2020 软考

信息安全工程师

--知识精炼手册

信息安全工程师《知识精炼手册》由力杨老师根据历年考试重点进行提炼，涵盖高频考点内容，手册仅限 SVIP 内部学员使用。

力杨老师

前言：

2020 年考试时间定于 11 月 7 日至 8 日进行，信息安全工程师《知识精炼手册》由力杨老师根据官方教材、历年考点、重点知识归纳总结，以图文并茂方式汇编完成，提供配套视频课程。

【力杨软考2020.11信安】信息安全工程师课程辅导清单

班型	学费（元）	课程目录清单	辅导方式	资料	备注
VIP标准会员	138	教材精讲	录播分享	PDF电子版	
		课堂演练（真题节选）	录播分享	PDF电子版	
		案例分析专题课	录播+直播	PDF电子版	
		“小牛试刀、每日一练”刷题	微信群	PDF电子版	
SVIP尊享会员	198	VIP全套服务	同VIP	同VIP	一次付费，通过为止
		增值1：每日一记、高频考点口袋书	直播讲解	提供无水印版	
		增值2：力杨模考押题卷	直播讲解	提供无水印版	
		增值3：《知识精炼手册》视频串讲	录播+直播	PDF电子水印版	
		增值4：+58元统一印制纸质版学习包（真题+每日一练+知识精炼手册）		纸质包邮	

2020年11月计算机软考考试时间安排

级别	资格名称	日期	考试时间	考试科目
高级	信息系统项目管理师	11.7	上午09:00-11:30	综合知识
			下午01:30-03:00	案例分析
			下午03:20-05:20	论文
中级	信息安全工程师		上午09:00-11:30	基础知识
			下午02:00-04:30	应用技术
	系统集成项目管理工程师	11.8	上午09:00-11:30	基础知识
			下午02:00-04:30	应用技术
	网络工程师		上午09:00-11:30	基础知识
			下午02:00-04:30	应用技术

