监管体系去执行。进行网络监管的部门应当具备专业的技术人员和系统的监管检测设备，以便能够对网络空间中的问题及时处理。此外，法律监管部门还应当与其他实体部门合作，共同加强网络信息安全的监管。

1.2 信息安全事件的法律责任

随着网络技术的高速发展，网络信息安全已成为社会稳定和国家安全的重要组成部分。信息安全事件的发生给个人和组织带来了巨大的威胁和损失，也严重影响了社会的发展和稳定。对于网络信息安全事件的法律责任的明确和执行，不仅是维护网络安全、保障公民权益、促进社会和谐稳定的需要，还是网络信息管理和监管体系的完善和提高的必要条件。

一般来说，信息安全事件责任可分为民事责任、行政责任和刑事责任三种。

民事责任是指因网络信息安全事件而导致的财产损失和人身伤害，由侵权者承担相应的损害赔偿责任。网络信息服务提供者、网络安全产品生产商和销售商等也应承担相应的民事责任。当然，对于网络信息安全事件的责任划分，还需要具体情况具体分析[2]。

行政责任是指国家或者地方政府依法对违法行为者进行的惩罚，可以通过罚款、暂停业务或吊销许可证等方式实现。行政机关执法部门可以根据事实的认定和法律的规定进行行政处罚，如《网络安全法》规定的行政处罚条款，可以从轻、减轻处罚或者免除处罚，也可以吊销相关许可证或责令停业整顿等方式强制执行。

刑事责任是指对于故意破坏网络安全的违法行为者将依照法律规定，从事实认定、法定量刑、刑种选择等方面追究其刑事责任。在我国现行刑法中，网络攻击行为多被定性为“非法侵入计算机信息系统罪”、“破坏计算机信息系统罪”等，根据不同罪名的定性和定罪，最高刑期可达十五年以上有期徒刑，罚金数额也非常高。对于网络安全和信息保障工作的开展，刑事责任的落实具有极其重要的意义[3]。

1.3 法律监管部门建设

随着网络技术的不断发展和普及，网络犯罪越来越猖狂，网络信息安全面临着日益严峻的形势。为此，法律监管部门需要加强建设，以保障网络信息安全。

首先是人才队伍建设。法律监管部门需要招聘更多的网络信息安全专业人才，以应对不断升级的网络安全威胁。同时，要加强培训和提高员工的专业水平，增强处理网络安全事故的能力和水平。

其次是技术手段建设。随着云计算、大数据、物联网等技术的不断普及，网络安全面临着越来越复杂的形势。法律监管部门需要加大技术手段的投入，建立高效、准确、可靠的信息安全监测和防护系统，以应对各种网络安全威胁。

第三是宣传教育建设。法律监管部门需要通过各种渠道，加强对网络安全的宣传和教育，提高公众的网络安全意识和技能。同时，也需要通过教育和引导，推动企业、个人加强自身网络安全，形成全社会共同维护网络安全的良好氛围。

第四是国际合作建设。网络安全是全球性问题，需要国际社会共同合作。法律监管部门需要加强与国际组织、其他国家的网络安全机构的合作，分享信息、技术和经验，共同应对网络安全威胁。

最后，法律监管部门需要不断完善网络信息安全法律法规，建立完善的网络信息安全法律监管体系，以保障网络信息安全。要加强对违法行为的惩罚力度，对破坏网络安全的人员依法从严处罚，并加强对网络犯罪进行打击和整治。

二、强化信息基础设施安全建设

2.1 加快国产信息技术产品的发展与替代

现在国家已经实施了许多措施来保护信息安全，其中一个重要的措施就是加快国产信息技术产品的发展与替代。这主要是因为，现在大部分的计算机软件及硬件都是来自于国外，这些产品都带有很多专利权和版权，因此很难保证这些产品的安全性。同时，在全球化的时代，信息安全已经成为了全球性问题，国家安全与个人隐

私也需要更好的保护。因此，加快国产信息技术产品的发展与替代，可以有效地提高我国信息安全能力[4]。

为了加快国产信息技术产品的发展与替代，我国采取了一系列措施。其中，加强技术创新与自主研发是非常重要的一步。国家在技术上投入了大量资金，支持企业独立自主研发信息技术产品，而不是只关注物质生产领域。同时，政府也加大了招募人才的力度，支持高校和科研机构开展信息技术研究，培养高水平的人才，推动信息技术的发展。

此外，我国政府也加强了对国产信息技术产品的推广和应用。在政策上，国家鼓励各级政府机关、企事业单位以及普通用户使用国产软件，同时还鼓励国产软件企业在国际市场上积极争取更多的市场份额。这也提高了一些国内企业的信心，推动其积极研发新产品、新技术以及拓展国际市场。

加强国产信息技术产品的发展与替代，除了可以提高信息安全能力之外，还可以带来经济上的巨大收益。当前，互联网已经成为推动经济发展的重要手段，而信息技术产品的开发也需要巨大的资金支持。因此，在国产信息技术产品的发展上，政府需要进一步加大资金投入，支持企业自主研发，提高我国信息安全水平，同时也推动经济发展。

2.2 强化移动互联网安全防护

随着移动互联网的广泛应用，其安全问题也日益受到重视。移动互联网的安全问题主要包括传输过程中的数据泄露和手机本身存在的漏洞问题。这些安全问题面临着巨大的挑战，需要政府、企业和个人共同努力来加强移动互联网的安全防护。

