人工智能时代计算机信息安全与防护策略分析

孙笑飞　周晓亮
广东亚视演艺职业学院　广东肇庆　526000

摘　要：就目前而言，计算机系统运行过程中仍然存在一些问题和不足，如非法攻击、恶意破坏以及信息泄露等，这些问题的出现影响着计算机系统发展的稳定性。针对此，需要行业相关技术人员对当前的信息安全问题进行调查和分析，意识到信息安全防护的重要性，从而针对暴露出的问题制定出科学具体的解决方案、保障计算机系统运行的稳定性。本文就如何维护计算机信息安全进行探究，旨在推动科学技术的发展。

关键词：人工智能时代；计算机信息安全；防护

随着科学技术的发展，计算机技术被广泛应用到各个行业，推动了行业的发展。但是与此同时，一些不安全因素威胁到了计算机系统的使用安全。如何保证计算机信息的完整性、维护计算机系统的稳定已经成为人工智能时代下计算机行业的重点研究课题。人工智能时代下，各类智能活动的开展均需要计算机技术的参与。因此，保证网络安全和信息安全是时代发展的关键环节。当前我国已经意识到了信息安全的重要性，并且结合实际发展情况制定出了有效的安全管理和防护措施。但是信息安全具有具有多发性和复杂性的特点，增加了信息安全管理难度。因此，需要对现阶段的安全问题及其不良影响进行分析，从而调整安全管理方案、为科学技术的稳定发展奠定基础。

一、人工智能时代计算机信息安全问题和影响

1.网络病毒复杂性和网络攻击多样性

互联网背景下，信息技术高速发展，推动着人工智能时代科学技术的发展。在这一背景下，人工智能与信息安全互相促进、相互影响。人机交互得到了广泛的应用，为了保证计算机信息的安全，行业技术人员对数据管理、安全防护等进行了深入的研究。对于人工智能技术来讲，随着研究的深入，信息安全管理水平有所提高，但是仍然存在安全风险和安全问题，其中最为突出的是网络病毒和网络攻击，这两种问题呈现出复杂性和多样性的特征。网络时代多发的安全问题为黑客攻击，通过对历来黑客攻击方式进行分析，主要入侵路径有三种，以木马病毒的植入为例，这种网络攻击占比最大，最为常见。该攻击主要是通过对带有病毒的页面进行点击，此时木马病毒已经侵入系统中，病毒的侵入影响计算机系统的安全稳定性。此外，还有一些病毒隐匿在垃圾短信中，如果此时点击网址，那么用户的个人信息则会遭到泄露，造成了用户的财产损失。最后则是通过软件的下载，病毒藏在软件中，在人们下载过程中，病毒随着软件的下载进入到计算机设备中，影响计算机的正常运转[1]。

2.网络信息脆弱性

人们在应用信息技术过程中，习惯于将数据信息储存到数据库中。由于数据量较为庞大，为了方便管理，数据库下会设置多个子系统。一般来讲，网络数据库出现信息泄露情况的几率较低。但是在信息利用和转移过程中，网络黑客以及不法分子会对传输系统进行攻击，极易出现信息泄露以及信息缺失的情况。与此同时，在信息传输和利用过程中，数据信息极易被盗取。信息系统管理存在一定局限性，只能对浅层次风险进行提示，对于较为复杂的安全风险无法及时识别[2]。

3.计算机网络安全漏洞的普遍性

现阶段的计算机漏洞主要表现在以下几方面，即软件、硬件以及系统安全等方面，这几种漏洞为不法分子提供了可乘之机，不法分子往往会从这几方面入手，对计算机系统进行入侵和破坏[3]。计算机系统的漏洞不仅会对系统本身造成不良影响，同时还会危及到其他软件和硬件。计算机系统中的硬件和软件种类较为多样，同时软件版本的不同也会增加系统漏洞出现的概率。智能时代下，信息技术被广泛应用于生活的各个领域，人们逐渐提高了对信息系统和安全的重视。同时行业技术人员积极参与到信息安全管理工作中，旨在通过接受专业的技能培训，对信息系统中出现的安全问题进行处理，使其得到妥善解决。但是当前行业技术和工作人员，仍然采用以往的安全管理手段保证数据信息的安全，缺乏技术创新、无法满足现代化信息系统安全管理的要求。这就导致信息安全问题频发，影响计算机系统的稳定运行，同时危害到了个人的信息安全[4]。

