职规作业_专业分析报告__2021学年秋学期周三蔡云班made by fcr，syc，fyf

信息安全

信息安全定义

在分析信息安全这个专业之前，我们有必要了解什么是**信息**。信息论奠基人香农（C.E.Shannon）认为：信息是用来消除随机不确定性的东西。说的通俗一点，信息是反应事物内部属性、状态、结构、相互联系以及与外部环境的互动关系，减少事物的不确定性。信息不同于消息，信息是消息的精准概念；信息也不同于数据，信息是数据的内涵。而我们这里常称的信息，其实更多的与**信息技术（Information Technology，IT）**有关。信息技术，是用于管理和处理信息所采用的的技术的总称。信息技术包括**生产**和**应用**两个方面，信息技术生产主要体现在信息技术产业本身，包括计算机软件、计算机硬件、设备制造、微电子电路等；信息技术应用体现在信息技术的扩散上，包括信息服务、信息管理系统等。而这些便是信息安全的主体。

所谓信息安全，就是关注信息本身的安全，而不管是否应用了计算机作为信息处理的手段，所以信息安全其实是非常交叉的一门学科，集计算机、通信、数学、法律、电子、管理等学科为一体的国家重点发展交叉学科，是研究信息获取、存储、传输和处理中的安全保障问题的一门学科。信息安全专业确保信息安全的科学与技术，培养能够从事计算机、通信、电子商务、电子政务、电子金融等领域的信息安全高级专门人才。

信息安全专业这个名字听起来普通且冷门，但随着5G智能时代的到来，安全得到了无论是国家还是民众空前的重视，国家和互联网大厂也是对信息安全专业的人才有迫切的需求。近年来，更是有不少关于信息安全的法律法规陆续出台，于2018年5月开始实施《信息安全技术个人信息安全规范》和2020年1月开始实施《密码法》，国家重视程度可见一斑。

目前，全球信息安全产业呈现出三大特点：其一，网络安全威胁危害性进一步增大，并且呈现出的攻击手段多样化、工具专业化、目的商业化、行为组织化等特点；其二，移动互联网在为用户带来便捷服务的同时，也为恶意软件的传播提供了快捷通道，致使网络安全攻击呈现明显的趋利性特征；其三，行业整合仍是产业发展的主旋律，企业通过人才、技术、市场等资源的整合，加快提升核心竞争力。

采用何种方式了解该专业

- 百度百科
- 信息安全全国几所知名大学的培养方案
- 知乎，举例：https://www.zhihu.com/question/336570836/answer/1786350375?utm_source=wechat_session&utm_medium=social&utm_oi=1386759243928760320&utm_content=group3_Answer&utm_campaign=shareopn
- CSIP之家，信息安全人才之家课程：首页-CISP之家官网,CISP/NISP认证服务中心
- 查找文献，知网等

学习所需要的特质

信息安全面临的大多是极为复杂的、隐蔽性很强的难题，不仅单个问题难度大，而且涉及面广、影响面宽，许多重大问题的关联范围已经超越计算机、工业、数学等理论和技术学科，其范围已经扩展至经济学、社会学、心理学等学科。因此，需要采用**全新的思维、架构、技术**来应对棘手问题，发展网络空间安全学科和信息安全，同时需要有**交叉学科**的知识。作为信息安全专业的学生，应该具有**大安全的观念，敏锐的眼光和清晰的思路，丰富的计算机、通信和电子等多学科知识和过硬的解决问题的本领**，既能够从纷繁复杂的表面现象背后找到实质问题，即**发现问题的能力**，也有运用**创新思想**，独辟蹊径地解决难题的能力。同时，作为信息安全学子，我们需要有**强烈的国家使命感和责任心**，愿意为人民、国家服务的决心和热情，性格上注重**细节**，能够**沉得住气**研究，有板凳甘做十年冷的魄力。最后，**兴趣**是最好的老师，学习信息安全专业的重要前提就是喜爱甚至是热爱信息安全技术，对相关知识和技术怀有强烈的**好奇心**，愿意为信息安全领域的研究和技术开发锐意探索、孜孜以求。

