21. ____的目的是阻止调查人员在取证分析阶段对获取的数据进行有效分析 [ ]

A. 数据隐藏　B. 数据加密　C. 数据伪装　D. 数据删除

22. 下列不属于可信计算应用的是 [ ]

A. 操作系统安全　B. 安全管理

C. 硬件系统的高可靠性　D. 网络保护

23. 日志系统是一种重要的安全措施。为了增强日志系统的安全,可信安全计算机采用了____级日志结构 [ ]

A. 2　B. 3　C. 4　D. 5

24. 下列哪些不是可信计算机的未来发展研究的领域 [ ]

A. 可信计算的相关人才　B. 可信计算的理论基础

C. 可信计算的关键技术　D. 可信计算的应用

25. 下列哪个不是对每个密钥都要做到的要求 [ ]

A. 需要一种能够生成不可预测的密钥的方法

B. 能够允许用户拥有多个公钥/私钥对

C. 必须维护自己的公钥/私钥对文件

D. 用户与公钥之间一对一的关系

26. 在信息安全系统总体设计阶段要对方案进行分析,下列哪些不是分析和论证的内容 [ ]

A. 技术可行性　B. 经济可行性

C. 人员配置可行性　D. 社会可行性

27. 信息安全系统的可行性研究要包括 [ ]

A. 社会可行性　B. 经济可行性

C. 运行环境可行性　D. 技术可行性

28. 在信息安全系统中,下列不属于系统分析的方法从系统立足点进行分析的分析方法是 [ ]

A. 面向功能的方法　B. 面向过程的方法

C. 面向对象的方法　D. 面向数据的方法

29. 数据流程图是描述信息安全系统逻辑模型的重要工具,其特点是 [ ]

A. 抽象性和概括性　B. 具体性和综合性

C. 结构性和可行性　D. 条理性和总结性

30. 保证计算机信息系统各种设备的____是这个计算机信息安全系统的前提 [ ]

A. 安全体系　B. 物理安全　C. 系统安全　D. 安全管理

得分	评卷人	复查人

二、多项选择题　(每小题2分,共20分)

在每小题的五个备选答案中选出二至五个正确答案,并将其代码写在题干后面的括号内。多选、少选、不选或错选者,该题无分。

1. 信息安全有以下____基本属性 [ ]

A. 完整性　B. 可用性　C. 保密性

D. 可控性　E. 可靠性

2. 管理风险的手段有哪些 [ ]

A. 降低风险　B. 避免风险　C. 转嫁风险

D. 建立风险　E. 接受风险

3. 古典密码包括 [ ]

A. 代替密码　B. CRC 码　C. 置换密码

D. 表格密码　E. 数字文件密码

4. 认证技术包括 [ ]

A. 站点认证　B. 报文认证　C. 数字认证

D. 身份认证　E. 密码认证

5. 身份认证的方式有 [ ]

A. 口令　B. 担保　C. 磁卡、智能卡

D. 生理特征识别　E. 零知识证明

6. 访问控制包括 [ ]

A. 物理设备　B. 数据文件　C. 内存或进程

D. 一个合法用户　E. 访问控制策略

7. 虚拟网采用了多种安全技术保护安全,主要的安全技术有 [ ]

A. 隧道技术　B. 密码技术　C. 密钥管理技术

D. 认证技术　E. 服务质量控制技术

8. 通用入侵检测系统模型的主要部件包括 [ ]

A. 事件发生器　B. 规则集　C. 时钟

D. 反馈　E. 活动记录器

9. 实现数据隐藏的常用方法有 [ ]

A. 数据加密　B. 更改文件的扩展名

C. 隐藏或伪装夹带技术　D. 利用移动设备转移

E. 更改系统运行环境

10. 密码协议设计的最基本准则是 [ ]

A. 每个消息应清楚地说明它的意思,对消息的解释应完全依靠其内容,而不必借助于上下文推断

B. 应清楚的说明一个消息起作用的条件,以便协议的使用者能够根据条件来判断是否采用该协议

密　封　线