

校级硕士 远程信息学



校级硕士 远程信息学

- » 模式:在线
- » 时间:12个月
- » 学历:TECH科技大学
- » 时间:16小时/周
- » 时间表:按你方便的
- » 考试:在线

网络访问: www.techitute.com/cn/information-technology/professional-master-degree/master-telematics

目录

01

介绍

4

02

目标

8

03

能力

14

04

结构和内容

18

05

方法

40

06

学位

48

01 介绍

计算机科学和通信技术在远程信息学中结合起来,为开发和实施能够有效发送和接收数据的技术,流程,知识和设备提供对策。这一领域的工作和技术进步的不断融入需要长期和广泛的更新。这项研究提供了专业人员所需要的更新或高质量的专业化,并提供了一个最新的和高素质的课程。一个高质量的课程,将使你在你的职业中得到提升。





“

该课程完整, 全面更新并可适应你的可用性, 对于希望拓宽其实际技能的计算机科学家来说, 这是一个高质量的工具”

电信业的进步不断发生, 因为这是发展最快的领域之一。因此, 有必要拥有能够适应这些变化的信息技术专家, 并了解这一领域出现的新工具和技术的最新资料。

远程信息学课程涵盖了该领域所涉及的所有科目。与其他专注于特定领域的课程相比, 该课程的学习具有明显的优势, 这使得学生无法了解与电信多学科领域中的其他领域的相互关系。此外, 课程的教学团队对该培训的每个科目都进行了精心挑选, 以便为学生提供尽可能完整的学习机会, 并始终与时事挂钩。

这个课程针对那些有兴趣在远程信息学方面获得更高水平知识的人。主要目的是培训学生在现实世界中, 在再现他们未来可能遇到的条件的工作环境中, 以严格和现实的方式应用本课程所学的知识。

此外, 由于这是一个100%在线的专业, 学生不受固定时间表的制约, 也不需要搬到另一个物理地点, 而是可以在一天中的任何时间访问内容, 平衡他们的工作或个人生活与学术生活。

这个**远程信息学校级硕士**包含市场上最完整和最新的课程。主要特点是:

- ◆ 由远程信息处理专家介绍案例研究的发展
- ◆ 该书的内容图文并茂, 示意性强, 实用性强为那些视专业实践至关重要的学科提供了科学和实用的信息
- ◆ 可以进行自我评估过程的实践, 以推进学习
- ◆ 其特别强调在远程信息处理方面的创新方法
- ◆ 理论课, 向专家提问, 关于有争议问题的讨论区和个人反思性论文
- ◆ 可以从任何有互联网连接的固定或便携式设备上获取内容

“

在你的能力中包括介入远程信息处理不同领域的的能力, 通过学习途径促进你的职业发展”

“

这个计划是你选择进修计划的
最佳投资,可以使你的远程
信息学技能达到最新水平”

教学人员包括来自电信信息学领域的专业人士,他们把自己的工作经验带到了这个培训中,还有来自领先公司和著名大学的公认专家。

多媒体内容是用最新的教育技术开发的,将允许专业人员进行情景式学习,即一个模拟的环境,提供一个身临其境的培训,为真实情况进行培训。

该课程的设计重点是基于问题的学习,通过这种方式,专业人员必须尝试解决整个学年出现的不同专业实践情况。为此,专业人员将得到一个由公认的,经验丰富远程信息学专家创建的创新互动视频系统的协助。

你将使用的教学材料是一个
高质量的汇编,将使你能以
一种舒适和简单的方式前进。

这个100%的在线课程将使你的
学习与你的专业工作相结合。



02 目标

远程信息学课程旨在为IT专业人士提供一个完整的, 最新的, 涉及远程信息学干预的所有领域的研究, 其安全性和质量是以完全卓越的标准创建的课程。





“

该课程的目的是为专业人士提供他/她在远程信息处理领域所需的理论和实践知识的完整概述”



总体目标

- ◆ 培养学生能够开发远程信息应用, 分析数据或执行数字安全任务, 以及其他方面

“

这是为寻求密集和有效课程的专业人士创造的机会, 以便在其专业实践中向前迈出重要一步”





具体目标

模块1. 计算机网络

- ◆ 掌握互联网上计算机网络的基本知识
- ◆ 了解定义网络系统的不同层的功能, 如应用层, 传输层, 网络层和链接层
- ◆ 了解局域网的组成, 其拓扑结构及其网络和互连元素
- ◆ 了解IP地址和子网的工作原理
- ◆ 了解无线和移动网络的结构, 包括新的5G网络
- ◆ 理解不同的网络安全机制, 以及不同的互联网安全协议

模块2. 分布式系统

- ◆ 掌握分布式系统的基本原理
- ◆ 学习根据一些基本参数对分布式系统进行特征描述和分类
- ◆ 理解分布式系统中使用的不同类型的模型
- ◆ 知道目前实现分布式文件系统概念的架构
- ◆ 能够分析进程和对象的同步算法, 逻辑时钟的定义和信息的时间一致性
- ◆ 了解互联网上使用的命名系统, 称为DNS (域名系统)
- ◆ 了解IP寻址和子网的工作原理

模块3. 通信系统和网络的安全

- ◆ 获得经典安全, 密码学和密码分析的全球视角
- ◆ 理解对称密码学和非对称密码学的基础知识, 以及主要算法
- ◆ 分析网络攻击的性质和不同类型的安全架构
- ◆ 了解保护系统和开发安全代码的不同技术
- ◆ 了解僵尸网络和垃圾邮件以及恶意软件和恶意代码的基本组成部分
- ◆ 为软件和计算机审计领域的取证分析奠定基础

模块4.企业网络和基础设施

- ◆ 掌握基础设施互连的先进方面,在设计和规划高速网络时至关重要
- ◆ 了解运输网络的主要特点和技术
- ◆ 了解经典的广域网架构,全以太网, MPLS, VPN
- ◆ 分析网络向NGN(下一代网络)发展的基本方面
- ◆ 了解先进的QoS,路由和拥堵控制以及可靠性要求
- ◆ 了解并知道如何应用国际网络标准

模块5.安全架构

- ◆ 理解IT安全的基本原则
- ◆ 掌握IT安全标准和认证程序
- ◆ 分析安全技术所基于的组织和密码学基础
- ◆ 识别ICT所涉及的不同元素的主要威胁和漏洞,以及其原因
- ◆ 对网络安全工具及其具体功能有深入了解
- ◆ 知道如何从不同角度应用构成ICT安全架构的技术

模块6.数据中心,网络运行和服务

- ◆ 能够设计,操作,管理和维护通过数据中心提供的网络,服务和内容
- ◆ 了解构成数据中心的所有基本要素以及现有的标准和认证
- ◆ 分析数据中心基础设施在性能和效率方面的经济影响
- ◆ 识别实际基础设施中数据中心的硬件元素
- ◆ 了解市场供应商提供服务的不同解决方案的安全影响
- ◆ 理解虚拟化过程是如何运作的
- ◆ 理解云的优势,好处和采用模式

模块7.高级编程

- ◆ 深化编程知识,特别是与面向对象编程有关的知识,以及现有类之间不同类型的关系
- ◆ 了解面向对象问题的不同设计模式
- ◆ 了解事件驱动编程和用Qt开发用户界面的知识
- ◆ 掌握并发编程,进程和线程的基本知识
- ◆ 学习如何管理线程和同步的使用,以及解决并发编程中的常见问题
- ◆ 理解软件开发中文档和测试的重要性

模块8.系统工程和网络服务

- ◆ 掌握服务工程的基本概念
- ◆ 了解不断发展的软件系统的配置管理的基本原则
- ◆ 熟悉远程服务提供的技术和工具
- ◆ 了解软件系统的不同架构风格,理解它们的差异,并知道如何根据系统要求选择最合适的架构
- ◆ 了解审定和验证过程及其与生命周期其他阶段的关系
- ◆ 能够为建设电信服务和远程信息应用,整合采集,表示,处理,存储,管理和展示多媒体信息的系统
- ◆ 知道软件系统详细设计的共同要素
- ◆ 掌握远程,网络化和分布式服务和应用的编程,模拟和验证技能
- ◆ 了解过渡,配置,部署和运行的过程和活动
- ◆ 了解网络管理,自动化和优化过程