对于不符合的同学，提供建议

1.习惯Trust no one & What if.. & Risk management的思维方式

首先，对所有事情抱有怀疑的态度，具有独立的判断力，从而善于发现问题。其次，广泛的尝试各类手段，尤其是非常规方法，进一步找寻矛盾结点。最后，风险评估，对所有可能发生的事情的概率和后果做一个预测，并且制定预案减少事件发生时的损失(mitigation plan)。全面的思维方式有助于培养对细节的关注能力。

2.不断激发求知欲与创新意识

充分利用身边的一切资源来获得感兴趣学科的有关知识，对一切存疑的点主动深究。同时注意摆脱思维定势，避免惯性思考，从不同角度看问题，用新方法解决问题，可以通过多与人交流，进行头脑风暴来获得更多元视角与更发散的思维。

3.了解历史与现在

从中华民族的历史中，尤其是中国近代史中培养自身的国家使命感和责任心。同时熟悉国家当下面临的境况，审视世界的局势，进而激发自身为中华民族伟大复兴奋斗的使命感。

4.以兴趣为导向

信息安全相对枯燥，唯有兴趣支撑才能保持长久的研究学习，没有十足的兴趣还是建议三思。

前置能力

1. 长期的学习能力 理由是：计算机技术发展日新月异，新技术层出不穷。
2. 知识的迁移和联系能力 理由是：信息安全专业包含的内容很广，同时需要相当的深度。
3. 基本的编程能力 理由：起码要会写程序，看程序。
4. 扎实的数学基础与大量的数学知识 理由：数学本就是计算机的基础，信息安全中的密码学以及一些攻击手段等需要的算法离不开强大的数学能力。

高考改革后应选何种科目

3+3省份（如浙江）

建议选择：物理+技术+政治

理由：1.物理，锻炼思考问题的严密性、逻辑、抽象思维等方面，而且是绝大多数高校工科招生的必选科目。

2.技术，浙江特有选考科目，提前学习VB知识，能够有抢先一步的编程基础。

3.政治，文理结合避免单一思维，树立正确的价值观并培养强烈的国家使命感和责任心。

3+1+2省份（如江苏、河北等）

建议选择：物理+政治+化学/生物

理由：1.物理，锻炼思考问题的严密性、逻辑、抽象思维等方面，而且是这些省份理科生必选科目。

2.政治，文理结合避免单一思维，树立正确的价值观并培养强烈的国家使命感和责任心。

3.化学/生物，锻炼理科生的思维能力，逻辑严密性等必备素养。

如何培养

1. 让学习变成习惯。找到自己的最佳学习时间， 最好每天都能有半个到一个小时保持热度，每周至少有两块完整的、单块大于2个小时的时间， 用于集中突破。这样一周大约10个小时左右，这样的时间投入，不大可能同时突破两个领域， 因此一段时间内应该设定一个学习主题， 围绕这个主题来安排你的学习计划；让学习变得有趣。好奇意味着我们并不仅是为了功利的目标而学习， 而是认识更广阔的世界本身就是一份奖赏。永远不要失去神圣的好奇心。每一个小孩天然都是好奇的，他们常常因为一些新的发现高兴一整天。不幸的是由于我们的教育体制， 好奇心在成长的过程中被压制、磨灭。如果我们能回归本心，找回这个本源动力， 学习对于我们来说将绝不会是一种负担，而是一种乐趣。
2. 注重理解知识的深度，而非广度。要想在能力上快速提升，需要以慢为快，在学习过程中如何慢下来吃透知识的的硬功夫。当接触一个新的有价值的理论时，追问自己还有哪些现象可以被这个理论所解释，将新的知识和原有的知识产生链接；追问自己我的哪些行为可以被这个知识所改进，将来我能用它在什么地方。提前训练我们将来应用这个知识的场景，就可以成为一种自发触动机制；追问自己学了这个知识不能够用在什么地方。因为所有的知识都是有它的使用边界的，防止生搬硬套。我们要对既有的经验中得出的知识做抽象处理触及问题本质，同时去掉不相干的因素避免干扰，才能得出适用范围更广的知识。
3. 养成制定学习目标的习惯，长短期目标结合；采用多途径结合的学习方法（课堂学习、自学等）；定期复习总结。
4. 进行知识结构构建；转换问题情境，采用“变式”扩展法与“类化”的归纳法；克服思维定势的影响，培养求异精神和发散思维能力。
5. 利用MOOC、B站等平台学习C、Java、Python等编程语言的基本编写知识，了解编程的框架；自行购买教材学习，旁听其他计算机老师的基础课程；自己找题练手。
6. 及时消化新学的数学知识，搭建数学框架；主动涉猎更多能应用于计算机算法的数学知识。

