外出培训人员学习心得体会

全面加强网络安全 推进教育信息化

(山西药科职业学院　付平)

根据“全面加强网络安全 推进教育信息化”专题培训示范班教学安排，我学习了《坚持网络主权 推进互联网全球治理法治化》、《应急与危机管理领导力建设》、《网络安全管理工作重点分析》等17门专家、教授所作的精彩讲座。通过学习使我清醒的认识到我们当前面临的新形势，进一步丰富了网络与信息安全知识，提高了政治站位，强化了网络安全意识，增加了网络安全工作本领，为今后更好的开展工作奠定了坚实的基础。下面结合实际，谈几点学习体会。

一、认清形势，提高政治站位

当今世界，信息网络技术迅猛发展，对国际政治、经济、文化、社会、军事等领域发展产生了深刻影响，互联网已经深度融入经济社会发展，深刻改变人类生活，人类的思维模式、行为方式和生活习惯，无不受到互联网的影响。互联网促进了人工智能的爆发，开启万物智能新时代，工业大数据成为制造业转型升级的助推器，VR/AR 的加速普及开拓技术产业新体系。国际上围绕互联网关键资源和网络空间国际规则的角逐将更加激烈，云计算、工控系统、智能硬件、个人隐私等都面临着安全威胁，黑客组织和“暗网”市场的横行令网络攻击与日俱增，破坏性难以估量。互联网是一把“双刃剑”，在对社会发展起到积极作用、给人类带来巨大便利的同时，也出现网络犯罪、网络攻击、网络泄密等诸多安全问题。

习近平总书记指出:“网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题。”“没有网络安全就没有国家安全。”

党的十八大以来，我们之所以能推动网信事业取得历史性成就，最根本的就在于有以习近平同志为核心的党中央的坚强领导，有网络

强国战略思想的正确引领。作为习近平新时代中国特色社会主义思想的重要组成部分，网络强国战略思想是我们党不断推进理论创新和实践创新的科学成果。长期坚持贯彻、不断丰富发展网络强国战略思想，我们才能始终沿着正确方向推进网络强国建设。作为一名基层网络服务工作者，必须深入思考，认真研究，直面问题，迎接挑战，因势而谋，应势而动，顺势而为，持续向着网络安全保障有力的目标不断前进。

二、加强学习，提高综合素质

身为一名信息化建设工作者，不仅要学习业务知识，还要反复学习研究十九大报告及习总书记关于网信工作的重要讲话精神，力求深刻领会、做到入脑入心。同时，大力发扬理论联系实际的学风，这是学习和落实的根本保证，只有学以致用，坚持用理论知识指导实践，同时在实践中不断加深对理论知识的理解，才能真正把所学所悟的知识落到实处。在深入学习上求“精”，在理论研究上求“实”，在学用结合上求“广”，牢固树立“四个意识”，做到对党忠诚、纪律严明，立足本职、服务发展的大局意识，树立正确的事业观、工作观和正气观，进一步创新工作思路，脚踏实地，埋头苦干，精于学习，勇于开拓，不断提高自身的综合素质，致力于本单位的信息化工作的发展建设。

三、牢记使命，改进提升工作

我们要牢记使命，结合学习成果将自己的本职工作精细化，切实将做到学以致用，推动工作开展的全过程和各方面。

一是要贯彻落实国家网络安全战略部署和法律法规，构建符合教育行业的安全标准规范体系。2018 年完成所有信息系统网络信息安全第三方测评工作，全面实施信息系统安全等级保护制度。

二是要进一步修订完善学院网站内容相关的审核制度，明确党委宣传统战部、院属电教中心是学院网络舆情监控管理的牵头部门，全面负责学院网络舆情引导与监控管理工作。院属各部门负责人为本部门网络舆情监控管理的第一责任人，并配备一名网络信息员，具体负责本部门网络舆情监控管理工作。各党总支书记为本单位网络舆情监控管理的第一责任人，党总支宣传委员具体负责本单位网络舆情监控管理工作。归属部门（单位）的舆情，该部门（单位）为责任单位，归属多个部门（单位）的，分别为责任单位。在院领导组织、协调和指导下，各责任单位负责网络舆情具体处置工作，其他相关部门通力

