园建设打下坚实的基础。

参考文献：

[1]吴驰，于俊清，王士贤.高校信息化建设与管理——技术篇[M].武汉：华中科技大学出版社，2020.

[2]吴驰，于俊清，王士贤.高校信息化建设与管理——制度篇[M].武汉：华中科技大学出版社，2021.

高职院校计算机信息网络安全技术和安全防范策略

◆张雪

（哈尔滨铁道职业技术学院　黑龙江　150060）

摘要：随着当前大数据的快速发展，我国已经全面进入“互联网+”的时代，将互联网与传统行业进行深度融合，虽然在一定程度上能够推动行业的整体发展，但是也会给行业带来一定的信息隐患。我国高职院校互联网信息时代安全方面存在较多的问题，本文围绕当前高职院校信息网络安全方面存在的问题，并结合高职院校自身情况做出分析，并提出相应的防护措施，以供参考。

关键词：高职院校；计算机信息；网络安全；安全防范

随着当前互联网快速发展，传统行业利用信息通信技术以及互联网平台，可以使得行业得到较好的发展，在现代技术的推动下我国已经进入全新的“互联网+”时代，同时大量的移动设备都已经融入互联网产业之中，其中高职院校引入计算机信息网络技术有利于更好进行教学，这也使得高职院校更多的引入互联网的相关设备，不过随着网络技术的不断更新，在安全方面自然会暴露一些不足，这也使得当前网络信息技术一定的安全隐患。在当前互联网新时代的网络发展下应该做好相关工作，并根据当前学校自身的发展做好改善，构建良好的网络安全结构，以此养成习惯确保个人隐私以此保护网络信息安全。

1　高职院校网络安全现状分析

高职院校在后续发展中可能会使用各种类型的网络，而且在网络的使用终端上也会不断增多，这也使得原来的访问形式实现了全面的改变，原本的主体是在网络拓扑途中的物理位置进行划分。不过目前来看，想要依然使用这种形式具有一定的难度，而且由于安全方面的问题，这样的方式会使得自身的安全区域无法进行设定，从而使得问题越来越多。当前网络系统的规模还在不断扩大，而且网络结构自身也比较复杂。自身的安全漏洞比较多，而且还可能导致一些其他的问题，当前阶段黑客的攻击手段相对比较多，根据相应的网络边界方面暴露出较多的问题。因此，作为一名从事证物网络安全方面的管理人员应该积极做好思考，并为当前的变化做好努力工作，积极的展开探索。

按照当前网络边界防护架构建设的安全体系来看，在网络中的物理位置将网络进行内网、外网以及 DMZ 等进行不同的划分，在各个区域之间做好部署防火墙，通过 IPS、WAF 等配置做好相应的侧影，构建相应的网络安全数字，根据当前来看，在不同的区域之间部署对应的防护装置和 IPS 以及 WAF 等配置各不相同，从而有效建立起相关的内部安全内容，并且按照当前分析，在未来办公网络会相对较多，并且相关的企业内部人员将能够利用不同的工作形式通过公开网络访问公司业务系统，或者利用不同的办公形式进行各项工作，在多单位的情况下还能够利用个人办公室电脑进行访问系统，在这样的情形下即使是对黑客木马进行了控制，也还能够使用权限更高的账号或者不同的指令进行改善，以此阻止他们进一步损害企业当前的大数据资源，以及网络安全问题。从而减少了一些其他的问题，因为这样可以更好建立一定的保护内容，也使得内网比外网更具有一定的安全性，对内部的访问来说，在安全监管方面并不算太严格，也因此一些内网比外网的安全设定也比较全面，从而使得一些的内部人员并没有认识到潜在的危险。

当前智能化的背景下，信息安全威胁的相关因素，主要体现在以下几点：（1）系统安全漏洞，与设计者开发系统时，不可能考虑到实际使用的多个方面网络系统自身，在设计过程中就存在一定的安全问题，随着当前攻击者的手段不断多样化，各种系统在使用的过程中都可能会出现各式各样的问题。系统安全漏洞导致攻击者有机可乘，从而造成破坏的风险，这样使得一些相关数据被窃取和损坏，从而导致信息网络出现严重的威胁。（2）黑客攻击，在当前互联网不断的普及下，网络的攻击来源形式越来越广泛，黑客可能来源于全国世界的各个地区，通过网络作为载体进行破坏。随着当前互联网技术知识的不断传播，掌握黑客技术的人越来越多，这也使得黑客技术自身的能力也在不断发展。黑客通过不正当的手段以及允许非法利益的形式对网络进行攻击，从而使得一些信息被他们盗取以及破坏。黑客攻击是当前信息安全的一个重大风险，同时也应该给予重视的主要问题。（3）病毒入侵，病毒入侵是对信息安全比较常见的一种文学形式，病毒作为一种程序，它的目的是为了给用户带来一定的困扰，从而使得用户使用信息的便捷性受到限制。病毒自身具有一定的传染性和潜伏性以及破坏性病毒一旦入侵相应的智能设备后，通常会通过有效的方式获取相应的数据信息，从而使得阻碍设备网络的正常传输影响网络设备的正常运用。病毒入侵后会造成大量的信息丢失以及窃取，从而使得信息面临较大的风险。（4）钓鱼网站，钓鱼网站其最为常见的形式是利用伪造网站的形式获取用户的相关信息。许多网站通过伪装官方网站的样子，诱惑用户输入自己的密码以及关键信息，在用户不知情的情况下窃取用户的一些相关资料从而使得账户被窃取，造成资金流失以及重要文件丢失等问题。在当前智能化时代的不断发展，越来越多的智能设备会存在假冒的 APP，从而使得用户面临欺诈等风险，导致一些危险因素不断出现，从而使用户使用带来一定的风险