优秀毕业生需要具备怎样的能力

现在安全行业的现状基本是：上层人才极度匮乏，下层人才极度饱和。因为信息安全领域太大太杂了，所以有很多优秀毕业生的专业能力不够精，不够强，所以造成了安全行业的现状。

按三种能力，暂时分成了以下能力

- 专业知识能力：坚实的数理、计算机编程及相关技术、工程知识基础、网络安全技术、通信技术方面的知识，优秀的科研及工程实践能力，包括创新、想象和动手能力，较好的人文社会科学素养。具有较强的信息安全分析、设计及开发能力。了解本领域技术前沿和发展趋势，具有较好获取新知识和新

技术的能力。具有良好的工程实践能力和科学研究能力，具有综合运用理论和可持续发展等方面的方针、政策和法律、法规，能正确认识工程对于客观世界和社会的影响。

- 可迁移能力：较强的沟通表达及职业发展能力，包括外语、文档写作和交流表达能力；具备一定的领导及组织管理能力。对终身学习有正确认识，具有不断学习和适应发展的能力
- 自我管理能力：厚基础、高素养、深钻研、宽视野的高素质、创新型本科生。思想、道德、文化素质高，有国家情怀和责任担当，身体强健。具备完整的认知结构、坚强的意志品质、较强的抗挫折能力、良好的人际关系，心理健康，乐观向上，积极主动。

与其他专业联系

1. 数学：信息安全本就是一门交叉学科，虽然表面侧重计算机科学，但数学是其基础，数学为底衍生出来的算法框架、逻辑语言在信息安全专业的实际应用中不可或缺。其中，离散数学更是作为计算机有关专业的专业课程，是计算机科学的核心。
2. 密码学：本身即作为数学和计算机科学延伸出的分支，与信息论密切相关。注重的加密、脱密等过程，也是信息安全的重要关注方向。该专业关注的文字、数码、语音、图像、数据与信息安全专业关注点高度一致。
3. 法学：《中华人民共和国数据安全法》《中华人民共和国网络安全法》的出台揭示了信息安全专业与法学密不可分的关系。修读信息安全专业的学生必须要具备基本的法学知识，以维护信息安全、维护法律尊严为基本任务，在法学的框架下才能规范的应用信息安全的知识来实现对信息安全的保护。而南开大学在2006年便开设了信息安全专业与法学双学位。
4. 社会学：在信息时代，大众与信息的密不可分便注定了信息安全需要考虑到社会影响、大众心理、伦理关系等各类社会学方面的因素。信息安全脱离了社会学会变得无用武之地。

目前前沿研究领域

目前前沿研究领域是信息系统安全的理论、信息系统的安全威胁、信息系统安全技术、信息系统的安全保障，主要大方向包括网络安全、系统安全、应用安全、数据安全（密码学）等内容。

