

정보보안학과 전공 교과목 해설

(1-1) 정보윤리 (전선/3-3-0) (Information Ethics)

정보통신 윤리를 체계적으로 학습함으로써 사이버 공간에서 발생하는 도덕적 문제점들을 해결하고 올바른 정보통신 윤리의식을 정립한다. 정보화 사회의 발달, 정보통신 윤리이론, 사이버 문화와 예절, 정보화 역기능과 대처방법, 정보통신 윤리 지도방법 등을 통하여 올바른 정보통신 윤리를 제시한다.

(1-1) 프로그램 기초 (전선/2-1-2) (Program Base)

프로그램 작성의 기초과정으로 프로그램의 구문적인 구성과 문법, 논리적인 기술을 통해 구현하려는 알고리즘을 완성하는 과정을 학습한다. 프로그램의 작성과 컴파일, 디버깅 과정을 통해 논리적인 구현과 문제해결, 입출력 내용의 제시 형식 등을 설계하고 완성하는 과정을 실습한다.

(1-1) 네트워크 일반 (전선/3-3-0) (Computer Practice)

다양한 환경에서 활용되는 컴퓨터의 기능을 이해하고 응용하기 위해 시스템 관리, 보안, 메일, 파일관리, 문서의 변환, 멀티미디어 자료들의 변환과 편집, SNS 등을 그에 적합한 유틸리티를 이용해서 처리할 수 있는 방안을 제시한다.

(1-2) 프로그램 응용 (전선/2-1-2) (Program Application) (Program Base)

프로그램 작성의 응용과정으로 프로그램의 구문적인 구성과 문법, 논리적인 기술을 통해 구현하려는 알고리즘을 완성하는 과정을 학습한다. 프로그램의 작성과 컴파일, 디버깅 과정을 통해 논리적인 구현과 문제해결, 입출력 내용의 제시 형식 등을 설계하고 완성하는 응용 과정을 숙달시켜 실무에 적용하고 업무 개발 수준에 이를 수 있도록 실습한다.

(1-2) 정보보안일반 (전선/3-3-0) (Information Security)

정보화 시대에서는 정보보호 크게 취약성, 기밀성, 가용성 중요성을 가지고 있다. 정보 보호의 관리적 대책과 위험관리, 위험분석에 대한 체계적인 대응이 필요하다. 정보보안을 통해 암호화 기법, 해쉬함수에 의한 키분배 및 관리등을 알아본다. 개방형시스템 상호연결에 따른 유,무선 보안 기술 도입 및 운영관리에 대한 정보보안 원리를 학습한다.

(1-2) 운영체제론 (전선/3-3-0) (Operating System)

시스템 관리를 위한 리눅스 유닉스 셸과 아파치 프로그래밍(Apache programming)을 목표로 LINUX/UNIX 명령어 익히기부터 BORUNE SHELL, C SHELL, BASH 익히기, APACHE CONFIGURATION 프로그래밍 등의 분야를 이론과 실습으로 학습한다.

(2-1) JAVA 프로그래밍 (전선/3-2-2) (JAVA Programming)

객체지향 언어의 새로운 프로그래밍 기법들을 실습하여 익히는 것이 목표이다. 이를 위해 클래스 및 객체의 정의, 클래스 추상화, 상속, 다중상속, 메소드, 정보 은닉 등 객체 지향 프로그래밍 언어의 개념들을 체계적으로 강의하고 실제로 Java 언어를 이용하여 실습한다.

(2-1) 데이터구조 (전선/3-3-0) (Data Structure)

데이터의 특성 및 레코드 간의 관계를 논리적 관점에서 이해하고, 리스트, 배열, 트리, 그래프, 큐, 스택, 테

이블, 파일 간에 관련성과 구조를 다룬다. 데이터 개체의 집합과 그 원소들 사이에 적용되는 연산의 의미를 살펴보고 추상적인 데이터와 알고리즘의 구현을 통하여 프로그래밍의 세계를 접목시키는 방법을 이해한다.