模块9.信息系统审计

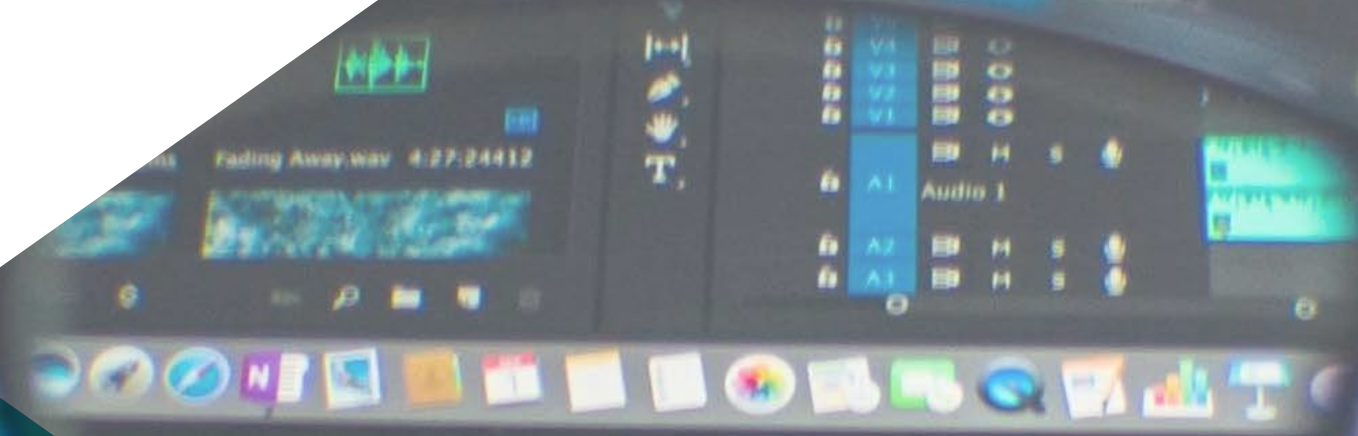
- ◆ 掌握系统审计的主要概念, 标准和方法
- ◆ 了解审计的组织要素和法律框架
- ◆ 获得设计的新的内部IT控制体系的参考指南
- ◆ 理解并识别技术发展带来的风险
- ◆ 检测不同的信息系统如何满足或不满足预期的安全要求
- ◆ 能够进行网络安全的持续改进过程

模块10.项目管理

- ◆ 了解项目管理的基本概念和项目管理的
- ◆ 了解项目管理的不同阶段, 例如启动, 计划, 管理利益相关者以及范围
- ◆ 学习时间管理, 预算制定和风险应对的进度安排
- ◆ 了解项目中质量管理的运作, 包括计划, 保证, 控制, 统计概念和可用
- ◆ 了解项目的采购, 执行, 监控, 控制和收尾流程的运作
- ◆ 从项目管理中获得与职业责任相关的基本知识

03 能力

通过远程信息学课程的评估后,你将获得必要的能力,以安全和最新的方式介入远程信息所开发的不同工作领域。一个能力增长的过程,将对你的职业生涯产生影响。



“

获得远程信息学专家的技能,并以尖端专业人员的眼光开始介入这一领域”



总体能力

- ◆ 开发远程信息处理应用程序并执行数字安全任务

“

与最好的人一起专业，
站在专业干预的最前沿”





具体能力

- ◆ 了解计算机网络的整个结构
- ◆ 掌握分布式系统并知道如何对其进行分类
- ◆ 执行通信系统和网络的安全任务
- ◆ 应用网络的国际标准
- ◆ 掌握所有的计算机安全程序
- ◆ 设计和管理数据中心
- ◆ 执行编程任务, 检测可能出现的问题并加以解决
- ◆ 了解系统设计的整个过程
- ◆ 进行系统审计和提高网络安全
- ◆ 了解项目管理的所有阶段及其生命周期, 以便知道如何管理它们

04 结构和内容

内容的结构是由电信IT部门最好的专业人士设计的。一个密集而完整的课程,包括从事远程信息处理的计算机科学家必须自信地处理的所有方面,以一种结构化和有效的方式为学生开发。



“

我们拥有市场上最完整和最新的课程。我们努力追求卓越,并希望你们也能实现这一目标”

模块1. 计算机网络

- 1.1. 计算机网络
 - 1.1.1. 网络和互联网
 - 1.1.2. 协议架构
- 1.2. 应用层
 - 1.2.1. 模型和协议
 - 1.2.2. FTP 和 SMTP 服务
 - 1.2.3. DNS服务
 - 1.2.4. HTTP 操作模型
 - 1.2.5. HTTP 消息格式
 - 1.2.6. 与高级方法的交互
- 1.3. 传输层
 - 1.3.1. 进程间通信
 - 1.3.2. 面向连接的传输: TCP 和 SCTP
- 1.4. 网络层
 - 1.4.1. 电路和分组交换
 - 1.4.2. IP 协议 (v4 和 v6)
 - 1.4.3. 路由算法
- 1.5. 链路层
 - 1.5.1. 链路层和错误检测和纠正技术
 - 1.5.2. 多接入链路和协议
 - 1.5.3. 链路级寻址
- 1.6. 网络 LAN
 - 1.6.1. 网络拓扑
 - 1.6.2. 网络和互连元素
- 1.7. IP寻址
 - 1.7.1. IP 寻址和子网划分
 - 1.7.2. 概述: HTTP 请求
- 1.8. 无线和移动网络
 - 1.8.1. 2G, 3G 和 4G 移动网络和服务
 - 1.8.2. 5G网络

- 1.9. 网络安全
 - 1.9.1. 通信安全基础
 - 1.9.2. 访问控制
 - 1.9.3. 系统安全
 - 1.9.4. 加密基础
 - 1.9.5. 电子签名
- 1.10. 互联网安全协议
 - 1.10.1. IP 安全和虚拟专用网络 (VPN)
 - 1.10.2. 使用 SSL/TLS 的网络安全

模块2. 分布式系统

- 2.1. 量子计算简介
 - 2.1.1. 基本概念
 - 2.1.2. 单片式, 分布式, 并行式和合作式计算
 - 2.1.3. 分布式系统的优势, 劣势和挑战
 - 2.1.4. 关于操作系统的初步概念: 进程和并发性
 - 2.1.5. 网络背景
 - 2.1.6. 关于软件工程的初步概念
 - 2.1.7. 本手册的组织
- 2.2. 分布式计算范式和进程间通信
 - 2.2.1. 进程间通信
 - 2.2.2. 事件同步
 - 2.2.2.1. 情景1: 同步发送和同步接收
 - 2.2.2.2. 情景2: 异步发送和同步接收
 - 2.2.2.3. 情景3: 同步发送和异步接收
 - 2.2.2.4. 情景4: 异步发送和异步接收
 - 2.2.3. 互锁和定时器
 - 2.2.4. 数据表示和编码
 - 2.2.5. 分布式计算范式的分类和描述
 - 2.2.6. Java作为分布式系统的开发环境

- 2.3. API de Sockets
 - 2.3.1. 套接字API, 类型和差异
 - 2.3.2. 数据报套接字
 - 2.3.3. 流套接字
 - 2.3.4. 联锁解决方案: 定时器和非阻塞事件
 - 2.3.5. 套接字的安全性
- 2.4. 客户端-服务器通信范式
 - 2.4.1. 分布式客户-服务器系统的基本特征和概念
 - 2.4.2. 设计和实施客户-服务器系统的过程
 - 2.4.3. 面向非连接的匿名客户的寻址问题
 - 2.4.4. 迭代式和并发式服务器
 - 2.4.5. 会话和状态信息
 - 2.4.5.1. 会话信息
 - 2.4.5.2. 全局状态信息
 - 2.4.6. 从服务器端接收异步响应的复杂客户端
 - 2.4.7. 复杂的服务器作为多个客户之间的中间机构
- 2.5. 团体通信
 - 2.5.1. 组播简介和常见用途
 - 2.5.2. 多播系统中的可靠性和排序
 - 2.5.3. 组播系统的Java实现
 - 2.5.4. 使用点对点群组通信的例子
 - 2.5.5. 可靠的组播实现
 - 2.5.6. 应用层面的组播
- 2.6. 分布式对象
 - 2.6.1. 分布式对象简介
 - 2.6.2. 基于分布式对象的应用程序的架构
 - 2.6.3. 分布式对象系统技术
 - 2.6.4. Java RMI客户端和服务器端软件层
 - 2.6.5. Java RMI分布式对象API
 - 2.6.6. 构建RMI应用程序的步骤
 - 2.6.7. 在RMI中使用Callback
 - 2.6.8. 远程对象存根的动态卸载和RMI安全管理器
- 2.7. 互联网应用 I: HTML, XML, HTTP
 - 2.7.1. 介绍互联网应用 I
 - 2.7.2. HTML 语言
 - 2.7.3. XML 语言
 - 2.7.4. HTTP互联网协议
 - 2.7.5. 动态内容的使用: 表单处理和CGI
 - 2.7.6. 互联网会话和状态数据处理
- 2.8. CORBA
 - 2.8.1. CORBA简介
 - 2.8.2. CORBA-架构
 - 2.8.3. CORBA接口描述语言
 - 2.8.4. GIOP互操作性协议
 - 2.8.5. IOR 远程对象引用
 - 2.8.6. CORBA 命名服务
 - 2.8.7. Java IDL实例
 - 2.8.8. 在IDL Java中设计, 编译和执行的步骤
- 2.9. 互联网应用II: 小程序, Servlet和SOA
 - 2.9.1. 互联网应用II简介
 - 2.9.2. 小应用程序
 - 2.9.3. Servlets简介
 - 2.9.4. HTTP小程序和它们的工作原理
 - 2.9.5. 维护Servlets中的状态信息
 - 2.9.5.1. 隐藏的表单字段
 - 2.9.5.2. Cookies
 - 2.9.5.3. Servlet变量
 - 2.9.5.4. 对象会议
 - 2.9.6. 网络服务
 - 2.9.7. SOAP 协议
 - 2.9.8. REST架构的简要概述