- 数据安全：云数据安全，安全多方计算，差分隐私，加密数据库技术、
    - 区块链安全：智能合约分析，共识算法设计，数字货币攻击溯源，电子钱包安全，区块链监管
- 应用与网络系统安全：涵盖网络与通信安全、无线与移动安全、云及边缘计算安全、网络主动防御、多媒体与内容安全、软件安全、金融与支付安全，空天一体化通信、漏洞挖掘、网络攻防等方向。 以大数据安全相关技术为重点突破方向，研究包括基于大数据的软件定义网络安全与测量，恶意机器学习，网络空间主动防御等。

操作系统安全包括程序分析技术，形式化安全技术，软硬件安全协同技术，RISC-V安全技术

- 应用安全
    - 物联网与工控安全：涵盖工业控制系统安全、关键基础设施安全、智慧城市、智能制造、智慧医疗、智能交通与物流、物理层安全等方向。以关键行业控制系统安全为重点突破方向，研究包括跨层综合的安全解决方案与技术，协议设计与实现统合的安全模式，行业数据驱动的安全优化和创新等。 可信感知与移动安全，物联网设备安全，生物认证技术，测信道安全技术
    - 硬件与通信系统安全：涵盖通信系统安全、电磁波攻防、器件安全、安全芯片设计、侧信道安全、低截获与隐蔽通信、计算机体系结构安全、以及车联网与自动驾驶安全、电网安全等应用方向。以通信和计算系统跨层安全理论与关键技术为重点、以核心器件和系统芯片安全为载体，研究与工业界、产业界紧密结合的重要相关课题。
    - 人工智能安全：算法与模型安全，对抗性样本攻击，可证明安全性

著名期刊

国外：

- 《(IN)SECURE Magazine》 出版方：net-security 国外著名的一本信息安全杂志，提供PDF下载
- 《Virus Bulletin 》 在线杂志，建立于1989年，主要关注计算机恶意软件的防御、检测、清除以及遭受攻击后数据的恢复，为电脑用户提供anti-malware 的相关技术资料，目的在于促进反恶意软件领域的发展。在其官方网站上有提供该杂志的PDF文件以及在线HTML浏览。
- 《hakin9》是一部关于hacking与IT安全的半月刊收费杂志，主要关注计算机系统渗透与防御技术。该杂志提供了各种语言版本，并在各国发行，主要有以下几种语言：英语、法语、西班牙语、波斯语、德语、意大利语、捷克语。
- 《phrack》创刊于80年代，是世界级的顶级黑客杂志，每年只有一期，纯TXT风格的

国内：

- 《信息网络安全杂志》公安部出的杂志，偏向于学术派研究。
- 《Ph4nt0m Webzine》电子杂志，由国内著名的安全组织幻影旅团Ph4nt0m创办于08年，主要关注于关注于于漏洞分析、加密解密、协议安全分析、后门与rootkit技术、web应用安全、系统底层分析、操作系统安全性、企业安全防护方案等等。

- 《信息安全研究》创刊于2015年10月，是由中华人民共和国国家发展和改革委员会主管、国家信息中心主办的期刊，系统报道信息安全技术领域的科研成果，刊登信息安全研究领域原创性研究成果。
- 《网络与信息安全学报》创刊于2015年，是中华人民共和国工业和信息化部主管、人民邮电出版社主办的信息安全领域的学术刊物，刊载信息安全领域有突破的基础理论研究、创新性的关键技术研究、热点安全问题研究，以及与信息安全技术相关的交叉领域的科研学术论文。