(2-1) 파일처리론 (전선/3-3-0) **(File Processing)**

파일처리란 대량의 데이터를 컴퓨터로 기억하여 그것을 관리하며, 그중에서 필요한 데이터를 검색해서 요구하는 형식으로 출력하는 등, 대량의 기록을 여러 가지로 처리에 대하여 학습한다. 파일저장장치, 순차파일, 정렬과 합병, 직접파일, 인덱스구조, 다중키 파일, 데이터 표현과 압축, 파일보안, 데이터베이스 상세항목에 관하여 논한다.

(2-1) 그래픽 프로그램 (전선/3-2-2) **(Graphic Program)**

직선그리기와 다각형 채우기를 비롯한 저수준 기법들의 알고리즘(Algorithm)들을 대화식 그래픽스 프로그램(interactive graphic program)의 작성을 배우면서 다룬다. 광-재질 상호작용, 음영, 모델링, 곡선과 곡면, 앤티앨리어싱, 텍스처 매핑, 합성 등의 응용 기법들을 학습한다.

(2-1) 데이터통신 (전선/3-3-0) **(Data Communication)**

데이터 통신 시스템에서는 데이터의 전송과 전송제어를 기본으로 컴퓨터간의 데이터 동기화를 알아본다. 데이터 전송원리는 노드들간의 회선교환 방법, 네트워크의 구성기법, OSI 참조모델에 따른 각 계층간의 데이터 전송 원리파악하고 지역간 네트워크 연결에 의한 데이터 전달 등을 다룬다

(2-1) 암호학 (전선/3-3-0) **(Cryptology)**

정보보호 필요성에는 인증, 식별, 지문인식을 통하여 무결성, 기밀성, 가용성에 의미를 가지고 있다, 각종 암호화 알고리즘을 통하여 정보를 암호화와 복호화를 위한 키(key)의 이용과 송신자와 수신자가 키를 가지고 복호화하는 방식 등을 통해 암호화 기술을 학습한다. 또한 송신된 메시지의 인증, 송신자의 개인식별이나 디지털 서명 등을 위한 기술도 학습한다.

(2-1) 개인정보 암호화 (전선/3-3-0) **(Personal Information Encryption)**

보안 침해란 개인정보의 보안, 기밀성 또는 무결성을 침해하는 컴퓨터 데이터의 비인가된 획득이다. 특정 개인 정보는 각종 번호와 문자, 그래픽 데이터로 이루어지는데 이들의 생성, 처리, 저장, 전송 등의 과정에서 비인가된 침해 사고가 발생하지 못하도록 하여 개인의 권익에 손해가 없도록 다양한 기법 중 암호화에 대하여 학습한다.

(2-1) 민간경비론 (전선/3-3-0) **(Theory of Private Security)**

안전정 보안 관리제도 운용의 기본원칙과 절차, 민간경비의 기능, 내부경비 및 외부경비, 절도와 화재의 예방, 컴퓨터의 안전관리, 한국 민간경비 산업의 과제의 발전방안 등에 관하여 연구한다.

(2-2) 네트워크 보안 (전선/3-3-0) **(Network Security)**

컴퓨터 네트워크 기본으로 통신 계층인 OSI 7 계층 모델과 TCP/IP 계층구조를 이해하고 각 계층별 정보 전달에 따른 프로토콜을 학습한다. 물리적 보안과 정보 보안을 융합한 보안 개념으로, 각종 내외부적 정보 침해에 따른 대응은 물론 네트워크를 포함한 물리적 보안 장비 및 각종 재난·재해 상황에 대한 관제를 포함하는 포괄적인 보안시스템을 학습한다.

(2-2) 디지털논리 (전선/3-3-0) (Digital Logic)

디지털 논리의 개념, 신호 정보 처리의 기초, 프로그램 가능한 논리 동작 등에 대한 기본적인 내용을 학습한다. 디지털 논리회로 해석 및 디자인의 대한 체계적인 내용뿐만 아니라, 정보 보안을 위한 디지털 신호의 근본 동작 원리를 자세히 다룬다.