- 2.10.. 高级范式
 - 2.10.1. 高级范式介绍
 - 2.10.2. MOM范式
 - 2.10.3. 移动软件代理范式
 - 2.10.4. 对象空间范式
 - 2.10.5. 协作式计算
 - 2.10.6. 分布式计算的未来趋势

模块3.通信系统和网络的安全

- 3.1. 经典安全, 密码学和密码分析的全球视角
 - 3.1.1. 计算机安全:历史视角
 - 3.1.2. 但安全到底是什么意思?
 - 3.1.3. 加密货币的历史
 - 3.1.4. 替换密码
 - 3.1.5. 案例研究:密码机
- 3.2. 对称密码学
 - 3.2.1. 简介和基本术语
 - 3.2.2. 对称加密
 - 3.2.3. 操作模式
 - 3.2.4. DES
 - 3.2.5. 新的 AES 标准
 - 3.2.6. 流密码
 - 3.2.7. 密码分析
- 3.3. 非对称密码学
 - 3.3.1. 公钥密码学的起源
 - 3.3.2. 基本概念和操作
 - 3.3.3. RSA 算法
 - 3.3.4. 数字证书
 - 3.3.5. 密钥存储和管理
- 3.4. 网络攻击
 - 3.4.1. 网络威胁和攻击
 - 3.4.2. 枚举
 - 3.4.3. 流量拦截:嗅探器
 - 3.4.4. 拒绝服务攻击
 - 3.4.5. ARP中毒攻击

- 3.5. 安全架构
 - 3.5.1. 传统安全架构
 - 3.5.2. 安全套接层:SSL
 - 3.5.3. SSH 协议
 - 3.5.4. 虚拟专用网络 (VPN)
 - 3.5.5. 外部存储单元的保护机制
 - 3.5.6. 硬件保护机制
- 3.6. 系统保护技术和安全代码开发
 - 3.6.1. 操作安全
 - 3.6.2. 资源和控制
 - 3.6.3. 监测
 - 3.6.4. 入侵检测系统
 - 3.6.5. 主机 IDS
 - 3.6.6. 网络 IDS
 - 3.6.7. 基于签名的 IDS
 - 3.6.8. 诱饵系统
 - 3.6.9. 代码开发的基本安全原则
 - 3.6.10. 故障管理
 - 3.6.11. 公敌一号:缓冲区溢出
 - 3.6.12. 加密货币
- 3.7. 僵尸网络和 垃圾邮件
 - 3.7.1. 问题的根源
 - 3.7.2. 垃圾邮件的过程
 - 3.7.3. 传送垃圾邮件
 - 3.7.4. 邮件列表的细化
 - 3.7.5. 保护技术
 - 3.7.6. Antispam 第三方提供的反垃圾邮件服务
 - 3.7.7. 案例研究
 - 3.7.8. 外来垃圾邮件

- 3.8. 审计和网络攻击
 - 3.8.1. 信息收集
 - 3.8.2. 攻击技术
 - 3.8.3. 工具
- 3.9. 恶意软件和恶意代码
 - 3.9.1. 什么是恶意软件?
 - 3.9.2. 恶意软件的类型
 - 3.9.3. 病毒
 - 3.9.4. 隐病毒
 - 3.9.5. 蠕虫
 - 3.9.6. 广告软件
 - 3.9.7. 间谍软件
 - 3.9.8. 恶作剧
 - 3.9.9. 网络钓鱼
 - 3.9.10. 木马
 - 3.9.11. 恶意软件的经济学
 - 3.9.12. 可能的解决方案
- 3.10. 取证分析
 - 3.10.1. 证据收集
 - 3.10.2. 证据分析
 - 3.10.3. 反法医技术
 - 3.10.4. 实际案例研究

模块4.企业网络和基础设施

- 4.1. 运输网络
 - 4.1.1. 运输网络的功能结构
 - 4.1.2. SDH中的网络节点接口
 - 4.1.3. 网络元素
 - 4.1.4. 网络质量和可用性
 - 4.1.5. 传输网络管理
 - 4.1.6. 传输网络的演变

- 4.2. 经典的广域网结构
 - 4.2.1. 广域网络
 - 4.2.2. WAN标准
 - 4.2.3. 广域网封装
 - 4.2.4. 广域网设备
 - 4.2.4.1. 路由器
 - 4.2.4.2. 调制解调器
 - 4.2.4.3. 转变
 - 4.2.4.4. 通信服务器
 - 4.2.4.5. 网关
 - 4.2.4.6. 防火墙
 - 4.2.4.7. 代理服务器
 - 4.2.4.8. NAT
 - 4.2.5. 连接类型
 - 4.2.5.1. 点对点链接
 - 4.2.5.2. 电路切换
 - 4.2.5.3. 分组交换
 - 4.2.5.4. 广域网虚拟电路
- 4.3. 基于ATM的网络
 - 4.3.1. 介绍, 特点和层模型
 - 4.3.2. ATM物理接入层
 - 4.3.2.1. 物理介质依赖子层
 - 4.3.2.2. 物理介质依赖子层
 - 4.3.3. ATM单元
 - 4.3.3.1. 标题
 - 4.3.3.2. 虚拟连接
 - 4.3.3.3. ATM交换节点
 - 4.3.3.4. 流量控制(链接加载)
 - 4.3.4. AAL单元的适应性
 - 4.3.4.1. AAL服务的类型

- 4.4. 高级排队模型
 - 4.4.1. 介绍
 - 4.4.2. 排队理论的基础知识
 - 4.4.3. 排队理论基本系统
 - 4.4.3.1. M/M/1, M/M/m和M/M/∞系统
 - 4.4.3.2. M/M/1/k和M/M/m/m/m系统
 - 4.4.4. 排队论高级系统
 - 4.4.4.1. M/G/1系统
 - 4.4.4.2. 有优先权的M/G/1系统
 - 4.4.4.3. 排队网络
 - 4.4.4.4. 通信网络的建模
- 4.5. 企业网络中的服务质量
 - 4.5.1. 基础知识
 - 4.5.2. 融合网络中的QoS因素
 - 4.5.3. QoS政策
 - 4.5.4. 实现QoS的方法
 - 4.5.5. QoS模型
 - 4.5.6. DiffServ QoS部署的机制
 - 4.5.7. 应用示例
- 4.6. 公司网络和全以太网基础设施
 - 4.6.1. 以太网网络拓扑结构
 - 4.6.1.1. 总线拓扑结构
 - 4.6.1.2. 星形拓扑结构
 - 4.6.2. 以太网和IEEE 802.3帧格式
 - 4.6.3. 交换式以太网网络
 - 4.6.3.1. 虚拟VLANs
 - 4.6.3.2. 端口聚合
 - 4.6.3.3. 连接冗余
 - 4.6.3.4. QoS管理
 - 4.6.3.5. 安全功能
 - 4.6.4. 快速以太网
 - 4.6.5. 千兆位以太网





- 4.7. MPLS基础设施
 - 4.7.1. 介绍
 - 4.7.2. 多协议标签服务
 - 4.7.2.1. MPLS的背景和演变
 - 4.7.2.2. MPLS-架构
 - 4.7.2.3. 重新装运贴有标签的小包
 - 4.7.2.4. 标签分发协议 (LDP)
 - 4.7.3. MPLS VPN
 - 4.7.3.1. VPN的定义
 - 4.7.3.2. VPN模型
 - 4.7.3.3. MPLS VPN模型
 - 4.7.3.4. MPLS VPN架构
 - 4.7.3.5. 虚拟路由转发 (VRF)
 - 4.7.3.6. RD
 - 4.7.3.7. 路由目标 (RT)
 - 4.7.3.8. VPN MPLS中的VPNv4路由传播
 - 4.7.3.9. MPLS VPN网络中的包转发
 - 4.7.3.10. BGP
 - 4.7.3.11. BGP扩展社区BGP标签传输
 - 4.7.3.12. 使用 BGP 传输标签
 - 4.7.3.13. 路线反射器 (RR)
 - 4.7.3.14. RR组
 - 4.7.3.15. BGP路由选择
 - 4.7.3.16. 数据包转发
 - 4.7.4. MPLS 环境中的常见路由协议
 - 4.7.4.1. 矢量距离路由协议
 - 4.7.4.2. 链路状态路由协议
 - 4.7.4.3. OSPF
 - 4.7.4.4. ISIS