当前壁垒防护形式很容易从内部找到突破口，一旦攻击者发起攻击就使得防护层被打破，原本网络安全措施也未起到相应作用。通过对当前公司相关的内部数据报告分析明确，当攻击者利用手段进入了学校网后，很多人并不是通过非常先进的技术手段，而只是使用了一些凭证或者爆破工具的形式加以攻破，进而获得了学校操作系统的授权，对当前学校内部的操作系统和数据进行了访问。这就可以看出，在当前网络边界保护的架构下，为了使得自己的设备拥有一定的安全，就必须合理的采用安全策略进行改善，而如果仅仅提高了网络边界保护能力，并无法取得更有效的保护效果，也因此就无法抵御那些源自于设备内部的入侵。所以，使用最新的网络安全架构来对于未来的技术发展问题，从而促进了互联网技术更好的发展。

2　当前对于高职院校网络安全信息形成影响的因素分析

（1）人工智能对高职院校信息安全的影响

人工智能是探究与开发运用模拟的形式形成多样化专业理论集成的科学技术，其核心包含智能化计算和。具体运用的过程中其智能核心在于辅助储存和迅速化的运作大批量数据，从而使得智能核心在机器中有效的运用与完善，同时帮助人类更好进行人类操作行为。在具体的开展中结合图像进行探究，已经语言进行识别，从而让机械模仿人类进行思考与运作，以此形成较好的生产。人工智能对信息安全影响相对比较深远，信息优势已被事实证明可以决定发展的走向，甚至决定当前的整体现象。目前人工智能在信息中的应用将会形成深远的影响，具体体现在以下几个方面：第一，信息获取样式发生变化，随着人工智能化的持续融合，以往信息运作的形式需要消耗大量的时间和精力，这样的情况下会浪费大量的时间，而智能化的出现可以根据观测和评定以及决策进行全面改善从而形成良好的系统，降低成本的使用，并利用相关技术实现替代，从而达到理想的效果。学校方面经常利

用相关技术获取大量的教学资源。第二，信息对抗精确性大大提高，大量的智能化无人设备投入，使得信息对抗的经济性有所提高，从而形成了有效的限制范围，通过相应的硬件升级与软件能够完美契合，这也使得设施具有较强的自动化特征，从而实现设备的进一步完善。智能无人系统是未来主要力量，为信息化探测等提供了较好的自主判定功能，这样有利于实现管控系统的衔接融入以此实现自动化定位等工作，这也使得探测设施具有较强的灵敏性和高效性，进一步对信息进行精准的分析，从而使得其影响效果进一步提升。第三，信息对抗手段发生重大变化，随着当前智能化设备的广泛运用，信息对抗手段已经出现了较大的颠覆性变化，传感器的不断提升一些新型设备的有效应用已经成为未来信息获取的主要来自形式，从而形成了对抗主角。

（2）大数据和云计算以及物联网对高职院校信息安全的影响

大数据虽然增加了信息泄漏的风险，但同时也遇到了难题与挑战。阶段在大数据运作的过程中，会面临较多的考验，例如数据量的不断提升以及传统模式无法实现高效化处理等问题。随着人工智能时代的不断发展信息数据处理智能化程序，可以对数据进一步高效化和精确化分析，从而有利于更好进行人力资源投放。人工智能化处理运用科学技术手段，使得数据分析更加精确，从而以有效的方式开展科学化的工作决策。在整体的开展过程中，利用数据进行挖掘深入相应的内容进行分析，从而形成较好的新技术对图像与语音进行深度的判定。并结合当前智能化等云端组网技术为大数据传输带来了较好的便捷，并形成了较好的信息支持通过跨媒体等数据结合形式，将大量的数据从中进行挖掘，从而为其发展形成了战略性意义。物联网的技术虽然在客观与主体形成较好的交互，但是也存在一定的信息泄漏问题，一旦发生信息泄漏才会成不堪的设想，而智能化技术又互相交织，可能是信息处理利器，也可能是信息泄漏的罪魁祸首。