(2-2) 암호화 알고리즘 (전선/3-3-0) (Encryption Algorithm)

네트워크를 이용한 각종 응용에서 필요한 정보보호 서비스를 제공하기 위한 핵심 기술과 전통적인 암호 기술에서부터 최근의 각종 암호 알고리즘들까지 학습한다. 이를 위해 대칭키 암호, 비대칭키 암호, 암호학적 데이터 무결성 알고리즘 등을 프로그램으로 구현하기 위한 이론적인 내용을 학습한다.

(2-2) 데이터베이스 (전필/3-3-0) (DataBase)

하나의 데이터베이스 관리 시스템을 구축하는 데 있어서 개발된 컴파일러 도구나 저장 관리자들을 이용하기 때문에 전체적인 데이터베이스 관리 시스템 자체의 구축에 대한 근본적인 이해를 목표로 간단하게 관계형 데이터베이스 관리 시스템을 설계하고 구현한다.

(2-2) GUI 프로그래밍 (전선/3-2-2) (GUI Programming)

C언어 개요, C/C++ 개발 환경, 상수와 변수, 수식과 연산자, 제어 명령문, 파생 자료형, 윈도우 프로그래밍 개요, 윈도우에서의 입출력, 리소스 등의 윈도우즈 환경에서 프로그램을 개발하기 위한 기본 문법과 윈도우, 타이틀바, 컨트롤 아이콘과 박스 등의 윈도우즈에서 사용되는 프로그램 리소스를 프로그래밍 하는 방법을 학습한다.

(2-2) 커널 프로그래밍 (전선/3-2-2) (Kernel Programming)

컴퓨터의 기본 구조, 가상기억 시스템, 멀티프로그래밍, 시 분할, 프로세스 구조 및 프로세스 스케줄링 등의 기본 개념과 이에 따라 발생하는 여러 문제들을 강의하고, 시스템 호출과 입출력 서브시스템, IPC 및 소켓 등을 학습한다. 그리고 중앙 처리 장치, 주기억장치, 주변 장치, deadlock, 병행 프로세스, 병행 프로그래밍 등에 대한 이론 및 관리 기법을 강의한다.

(2-2) 방화벽 구성 (전선/3-2-2) (Firewall Configuration)

서로 다른 보안환경을 갖는 네트워크나 호스트 사이의 네트워크 데이터를 통제하는 프로그램이나 장비를 방화벽이라 한다. 다양한 방화벽 장비에 대한 구성 방법에서 운영에 이르기까지 자세한 통제방법 명령과 이에 수반하는 구성환경과 정책, 요구사항, 룰셋 등을 학습한다.

(2-2) 서버 관리 (전선/3-2-2) (Server Management)

서버 운영 전반에 관한 이해력을 향상시키고 운영환경을 구축할 수 있도록 학습한다. 서버 운영의 기본 개념과 서버의 특징, 설치 과정, 부팅방법, 자주 사용하는 명령어, 프로그램 관리, 웹 개발 및 운영 환경 구축 등을 실습과 이론으로 학습한다.

(3-1) 웹 어플리케이션 (전선/3-2-2) (Web Application)

서버와 클라이언트 사이의 정보교환을 위한 Perl, ASP, PHP나 VB SCRIPT등 웹에서 사용되는 프로그래밍 언어에 대해 학습하고, 각 언어들을 이용하여 실제로 웹 응용프로그램을 구현하고 원활한 정보교환을 위한 방법들을 실습한다.

(3-1) JAVA 프로그램 응용 (전선/3-2-2)

(JAVA Programming Application)

플래시 빌더에 대한 사용법과 플렉스 SDK를 사용한 애플리케이션 개발에 대한 이론과 웹 서비스 아키텍처 및 애플리케이션 서버와 애플리케이션을 연동하는 방법을 학습한다. 또한 웹과 데스크톱용 플렉스 애플리케이션을 개발하고 배포하는 데 필요한 레퍼런스, 튜토리얼 등을 활용하는 방안을 제시한다.