- 4.8. 运营商服务和VPN
 - 4.8.1. 介绍
 - 4.8.2. VPN的基本要求
 - 4.8.3. VPN类型
 - 4.8.3.1. 远程访问VPN
 - 4.8.3.2. 点对点VPN
 - 4.8.3.3. 内部VPN (通过局域网)
 - 4.8.4. VPN中使用的协议
 - 4.8.5. 实施和连接类型
- 4.9. NGN (下一代网络)
 - 4.9.1. 介绍
 - 4.9.2. 背景介绍
 - 4.9.2.1. NGN网络的定义和特点
 - 4.9.2.2. 迁移到下一代网络
 - 4.9.3. NGN-架构
 - 4.9.3.1. 主连接层
 - 4.9.3.2. 接入层
 - 4.9.3.3. 服务层
 - 4.9.3.4. 管理层
 - 4.9.4. IMS
 - 4.9.5. 标准化组织
 - 4.9.6. 监管趋势
- 4.10. 对ITU和IETF标准的审查
 - 4.10.1. 介绍
 - 4.10.2. 正常化
 - 4.10.3. 一些标准组织
 - 4.10.4. 广域网物理层协议和标准
 - 4.10.5. 面向介质的协议实例

模块5. 安全架构

- 5.1. 计算机安全的基本原则
 - 5.1.1. 什么是计算机安全的含义
 - 5.1.2. 计算机安全的目标
 - 5.1.3. 计算机安全服务
 - 5.1.4. 缺乏安全的后果
 - 5.1.5. 安全防御"原则"
 - 5.1.6. 安全政策, 计划和程序
 - 5.1.6.1. 用户账户管理
 - 5.1.6.2. 用户识别和认证
 - 5.1.6.3. 授权和逻辑访问控制
 - 5.1.6.4. 服务器监控
 - 5.1.6.5. 数据保护
 - 5.1.6.6. 远程连接的安全性
 - 5.1.7. 人为因素的重要性
- 5.2. IT安全的标准化和认证
 - 5.2.1. 安全标准
 - 5.2.1.1. 标准的目的
 - 5.2.1.2. 负责机构
 - 5.2.2. 美国的标准
 - 5.2.2.1. TCSEC
 - 5.2.2.2. 联邦标准
 - 5.2.2.3. FISCAM
 - 5.2.2.4. NIST SP 800
 - 5.2.3. 欧洲标准
 - 5.2.3.1. ITSEC
 - 5.2.3.2. ITSEM
 - 5.2.3.3. 欧洲网络和信息安全局 (ENISA)
 - 5.2.4. 国际标准
 - 5.2.5. 认证过程

- 5.3. 对IT安全的威胁:漏洞和恶意软件
 - 5.3.1. 介绍
 - 5.3.2. 系统的易损性
 - 5.3.2.1. 网络安全事件
 - 5.3.2.2. 计算机系统漏洞的原因
 - 5.3.2.3. 漏洞的类型
 - 5.3.2.4. 软件制造商的责任
 - 5.3.2.5. 漏洞评估工具
 - 5.3.3. 计算机安全威胁
 - 5.3.3.1. 网络入侵者的分类
 - 5.3.3.2. 攻击者的动机
 - 5.3.3.3. 攻击的阶段
 - 5.3.3.4. 攻击的类型
 - 5.3.4. 计算机病毒
 - 5.3.4.1. 一般特征
 - 5.3.4.2. 病毒的类型
 - 5.3.4.3. 病毒的损害
 - 5.3.4.4. 如何防治病毒
- 5.4. 网络恐怖主义和事件应对
 - 5.4.1. 介绍
 - 5.4.2. 网络恐怖主义和网络战争的威胁
 - 5.4.3. 企业失败和被攻击的后果
 - 5.4.4. 计算机网络中的间谍活动
- 5.5. 用户识别和生物识别系统
 - 5.5.1. 用户认证,授权和注册介绍
 - 5.5.2. AAA安全模型
 - 5.5.3. 访问控制
 - 5.5.4. 用户识别
 - 5.5.5. 密码验证
 - 5.5.6. 用数字证书进行认证
 - 5.5.7. 远程用户识别
 - 5.5.8. 单点登录
 - 5.5.9. 密码管理器
 - 5.5.10. 生物识别系统
 - 5.5.10.1. 一般特征
 - 5.5.10.2. 生物识别系统
 - 5.5.10.3. 系统的实施
- 5.6. 密码学和密码协议的基础知识
 - 5.6.1. 密码学简介
 - 5.6.1.1. 密码学,密码分析和密码学
 - 5.6.1.2. 加密系统的运作
 - 5.6.1.3. 加密系统的历史
 - 5.6.2. 密码分析
 - 5.6.3. 加密系统的分类
 - 5.6.4. 对称和非对称密码系统
 - 5.6.5. 用密码系统进行认证
 - 5.6.6. 电子签名
 - 5.6.6.1. 什么是电子签名?
 - 5.6.6.2. 电子签名的特点
 - 5.6.6.3. 认证机构
 - 5.6.6.4. 数字证书
 - 5.6.6.5. 基于可信的第三方系统
 - 5.6.6.6. 使用电子签名
 - 5.6.6.7. 电子身份证
 - 5.6.6.8. 电子发票
- 5.7. 网络安全工具
 - 5.7.1. 外部网络安全
 - 5.7.2. Proxy的作用
 - 5.7.3. 防火墙的作用
 - 5.7.4. 远程连接的认证服务器
 - 5.7.5. 活动日志的分析
 - 5.7.6. 入侵检测系统
 - 5.7.7. 诱饵

- 5.8. 虚拟专用网络和无线网络的安全
 - 5.8.1. 虚拟专用网络的安全
 - 5.8.1.1 VPN的作用
 - 5.8.1.2 VPN的协议
 - 5.8.2. 无线网络中的传统安全
 - 5.8.3. 对无线网络可能的攻击
 - 5.8.4. WEP 协议
 - 5.8.5. 无线网络安全的标准
 - 5.8.6. 加强安全的建议
- 5.9. 使用互联网服务的安全问题
 - 5.9.1. 安全浏览网页
 - 5.9.1.1. www服务
 - 5.9.1.2. www上的安全问题
 - 5.9.1.3. 安全建议
 - 5.9.1.4. 保护互联网上的隐私
 - 5.9.2. 照明技术电子邮件安全
 - 5.9.2.1. 电子邮件的特点
 - 5.9.2.2. 电子邮件的安全问题
 - 5.9.2.3. 电子邮件安全建议
 - 5.9.2.4. 高级电子邮件服务
 - 5.9.2.5. 雇员对电子邮件的使用
 - 5.9.3. 垃圾邮件
 - 5.9.4. Phising
- 5.10. 内容控制
 - 5.10.1. 互联网上的内容传播
 - 5.10.2. 打击非法内容的法律措施
 - 5.10.3. 对内容进行过滤, 编目和封锁
 - 5.10.4. 对形象和声誉的损害

模块6. 数据中心, 网络运行和服务

- 6.1. 数据中心: 基本概念和组成部分
 - 6.1.1. 介绍
 - 6.1.2. 基本概念
 - 6.1.2.1. CD的定义
 - 6.1.2.2. 分类和重要性
 - 6.1.2.3. 灾害和损失
 - 6.1.2.4. 演变趋势
 - 6.1.2.5. 复杂性的成本
 - 6.1.2.6. 冗余的支柱和层次
 - 6.1.3. 设计理念
 - 6.1.3.1. 目标
 - 6.1.3.2. 地点选择
 - 6.1.3.3. 可提供的服务
 - 6.1.3.4. 关键要素
 - 6.1.3.5. 成本评估和分析
 - 6.1.3.6. IT预算
 - 6.1.4. 基本组成部分
 - 6.1.4.1. 技术楼层
 - 6.1.4.2. 瓷砖的类型
 - 6.1.4.3. 总体考虑
 - 6.1.4.4. CD的尺寸
 - 6.1.4.5. 机架
 - 6.1.4.6. 服务器和通信设备
 - 6.1.4.7. 监测
- 6.2. 数据中心: 控制系统
 - 6.2.1. 介绍
 - 6.2.2. 电力供应
 - 6.2.2.1. 主电源
 - 6.2.2.2. 电力
 - 6.2.2.3. 电力分配战略
 - 6.2.2.4. 不间断电源
 - 6.2.2.5. 发电机
 - 6.2.2.6. 电力问题