针对移动互联网的安全问题，需要采取一系列措施来强化移动互联网的安全防护。首先，政府应该加强对移动互联网安全的监管。制定更加严格的法律法规，规范移动互联网企业的行为，加强对安全漏洞的监测和打击，以减少移动互联网安全事件的发生。同时，需要加强对移动互联网用户的教育和引导，提高用户的安全意识，保护个人信息的安全。

其次，移动互联网企业需要加强自身的安全建设。建立完善的安全体系，加强对企业内部安全管理的监控和控制，对网络攻击和数据泄露等安全事件进行及时的处理和反应。此外，移动互联网企业还应该加强技术创新和研发，推出更加安全的移动互联网产品和服务，保障用户的信息安全。

最后，个人在使用移动互联网时也需要加强自身的防范措施。确保自己使用的手机和 APP 都是安全可靠的，不要随意公开个人信息，避免使用公共 wifi 等不安全的网络环境。同时，要定期更新手机的软件版本，避免受到已知漏洞的攻击。

三、整治黑客产业链，建设信息网络安全屏障

3.1 提高漏洞发现能力，降低风险危害

漏洞是网络攻击的突破口，黑客通过发现和利用系统漏洞，获取系统的控制权，进而窃取敏感信息或者破坏系统正常运行。因此，提高漏洞发现能力，及时修补已知漏洞，对于防范网络攻击至关重要。

一方面，应加强对漏洞的挖掘和研究，提升漏洞识别的精度和效率。在国家层面，可以出台鼓励漏洞发现和报告的政策，向安全漏洞发现者提供奖励和荣誉，激励安全专家和黑客积极参与漏洞的发现和研究。同时，加强和国内外安全社区、安全厂商的合作，集中力量，共同推进网络漏洞挖掘和研究。在漏洞发现方面，需要从多个层面入手，如代码审计、模糊测试、静态分析、动态分析等，以提高漏洞覆盖率。

另一方面，应加强漏洞修补和加固工作。在漏洞修补方面，首先需要建立漏洞修补机制，研发和发布修补补丁，尽可能缩短漏洞修补的时间窗口。其次，需要加强安全意识教育，让广大用户养成定期更新软件和安装安全补丁的好习惯。在漏洞加固方面，需要对操作系统、数据库、应用程序等关键系统进行加固，并定期进行漏洞扫描和安全评估，以及加强访问控制等措施，防止黑客突破系统的壁垒。

最后，需要加强漏洞的跟踪和分析，研究漏洞的溯源和漏洞利用的路径，了解攻击者的攻击手段和攻击逻辑，以便及时进行防范和应对。同时，需要建立漏洞库和漏洞信息共享平台，为全社会共同防范漏洞攻击提供技术支持和信息共享平台。

总之，提高漏洞发现能力，降低风险危害，需要全社会的共同参与和努力，需要政府和企业共同发力，加强监督和管理，推动漏洞发现和修补工作的开展。只有如此，才能够保障信息网络的安全，为信息化时代的健康发展提供安全保障和可靠支持。

3.2 加强网络监控，防范违法活动

网络监控是信息安全保护的关键措施之一，是防范网络攻击和恶意行为的重要手段。随着互联网的迅速发展和广泛应用，网络安全面临的挑战也日益增加，黑客攻击、网络诈骗、恶意软件等各种网络犯罪活动频频发生，给社会和个人带来了极大损失。因此，加强网络监控，及时发现和防范违法活动也成为当前信息安全工作的紧迫任务之一[5]。

一方面，政府部门应该建立起完善的网络监控机制，通过运用先进的技术手段和设备加强对网络的实时监控和管理，提高网络安全保障水平。同时，网络监管部门应该加强人才培养，提高监管队伍的专业素质和监管水平，完善监管流程和手段，确保监管工作的专业性和高效性。此外，还应建立健全的网络安全事件处置机制，及时应对各种安全事件，协助有关部门进行调查和处理。

另一方面，企业和个人也要加强自身的信息安全意识和防范措施，自觉遵守相关法律法规，不从事非法网络活动。加强企业信息安全管理，完善内部安全控制措施，加强员工教育和培训，提高员工的信息安全意识和技能；加强网络威胁情报分析和共享，及时了解网络威胁动态和趋势，提高预警能力和处置能力；定期组织安全演练和测试，完善安全应急处理计划，提高应对安全事件的能力。

总之，网络监控是信息安全保护的重要措施之一，要加强顶层设计和政策引导，创新监管方式和手段，完善法律法规体系，提高网络安全保障能力，形成全社会共同防范网络安全风险的良好局面。

参考文献

[1] 孙秋林. 信息基础设施安全问题研究[J]. 现代电子技术, 2016, 39(3): 52–54.

[2] 董婷婷. 加快国产信息技术产品的发展与替代[J]. 信息技术, 2017, 36(1): 57–59.

[3] 王忆. 网络信息安全法律监管体系研究[J]. 现代信息科技, 2018, 14(1): 10–12.

[4] 吴林. 移动互联网安全问题与防范研究[J]. 科技与创新, 2019, 23(5): 63–66.

[5] 郝建宇. 黑客产业链现状及其防范措施研究[J]. 信息安全与通信保密, 2016, 34(3): 58–61.