(3-1) 소프트웨어공학 (전선/3-3-0) (Software Engineering)

소프트웨어의 라이프 사이클을 축으로 하여, 프로그램의 개발 단계로서 소프트웨어의 사양과 요구 사항 분석, 개략 설계, 정밀 설계, 코딩 및 시험 운영 그리고 유지 보수 등의 방법론을 학습한다. 소프트웨어 설계 방법으로 자료 흐름 중심의 설계, 대상 중심의 설계, 자료구조 중심의 설계 등을 강의한다. 도메인 분석, 소프트웨어 설계, 구조적 프로그래밍, 자동 코딩, Reverse Engineering 등 여러 가지 방법론을 소개하며, 소프트웨어 문서화와 유지, 프로젝트 관리 등에 대한 내용도 다룬다.

(3-1) 사이버범죄론 (전선/3-3-0) (Theory of Cyber Crime)

컴퓨터의 발달과 IT 융복합 서비스의 진화로 인한 각종 사이버 범죄, 즉 정보유출, 전자상거래, 전자화폐, 신용 카드, 보험관련 범죄 등의 IT 활용 범죄 현상을 분석 검토하고 그 해결방안을 모색한다.

(3-1) 정보보안기술 (전선/3-3-0) (Information Protection Technology)

개인정보를 관리하는 관리자뿐만 아니라 개인정보의 주체인 각 개인에도 개인정보관리의 중요성을 일깨우기 위해 개인정보보호 법률과 제도, 개인정보 소송사례, 개인정보의 기술적 보호대책, 개인정보 유출방지시스템, 개인정보 영향평가 시스템, 데이터베이스 방화벽, 데이터베이스 방화벽 구축, 보안서버, 개인정보 운영센터 등을 학습한다.

(3-1) 해킹 및 악성코드 (전선/3-3-0) (Hacking and Malignant Code)

네트워크 공격은 물론, 악성코드에서 사용되는 기법과 관련된 구현원리를 학습하고 그것에 대한 응용기술을 습득한다. 특히 와이어샤크뿐 아니라, 버퍼 오버플로우 공격코드 등의 구현원리를 학습하고 아울러 DLL 인젝션 기법 등에 대해서도 이해하고 응용기술을 이해한다.

(3-1) 시스템보안 (전선/3-3-0) (System Security)

컴퓨터 보안의 개념적인 정의에서부터 구체적인 기술 도입과 진단 방법에 이르기까지 실무에서 사용되는 기술들을 학습한다. 특히 네트워크 보안업무 및 운영체제의 시스템상 취약점을 분석하고 파악하여 정보 보호한다. 시스템 보안 구축 과정을 기획-설계-구축-운영으로 구분하고 각 단계에서 접근제어, 암호화, 작업결재, 취약점 분석과 같은 기술요소들을 도입하고 운영하기 위해 어떠한 계획과 활동이 필요한지 이해한다.

(3-1) 쇼핑몰 구축 (전선/3-2-2) (Shopping Mall Installation)

전자상거래를 위한 구성하기 위한 구매자, 상점, 지불시스템 그리고 인증기관 정보시스템과 정보통신 환경, 각 구성 요소 시스템의 기능과 관련 시스템들과의 상호작용을 이해하고 이들의 거래 정보와 관리정보를 안전하게 처리하기 위한 기술과 장비들을 이용하여 쇼핑몰-몰을 구축한다.

(3-1) 컴퓨터 구조 (전선/3-3-0) (Computer Architecture)

컴퓨터 구조 시스템에 자료의 표현과 연산 및 주기억장치의 구분과 원리, 중앙처리장치의 구조와 명령어 형식과 종류를 알아본다. 특히 제어장치에서 레지스터 전송, 마이크로 오퍼레이션 메이저와 타이밍 상태의 파악하여 연산장치와 주변장치와의 데이터 제어와 데이터 처리 흐름의 원리 분석하고 이해한다.