- 6.2.3. 环境监测
 - 6.2.3.1. 温度
 - 6.2.3.2. 湿度
 - 6.2.3.3. 空气调节
 - 6.2.3.4. 热量估计
 - 6.2.3.5. 冷却策略
 - 6.2.3.6. 走廊设计空气循环
 - 6.2.3.7. 传感器和维护
- 6.2.4. 安全和防火
 - 6.2.4.1. 物理安全
 - 6.2.4.2. 火灾及其分类
 - 6.2.4.3. 灭火系统的分类和类型
- 6.3. 数据中心:设计和组织
 - 6.3.1. 介绍
 - 6.3.2. 布线
 - 6.3.2.1. 类型学
 - 6.3.2.2. 结构化布线
 - 6.3.2.3. 主干线
 - 6.3.2.4. UTP和STP网线
 - 6.3.2.5. 电话线
 - 6.3.2.6. 终端元件
 - 6.3.2.7. 光纤电缆
 - 6.3.2.8. 同轴电缆
 - 6.3.2.9. 无线传输
 - 6.3.2.10. 建议和标示
 - 6.3.3. 组织机构
 - 6.3.3.1. 简介
 - 6.3.3.2. 基本措施
 - 6.3.3.3. 电缆管理的策略
 - 6.3.3.4. 政策和程序
 - 6.3.4. CD管理
 - 6.3.5. 数据中心标准
- 6.4. Data Center: 商业模式和可持续性
 - 6.4.1. 介绍
 - 6.4.2. 优化
 - 6.4.2.1. 优化技术
 - 6.4.2.2. 绿色数据中心
 - 6.4.2.3. 当前的挑战
 - 6.4.2.4. 模块化心Data Centers
 - 6.4.2.5. 住房
 - 6.4.2.6. Data Centers的合并
 - 6.4.2.7. 监测
 - 6.4.3. 业务连续性
 - 6.4.3.1. BCP业务连续性计划关键点
 - 6.4.3.2. 灾难恢复灾难恢复计划
 - 6.4.3.3. DR的实施
 - 6.4.3.4. 备份和策略
 - 6.4.3.5. 备份数据中心
 - 6.4.4. 更好的做法
 - 6.4.4.1. 建议
 - 6.4.4.2. 使用ITIL方法论
 - 6.4.4.3. 可用性指标
 - 6.4.4.4. 环境监测
 - 6.4.4.5. 风险管理
 - 6.4.4.6. 负责CD的工作
 - 6.4.4.7. 工具
 - 6.4.4.8. 实施建议
 - 6.4.4.9. 角色描述
- 6.5. 云计算:介绍和基本概念
 - 6.5.1. 介绍
 - 6.5.2. 基本概念和术语

- 6.5.3. 目标和益处
 - 6.5.3.1. 可提供的服务
 - 6.5.3.2. 可靠性
 - 6.5.3.3. 可扩展性
- 6.5.4. 风险和挑战
- 6.5.5. 角色提供者消费者
- 6.5.6. 云的特征
- 6.5.7. 服务交付模式
 - 6.5.7.1. IaaS
 - 6.5.7.2. PaaS
 - 6.5.7.3. SaaS
- 6.5.8. 云的类型
 - 6.5.8.1. 公众
 - 6.5.8.2. 混合型
 - 6.5.9.3. 混合型
- 6.5.9. 云支持技术
 - 6.5.9.1. 网络架构
 - 6.5.9.2. 宽带网络互联性
 - 6.5.9.3. 数据中心技术
 - 6.5.9.3.1. 计算
 - 6.5.9.3.2. 储存
 - 6.5.9.3.3. 联网
 - 6.5.9.3.4. 高可用性
 - 6.5.9.3.5. Backup系统
 - 6.5.9.3.6. 平衡器
 - 6.5.9.4. 虚拟化
 - 6.5.9.5. 网络技术
 - 6.5.9.6. 多租户技术
 - 6.5.9.7. 服务技术



- 6.5.9.8. 云安全
 - 6.5.9.8.1. 术语和概念
 - 6.5.9.8.2. 完整性, 认证
 - 6.5.9.8.3. 安全机制
 - 6.5.9.8.4. 安全威胁
 - 6.5.9.8.5. 云安全攻击
 - 6.5.9.8.6. 案例分析
- 6.6. 云计算: 云中的技术和安全
 - 6.6.1. 介绍
 - 6.6.2. 云基础设施机制
 - 6.6.2.1. 网络周界
 - 6.6.2.2. 储存
 - 6.6.2.3. 服务器环境
 - 6.6.2.4. 云监控
 - 6.6.2.5. 高可用性
 - 6.6.3. 云安全机制(第一部分)
 - 6.6.3.1. 自动化
 - 6.6.3.2. 负载均衡器
 - 6.6.3.3. SLA监控
 - 6.6.3.4. 按使用付费的机制
 - 6.6.4. 云安全机制(第二部分)
 - 6.6.4.1. 可追溯性和审计系统
 - 6.6.4.2. 故障转移系统
 - 6.6.4.3. 次级管理程序
 - 6.6.4.4. 聚类
 - 6.6.4.5. 多租户系统
- 6.7. 云计算: 基础设施控制和安全机制
 - 6.7.1. 云管理机制介绍
 - 6.7.2. 远程管理系统
 - 6.7.3. 资源管理系统
 - 6.7.4. 服务水平协议管理系统
 - 6.7.5. 计费管理系统
 - 6.7.6. 云安全机制
 - 6.7.6.1. 加密
 - 6.7.6.2. 哈希
 - 6.7.6.3. 电子签名
 - 6.7.6.4. PKI
 - 6.7.6.5. 身份和访问管理
 - 6.7.6.6. SSO
 - 6.7.6.7. 基于云的安全组
 - 6.7.6.8. 堡垒系统
- 6.8. 云计算: 云架构
 - 6.8.1. 介绍
 - 6.8.2. 基本云架构
 - 6.8.2.1. 工作负载分配架构
 - 6.8.2.2. 资源使用架构
 - 6.8.2.3. 可扩展架构
 - 6.8.2.4. 负载均衡架构
 - 6.8.2.5. 冗余架构
 - 6.8.2.6. 实例
 - 6.8.3. 高级云架构
 - 6.8.3.1. 管理程序集群架构
 - 6.8.3.2. 虚拟负载均衡架构
 - 6.8.3.3. 不停顿架构
 - 6.8.3.4. 高可用性架构
 - 6.8.3.5. 裸机架构
 - 6.8.3.6. 冗余架构
 - 6.8.3.7. 混合架构
 - 6.8.4. 专门的云计算架构
 - 6.8.4.1. 直接I/O访问架构
 - 6.8.4.2. LUN直接访问架构
 - 6.8.4.3. 弹性网络架构
 - 6.8.4.4. SDDC架构
 - 6.8.4.5. 特殊架构
 - 6.8.4.6. 实例

- 6.9. 云计算:服务提供模式
 - 6.9.1. 介绍
 - 6.9.2. 云服务提供
 - 6.9.3. 服务提供商的观点
 - 6.9.4. 服务提供商的观点
 - 6.9.5. 案例研究
- 6.10. 云计算:签约模式,衡量标准和服务提供商
 - 6.10.1. 计费模式和指标介绍
 - 6.10.2. 计费模式
 - 6.10.3. 按使用量付费的指标
 - 6.10.4. 服务质量指标和服务水平协议介绍
 - 6.10.5. QoS指标和SLA介绍
 - 6.10.6. 服务质量的衡量标准
 - 6.10.7. 服务性能指标
 - 6.10.8. 服务可扩展性指标
 - 6.10.9. 服务模式SLA
 - 6.10.10. 案例研究

模块7.高级编程

- 7.1. 面向对象编程简介
 - 7.1.1. 面向对象编程简介
 - 7.1.2. 分类的设计
 - 7.1.3. 用于问题建模的UML简介
- 7.2. 分类之间的关系
 - 7.2.1. 抽象和继承
 - 7.2.2. 高级继承概念
 - 7.2.3. 多态性
 - 7.2.4. 组合和聚合
- 7.3. 面向对象问题的设计模式简介
 - 7.3.1. 什么是设计模式?
 - 7.3.2. 工厂模式
 - 7.3.3. 单子模式
 - 7.3.4. 观察者模式
 - 7.3.5. 复合模式

- 7.4. 例外情况
 - 7.4.1. 什么是例外?
 - 7.4.2. 异常捕获和处理
 - 7.4.3. 引发例外
 - 7.4.4. 创建例外
- 7.5. 用户界面
 - 7.5.1. Qt简介
 - 7.5.2. 定位
 - 7.5.3. 什么是事件?
 - 7.5.4. 事件:定义和捕捉
 - 7.5.5. 用户界面的发展
- 7.6. 并发编程简介
 - 7.6.1. 并发编程简介
 - 7.6.2. 进程和线程的概念
 - 7.6.3. 进程或线程之间的交互
 - 7.6.4. C++的线程
 - 7.6.5. 并发编程的优缺点
- 7.7. 线程管理和同步
 - 7.7.1. 线程的生命周期
 - 7.7.2. 线程类型
 - 7.7.3. 线程规划
 - 7.7.4. 线程组
 - 7.7.5. 守护线程
 - 7.7.6. 同步
 - 7.7.7. 锁定机制
 - 7.7.8. 沟通机制
 - 7.7.9. 监视器
- 7.8. 并发编程中的常见问题
 - 7.8.1. 生产者消费者的问题
 - 7.8.2. 读者和作者的问题
 - 7.8.3. 哲学家的晚餐问题

- 7.9. 软件文档和测试
 - 7.9.1. 为什么记录软件很重要?
 - 7.9.2. 设计文件
 - 7.9.3. 使用文档工具
- 7.10. 软件测试
 - 7.10.1. 软件测试简介
 - 7.10.2. 证据的类型
 - 7.10.3. 单元测试
 - 7.10.4. 集成测试
 - 7.10.5. 验证测试
 - 7.10.6. 系统测试

