

附件1

## 《网络系统管理与维护》 课程思政教学设计方案

教师姓名：\_\_\_\_\_任虹霞\_\_\_\_\_

所属学院：\_\_\_\_\_海盐学院\_\_\_\_\_

教学主题：\_\_\_\_\_防治结合——构筑网络安全体系\_\_\_\_\_

所属课程：\_\_\_\_\_网络系统管理与维护\_\_\_\_\_

课程信息			
教学主题 名称	防治结合——构筑网络安全体系		
所属课程	网络系统管理与维护		
所属专业	<input type="checkbox"/> 会计 <input type="checkbox"/> 英语 <input checked="" type="checkbox"/> 计算机	类别	<input type="checkbox"/> 本科 <input checked="" type="checkbox"/> 专科
教学目标	<p>(一) 知识目标：了解网络安全的基本概念，理解计算机病毒、防火墙和入侵检测的含义，掌握防病毒软件、防火墙的应用。</p> <p>(二) 能力目标：以“任务驱动法”为主要教法，调动学生的学习兴趣，激发学生的学习动力，使学生能从中体验到成功的喜悦，将知识点的讲解贯穿到实例中，着重培养学生学以致用能力；以“自主”、“合作”为主要学法，通过自主探究、合作学习，加强分析和解决问题的能力。</p> <p>(三) 思政目标：把工程师的爱国守法作为主线贯穿整个课堂的教学活动，强化学生法治意识，严守网络安全法律法规；培养学生爱岗敬业的职业素养，勤学会思的学习能力，严谨负责的工匠精神，合作共赢的团队意识。</p>		
学情分析	<p>(一) 学习基础分析：本课学习者开放大学专科学生，在前期学习中已经有了计算机网络基础，但理论基础薄弱，专业知识的系统性和完整性不足。</p> <p>(二) 学习能力分析：本专业学生大多为18—30岁，学习能力较强，接收新知识快；少部分30—50岁的学生事业基本趋于稳定，参加开放大学学习以考证和毕业为主，学习能力较弱。</p> <p>(三) 学习动机分析：学生大多在工作中常用到计算机，网络安全知识对学生来说十分实用，故有较强的学习动机。</p> <p>(四) 学习方式分析：学生基本具备线上学习能力，能完成网上实训和作业，这为本课的学习提供了技术支撑，本课的学习是可以完成的。</p>		

<p>教学内容</p>	<p>【主要内容 1】了解网络安全的基本内容，安全服务、安全机制等概念。</p> <p>【思政融入】以习近平总书记语录“在信息时代，网络安全对国家安全牵一发而动全身，同许多其他方面的安全都有着密切关系。”“没有网络安全就没有国家安全，没有信息化就没有现代化。”强调网络安全对国家安全的重要性，激发学生爱国主义的情怀和学好网络技能的动力。</p> <p>【主要内容 2】理解计算机病毒的特征、危害，掌握常用的防病毒策略。</p> <p>【思政融入】引导学生对计算机病毒和生物病毒进行对比发现相似性，通过类比学习体验知识的相通性，培养学生勤学习爱思考的学习态度。</p> <p>【主要内容 3】理解防火墙的含义和分类，掌握防火墙的配置。</p> <p>【思政融入】通过一定提示引导学生自主探究完成防火墙配置，培养学生自主钻研的能力，同时配置中稍有不慎会对网络安全造成极大影响，培养学生严谨认真的工匠精神。</p> <p>【主要内容 4】理解入侵检测系统的含义和常见的入侵手段、入侵检测系统的分类。</p> <p>【思政融入】引导学生理解没有绝对的网络安全技术，只有不断更新防护技术和手段才能更好的保障网络安全，培养学生不断发展和创新的精神。</p>
-------------	--