(3-1) 보안망 분석 (전선/3-3-0)

(Security Network Analysis)

보안시스템에 대한 전체를 다루는 보안 분석과정으로 보안과 해킹의 역사, 네트워크의 근본적인 흐름, 프로그램의 속사정, 암호의 원리와 응용, 보안 솔루션의 구성, 조직/사회적인 문제, 보안 전문가가 갖추어야 할 요건 등을 다룬다. 보안을 공부하거나 실무에 종사하면서 체득한 유용한 이슈를 학습한다.

(3-1) 현대사회와범죄 (전선/3-3-0) (Crime in Modern Society)

현대 산업사회와 정보화시대의 등장과 그로 인한 도시화의 역기능 등에서 나오는 각종 범죄, 즉 매춘, 약물 및 알콜중독, 인명경시, 노인문제, 정신병리, 물질만능주의, 소외감, 사이버 범죄 등의 현상을 분석 검토하고 그 해결 방안을 모색한다.

(3-1) 보안스크립트 기초 (전선/3-3-0) (Basic of Security script)

파이썬(python)은 스크립트 언어로 짧은 코드 적용으로 신속한 프로그램 개발이 가능하고, 저수준 영역인 커널 접근이 가능한 장점을 갖고 있어 보안언어로 많이 활용되고 있다. 최근에는 파이썬을 이용한 해킹보안 기술이 대두되고 있다. 파이썬 언어의 직관적인 코딩 기법과 GUI프로그래밍을 학습한다.

(3-2) 모바일 디바이스 관리 (전선/3-3-0) (Movable Device Management)

정보기기의 소형화와 이동성 증가에 따라 모바일 프로그램의 수요가 급격히 증가하고 있다. 이에 무선 환경에서의 앱 개발과 JAVA SDK 기초개념을 학습하고 관련 기기들의 관리 사항에 대하여 학습하는 과정이다. 자바의 기초문법, 객체지향 개념, 스레드, 예외처리 등을 바탕으로 앱의 설계, 구현, 배포 과정을 학습한다.

(3-2) 어플리케이션 보안 (전선/3-3-0) (Application Security)

컴퓨터 일반에 관련된 DNS보안, FTP보안, 메일보안, DB보안, 전자상거래보안 등을 분석과 방지에 대하여 학습한다. 컴퓨터 활성화에 맞추어 시스템의 실용화와 조속한 보급을 위해 인터넷 보안의 개념과 다양한 보안 기술 사항을 학습한다. 인터넷에 대한 기본 개념부터 전자상거래 현황, 대칭/비대칭 암호기법, 인증과 관련된 전자 서명 기법 및 응용 분야들을 학습하고 전자상거래를 위한 필수적 요구사항과 공개키 기반구조 그리고 전자지불 기술 등 전자상거래 시스템 구성과 관련된 필수 보안 기술을 학습한다.

(3-2) 멀티미디어 시스템 (전선/3-2-2) (Multimedia System)

멀티미디어가 인터넷 환경에서 정보전달에서 중요한 매체 역할을 한다. 기기의 소형화와 이동성 증가에 따라 시간과 장소에 관계 없이 실시간으로 급격히 증가하고 있다. 이런 환경에서의 디지털 영상처리 제작과 편집 및 동영상앱 개발과 JAVA 개념을 응용하여 기법을 배양하는 과정이다. 웹에서 자바의 객체지향 등을 바탕으로 설계, 구현, 배포 과정을 학습한다.

(3-2)(4-1) 컴퓨팅환경 1,2 (전선/3-3-0) (Computing Environment 1,2)

IT 패러다임을 바꾸는 새로운 컴퓨팅 환경은 클라우드 컴퓨팅이다. 클라우드 컴퓨터의 개념과 아마존, 구글, 마이크로소프트 등에서 제공하는 다양한 서비스와 애플리케이션에서 클라우드 컴퓨팅이 사용되고 있는 사례를 통해 이해한다. 또한 라이선스 모델, 투자 수익(ROI) 등 클라우드 컴퓨팅의 가치 비용 평가법을 소개하여 실제 클라우드 서비스를 구축할 수 있는 능력과 IT산업의 미래를 예측하는 데 필요한 다양한 정보를 학습한다.