第 1 章 信息安全基础

题型	分值
综合选择	9-10 分
案例分析	

引言：本章为信息安全基础内容，需要重点掌握信息安全特性、国家信息安全、安全等级保护等概念。

1. 信息安全概念

✧ 我国居民二代身份证正在使用 256 位的**椭圆曲线密码 ECC**，国内外的许多电子商务系统正在使用 1024 位的 **RSA 密码**。

✧ 目前可用于密码破译的量子计算算法主要有 Grover 算法和 Shor 算法。

2. 信息安全属性：

信息安全属性	核心要点
完整性	信息是正确的、真实的、未被篡改的、完整无缺的属性
秘密性	信息不被未授权者知晓的属性
可用性	信息可以随时正常使用的属性

【课堂演练】

❖ 确保信息仅被合法实体访问，而不被泄露给非授权的实体或供其利用的特性是指信息的（ ）。（2019 年真题）

A、完整性

B、可用性

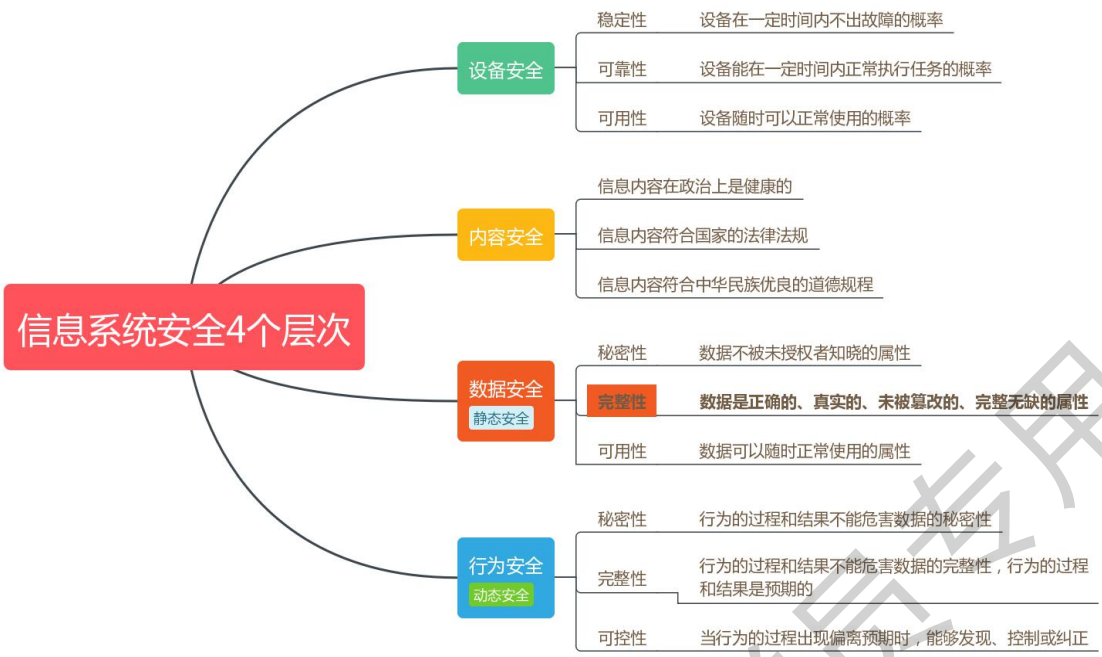
C、保密性

D、不可抵赖性

参考答案：C

3. 信息安全 4 个层次：设备安全、内容安全、数据安全、行为安全。

（力杨记忆：数据安全是传统的信息安全）



4. **理论基础：**

✧ **信息论、控制论和系统论**是现代科学的理论基础，因此也是网络空间安全学科的理论基础。

✧ **数学、信息**理论(信息论、系统论、控制论)、**计算**理论(可计算性理论、计算复杂性理论)是网络空间安全学科的理论基础，而博弈论、访问控制理论和密码学理论是网络空间安全学科所特有的理论基础。

✧ 保护、检测、响应（PDR）策略是确保信息系统和网络系统安全的基本策略。

✧ 网络空间安全学科包括**理论分析、逆向分析、实验验证、技术实现**四个核心内容。（力杨记忆：逆向分析是特有的）

5. **网络安全法：**

✧ 为适应目前形势，2015 月，第十二届全国人大常委会第十五次会议初次审议了《中华人民共和国网络安全法(草案)》 。

✧ 《中华人民共和国网络安全法》已由中华人民共和国第十二届全国人民

代表大会常务委员会第二十四次会议于 2016 年 11 月 7 日通过，现予公布，自 2017 年 6 月 1 日起施行。

✧ 第三条 国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

✧ 第八条 国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

✧ 第二十一条 国家实行网络安全等级保护制度。采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月。

✧ 第五十一条 国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

✧ 第五十八条 因维护国家安全和社会公共秩序，处置**重大突发社会安全事件**的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

✧ 第五十九条 网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

✧ 关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告;拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

【课堂演练】

❖ 《中华人民共和国网络安全法》第五十八条明确规定，因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经（ ）决定或者批准，可以在特定区域对网络通信采取限制等临时措施。（2019 年真题）

A、国务院

B、国家网信部门

C、省级以上人民政府

D、网络服务提供商

参考答案：A

6. 计算机犯罪分类：

✧ 窃取和破坏计算机资产

✧ 未经批准使用计算机信息系统资源

✧ 批准或超越权限接受计算机服务

✧ 篡改或窃取计算机中保存的信息或文件

✧ 计算机信息系统装入欺骗性数据和记录

✧ 窃取或诈骗系统中的电子钱财

7. 密码管理：

✧ 我国发展和管理商用密码实行"统一领导，集中管理，定点研制，专控经营，满足使用"的 20 字方针。

✧ 国家密码管理局于 2006 日发布公告，公布了"无线局域网产品须使用的系列密码算法"：对称密码算法 SMS4；签名算法 ECDSA；密钥协商算法 ECDH；杂凑算法 SHA-256；随机数生成算法（自行选择）。ECDSA、ECDH 密码算法**须采用国家密码管理局指定的椭圆曲线和参数**。

8. 知识产权：

✧ 知识产权包括：著作权（版权）、工业产权（专业权、商标权）、技术秘密、商业秘密。

✧ 计算软件保护的条件：**原创性、可感知性、可再现性**。

✧ 2002 年，国务院《计算机软件保护条例》正式施行。该条例称**软件是指计算机程序及其有关文档**。同一计算机程序的**源程序和目标程序**为同一作品。对软件著作权的保护**不延及**开发软件所用的思想，处理过程，操作方法或者数学概念等

