# 高职院校网络安全问题与对策探究

李果果

（长沙民政职业技术学院，湖南 长沙 410116）

摘要：在互联网时代来临的当前，高职院校在迎来发展机遇的同时，也面临着一定的网络信息安全风险，这对高职院校网络安全防护能力提出了比较高的要求。而这便需要高职院校及时革新自身的发展思路，提高对网络安全的重视度，采用有效的防护对策提高网络信息防护水平。对此，本文首先阐述高职院校开展网络安全防护的意义，接着明确现阶段高职院校网络安全存在的问题，进而提出高职院校开展网络安全防护有效对策，以期能为其他研究者提供借鉴与参考。

关键词：高职院校；网络安全；问题；对策

随着互联网高速发展，计算机技术被广泛应用高职院校各个领域。而且在高职教育中，现代化教育技术越来越受师生青睐，使得教育活动不再受时间、空间的制约，不断提高教育教学质量。然而由于网络环境相对复杂，再加之网络本身有着比较强的虚拟性，导致网络安全问题日益凸显。对此，高职院校需要意识到这一问题的迫切性，及时采取有效对策解决这些网络安全问题，为学校、学校实现健康发展保驾护航。

## 一、高职院校开展网络安全防护的意义

### （一）有利于提高学校网络安全的实力

在当前社会发展形势下，高职院校重视网络安全防护，对推动自身实现持续化发展起着比较积极的作用。而且学校通过开展网络信息安全防护，不仅仅能解决潜在的网络安全问题，也会主动思考学校怎样才会实现安全发展。另外，通过应用各种计算机技术来优化、加强网络安全防护，可以推动高职院校数字化转型进程，引领教职工、学生主动应用计算机技术来完成相关任务，并且他们在使用计算机技术过程中，能够在第一时间内发现网络安全防护中潜在的问题与漏洞，及时修正问题、修补漏洞，切实提高高职院校安全防护水平。所以，高职院校通过开展网络安全防护，有利于为高职院校稳定、安全运作保驾护航，进而充分彰显高职院校在网络安全防护中的实力。

### （二）有利于保障学生实现健康成长

当前，网络环境具有复杂多变的特征，而且学生对于互联网越来越依赖，这给高职院校网络安全防护带来很大的挑战。一方面，互联网时代下，不良思潮传播方式比较错隐匿，而高职院校学生的辨别能力有待加强，不能准确辨别这些不良思潮，如果学生被不良思潮长期浸润，对其健康发展是不利的。另一方面，高职院校学生正处于价值观成型的关键期，容易受到网络上错误思潮和舆论的蛊惑。在此情形下，高职院校通过加强网络安全防护，可以为学生营造出健康的网络环境，最大限度地避免不良思潮侵害他们思想意识形态，而且学生的辨别能力也会得到显著增强，可以辩证地看待网络上的观点，坚定他们的理想信念，进而确保高职院校学生实现健康成长。

## 二、现阶段高职院校网络安全存在的问题

### （一）网络监测管理技术须提高

现阶段，网络病毒的威胁与黑客入侵的攻击是影响高职院校网络安全的主要因素。而且，随着技术的不断革新，网络病毒的种类不断增加，传播速度越来越快，造成的危害也愈加严重。与此同时，黑客入侵与攻击网络的手段也更加多样，其入侵速度不断加快，技术水平也日益提高，为网络安全问题的解决带来了新的难点。然而，在实际的安全网络防护中，网络监测技术还存在开发不到位的情况，容易出现以下问题：网络病毒数据的收集不够全面，不能准确识别不同黑客入侵技术，难以判断网络信息的安全性，导致较多安全漏洞与隐患不能及时弥补修复。因此，这便会导致高职院校在面对网络安全问题的时候，难以及时做出响应进行管理控制，使得信息数据的泄露、篡改、损毁等现象的发生概率大大增加，进而无法为学校、学生发展提供一个安全的网络环境。

### （二）防护系统与保护机制亟须完善

当前，高职院校未能构建完善的网络安全防护系统与保护机制。以网络安全保护机制为例，所开展的工作不够全面，缺乏完善性。在网络安全保护工作中，教师与学生属于中心管理，而高职院校则未能与他们建立直接关联。另外，学校也会错误认为网络安全防护的实质，便是利用不同的安全防护软件与技术进行防护，导致网络安全防护的渠道相对单一，进一步制约了网络安全防护成效性的提高。然而，实际上，网络安全防护不但需要技术层的安全与管理层政策的支持，还必须在法律上获得有力保障。所以，防护系统与保护机制亟须完善。