期刊补充（与计算机有关）：

- 《Journal of the ACM》(JACM) ACM（Association for Computing Machinery 国际计算机学会）的官方学刊，受到最广泛的尊敬。
- 《计算机学报》是中国计算机领域的权威学术刊物。 其宗旨是报道我国计算机科学和技术领域最高水平的科研成果。《计算机学报》创立于1978年，以中文编辑形式与读者见面，同时以英文摘要形式向国际各大检索系统提供基本内容介绍。 本刊是中国计算机领域的代表性学术刊物，作为科学研究档案，代表了计算机领域各研究阶段的水平。
- 《计算机研究与发展》(月刊)创刊于1958年，中国科学医院计算技术研究所，中国计算机学会主办。刊载内容：计算机科学技术领域高水平的学术论文，最新科研成果和重大应用成果。刊载内容：评估、计算机基础理论、软件技术、信息安全、计算机网络、图形图像、体系结构、人工智能、计算机应用、数据库技术、存储技术和计算机相关领域。
- 《计算机科学与探索》是由中国电子科技集团公司主管、华北计算技术研究所主办的国内外公开发行的高级学术期刊。报道计算机(硬件、软件)各学科具有创新性、前沿性、开拓性、探索性的科研成果。

最新热点

随着移动互联网、物联网的发展，信息安全已经从原先保护虚拟资产，逐渐转向保护实体资产（如在线金融）、甚至人身安全（车联网、健康医疗联网等），保护的资产价值越高，对用户的意义就越大，对安全的要求也越来越高。

云安全、人工智能安全、虚拟化安全、无线安全、支付安全等等新课题也会浮出水面。

专业就业方向

大体有以下方向：

- 威胁猎手
- 系统、网络和/或 Web 渗透测试员

- 网络/终端取证分析师
- 事件响应员
- 网络和安全架构师
- 恶意软件分析师
- 软件测试工程师
- 网络安全分析师/工程师
- 媒体搜证分析师/司法计算机犯罪调查员
- CISO/ISO 或安全总监
- 安全运营中心分析师
- 漏洞研究员/漏洞利用程序开发者
- 安全审计和风险管理专家
- 安全软件开发者
- 移动安全经理
- 应用程序渗透测试员
- 灾难恢复/业务连续性分析师/经理
- 技术总监和副CISO
- 入侵分析师
- 物联网/关键基础设施安全总监

以下详细介绍一些就业方向

威胁猎手

每天都能感受狩猎的刺激！每个案例都是如此独特！

工作职责描述

分析攻击者如何渗透基础设施，识别已经被入侵的系统/网络。调查复杂攻击留下的痕迹需要取证专家不仅精通最新取证、响应和逆向工程技术，还要熟悉最新的漏洞利用方法。

价值亮点

威胁捕手在公司与黑客/恶意软件之间增加了一个重要的安全防御维度。

过去两年间，在安全运营中引入了威胁追捕职能的公司企业，入侵到检测的耗时从数月缩短到了数周。成功捕捉威胁的关键在于终端&网络分析技术与威胁情报的融合。

系统、网络和/或 Web 渗透测试员

在安全防御实战化的今天，企业内部的 “白帽子” 渗透测试专业人士是企业培养 “攻击性思维” 和主动式防御的关键环节。

工作职责描述

找出目标系统、网络和应用程序中的安全漏洞，帮助企业巩固安全。通过识别出哪些漏洞可被利用而导致业务风险，渗透测试员能提供最紧迫问题的重要洞见，并对如何排序安全资源给出合理建议。

价值亮点

“你才是那个企业网络安全与否的终极确认者。你需要用过人的智商、毅力和创造力来突破企业网络安全的每一道防线，找出可利用漏洞的位置，以便能够在坏人染指之前自补。道德黑客/渗透测试人员是当下炙手可热的顶级网络安全人才。”

CISO/ISO 或安全总监

领导安全运营仍然是信息安全领域中最重要、最酷的工作。

工作职责描述

当今首席信息安全官的职责不再与以往相同。尽管仍然是技术人员，今天的 CISO/ISO 必须拥有商业洞察力、沟通技巧和面向过程的思维方式。他们需将法律、监管和企业自身要求与风险承受、预算限制和技术采纳结合起来。

价值亮点

“你可以极富创意地影响公司的整体安全，为提升公司安全做出直接贡献。你是企业安全的顶级玩家，CEO 唯一信任的人。”