9. 网络管理：

✧ 网络管理体系包括四个方面：**协议、表示、安全、对象**。

① 协议：SNMP 属于应用层

② 表示：适用面向对象式的表示方法

③ 安全：管理者和被管理者之间要有认证和加密协议

④ 对象：包括设备，各种协议，业务和交易过程

✧ 网络管理的 4 个确定性特征：统一化、智能化、安全化、主动化。

10. 人员管理：

✧ 人员管理的核心是要确保有关业务人员的思想素质、职业道德和业务素

质。

✧ 信息安全人员管理的安全教育对象，应当包括信息安全相关的所有人员。

✧ **法规教育**是信息安全教育的核心，只要与信息系统相关的人员都应该接受信息安全的法规教育。

✧ 所有信息系统相关人员都应当接受信息安全意识教育。

11. 国家安全等级保护：

✧ 国家信息安全等级保护坚持自主定级、自主保护的原则。

✧ 信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对**国家安全、社会秩序、公共利益以及公民、法人和其他组织**的合法权益的危害程度等因素确定。

第一级：国家不损害、社会公共利益不损害、公民及个人受损害。

第二级：国家不损害、社会公共利益受损害、公民及个人受严重损害。

第三级：国家受损害、社会公共利益受严重损害。

第四级：国家受严重损害、社会公共利益受特别严重损害。

第五级：国家受特别严重损害。

（力杨记忆：重点看国家客体是否受到损害，若有直接判定第三级）

12. 计算机系统安全保护等级：（用-系-安-结-访）

5 个等级	名称	内容	主要应用
第一级	用户自主保护级	本级实施的是自主访问控制，即计算机信息系统可信计算基定义和控制系统中命名用户对命名客体的访问。	普通互联网用户
第二级	系统审计保护级	本级的身份鉴别通过为用户提供唯一标识、计算机信息系统可信计算基能够使用户对自己的行为负责。	内联网以及国际网商务活动，需要保密的非重要单位

第三级	安全标记保护级	本级的计算机信息系统可信计算基具有系统审计保护级所有功能，本级的主要特征是计算机信息系统可信计算基对所有主体及其所控制的客体(例如:进程、文件、段、设备)实施强制访问控制。	用于地方各级国家机关、金融单位机构、邮电通信、能源与水源供给部门、交通运输、大型工商与信息技术企业、重点工程建设单位
第四级	结构化保护级	在第三级实施的自主和强制访问控制基础上，进一步扩展到所有主体和客体。	用于中央级国家机关、广播电视部门、重要物资储备单位、社会应急服务部门、尖端科技企业集团、国家重点科研单位机构和国防建设等部门
第五级	访问验证保护级	与第四级相比，自主访问控制机制根据用户指定方式或默认方式，**阻止非授权用户访问客体**	用于国防关键部门和依法需要对计算机信息系统实施特殊隔离的单位

【课堂演练】

❖ 《计算机信息系统安全保护等级划分准则》(GB17859-1999)中规定了计算机系统安全保护能力的五个等级，其中要求对所有主体和客体进行自主和强制访问控制的是（ ）。（2018 年真题）

A、用户自主保护级

B、系统审计保护级

C、安全标记保护级

D、结构化保护级

参考答案：D

13. 分级保护：

涉密信息系统安全分级保护根据其涉密信息系统处理信息的最高密级，可以划分为秘密级、机密级（增强）、绝密级三个等级。

分级保护	核心要点
秘密级	信息系统中包含有最高为秘密级的国家秘密，其防护水平不低于国家信息安全等级保护三级的要求，并且还必须符合分级保护的保密技术要求。
机密级	信息系统中包含有最高为机密级的国家秘密，其防护水平不低于国家信息安全等级保护四级的要求，还必须符合分级保护的保密技术要求
绝密级	信息系统中包含有最高为绝密级的国家秘密，其防护水平不低于国家信息安全等级保护五级的要求，还必须符合分级保护的保密技术要求，绝密级信息系统应限定在封闭的安全可控的独立建筑内，不能与城域网或广域网相连。