### （三）工作人员专业素养有待提高

网络安全维护是一项高难度、高技术的工作，工作人员必须具备比较丰富的实战经验与理论知识，其工作态度也需保持细致严谨，这样才可有效排查网络中存在的安全隐患并及时处理，切实提高网络的安全性。但现阶段，高职院校工作人员未能满足网络安全维护的需求。首先，部分工作人员未能储备丰富的专业知识，也未能及时研究与开发计算机信息管理技术，导致户他们在面对风险的时候，无法利用专业知识快速解决网络安全问题。其次，由于工作人员的实战经验比较有限，导致工作人员无法将已掌握的专业知识解决实际问题，使得工作质量大打折扣。另外，有些工作人员没有树立正确的职业观，工作态度也不够严谨，缺乏足够的责任感，过度重视个人利益，这些都会影响网络安全维护工作的有序开展，不利于提高网络安全的质量。

## 三、高职院校开展网络安全防护有效对策

### （一）应用多种安全防护技术，增强网络安全防护成效

在网络安全防护中，高职院校要想提高网络安全防护的成效性，应当尝试应用多种安全防护技术，具体举例如下：

第一，防火墙技术。在网络安全防护中应用防火墙技术，如同在外部网络与校园网之间建造“壁垒”，保障用户数据始终处于安全状态。而且当黑客想要攻击校园网络时，先要访问防火墙，当防火墙识别到潜在的安全风险后，便会自动采取相应的防御措施，切实维护用户数据的安全性。

第二，VLAN 技术。VLAN 作为虚拟局域网，物理节点会根据高职真实需求加入不同的逻辑子网。高职院校通过应用该技术，能够根据不同部门的职能需求，建立与之对应的虚拟局域网，便于各个职能部门根据实际需求，对流量进行控制，或者限制其他用户的访问范围。而且，当某一个局域网遭到攻击的时候，管理

员可以及时暂停该网络与其他虚拟网络的联通，以此有效保障其他网络的安全，进而有效提高高职院校网络安全水平。

第三，入侵检测技术。入侵检测技术是防火墙技术的补充，相比于防火墙技术，它属于主动型防御技术。在实际应用过程中，工作人员会根据节点的不同，应用与之相对应的入侵检测技术，当信息经过这些节点的时候，入侵检测技术便会对其展开主动搜集与分析，发现潜在安全风险的时候，便会立即反馈给管理人员。

第四，身份认证技术。应用这一技术，高职院校会在校园网所覆盖的区域，会构建用户身份认证系统，系统中应该包含用户在校各项信息以及真实姓名等，这些信息会成为用户访问校园网、询虚拟局限网的门槛，只有当身份验证正确，才能进行访问，而且系统也会根据用户流利记录、使用信息形成相应的日志，以此实时全面地监控每个用户，一旦出现问题能以最快的速度找到源头。

（二）加大网络安全管理力度，切实维护网络安全

在具体的网络安全防护中，高职院校除了要应用多种防护技术之外，还要加大网络安全管理力度，以此切实维护网络安全，具体举例如下：

第一，定期开展网络安全培训。高职院校通过开展培训活动，或者举办讲座，能够使管理者、用户明确好自身的职责，并养成健康上网、文明上网的良好习惯。另外，在培训活动中，学校还应该讲解如何安装杀毒软件以及正确使用方法，引领他们树立及时杀毒的意识，增强用户的整体防范意识，有效地将病毒的传播从源头上阻断。此外，用户在使用网络时，应该签订好入网协议，促使每个用户都能意识到维护网络安全是应尽的义务，以此有效维护网络安全。

第二，做好口令与密码管理。为了使网络安全保护机制趋于完善，高职院校应当定期更新口令以及密码，而且对多媒体教室、公共机房的管理力度也要不断加大，同时也要派遣专业人员来管理校园内部网络，要做到责任到人，便于追根溯源。

第三，做到定期维护与更新。因为互联网技术更新换代的速度比较快，所以高职院校应当做到定期维护与更新，而且在更新维护过程中，要做到常优化、常杀毒。另外，网络管理人员要做到主动学习，及时更新自身的知识储备，进而提高网络安全防护水平。