“这一职位通常向高层报告，能够看到并影响大局。你的工作伙伴包括实体安全部门、IT 部门、业务部门，甚至国家安全和相关司法机构。”

“你就是大老板，可以决定谁做什么、谁得到什么，激励你的手下，然后与他们分享成果。你每天都在产生切实的影响。”

安全软件开发者

很酷的头衔，目前还属于极为珍稀的 “物种”，如果说 DevOps 和敏捷化是少数头部企业才能玩转的法拉利赛车，那么优秀的 DevSecOps 安全开发者就意味着你需要给法拉利装上防弹钢板和全新引擎，不降低其圈速，而且把引擎的寿命从 400 公里提高到 40 万公里，难度可想而知。

工作职责描述

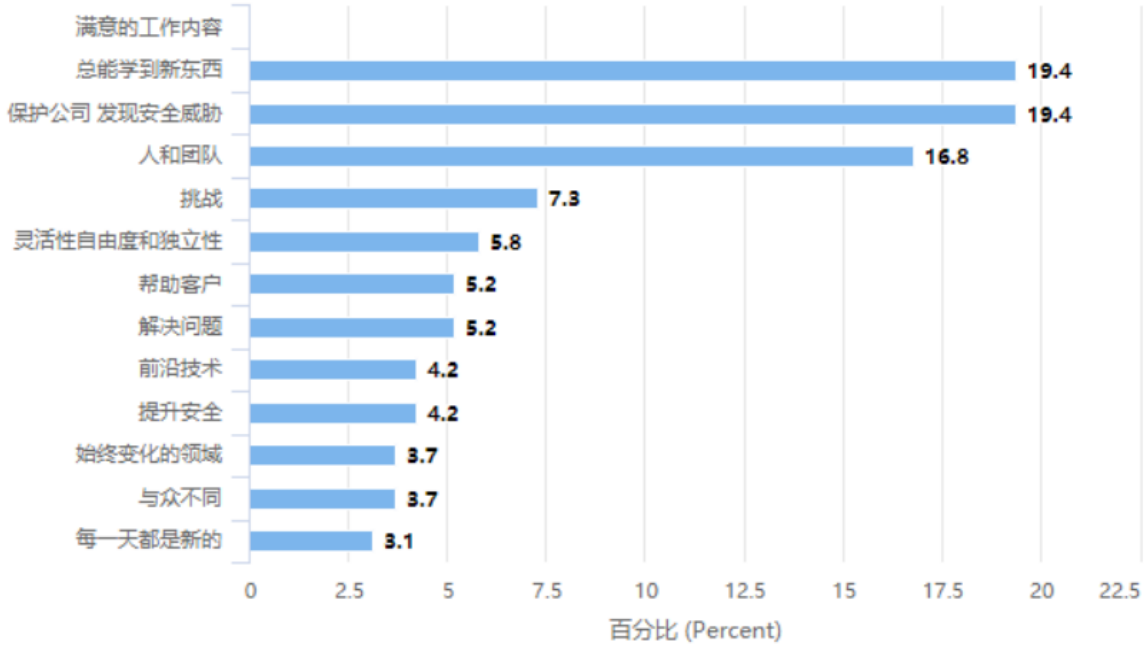
注重安全的软件开发者，在安全软件开发方面超越所有开发人员，实现不含逻辑设计漏洞和技术实现缺陷的安全编程技术。此类专家最终负责确保客户软件没有可被攻击者利用的漏洞。

价值亮点

再好的安全架构或策略都“遭不住”编写糟糕、满是漏洞的不安全软件。如果在最初开发的时候就注重产品的安全，又何须事后返回去添加安全措施。

代码级安全是应用安全的根本所在。这些人是撑起当今软件世界的中流砥柱。

附上《**安全从业人员对安全职业最满意（最看重）的要素**》



《 安全岗位的满意度指数：冰火两重天》