二、人工智能时代计算机信息安全与防护策略

1.引进信息技术，把控计算机信息安全

人工智能时代下，通过加强对信息安全的管理可以推动信息技术的发展、减少信息泄露以及信息缺失等情况的出现[5]。因此，为了保证工作质量，需要引进专业化技术手段，对信息安全进行全面把控和防护，只有这样才可以保证网络系统的健康稳定运行，减少信息安全事故的发生频次。从国家层面来讲，需要我国各级政府意识到信息安全管理工作的重要性，发挥政府部门的指导作用对信息安全管理提供有力支持，通过专项资金的设立，为信息安全技术研发提供资金，对市面上的信息技术设备进行考察和分析，从而引进有效的信息技术和手段、提高信息安全管理有效性；其次，需要对当前的数据加密技术进行创新和改革，在此基础上引进新技术对数据记性保护，确保数据传输过程的安全性、避免信息系统在数据传输过程中被攻击；第三可以利用数字签名技术对文件进行加密处理，双重加密可以减少信息被篡改的几率。数字签名技术主要对计算机信息的不对称性加以利用，从而保证信息的安全性。该技术在应用过程中，用户为了保证信息的安全性，往往会将重要文件和重要信息存储到特定的账号下，设立专门的密码。通过实验，将密码设置为数字+字母+符号的形式，被破解的几率最小。另外，需要定期对密码进行设置，从而是文件能够安全储存。第四，需要技术人员对当前的智能算法进行学习，从而应用到已有的信息系统中，从而提高信息安全性。在具体工作中，可以积极利用人工智能识别技术对计算机系统运行中的潜在风险进行识别，对其危险级别进行评估，从而对其违法行为进行检测，通过系统对危险行为的检测和整理自动提交到网络安全监管部门，提高安全监管部门的工作效率和质量。最后，需要搭建信息监控平台，对于系统内的一切操作进行监测和评估。依据收集到的信息出示系统严谨的监测报告，从而保证信息安全的稳定性[6]。

2.构建安全感知系统，加强对信息系统的保护

人工智能系统在计算机信息安全领域的主要作用是对用户的指令进行识别，对系统内的数据信息进行收集和管理，在此基础上利用具体算法对网络行为进行评估，对其中的危险行为进行明确、帮助管理人员对系统中的风险和安全威胁进行明确和预警，便于管理人员及时采取有效措施对问题进行处理。例如，一些不法人员通过用户的上网行为盗取个人隐私行为进行诈骗，或者对于用户的电话以及个人信息等进行售卖，勇于网络推销以及网络诈骗。这些行为阻碍了和谐社会的发展，更严重者会威胁到国家安全，造成一定经济损失。因此，针对于这种情况的出现，需要行业技术人员意识到网络信息安全的重要性，积极引进多样化的技术手段、应用到具体安全管理工作中，从而构建安全感知系统，对网络中的潜在威胁和安全隐患进行监测和管理，从而提高安全防护有效性。利用可视化技术对安全事件进行分析和探究，便于用户对网络安全事件形成正确的认识，为用户提供安全信息[7]。