（三）开展网络道德教育，增强网络安全意识

高职院校作为人才培养主阵地，会培养出大量的计算机人才，并且他们会服务于各个领域。而且相关研究表明，高职院校网络入侵事件 70% 来自校园网内部，这也从侧面说明校内网络入侵多由在校学生发起。在此情形下，如果网络道德教育脱节，会加重学生入侵网络的行为，对此，高职院校应当在教学计划中纳入网络道德教育，并通过“两课”、校公众号、网络安全教育讲座等渠道，灵活开展网络道德教育，以此引领学生树立正确的网络观，做到自觉规范自己的上网行为。除了需要开展网络道德教育之外，管理人员也要掌握相应的网络安全防护措施。例如，在传输机密、重要信息的时候，管理人员应当单独设立专用计算机，定期检查系统日志文件，及时做好数据备份工作并异地备份，制定详尽的入侵应急措施及汇报制度、安装防病毒软件、设立防火墙等。此外，高职院校在建设校园网的时候，不仅仅要建设好基础网络设施，还要加大建设网络管理队伍的力度，因此要多渠道、多方式、高起点来培养网络安全防护队伍，并且在组建网络安全管理队伍的过程中，也要对他们进行网络道德教育，不断增幅他们的网络安全意识，并引导其形成良好的职业道德，进而保障高职院校安全防护水平得到进一步提升。

（四）增强安全应急能力，提高网络信息安全

当前，无线问题是引发网络安全风险的主要因素之一，因此，高职院校要增强网络安全应急管理能力，并制定有效的突发事件应急管理措施。比如，制定完善的网络安全应急处理机制，确保高职院校可以及时应对突发性网络安全事件，切实增强学校解决网络突发事件的能力。另外，高职院校不仅仅增强安全应急能力，还要采取相应对策提高网络信息安全，比如，高职院校可建立舆情预警与防御体系，实现多层级舆情信息筛查与防御，对不良信息进行预判与抽检，增强校园网络舆情监管能力，形成自上而下、层层递进的信息管理体系。针对舆情信息，高职院校需掌握主导权，对网络负面消息进行锚点式整顿，在舆情尚未传播时将其扼杀在摇篮中，以先入为主、先声夺人为原则，把握舆情的主导权。这样，高职院校的网络安全防护水平会得到切实提高，以此为学生营造出优质的网络环境，进而为他们实现健康发展保驾护航。

（五）及时完善软硬件配置，为网络安全防护奠基

当前，提高高职院校网络安全防护水平，首要前提便是定期更新计算机系统软件、硬件配置，在这在某种程度上会有效维护高职院校网络信息安全。随着我国的科技飞速发展，网络信息技术也在不断地更新迭代，黑客技术也在此背景之下获得了提升，不少网络不法分子仍然活跃在高校的网络系统之中。因此，在高职院校在网络信息安全防护过程中，高职院校不可以只局限于传统模式下的网络信息安全模式和理念，还应该针对高职院校现有的计算机系统以及网络信息安全防护工作的相关设施和策略进行进一步的完善和改革。除此之外，对于高职院校来讲，应该去构建一个更为全面和系统的网络安全检测机制和体系，从而做到对一些具有特殊学术价值或者意义的计算机资源以及信息做到一个有效的存储和防护，避免与此相关的计算机系统被侵入从而窃取一些重要资源或者发布一些不良网络信息，进而为网络安全防护高效开展奠定。

**四、总结**

总而言之，随着互联网不断发展，网络被广泛地应用到高职院校的方方面面，并且也成为当前必不可少的东西，但是网络在带给学校便捷的同时，也带来了一些危害，因此需要高度重视网络安全。为此，高职院校可以从以下环节着手：应用多种安全防护技术，增强网络安全防护成效；加大网络安全管理力度，切实维护网络安全；开展网络道德教育，增强网络安全意识；增强安全应急能力，提高网络信息安全；及时完善软硬件配置，为网络安全防护奠基进而有效提高高职院校网络安全防护工作的质量。

**参考文献：**

[1] 陈曦 . 新时代高职院校学生网络安全观教育研究 [J]. 常州信息职业技术学院学报，2022，21（06）：13-15.

[2] 邓国记 . 基于 2.0 等级保护标准下的高职院校网络安全防护体系研究 [J]. 辽宁师专学报（自然科学版），2022，24（03）：52-55.

[3] 吴和生 . 高职院校网络安全管理分析与对策 [J]. 电声技术，2022，46（08）：23-25.

[4] 刘阳 . 大数据背景下高职院校学生网络安全教育存在的问题及对策 [J]. 网络安全技术与应用，2022（07）：82-83.

[5] 顾浩琦 . 新形势下高职院校网络安全问题及对策研究 [J]. 江西电力职业技术学院学报，2021，34（07）：124-126.