模块8. 系统工程和网络服务

- 8.1. 系统和网络服务工程简介
 - 8.1.1. 计算机系统概念和计算机工程
 - 8.1.1.1. 软件功能
 - 8.1.2. 软件的迷思
 - 8.1.3. 软件的新挑战
 - 8.1.4. 软件工程中的职业道德
 - 8.1.5. SWEBOK. 软件工程知识体系
- 8.2. 发展过程
 - 8.2.1. 解决问题的过程
 - 8.2.2. 软件开发过程
 - 8.2.3. 软件过程与生命周期
 - 8.2.4. 生命周期。过程模型(传统的)
 - 8.2.4.1. 级联模型
 - 8.2.4.2. 基于原型的模型
 - 8.2.4.3. 渐进式发展模式
 - 8.2.4.4. 快速应用开发(RAD)
 - 8.2.4.5. 螺旋模型
 - 8.2.4.6. 统一开发流程或理性统一流程(RUP)
 - 8.2.4.7. 基于组件的软件开发

- 8.2.5. 敏捷宣言。敏捷方法
 - 8.2.5.1. 极端编程(XP)
 - 8.2.5.2. Scrum
 - 8.2.5.3. 特征驱动开发(FDD)
- 8.2.6. 软件过程标准
- 8.2.7. 软件过程的定义
- 8.2.8. 软件过程成熟度
- 8.3. 敏捷项目规划和管理
 - 8.3.1. 什么是敏捷?
 - 8.3.1.1. 敏捷的历史
 - 8.3.1.2. 敏捷宣言
 - 8.3.2. 敏捷的基本原理
 - 8.3.2.1. 敏捷的思维方式
 - 8.3.2.2. 敏捷的配合
 - 8.3.2.3. 产品开发生命周期
 - 8.3.2.4. 铁三角
 - 8.3.2.5. 应对不确定性和波动性的工作
 - 8.3.2.6. 定义的过程和经验的过程
 - 8.3.2.7. 敏捷的神话
 - 8.3.3. 敏捷环境
 - 8.3.3.1. 运营模式
 - 8.3.3.2. 敏捷的角色
 - 8.3.3.3. 敏捷技术
 - 8.3.3.4. 敏捷实践
 - 8.3.4. 敏捷框架
 - 8.3.4.1. e-Xtreme编程(XP)
 - 8.3.4.2. Scrum
 - 8.3.4.3. 动态系统开发法(DSDM)
 - 8.3.4.4. 敏捷风险管理
 - 8.3.4.5. 看板
 - 8.3.4.6. 精益软件开发
 - 8.3.4.7. 精益创业
 - 8.3.4.8. 规模化敏捷框架(SAFE)

- 8.4. 配置管理和协作存储库
 - 8.4.1. 软件配置管理基础知识
 - 8.4.1.1. 什么是软件配置管理?
 - 8.4.1.2. 软件配置和软件配置要素
 - 8.4.1.3. 基线
 - 8.4.1.4. 版本, 修订, 变体和发布
 - 8.4.2. 配置管理活动
 - 8.4.2.1. 配置识别
 - 8.4.2.2. 配置变更控制
 - 8.4.2.3. 状况报告的生成
 - 8.4.2.4. 配置审计
 - 8.4.3. 配置管理计划
 - 8.4.4. 配置管理工具
 - 8.4.5. 计量学v.3方法中的配置管理
 - 8.4.6. SWEBOK中的配置管理
- 8.5. 系统和服务的测试
 - 8.5.1. 一般测试概念
 - 8.5.1.1. 核实和验证
 - 8.5.1.2. 测试的定义
 - 8.5.1.3. 测试的原则
 - 8.5.2. 测试的方法
 - 8.5.2.1. 白盒测试
 - 8.5.2.2. 黑盒测试
 - 8.5.3. 静态测试或修订
 - 8.5.3.1. 正式的技术审查
 - 8.5.3.2. 演练
 - 8.5.3.3. 法规检查





- 8.5.4. 动态测试
 - 8.5.4.1. 单元测试
 - 8.5.4.2. 集成测试
 - 8.5.4.3. 系统测试
 - 8.5.4.4. 验收测试
 - 8.5.4.5. 功能性和非功能性测试
- 8.5.5. α 测试和 β 测试
- 8.5.6. 测试过程
- 8.5.7. 错误, 缺陷和失败
- 8.5.8. 自动测试工具
 - 8.5.8.1. Junit
 - 8.5.8.2. 负载运行器(LoadRunner)
- 8.6. 网络架构的建模和设计
 - 8.6.1. 介绍
 - 8.6.2. 系统的特点
 - 8.6.2.1. 每个系统的描述
 - 8.6.2.2. 服务的描述和特点
 - 8.6.2.3. 可操作性要求
 - 8.6.3. 需求分析
 - 8.6.3.1. 用户需求
 - 8.6.3.2. 申请要求
 - 8.6.3.3. 网络要求
 - 8.6.4. 网络架构的设计
 - 8.6.4.1. 参考架构和组件
 - 8.6.4.2. 建筑模型
 - 8.6.4.3. 系统和网络架构

- 8.7. 分布式系统建模和设计
 - 8.7.1. 介绍
 - 8.7.2. 路由和寻址结构
 - 8.7.2.1. 路由策略
 - 8.7.2.2. 路由策略
 - 8.7.2.3. 设计考虑因素
 - 8.7.3. 网络设计概念
 - 8.7.4. 设计过程
- 8.8. 平台和部署环境
 - 8.8.1. 介绍
 - 8.8.2. 分布式计算机系统
 - 8.8.2.1. 基本概念
 - 8.8.2.2. 计算模型
 - 8.8.2.3. 优势,劣势和挑战
 - 8.8.2.4. 操作系统基础知识
 - 8.8.3. 虚拟化网络部署
 - 8.8.3.1. 改革的需要
 - 8.8.3.2. 网络的转型:从 "全IP "到云计算
 - 8.8.3.3. 云中的网络部署
 - 8.8.4. 例子:Azure中的网络架构
- 8.9. E2E性能:延迟和带宽QoS
 - 8.9.1. 介绍
 - 8.9.2. 性能分析
 - 8.9.3. QoS
 - 8.9.4. 确定优先次序和交通管理
 - 8.9.5. 服务水平协议
 - 8.9.6. 设计考虑因素
 - 8.9.6.1. 绩效评估
 - 8.9.6.2. 关系和互动

- 8.10. 网络自动化和优化
 - 8.10.1. 介绍
 - 8.10.2. 网络管理
 - 8.10.2.1. 管理和配置协议
 - 8.10.2.2. 网络管理架构
 - 8.10.3. 协调和自动化
 - 8.10.3.1. ONAP-架构
 - 8.10.3.2. 控制器和功能
 - 8.10.3.3. 政策
 - 8.10.3.4. 网络库存
 - 8.10.4. 优化

模块9.信息系统审计

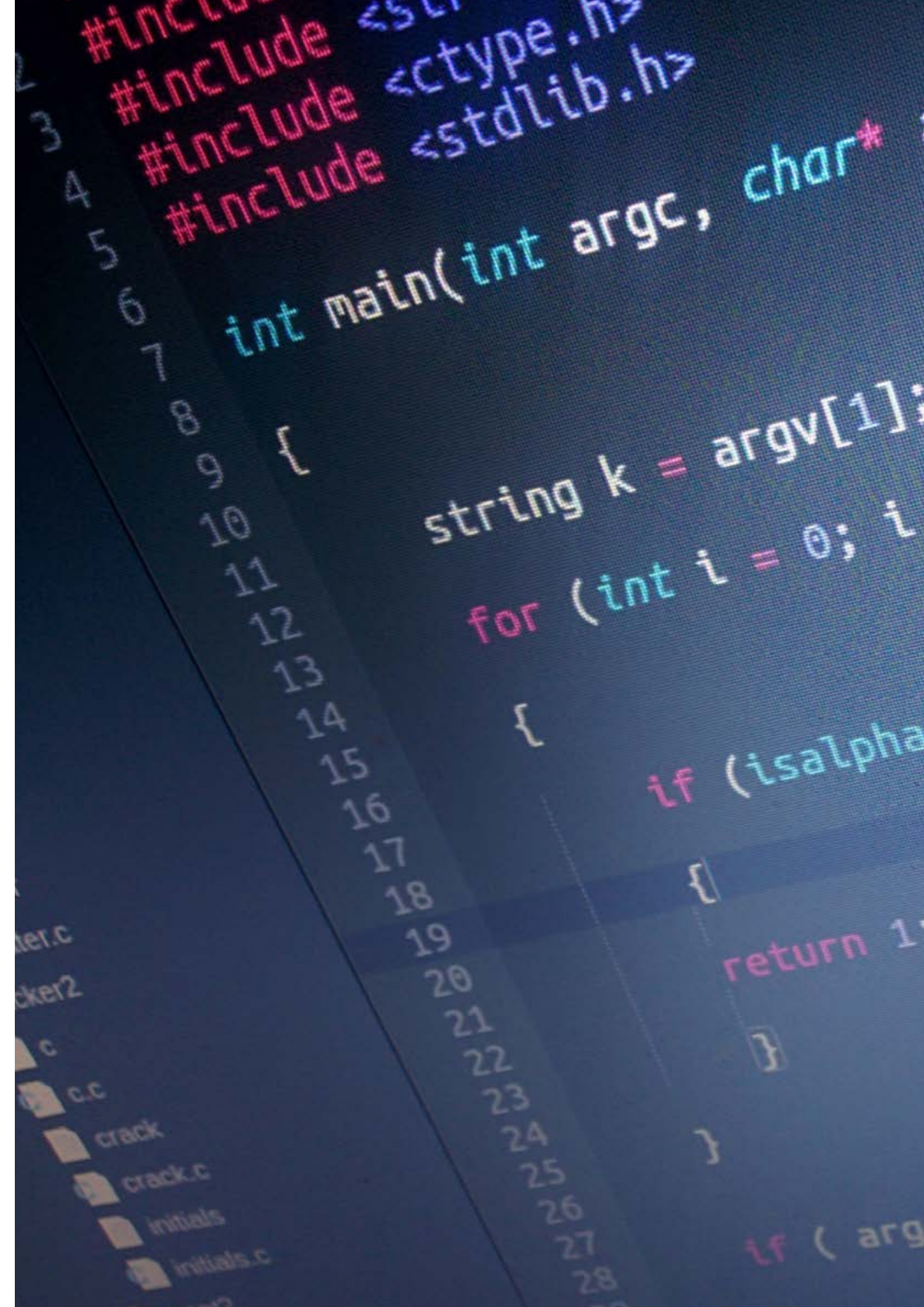
- 9.1. 信息系统审计良好做法的标准
 - 9.1.1. 介绍
 - 9.1.2. 审计和COBIT
 - 9.1.3. 对TIC统的审计
 - 9.1.4. 认证
- 9.2. 系统审计的概念和方法
 - 9.2.1. 介绍
 - 9.2.2. 系统评估的方法:定量和定性
 - 9.2.3. IT审计方法
 - 9.2.4. 审计计划
- 9.3. 审计合同
 - 9.3.1. 审计工作的法律性质
 - 9.3.2. 审计业务的各方
 - 9.3.3. 审计业务的主题
 - 9.3.4. 审计报告
- 9.4. 审计的组织要素
 - 9.4.1. 介绍
 - 9.4.2. 审计部门的任务
 - 9.4.3. 审计规划
 - 9.4.4. IS审计方法