教学过程  
教学方法

## 一、教学方法

### (一) 主要教法

1、任务驱动法：让学生在典型任务的驱动下，有序地开展学习活动，先根据提示进行自主探究，应用所学知识完成任务。

2、启发式教学法：先提出问题，启发学生在实际生活中如何解决问题，根据学生回答再进一步提出问题让学生思考回答。

### (二) 主要学法

1、自主探究式学习：本次课程引导学生既动手又动脑，在实践中掌握和运用知识，给学生一个自由发挥的空间，培养学生的实践能力和思考能力。

2、合作学习：为了学生更好的掌握知识和技能，激励学生互相帮助，互相交流，协作学习，从而培养他们的团队精神。

## 二、教学过程

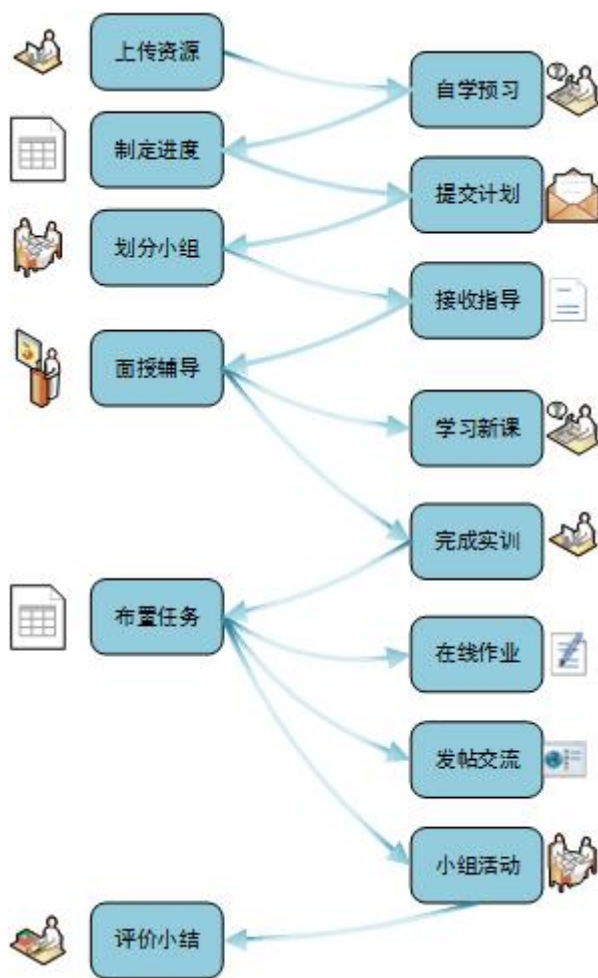


图1 教学过程示意图

### (一) 创设情境，导入新课

【创设情境】同学们进行了半学期的学习也辛苦了，老师发送一个小游戏到大家计算机桌面上。

随后打开了游戏的学生机出现蓝屏，请学生寻找原因。

【引出主题】老师发送的游戏程序藏有计算机病毒，一旦打开就会蓝屏。

【设计意图】创设真实紧张的情境，将新知识的学习过程与生活实际相结合，增强学生关注度，激发学生学习新知的兴趣。

【思政元素】以习近平总书记语录“没有网络安全就没有国家安全，没有信息化就没有现代化。”强调网络安全的重要性，激发学生爱国爱岗的学习动力。

### (二) 类比讲解，任务驱动

引出网络安全第一节：病毒防护。

任务一：认识“凶手”

【类比讲解】介绍计算机病毒概念。并与生物病毒类比，讲解计算机病毒的感染过程。

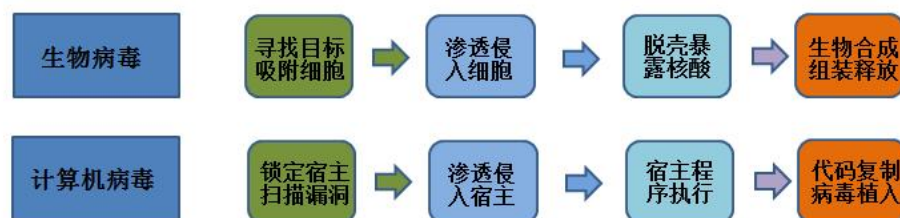


图2 生物病毒和计算机病毒复制过程对比图

【思政元素】引导学生体会计算机病毒和生物病毒的高度类似，体验知识的相通性，培养学生勤学习爱思考的学习态度。

任务二：了解“凶手”

【观察学习】观看勒索病毒小视频了解病毒。

【自主思考】请学生讲出计算机病毒特点，教师总结并继续讲解计算机病毒传染方式。



图3 病毒特点图

### 任务三：深入“凶手”

【知识讲解】介绍计算机病毒可能造成的危害。

【思政元素】制作和传播计算机病毒是违法行为，网络不是法外之地，引导学生做爱国守法的公民。

### 任务四：通缉策略

【小组讨论】请同学们参照计算机病毒的复制过程、特点和新冠病毒的防治方法，思考计算机病毒防护的方法。

【教师总结】对病毒防护方法进行归纳，介绍常用防毒软件。

【实战演练】学生进行防病毒软件安装和使用。

【设计意图】这一环节设置了实际任务，通过任务驱动法，将新知识的学习贯穿其中，调动每位学生参与的积极性。学习这一内容时，设计生物病毒的防治与计算机病毒防护进行类比，有助于学生理解。