(3-2) 모의해킹 1,2(전선/3-2-2) (Hacking Simulation(Permeation))

침투와 방어는 모의 훈련은 해킹의 전 과정을 습득하는데 필수적인 과정이다. 네트워크, 서버 시스템, 보호 장비 등을 소규모로 준비하여 실제 운영과 같게 준비한 후 공격과 방어의 두 부분으로 그룹을 나누어 서로가 임무를 바꾸어 가면서 해킹의 공격과 방어의 실제적인 내용을 학습한다.

(3-2) 네트워크 분석 (전필/3-3-0)
(Network Analysis)

네트워크 운영 및 분석에 대한 정의에서 출발하여 네트워크 문제점 해결 작업, 보안 작업, 최적화 작업 및 애플리케이션 네트워크 분석과 관련된 보안 이슈 이해를 학습한다. 네트워크 트래픽이 들어있는 파일의 안전성에 있어서는 원치 않은 ‘스니퍼’로부터 네트워크 보호에 대한 법적 이슈 운영 및 분석 작업 체크리스트 검토, 스위칭, 라우팅의 이해 등을 강의한다.

(3-2)(4-1) 서버보안 1,2 (전선/3-2-2)
(Server Security 1,2)

실무에서 활용할 수 있는 내용중심의 보안에 대한 시스템과 네트워크의 통합된 관점을 학습한다. 이를 위해 서버 설치 후 점검사항, 포트 점검 및 제어, 웹서버 보안, 메일 서버 보안, 큐잉서버를 이용한 메일 서비스 가용성 강화, 암호화, 바이러스 메일 필터링, Viruswall 설치, 스팸메일 차단, DNS 서버 보안, FTP 서버 보안, SQL 보안, 방화벽(Firewall) 구축 및 운영, 침입탐지시스템(IDS) 구축 및 운영, 네트워크 취약성과 대책 등을 학습한다.

(3-2) 개인정보보호법 (전선/3-3-0)
(Privacy Protection Law)

개인정보 보호법 시행에 따른 대응 전략, 성공적인 기업경영을 위한 개인정보 보호 강화 방안, 효율적인 개인정보 보호 솔루션 도입 및 구축사례, 사업자를 위한 개인정보 보호 등의 내용을 통해 정보보호 관련 법규의 내용을 학습하고 이해한다.

(3-2) 전자상거래 (전선/3-3-0)
(Electronic Commerce)

전자상거래를 위한 구성하기 위한 구매자, 상점, 지불시스템 그리고 인증기관 정보시스템과 정보통신 환경, 각 구성 요소 시스템의 기능과 관련 시스템들과의 상호작용을 이해하고 이들의 거래 정보와 관리정보를 안전하게 처리하기 위한 기술과 장비들을 이용하는 기술을 습득한다.

(4-1) 빅데이터 컴퓨팅 (전선/3-3-0)
(Big Data)

빅데이터 관련 분야중 특히 컴퓨팅기술에 대한 큰 개념을 인식시켜 줄 빅데이터에 대한 기본 개념 정의부터 시작해 빅데이터 처리 과정별 주요 기술을 익히며, 빅데이터를 위해 어떤 기술을 사용할 수 있으며 어떤 상황에 어떤 기술을 선택해야 하는 지에 대해 학습한다.

(4-1) 정보보호 정책(전선/3-3-0)
(Information Security Policy)

정보보호 정책 및 관리체계에 대해 강의를 진행한다. 아울러 정보보호법과 해킹사건사고 분석을 통해 정보 자산을 보호하기 위해 정보보호관리 절차와 과정을 체계적으로 수립 및 지속적으로 관리 및 운영하기 위해 구축한 종합적인 체계와 관련분야의 기술 및 정보보호 정책에 대하여 학습한다.