- 9.5. 审计的法律框架
 - 9.5.1. 个人数据的保护
 - 9.5.2. 软件的法律保护
 - 9.5.3. 技术犯罪
 - 9.5.4. 签约, 签名和电子身份证
- 9.6. 外包审计和参考框架
 - 9.6.1. 介绍
 - 9.6.2. 外包基础知识
 - 9.6.3. 审计IT外包的情况
 - 9.6.4. 参考框架CMMI, ISO27001, ITIL
- 9.7. 安全审计
 - 9.7.1. 介绍
 - 9.7.2. 物理和逻辑安全
 - 9.7.3. 环境的安全
 - 9.7.4. 物理安全审计的计划和执行
- 9.8. 网络和互联网审计
 - 9.8.1. 介绍
 - 9.8.2. 网络漏洞
 - 9.8.3. 互联网上的原则和权利
 - 9.8.4. 数据控制和处理
- 9.9. 计算机应用和系统的审计
 - 9.9.1. 介绍
 - 9.9.2. 参考模型
 - 9.9.3. 对申请质量的评估
 - 9.9.4. 对开发和维护领域的组织和管理的审计
- 9.10. 对个人数据的审计
 - 9.10.1. 介绍
 - 9.10.2. 数据保护法律和法规
 - 9.10.3. 审计的发展
 - 9.10.4. 侵权和制裁

模块10.项目管理

- 10.1. 了解项目管理的基本概念和项目管理的生命周期
 - 10.1.1. 什么是项目?
 - 10.1.2. 通用方法
 - 10.1.3. 什么是项目方向/管理?
 - 10.1.4. 什么是项目计划?
 - 10.1.5. 益处
 - 10.1.6. 项目的生命周期
 - 10.1.7. 项目管理的过程或生命周期组
 - 10.1.8. 过程组和知识领域之间的关系
 - 10.1.9. 产品和项目生命周期之间的关系
- 10.2. 开始和计划
 - 10.2.1. 从想法到项目
 - 10.2.2. 项目法的制定
 - 10.2.3. 项目启动会
 - 10.2.4. 启动过程的任务, 知识和技能
 - 10.2.5. 项目计划
 - 10.2.6. 制定基本计划步骤
 - 10.2.7. 规划过程的任务, 知识和技能
- 10.3. 有权益关系者和范围的管理
 - 10.3.1. 辨识利益相关者
 - 10.3.2. 制定利益相关者的管理计划
 - 10.3.3. 管理利益相关者的参与
 - 10.3.4. 控制利益相关者的参与
 - 10.3.5. 项目目标
 - 10.3.6. 范围管理和计划
 - 10.3.7. 收集需求
 - 10.3.8. 定义范围说明
 - 10.3.9. 创建WBS (EDT)
 - 10.3.10. 年3月10日检查和控制范围

- 10.4. 时间表的制定
 - 10.4.1. 时间管理和计划
 - 10.4.2. 定义活动
 - 10.4.3. 确定活动顺序
 - 10.4.4. 活动资源估算
 - 10.4.5. 活动的估计时间
 - 10.4.6. 进度制定和关键路径计算
 - 10.4.7. 进度控制
- 10.5. 预算制定和风险应对
 - 10.5.1. 估算成本
 - 10.5.2. 制定预算和 S 曲线
 - 10.5.3. 成本控制与挣值法
 - 10.5.4. 风险概念
 - 10.5.5. 如何进行风险分析?
 - 10.5.6. 制定应对计划
- 10.6. 质量管理
 - 10.6.1. 质量规划
 - 10.6.2. 质量保证
 - 10.6.3. 质量控制
 - 10.6.4. 基本统计概念
 - 10.6.5. 质量管理工具
- 10.7. 沟通和人力资源
 - 10.7.1. 规划沟通管理
 - 10.7.2. 通信需求分析
 - 10.7.3. 通讯技术
 - 10.7.4. 沟通模式
 - 10.7.5. 沟通方式
 - 10.7.6. 通讯管理计划
 - 10.7.7. 管理通讯
 - 10.7.8. 人力资源管理
 - 10.7.9. 主要参与者及在项目中的角色
 - 10.7.10. 年7月10日组织的类型
 - 10.7.11. 项目组织
 - 10.7.12. 工作团队



```
argv[1])
```

```
< strlen(k); i++)
```

```
(k[i] == 0)
```

```
c = 2 )
```

- 10.8. 供应
 - 10.8.1. 采购流程
 - 10.8.2. 规划
 - 10.8.3. 搜索供应商并请求报价
 - 10.8.4. 合同的授予
 - 10.8.5. 合同的管理
 - 10.8.6. 合同
 - 10.8.7. 合同的类型
 - 10.8.8. 合同的谈判
- 10.9. 执行, 监控和控制以及关闭
 - 10.9.1. 进程组
 - 10.9.2. 项目实施
 - 10.9.3. 项目监控
 - 10.9.4. 项目的关闭
- 10.10. 职业责任
 - 10.10.1. 职业责任
 - 10.10.2. 社会和职业责任的特征
 - 10.10.3. 项目负责人的道德规范
 - 10.10.4. 责任和PMP®
 - 10.10.5. 责任的例子
 - 10.10.6. 专业化的好处



一个专业和个人成长的过程, 将成为你竞争力的巨大推动力"

05 方法

这个培训计划提供了一种不同的学习方式。我们的方法是通过循环的学习模式发展起来的：**再学习**。

这个教学系统被世界上一些最著名的医学院所采用，并被**新英格兰医学杂志**等权威出版物认为是最有效的教学系统之一。





“

发现再学习, 这个系统放弃了传统的线性学习, 带你体验循环教学系统: 这种学习方式已经证明了其巨大的有效性, 尤其是在需要记忆的科目中”

案例研究, 了解所有内容的背景

我们的方案提供了一种革命性的技能和知识发展方法。我们的目标是在一个不断变化, 竞争激烈和高要求的环境中加强能力建设。

“

和TECH, 你可以体验到一种正在动摇世界各地传统大学基础的学习方式”



你将进入一个以重复为基础的学习系统, 在整个教学大纲中采用自然和渐进式教学。



学生将通过合作活动和真实案例，学习如何解决真实商业环境中的复杂情况。

一种创新并不同的学习方法

该技术课程是一个密集的教学计划，从零开始，提出了该领域在国内和国际上最苛刻的挑战和决定。由于这种方法，个人和职业成长得到了促进，向成功迈出了决定性的一步。案例法是构成这一内容的技术基础，确保遵循当前经济、社会和职业现实。

“我们的课程使你准备好在不确定的环境中面对新的挑战，并取得事业上的成功”

在世界顶级计算机科学学校存在的时间里，案例法一直是最广泛使用的学习系统。1912年开发的案例法是为了让法律学生不仅在理论内容的基础上学习法律，案例法向他们展示真实的复杂情况，让他们就如何解决这些问题作出明智的决定和价值判断。1924年，它被确立为哈佛大学的一种标准教学方法。