3　高职院校在信息安全建设相关建议

（1）加强计算机硬件与软件的防护功能

计算机的自身漏洞并不能永久性消除，但是可以在一定的程度上降低其自身的整体数量，通过改善确保漏洞不被他人有效利用。当前高职院校可以通过增加资金的形式加强该方面的投入，通过更新设备和交换机的融入，使得自身的硬件得以提升，这样有利于将各项工作落实到各个方面，以此实现设备的全面检测，这样有利于更好做好网络维护工作。相关学校还应该安排几个专业人员做好检测工作，这样有利于做好管理工作，同时还要定期做好检查工作，针对一些密码以及登录做好防护，再定期对光纤线路进行检修，这样可以提升整体的防护水平。

在相应的基础上，学校计算机网络软件系统也应该定期进行升级，这样可以确保校园网络的整体安全，通过防护的形式构建防护系统，防止外界网络攻击和病毒破坏，以此实现各方面的优化，达到良好的运作效果，以此达到良好的目的，推动教育行业的整体发展。

（2）构建纵深防御

纵深防御的基本速度是多处设防，多层保卫，具体的开展中针对一些重要的相关数据信息应该加强防护，同时还要采用重点布设的方法在完成相应的操作后，应该进行多处释放，可以通过强行加密或是指纹解锁等形式进行严格防护，一般情况下尽量要满足三个标准以上才能启动相应的操作，这样有利于提高整体的防御效果，确保信息安全水平的有效提升，同时还能降低人为操作的一些失误，防止受到一些外来因素的干扰，降低黑客攻击的概率。

（3）加强安全管理

当前网络系统以及相关的设备都应该加强安全管理，通过有效的方法对其内容进行全面识别，还有采取有效的方法设定警告性能这样能够针对一些存在的问题作出辨别，从而形成良好的防护系统，加强安全管理。因为当前系统和一些软件自身就存在漏洞，所以应该提高其防护工作，避免一些其他问题出现，发展中应该防止被绕过安全登录，这样能够减少他人获取信息数据的形式降低存在的风险。网络使用者应该结合当前时代情况分析并合理的获取相应的信息资源，这样能够确保一些相关资讯的丢失，防止他人盗用重要信息的。

4　结束语

综上所述，网络信息是当前运作的一种主要形式，其能够推动信息化发展。网络信息自身具有一定的特殊性，也具有较为显著的思维和运作能力，在一些活动当中能够起到决定性的作用，其自身也有一定的负面影响，高职院校应该给予一定的重视。当前时代的快速发展下，应该结合实际情况做好相关分析，同时还要合理利用网络信息安全方面存在的问题做好改善，减少一些其他因素的影响，从而防止信息泄漏造成危险。在此情况，下能够使得智能化背景下的信息得到较好运用，以此推动我国教育全面发展。

参考文献：

[1]郭福燕，夏玉荣. 高职院校计算机信息网络安全技术和安全防范策略[J].网络安全技术与应用，2019（04）：66-67.

[2]付鹏. 高职院校计算机信息网络安全技术和安全防范策略[J].信息与电脑（理论版），2019（12）：207-208.

[3]宋龙泽. 高职院校计算机信息网络安全技术和安全防范策略研究[J].信息与电脑（理论版），2018（10）：188-189.

[4]王珊珊. 高职院校计算机信息网络安全技术和安全防范策略[J].大众标准化，2021（08）：177-179.

[5]肖承望.中职院校计算机信息网络安全技术和安全防范策略探讨[J].网络安全技术与应用，2021（11）：99-100.

等保2.0下基层开放大学网络安全体系建设研究

◆陈华清

（中山开放大学　广东　528400）

摘要：随着开放大学承担的终身教育规模不断扩大，在线学习人数不断增多，对网络安全的要求也越来越高。本文基于等保 2.0 标准，结合开放大学实际，分析开放大学网络安全存在的问题，提出构建开放大学网络安全体系的建议。

关键词：开放大学；网络安全；等保 2.0

当前大数据、人工智能、云计算、物联网、虚拟技术等信息技术的高速发展，促进在线教育和教育领域信息化迅速发展。开放大学是以现代信息技术与远程教育深度融合为支撑，满足全体社会成员终身学习需要为目标的新型高校。随着开放大学承担的终身教育规模不断扩大，在线学习人数不断增多，对网络安全的要求也越来越高。基于网络安全等级保护 2.0 构建开放大学网络安全体系，为学习者提供安全可靠的网络环境是至关重要的。

1　网络安全等级保护 2.0 标准

2019 年 5 月，国家标准化委员会发布了包括《网络安全等级保护基本要求》、《网络安全等级保护测评要求》、《网络安全等级保护安全设计技术要求》的网络安全等级保护 2.0 国家标准体系（以下简称等保 2.0 标准），推动了新形势下网络安全等级保护工作。

2.1 等保 2.0 标准的特点

网络安全等级保护制度是国家网络安全工作的基本制度，是履行安全保护义务、保障网络免受破坏、防止网络数据被窃取篡改的基本方法，等保 2.0 具有以下特点。

（1）等级保护的对象更加广泛。等级保护 2.0 的对象更加广泛，包括基础信息网络、物联网、信息系统（含采用移动互联技术的系统）、大数据应用/平台/资源、云计算平台/系统、工业控制