协作、密切配合。

三是要进一步建立健全网络与信息安全管理制度和安全可控的技术保障措施。

1.通过网络中心机房安装的硬件防火墙、硬件防篡改设备，加强防篡改、防病毒、防攻击、防瘫痪、防泄密等方面工作的有效性。

2.网站管理人员对网站实行动态化密码管理，用户名和开机密码专有且不得外泄，同时每 1 个月修改一次；及时对系统和软件进行更新，对网站重要文件、信息资源、数据库文件及时备份。

3.积极与校外网络安全保障工作能力强、经验丰富的人员取得联系，聘请其为兼职管理员，定期对网站安全保障工作进行检查指导，并在突发安全事件时给予技术支持。

四是要加强队伍建设，为推进各项工作的顺利实施，打造一支高素质的讲政治、懂网络、敢担当、善创新的信息化建设队伍。通过各项措施的落实，解决工作人员思想理念跟不上新要求，业务技术水平不高，研究学习积极性不高，信息化建设能力“恐慌”等突出问题。

五是要建立完善相关的培训制度与培训规划。定期召开信息员工作例会与培训,切实增强信息员把关意识提升网络宣传业务管理能力。

学院网络安全发展规划与实践

（杨海北）

物理安全设计 为保证校园网信息网络系统的物理安全,除在网络规划和场地、环境等要求之外，还要防止系统信息在空间的扩散。计算机系统通过电磁辐射使信息被截获而失密的案例已经很多，在理论和技术支持下的验证工作也证实这种截取距离在几百甚至可达千米的复原显示技术给计算机系统信息的保密工作带来了极大的危害。为了防止系统中的信息在空间上的扩散，通常是在物理上采取一定的防护措施，来减少或干扰扩散出去的空间信号。正常的防范措施主要在三个方面：对主机房及重要信息存储、收发部门进行屏蔽处理，即建设一个具有高效屏蔽效能的屏蔽室，用它来安装运行主要设备，以防止磁鼓、磁带与高辐射设备等的信号外泄。为提高屏蔽室的效能，在屏

蔽室与外界的各项联系、连接中均要采取相应的隔离措施和设计，如信号线、电话线、空调、消防控制线，以及通风、波导，门的关起等。对本地网 、局域网传输线路传导辐射的抑制，由于电缆传输辐射信息的不可避免性，现均采用光缆传输的方式，大多数均在 Modem 出来的设备用光电转换接口，用光缆接出屏蔽室外进行传输。

网络共享资源和数据信息安全设计 针对这个问题,我们决定使用 VLAN 技术和计算机网络物理隔离来实现。VLAN（Virtual LocalArea Network）即虚拟局域网，是一种通过将局域网内的设备逻辑地而不是物理地划分成一个个网段从而实现虚拟工作组的新兴技术。IEEE 于 1999 年颁布了用以标准化 VLAN 实现方案的 802.1Q 协议标准草案。VLAN 技术允许网络管理者将一个物理的 LAN 逻辑地划分成不同的广播域（或称虚拟 LAN，即 VLAN），每一个 VLAN 都包含一组有着相同需求的计算机工作站，与物理上形成的 LAN 有着相同的属性。但由于它是逻辑地而不是物理地划分,所以同一个 VLAN 内的各个工作站无须放置在同一个物理空间里，即这些工作站不一定属于同一个物理 LAN 网段。一个 VLAN 内部的广播和单播流量都不会转发到其它 VLAN 中，即使是两台计算机有着同样的网段，但是它们却没有相同的 VLAN 号，它们各自的广播流也不会相互转发，从而有助于控制流量、减少设备投资、简化网络管理、提高网络的安全性。VLAN 是为解决以太网的广播问题和安全性而提出的，它在以太网帧的基础上增加了 VLAN 头，用 VLANID 把用户划分为更小的工作组，限制不同工作组间的用户二层互访，每个工作组就是一个虚拟局域网。虚拟局域网的好处是可以限制广播范围，并能够形成虚拟工作组，动态管理网络。从目前来看，根据端口来划分 VLAN 的方式是最常用的一种方式。许多 VLAN 厂商都利用交换机的端口来划分 VLAN 成员,被设定的端口都在同一个广播域中。例如，一个交换机的 1，2，3，4，5 端口被定义为虚拟网 AAA，同一交换机的 6，7，8 端口组成虚拟网 BBB。这样做允许各端口之间的通讯，并允许共享型网络的升级。这种划分模式将虚拟网络限制在了一台交换机上。第二代端口 VLAN 技术允许跨越多个交换机的多个不同端口划分 VLAN，不同交换机上的若干个端口可以组成同一个虚拟网。以交换机端口来划分网络成员，其配置过程简单明了。