### （三）自主探究，深入学习

【过渡】网络安全不止需要防病毒，还需要“防火”“防入侵”，引入防火墙和入侵检测系统。

【类比学习】以徽式建筑防火墙做解释，帮助学生理解网络防火墙。

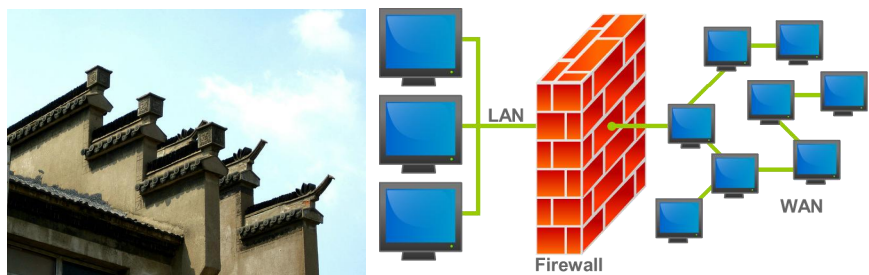


图4 虚实防火墙示意图（左实右虚）

### 1、防火墙的处理方式

允许、拒绝、丢弃

### 2、防火墙分类

按载体分：硬件、软件

按技术分：包过滤、应用层、电路层、状态监测

**【自主探究】**作为一名网络安全管理员，防火墙应该怎么配置呢？请尝试使用服务器上的高级安全 Windows 防火墙功能，阻止对其 53、80 和 443 端口的访问。

关键步骤提示：

在桌面左下角右击“Win 图标”→“运行”，在对话框中输入 firewall.cpl，然后单击“确定”；

在“本地计算机上的高级安全 Windows 防火墙属性”对话框中，选择当前计算机所在的网络位置（域网络）的配置文件选项卡，在“日志”区域单击“自定义”；

在“协议和端口”对话框中，选择“协议类型：TCP”、“本地端口：特定端口：80”（Web 服务是基于 TCP 协议，端口号为 80），单击“下一步”。

**【教师总结】**对防火墙配置进行演示与小结。

**【设计意图】**这一环节设置了实验任务，通过自主探究法，要求每位学生独立完成，提高学生动手操作的能力。

**【思政元素】**引导学生自主探究完成防火墙配置，配置中稍有不慎会对网络安全造成极大影响，要求学生具有一丝不苟的工匠精神，培养学生树立严谨负责的职业道德观。

### （四） 小组讨论，温故知新

**【过渡】**防火墙是加强网络安全的一种方法，但不是绝对有效，

那些没有防住的“火”怎么办？

引出第二道安全屏障——入侵检测系统。

### 【新知讲授】

#### 1、介绍常见的网络入侵手段



图5 常见入侵手段图

#### 2、介绍入侵检测系统的分类

根据检测对象分类：基于主机的入侵检测系统、基于网络的入侵检测系统、混合型入侵检测系统。

【小组讨论】根据前面所学，分学习小组讨论防火墙和入侵检测的区别。

【教师总结】防火墙和入侵检测在功能上有所区别，防火墙类似大门警卫，入侵检测类似全域摄像头，是防火墙后的第二道补充屏障。同时，因为攻击手段不是一成不变的，故这两道防范也不是百分百完善的，需要不断更新进步。

【设计意图】这一环节的设计采用小组讨论学习的方式来帮助学生理解防火墙和入侵检测的区别，通过自主思考——讨论交流——教师讲解突破不同安全策略逻辑区分的难点。

【思政元素】引导学生理解只有不断更新的防护技能才能更好的保障网络安全，使学生学会用创新发展的眼光看问题，通过小组讨论培养学生团队合作的品质。

## （五） 小结评价，作业布置

### 1、对于本课，进行小结评价

- （1）病毒的特征、常见的病毒及防护；
- （2）防火墙的设置；
- （3）入侵检测的作用；
- （4）学生本课实践完成情况。

### 2、线上线下，实训作业拓展

（1）登录国家开放大学学习网，自主开展网上学习并完成实训作业：

（2）对于课程的疑难问题，请学生在网络系统管理与维护论坛中发帖交流；

（3）通过钉钉等途径，推送计算机病毒、防火墙和入侵检测等相关微课等材料，进一步拓展课程效果。

<p>特色创新</p>	<p>(一) 巧妙融合，润物无声</p> <p>本课作为计算机网络技术专业课程，专业性强、实践要求高，融入思政更困难。在本课设计中，通过当下受关注的新冠病毒问题引入课程知识点，自然的引入思政内容，并将思政内容和专业知识深度糅合，避免生硬、刻意的思政，从而更能打动学生，取得良好的学习效果和思政育人功能，达到润物细无声的效果。</p> <p>(二) 整体把握，全面设计</p> <p>对本课程进行全面设计，致力于实现课程思政的全方位覆盖、全内容贯通、全平台体现。如病毒讲解时贯穿制作传播病毒的违法案例培养学生爱国守法的意识；防火墙技术配置中让学生明白配置不慎会对网络造成极大安全隐患，培养学生一丝不苟、严谨负责的职业道德观；学习入侵检测系统时和防火墙进行比较，引导学生进行前后知识的比较学习，融会贯通，并通过小组讨论培养学生团队合作的品质等。</p> <p>(三) 技术支撑，创新教学</p> <p>开放教育强调教育教学与信息技术深度融合。本课通过钉钉、微课等多种形式，将线上线下融为一体，助力学生克服工学矛盾；依托国家开放大学学习网等给予学生充足的学习资源，满足学生个性化学习；结合网络热点问题，积极创新教学案例，激发学生学习兴趣，带动学生发现问题，指导学生分析问题，诱导学生解决问题，着重体现学生为主体的教学思想。</p>
-------------	--