在特定情况下，专业人士应该怎么做？这就是我们在案例法中面对的问题，这是一种以行动为导向的学习方法。在整个课程中，学生将面对多个真实的案例。他们必须整合所有的知识，研究、论证和捍卫他们的想法和决定。

再学习方法

TECH有效地将案例研究方法与基于循环的100%在线学习系统相结合,在每节课中结合了个不同的教学元素。

我们用最好的100%在线教学方法加强案例研究:再学习。

在2019年,我们取得了世界上所有西班牙语在线大学中最好的学习成绩。

在TECH,你将用一种旨在培训未来管理人员的尖端方法进行学习。这种处于世界教育学前沿的方法被称为再学习。

我校是唯一获准使用这一成功方法的西班牙语大学。2019年,我们成功地提高了学生的整体满意度(教学质量,材料质量,课程结构,目标.....),与西班牙语最佳在线大学的指标相匹配。





在我们的方案中,学习不是一个线性的过程,而是以螺旋式的方式发生(学习,解除学习,忘记和重新学习)。因此,我们将这些元素中的每一个都结合起来。这种方法已经培养了超过65万名大学毕业生,在生物化学,遗传学,外科,国际法,管理技能,体育科学,哲学,法律,工程,新闻,历史,金融市场和工具等不同领域取得了前所未有的成功。所有这些都是在一个高要求的环境中进行的,大学学生的社会经济状况很好,平均年龄为43.5岁。

再学习将使你的学习事半功倍,表现更出色,使你更多地参与到训练中,培养批判精神,捍卫论点和对比意见:直接等同于成功。

从神经科学领域的最新科学证据来看,我们不仅知道如何组织信息,想法,图像y记忆,而且知道我们学到东西的地方和背景,这是我们记住并将其储存在海马体的根本原因,并能将其保留在长期记忆中。

通过这种方式,在所谓的神经认知背景依赖的电子学习中,我们课程的不同元素与学员发展其专业实践的背景相联系。

该方案提供了最好的教育材料,为专业人士做了充分准备:



学习材料

所有的教学内容都是由教授该课程的专家专门为该课程创作的,因此,教学的发展是具体的。

然后,这些内容被应用于视听格式,创造了TECH在线工作方法。所有这些,都是用最新的技术,提供最高质量的材料,供学生使用。



大师课程

有科学证据表明第三方专家观察的有用性。

向专家学习可以加强知识和记忆,并为未来的困难决策建立信心。



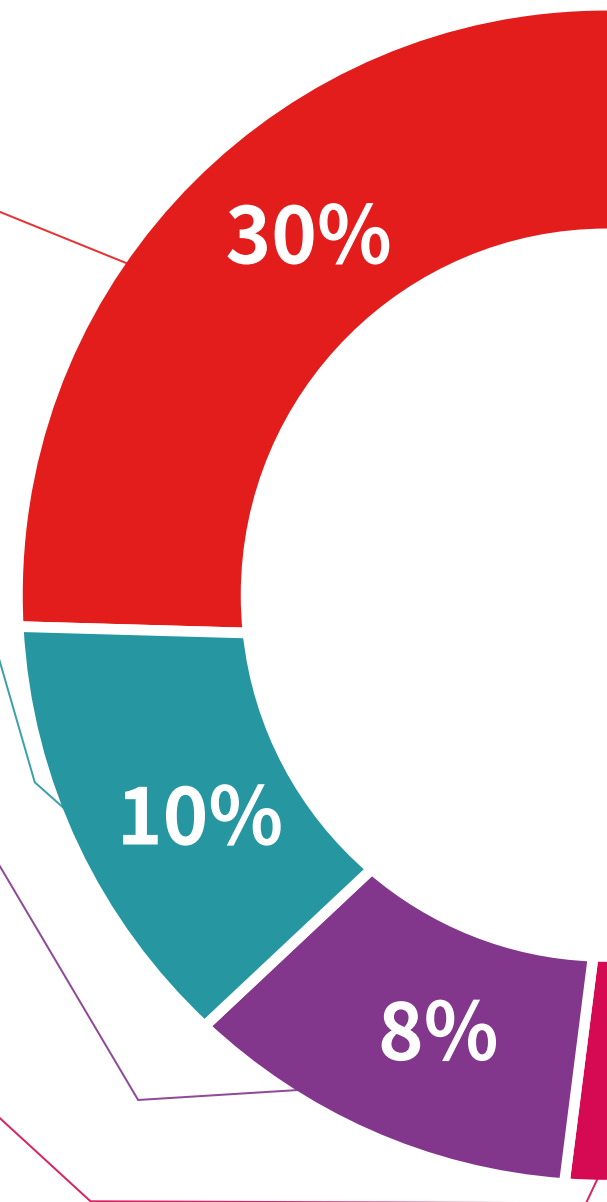
技能和能力的实践

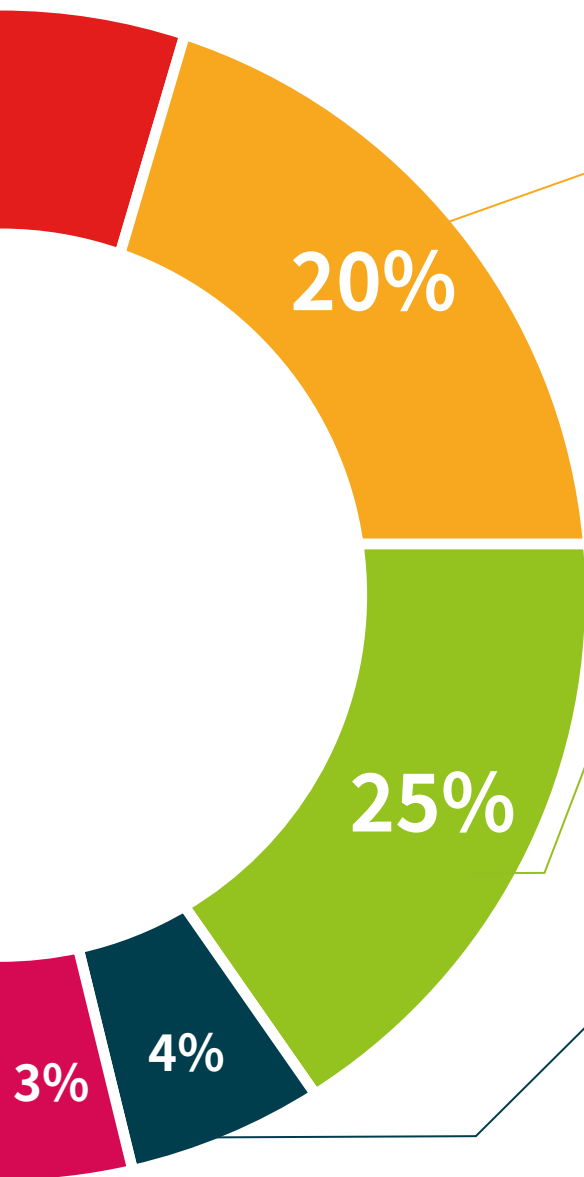
你将开展活动以发展每个学科领域的具体能力和技能。在我们所处的全球化框架内,我们提供实践和氛围帮你取得成为专家所需的技能和能力。



延伸阅读

最近的文章,共识文件和国际准则等。在TECH的虚拟图书馆里,学生可以获得他们完成培训所需的一切。





案例研究

他们将完成专门为这个学位选择的最佳案例研究。由国际上最好的专家介绍,分析和辅导案例。



互动式总结

TECH团队以有吸引力和动态的方式将内容呈现在多媒体中,其中包括音频,视频,图像,图表和概念图,以强化知识。
这个用于展示多媒体内容的独特教育系统被微软授予“欧洲成功案例”称号。



测试和循环测试

在整个课程中,通过评估和自我评估活动和练习,定期评估和重新评估学习者的知识:通过这种方式,学习者可以看到他/她是如何实现其目标的。



06 学位

远程信息校级硕士除了保证最严格和最新的培训外,还可以获得由TECH科技大学颁发的校级硕士学位证书。





“

顺利完成该课程并获得大学学位, 无需旅行或通过繁琐的程序”

这个**远程信息学校级硕士**包含了市场上最完整和最新的科学课程。

评估通过后, 学生将通过邮寄收到**TECH科技大学**颁发的相应的**校级硕士学位**。

学位由**TECH科技大学**颁发, 证明在校级硕士学位中所获得的资质, 并满足工作交流, 竞争性考试和职业评估委员会的要求。

学位:**远程信息学校级硕士**

官方学时:**1,500小时**



*海牙加注。如果学生要求为他们的纸质资格证书提供海牙加注, TECH EDUCATION将采取必要的措施来获得, 但需要额外的费用。

健康 信心 未来 人 导师
教育 信息 教学
保证 资格认证 学习
机构 社区 科技 承诺
个性化的关注 现在 创新
知识 网页 质量
网上教室 发展 语言 机构



校级硕士 远程信息学

- » 模式:在线
- » 时间:12个月
- » 学历:TECH科技大学
- » 时间:16小时/周
- » 时间表:按你方便的
- » 考试:在线

校级硕士
远程信息学

TELEMATICS

tech 科学技术大学