(4-1) 웹보안 프로그래밍 (전선/3-2-2)
(Web Protection Programming)

웹 해킹 및 웹 바이러스로부터 웹 애플리케이션을 보호하는 전용솔루션에 대한 요구가 증대되는 추세이다. 이런 기능을 갖춘 솔루션은 웹 프로그래밍 오류에 의한 역기능을 최소화하고, 방화벽에 의해 외부로 분리되지는 않지만 내부와는 DMZ 혹은 웹 구간을 방어하는 보안솔루션으로 지칭할 수 있다. 이러한 웹 보안 솔루션에 대한 구축과 활용, 관리 등에 대해 학습한다.

(4-1) 정보보호 특강(전선/3-3-0)
(Special lecture on Information Security)

고객의 정보 자원을 안전하게 지키기 위해 고객의 주요 IT 인프라 및 각종 보호 장비에 대하여 통합 보호 관리

솔루션과 체계적인 보호 관리 센터 등을 이용하여 정보보호 정책을 다루는 한편, 불법적인 침입도 막아 낼 수 있도록 감시 업무에 대한 내용을 특강 형식으로 학습한다.

(4-1) 정보보안 특론(전선/3-3-0)
(advanced Information Security)

고객의 정보 자원을 안전하게 지키기 위해 고객의 주요 IT 인프라 및 각종 보호 장비에 대하여 통합 보호 관리 솔루션과 체계적인 보호 관리 센터 등을 이용하여 정보보호 정책을 다루는 한편, 불법적인 침입도 막아 낼 수 있도록 감시 업무에 대한 내용을 학습한다.

(4-1) 정보보안 프로젝트 (전선/3-3-0)
(Information Security Project)

정보보안 프로젝트를 통해 정규 교과 과목에서 다루지 못하는 주요 관심 대상의 최신 기술 동향 및 주제를 파악하여 현장에서 필요로 하면서 수강자가 원하는 관련 기술들을 선정하고, 그 내용을 구체적으로 연구, 발표, 토론한다. 이를 통해, 졸업 후 실무에 직접 이용할 수 있도록 지도한다.

(4-1) 정보보안수행계획 (전선/3-3-0)
(Performance planning for Information Security)

사이버 침해사고 발생 건수가 지속적으로 증가하고, 해킹, 바이러스, 개인정보 유출 등 새로운 위협 요소로부터 정보보호 강화를 위한 종합적인 보안 체제 구축 방법 등을 학습한다.

(4-1) 하드웨어 프로그래밍 (전선/3-2-2)
(Hardware Programming)

SOC를 이용한 새로운 컴퓨터구조와 이에 적합한 알고리즘, 특수 목적용 프로세서(ASIC)의 설계방법을 공부한다. 주요 실습 내용으로는 소프트웨어 도구를 이용하여 실제적으로 프로세서 칩을 설계하고, 시간출력을 분석하는 방법을 학습한다.

(4-1) 컴퓨터시스템 (전선/3-3-0)
(Computer System)

보안 처리 시스템인 컴퓨터의 하드웨어 구조 및 특성과 설계방법을 강의한다. 각 구성 요소인 명령어 세트, 프로세서 구조, 파이프라인 처리, 메모리 구조 등을 연구하고 강의한다. 또한 컴퓨터 아키텍처 시뮬레이터를 이용하여 성능을 평가한다.

(4-1) 현장실습 (전선/ P/F)
(Practical Training)

실제 직무를 수행하면서 감독자 또는 선임자로부터 직무 수행에 관한 지식과 기술을 배우기 때문에 현장의 분위기와 실무를 익히는 데 적합하다. 이 훈련을 통해 직책의 성격이 기술·전문성·정밀성을 요구하는 경우의 훈련에 좋은 효과를 얻을 수 있다.

(4-2) 취약점 분석 (전선/3-3-0)
(Vulnerability Analysis)

악성 코드의 유포, 해킹 등 사이버 위협에 직간접적으로 노출되는 주요 네트워크 장비, 보안 장비, 시스템 장비와 주변 시설들에 대한 취약점 분석 작업을 통하여 사이버 위협을 낮출 수 있도록 하여야 한다. 취약점 분석의 계획 수립에서 대상 선별, 그리고 분석 수행과 평가를 학습한다.