14. 涉密信息系统分级保护分为八个阶段：

- ✧ 系统定级阶段：涉密信息系统定级遵循"谁建设、谁定级"的原则
- ✧ 安全规划方案：
- ✧ 设计阶段：
- ✧ 安全工程实施阶段：调整应以不降低涉密信息系统整体安全保护强度，确保国家秘密安全为原则
- ✧ 信息系统测评阶段：
- ✧ 系统审批阶段：
- ✧ 安全运行及维护阶段：在安全运行及维护阶段，当局部调整等原因导致安全措施变化时，如果不影响系统的安全分级，应从安全运行及维护阶段进入安全工程实施阶段，重新调整和实施安全措施，确保满足分级保护的要求；当系统发生重大变更影响系统的安全分级时，应从安全运行及维护阶段进入系统定级阶段，重新开始一次分级保护实施过程。
- ✧ 定期评测与检查阶段和系统隐退终止阶段等：

15. 网络隔离：

- ✧ 凡涉及国家秘密的计算机信息系统，不得直接或间接地与国际互联网或者其他公共信息网络相连接，必须实行物理隔离。
- ✧ 网络隔离是一项网络安全技术，它消除了基于网络和基于协议的安全威胁，但网络隔离技术也存在局限性，对非网络的威胁如内容安全，就无法从理论上彻成排除，就像人工拷盘一样，交换的数据本身可能带有病毒，即使查杀病毒也不一定可以查杀干净。但它不是网络安全问题，不存在攻击和入侵之类的威胁。如果用户确定交换的内容是完全可信和可控的，那么网络隔离是用户解决网络安全问题的最佳选择。

✧ 防火墙是最常用的网络隔离手段，主要是通过网络的路由控制，也就是访向控制列表技术。

✧ 网闸的安全理念是：**网络隔离**-"过河用船不用桥":用"摆渡方式"来隔离网络。**协议隔离**-"禁止采用集装箱运输"通讯协议落地，用专用协议或存储等方式阻断通讯协议的连接，用代理方式支持上层业务。按国家安全要求是需要涉密网络与非涉密网络互联的时候，要采用网闸隔离；若非涉密网络与互联网连通时，采用单向网闸，若非涉密网络与互联网不连通时，采用双向网闸。

网络隔离	技术
第一代	完全地隔离
第二代	硬件卡隔离
第三代	数据转播隔离
第四代	空气开关隔离
第五代	安全通道隔离

16. 网络隔离技术安全要点：

✧ 要确保网络之间是隔离的

✧ 要具有高度的自身安全性

✧ 要保证网间交换的只是应用数据

✧ 要对网间的访问进行严格的控制和检查

✧ 要在坚持隔离的前提下保证网络畅通和应用透明

17. 安全监控：

系统安全监控是指对系统的运行状况和系统中的用户的行为进行监视、控制和记录。安全监控可以分为网络安全监控和主机安全监控两大类。

安全监控	主要功能
网络安全监控	**全面的网络安全控制：**除了简单的访问控制以外，还应该有入侵检测等功能。 **细粒度的控制：**除了根据数据抱头为依据，还应该对应用层协议和数据包内容进行过滤。 **网络审计：**对所有网络活动进行跟踪，对应用层协议(如 HTTP、FTP，SMTP，POP3、TELNET

	等)会话过程进行实时与历史的重现。 **其他：**包括日志、报警、报告和拦截等功能。
主机安全监控	**访问控制：**加强用户访问系统资源及服务时的安全控制，防止非法用户的入侵及合法用户的非法访问。 **系统监控：**实时监控系统的运行状态，包括运行进程、系统设备、系统资源、网络服务等，判断在线用户的行为，禁止其非法操作。 **系统审计：**对用户的行为及系统事件进行记录审计。 **系统漏洞检查：**检测主机系统的安全漏洞，防止因主机设置不当带来的安全隐患。

18. 风险评估的主要任务：

- ✧ 识别组织面临的各种风险
- ✧ 评估风险概率和可能带来的负面影响
- ✧ 确定组织承受风险的能力
- ✧ 确定风险降低和控制的优先等级推荐风险降低政策

19. 风险评估的主要过程：

① 确定资产

② 脆弱性和威胁分析

③ 制定及评估控制措施

④ 决策

⑤ 沟通与交流

⑥ 监督实施

（力杨记忆：注意排序，资产分析-评估决策-沟通监督）

20. 典型的风险评估方法：层次分析法，它的基本步骤是：

① 系统分解

② 构造判断矩阵

③ 层次总排序

21. 风险管理：

- ✧ **风险管理**就是以可以接受的费用识别，控制，降低或消除可能影响信息系统的安全风险的过程。降低风险的途经：
  - ➢ **避免**风险
  - ➢ **转移**风险
  - ➢ **减少**威胁
  - ➢ **减少**脆弱性
  - ➢ **减少**威胁可能的影响
  - ➢ **检测**意外事件
- ✧ **风险接受**是一个对残留风险进行确认和评价的过程。