3.制定法律法规，提高网络安全法制化水平

为了减少计算机信息安全事件的发生，提高信息安全防护质量和水平，需要发挥政府部门的指导作用，结合现阶段计算机安全事件发生特点以及信息安全管理技术，制定出有针对性的法律法规。在法律法规制定前，需要当前各个行业的计算机信息安全事故种类以及风险进行深入调研，从而进行法条的制定，增强立法效果。我国以往对于网络安全重视程度不高，未能制定出专业的法律法规。人工智能背景下，需要推出网络安全法，从而做到有法可依、有法必依，对当前的不法行为进行约束，为信息技术的安全发展提供支持。相关部门需要提高思想站位，将党的思想作为建设作为法律法规制定的依据，保证法律法规制定的合理性和科学性，从而发挥出法律法规的价值。具体工作开展中，需要我国安全部门对当前的网络安全事件所造成的不良后果进行分析，从而从多个角度对网络安全工作进行考量，制定出安全维护措施。另外，需要强化责任意识，明确各部门人员的责任与义务，便于在网络安全事件发生后，第一时间找到相关责任人。制定奖惩制度，提高工作人员的责任感，从而使工作人员能够各司其职，承担起自己的责任。最后，需要完善个人保护制度，网络安全制度等，从源头上减少网络安全事件的发生。对网络行为进行规范和约束、保护个人信息安全[8]。

4.加强信息化人才队伍建设，提高信息安全防护能力

如果想要达到预期的信息安全防护效果，需要重视信息化人才队伍的建设，确保其在工作中能够正确应用先进化信息管理技术对网络行为进行规范和约束，保证信息安全。因此，需要加大人才引进力度，专业院校需要结合现阶段的信息安全事件，调整人才培养方案，从而为社会输送远远不断的人才。企业定期为专业院校的学生提供参观和实习机会，使其能够对现阶段社会人才要求进行掌握，朝着理想的方向发展。此外，需要意识到专业化培训的重要性。在实际工作开展中，积极组织

各项专业培训，使其能够掌握先进的网络安全管理技术。通过不断学习和实践提高专业技术人员的专业素养和综合应用能力、保证信息安全。另外，将专业能力考核纳入到绩效考核中，通过定期考核的形式，提高技术人员工作积极性。网络信息安全防护工作所涉及到的内容较为复杂，需要提高技术人员的薪资水平，使其能够提高工作积极性，积极参与到技术研发和创新中，为行业的发展保驾护航。

三、结束语

人工智能背景下，信息技术应用范围不断扩大。信息技术虽然为人们的生活带来了一定便利，但是由于网络系统自身存在漏洞，威胁到了信息安全的完整性。在具体工作开展中，需要国家意识到当前网络安全事件的发生所造成的不良影响，从而对这些问题进行分析和研究，制定出合理的解决策略使暴露出的问题得到有效解决。积极引入先进的安全防护手段和技术，落实到具体工作中，建立信息安全防护平台。各级政府需要发挥宏观指导作用，通过加强立法监督、建立安全管理条例等形式为信息安全管理工作提供理论依据。最后，需要提高专业技术人员的素养和能力，建设专业化管理团队，使计算机能够正常运行、促进计算机活动的有序实施。

参考文献：

[1]张慧珍.人工智能时代计算机信息安全与防护策略分析[J].中国新通信，2023，25（15）：107-109.

[2]胡化猛，马麟.人工智能时代计算机信息安全与防护策略分析[J].信息系统工程，2023（04）：77-79.

[3]陆芸.人工智能时代计算机信息技术安全与防护策略探讨[J].长江信息通信，2023，36（03）：175-177.

[4]亢婉君.人工智能时代计算机信息技术安全与防护策略探讨[J].信息记录材料，2022，23（06）：84-87.

[5]闫卫刚.人工智能时代计算机信息安全与防护策略探讨[J].电子测试，2020（19）：135-136.

[6]李志达.人工智能时代计算机信息安全与防护策略探讨[J].计算机产品与流通，2020（07）：140.

[7]董明.浅谈人工智能时代计算机信息安全与防护[J].网络安全技术与应用，2022（07）：132-133.

[8]陈昆良.信息化时代的接棒者与发展者知识化时代来临[J].工业控制计算机，2022，35（06）：151-152.