(4-2) 리버스 엔지니어링 (전선/3-3-0)
(Reverse Engineering)

리버스 엔지니어링을 통해 소프트웨어에 대한 분석이나 자신이 만든 프로그램의 안전성을 테스트하는 방법을 학습할 수 있다. 또한 악성코드 분석 방법뿐 아니라, 안티 디버깅 기법을 학습함으로써, 크랙에 대비할 수 있다.

(4-2) 사물인터넷 (전선/3-3-0) **(Internet of Things)**

사물인터넷은 인간 주변의 모든 사물을 연결하고, 인간과 상호 소통할 수 있다. 헬스케어, 생활, 보안, 육아 등 다양한 분야에서 활용 가능한 사물인터넷 상품들에 대해서 소개하고, 각 산업 분야별로 보다 자세하게 살펴본다. 사물인터넷의 대표적 활용분야인 스마트홈에서 가정 내 사물들을 단순히 제어하는 기능, 화재, 침입 등 위험을 스스로 감지하고 차단방법 등의 핵심 주제를 강의한다.

(4-2) 디지털 포렌식 (전선/3-3-0) **(Digital Forensic)**

디지털 포렌식이란 PC나 휴대전화 등에 내장된 디지털 자료를 근거로 발생한 사실관계를 증명하는 보안 서비스 분야이다. 이를 위해 각종 디지털 데이터와 통화기록 등을 증거로 확보, 분석하는 것으로 증거 수집, 증거분석, 증거 제출과 같은 절차를 학습한다.

(4-2) 보안기술 특강 (전선/3-3-0) **(Protection Technology Special Lecture)**

정보보호 및 보안에 관한 종합적인 기술을 응용하여 활용할 수 있는 실습과 정보보안 전반적인 기술의 동향을 파악하기 위하여 자체 및 외부 관련 분야 인사를 초빙하여 특강을 청취하는 등 체계적이고 종합적인 보안 기술을 습득한다.

(4-2) 네트워크운영 특강 (전선/3-3-0) **(Topics in Network Operation)**

네트워크 운영 및 분석에 대한 정의에서 출발하여 네트워크 문제점 해결 작업, 보안 작업, 최적화 작업 및 애플리케이션 네트워크 분석과 관련된 보안 이슈 이해를 학습한다. 네트워크 트래픽이 들어있는 파일의 안전성에 있어서는 원치 않은 ‘스니퍼’로부터 네트워크 보호에 대한 법적 이슈 운영 및 분석 작업 체크리스트 검토, 스위칭, 라우팅의 이해 등을 강의한다.

(4-2) 정보벤처창업론 (전선/3-3-0) **(Venture Startup for Cyber Security)**

정보 보안 분야의 창의성을 구현하면서, 창의적인 아이디어를 실제로 현실화하여 새로운 상품과 서비스를 제공하는 생태계를 조성하는 방안을 연구하고, 벤처 창업을 위한 창업 이야기, 창업에 대한 노하우, 기업 문화 등의 주제를 특강 형식으로 진행한다.

(4-2) 졸업 프로젝트 (전선/3-3-0) **(Graduation Project)**

컴퓨터 분야의 최신 기술 및 동향에 관한 주제를 설정하고, 팀을 구성하며, 프로젝트 일정에서부터 단계적 진척 과정을 주차별로 로드맵을 완성하여 진행한다. 최종 졸업프로젝트 전시작품에 올려지고 발표회를 통하여 평가를 받는 창의적인 탐구과정이 포함된다. 진행과정에서 커뮤니티를 통한 수강학생들의 조언을 참고할 수 있는 열린 강의형태를 취한다.

(4-2) 인턴십 (전선/P/F) **(Internship)**

실무를 중심으로 학습하고 업무 적응능력을 배양하고 진로를 결정한 후 정보보안관련 업체에서 업무수행능력을 증대시킬 뿐만 아니라 직접 취업으로 연결시킬 수 있도록 한다.