22. 技术标准的基本知识：

- ✧ 统一标准是互联互通、信息共享、业务协商的基础；是信息系统互通、互连、互操作的前提。
- ✧ 在我国，将标准级别依据《中华人民共和国标准化法》划分为国家标准、行业标准、地方标准和企业标准等 4 个层次。
- ✧ 依据《中华人民共和国标准化法》的规定，**国家标准、行业标准**均可分为强制性和推荐性两种属性的标准。保障人体健康、人身、财产安全的标准和法律、行政法规规定强制执行的标准是强制性标准，其他标准是推荐性标准。省、自治区、直辖市标准化行政主管部门制定的工业产品安全、卫生要求的地方标准，在本地区域内是**强制性标准**。
- ✧ 强制性标准是由法律规定必须遵照执行的标准。强制性标准以外的标准是推荐性标准，又叫非强制性标准。推荐性国家标准的代号为 "GB/T"，强制性国家标准的代号为"GB"。行业标准中的推荐性标准也是在行业标准代号后加个 "T" 字，如 "JB/T" 即机械行业推荐性标准，不加 "T"

字即为强制性行业标准。

【课堂演练】

❖ 在我国，依据《中华人民共和国标准化法》可以将标准划分为：国家标准、行业标准、地方标准和企业标准 4 个层次。《信息安全技术信息系统安全等级保护基本要求》（GB/T 22239-2008）属于（ ）。（2019 年真题）

A、国家标准

B、行业标准

C、地方标准

D、企业标准

参考答案：A

23. 标准化组织：

✧ 目前国际上有两个重要的标准化组织，即**国际标准化组织 OSO** 和**国际电工委员会 OEC**。

✧ SC27 下设三个工作组，各工作组的名称体现了各自的工作范围：

① 第一工作组（WG1）：**需求、安全服务及指南**工作组

② 第二工作组（WG2）：**安全技术与机制**工作组

③ 第三工作组（WG3）：**安全评估准则**工作组

✧ BS7799 标准是英国标准协会（BSI））制定的信息安全管理体系标准它包括两部分：

① 第一部分：《**信息安全管理实施指南**》，这一部分主要提供了信息安全管理的一些通常做法，用于指导企业信息安全管理体系的建设。

② 第二部分：《**信息安全管理体系规范和应用指南**》，是一个认证标准，描述了信息安全管理体系各个方面需要达到的一些要求，可以以此为标准对机构的信息安全管

理体系进行考核和认证。

24. 信息安全标准：

✧ 信息安全标准是我国信息安全保障体系的重要组成部分，是政府进行宏观管理的重要依据。

✧ 国际上已制定了大量有关信息安全管理的国际标准，主要可分为**信息安全管理与控制类标准**和**技术与工程类标准**。

✧ CC 标准定义了作为评估信息技术产品和系统安全性的基础准则，提出了目前国际上公认的表述信息技术安全性的结构，即把安全要求分为规范产品和系统安全行为的功能要求以及解决如何正确有效地实施这些功能的保证要求。

✧ **CC 标准分为 3 个部分：**

① 第一部分：″**简介和一般模型**″

② 第二部分：″**安全功能要求**″

③ 第三部分：″**安全保证要求**″

✧ **CC 标准的核心思想有两点：**

① 一是信息安全技术提供的安全功能本身和对信息安全技术的保证承诺之间独立。

② 二是安全工程的思想，即通过对信息安全产品的开发、评价、使用全过程的各个环节实施安全工程来确保产品的安全性。

CC 标准强调在 IT 产品和系统的整个生命周期确保安全性。因此，CC 标准可以同时面向**消费者、开发者、评价者**类用户，同时支持他们的应用。

✧ **CC 标准的 3 种主要应用形式：**

① **定义安全需求**

② **辅助安全产品开发**

③ **评价产品安全性**

25. 可信计算机系统评估准则 TCSEC：

✧ 可信计算机系统评估准则 TCSEC，俗称**橘皮书**，是美国国防部在 1985 年发表的一份技术文件，制定该准则的目的是向制造商提供一种制造标准，同时向用户提供一种验证标准。