计算机病毒、黑客以及电子邮件应用风险防控设计 我们采用防病毒技术，防火墙技术和入侵检测技术来解决相关的问题。防火墙和入侵检测还对信息的安全性、访问控制方面起到很大的作用。 第一，

防病毒技术。病毒伴随着计算机系统一起发展了十几年，目前其形态和入侵途径已经发生了巨大的变化，几乎每天都有新的病毒出现在 INTERNET 上，并且借助 INTERNET 上的信息往来，尤其是 EMAIL 进行传播，传播速度极其快。计算机黑客常用病毒夹带恶意的程序进行攻击。为保护服务器和网络中的工作站免受到计算机病毒的侵害，同时为了建立一个集中有效地病毒控制机制，天下论文网需要应用基于网络的防病毒技术。这些技术包括：基于网关的防病毒系统、基于服务器的防病毒系统和基于桌面的防病毒系统。例如，我们准备在主机上统一安装网络防病毒产品套间，并在计算机信息网络中设置防病毒中央控制台，从控制台给所有的网络用户进行防病毒软件的分发，从而达到统一升级和统一管理的目的。安装了基于网络的防病毒软件后，不但可以做到主机防范病毒，同时通过主机传递的文件也可以避免被病毒侵害，这样就可以建立集中有效地防病毒控制系统，从而保证计算机网络信息安全。形成的整体拓扑图。第二，防火墙技术。企业防火墙一般是软硬件一体的网络安全专用设备,专门用于 TCP/IP 体系的网络层提供鉴别，访问控制，安全审计，网络地址转换（NAT），IDS，VPN，应用代理等功能，保护内部局域网安全接入 INTERNET 或者公共网络，解决内部计算机信息网络出入口的安全问题。

校园网的一些信息不能公布于众，因此必须对这些信息进行严格的保护和保密，所以要加强外部人员对校园网网络的访问管理，杜绝敏感信息的泄漏。通过防火墙，严格控制外来用户对校园网网络的访问，对非法访问进行严格拒绝。防火墙可以对校园网信息网络提供各种保护，包括：过滤掉不安全的服务和非法访问，控制对特殊站点的访问，提供监视 INTERNET 安全和预警，系统认证，利用日志功能进行访问情况分析等。通过防火墙，基本可以保证到达内部的访问都是安全的可以有效防止非法访问，保护重要主机上的数据，提高网络完全性。校园网网络结构分为各部门局域网（内部安全子网）和同时连接内部网络并向外提供各种网络服务的安全子网。防火墙的拓扑结构图。

内部安全子网连接整个内部使用的计算机,包括各个 VLAN 及内部服务器，该网段对外部分开，禁止外部非法入侵和攻击，并控制合法的对外访问,实现内部子网的安全。共享安全子网连接对外提供的 WEB，EMAIL，FTP 等服务的计算机和服务器，通过映射达到端口级安全。外部用户只能访问安全规则允许的对外开放的服务器，隐藏服务器的其它服务，减少系统漏洞。

学时证明

付平 同志：

于2018年4月至2018年6月参加教育部科技司举办的“全面加强网络安全 推进教育信息化”专题网络培训示范班，考核合格，计32学时。

特此证明

证书编号：2018A0114720570

国家教育行政学院

2018 年 6 月

学时证明

杨海北同志，于2020年10月12日至11月30日参加2020年教育系统网络安全网络培训示范班，经考核合格，计40 学时（45分钟/学时）。

特此证明

证书编号：2020A01143505364

国家教育行政学院

二〇二〇年十二月

参加教育部组织的网络安全培训班学习证明