情 報 保 護 學 會 誌
第 11 券 第 3 號, 2001. 6

대학의 정보보호 교육과정 개발 연구

김 철*

요 약

본 논문에서는 교육과정 개발의 일반적 방법론과 국내외 정보보호 교육과정 및 그 특징의 조사를 바탕으로 정보보호 교육을 위한 국내 여건에 최적화된 교과과정 모델을 제공하여, 각 대학의 학부 및 대학원 과정에서 정보보호 인력을 내실있게 양성할 수 있는 교과목등을 제시함으로 미래의 정보보호 산업 인력의 수요에 적극 대응할 수 있는 기본적인 틀을 제공한다. 본 논문은 대학에서의 정보보호 교과과정 모델 제시를 그 주 목적으로 하고 있는 바, 현재의 교육법시행령등의 대학 교육 환경과 국내외 대학의 현실을 고려하여 국내에서는 최초로 학부 및 대학원 교과과정을 실질적으로 적용 가능한 형태로 제시하고 있다.

Ⅰ. 서 론

정보보호 교육은 정보보호 전문 인력 양성을 위한 필수적인 분야의 하나이다. 정보보호에 대한 인식 확산과 초 중등학교에서의 정보통신 윤리 교육, 그리고 각종 전환교육과 보수 교육등과 더불어 대학에서의 정보보호 교육은 정보보호 전문 인력의 양성과 기술 확보의 추춧돌이라고 할 수 있다. 특히 1999년부터 확산된 국내 정보보호 산업은 많은 정보보호 전문 인력을 필요로 하고 있으며, 기업 및 국가 기관, 공공 기관에서도 정보보호 전문 인력에 대한 수요는 증대되리라 예상된다.

그러나 정보보호 교육을 행하고 있는 국내 대학의 환경은 이러한 수요에 신속하게 효과적으로 대응하고있지 못한 현실이다. 많은 대학들에서 관련 학과목을 개설하고 있고, 학부와 대학원에서 정보보호 전공을 개설하고 있으나, 교수진 확보, 개설 과목의 한계등 다른 전공이 가지고 있는 교과과정 상의 문제점을 모두 내포하고 있는 실정이다. 특히 정보보호 전공의 교과과정에 대한 연구나 표준화 과정이 없었으므로 학부, 대학원, 특수 대학원에서의 개설 교과목등은 정보보호 관련 학계등에서조차 다양한 이견의 대상이 되고 있는 실정이다. 이것은 급변하는 정보보호 분야의 기술 발전 특성을 수용하거나 균형있는 전문 지식 축척을 위하여 부정적 요소로 작용하고 있다.

이에 본 논문에서는 이러한 논의를 촉발시켜서 보다 효율적인 교과과정 수립을 통한 내실있고 균형있는 정보보호 전문 인력의 양성을 도모하고, 나아가 지속적으로 정보보호 교육 분야의 심화발전을 꾀하려는 목적을 가지고 있다.

본 논문은 제 2절에서 교과과정의 일반적인 개발 모형을 살펴본 후, 국내외 정보보호 교육과정의 특징등을 논의한다. 제 3절에서는 학부의 교과과정 모델과 그 특징을 설명하며, 현재 각 대학의 현실을 고려한 교과과정 모형을 제시한다. 제 4절에서는 대학원 교과과정의 모델을 제시하며, 정규 대학원보다 많이 개설되어 있는 특수 대학원에서도 원용할 수 있는 교과과정을 제안한다.

Ⅱ. 교과과정의 개발 모형과 정보보호 교과과정 특징

본 절에서는 교육학 분야에서 전통적으로 다루어 왔던 교과과정의 일반적인 개발 모형을 살펴본 후, 국외의 정보보호 교육과정의 특징등을 논의한다. 아울러 국내 정보보호 교육과정의 특징을 파악하여 현실성 있는 교과과정 모형을 제안하기 위한 기본 논리로서 제시한다.

* 광운대학교(kimch@daisy.kwangwoon.ac.kr)

1. 교과과정의 개발 모형

일반적으로 교과과정 개발 모형과 교과과정 재구성 모형은 상황에 따라 일치할 수도 있고 다를 수도 있다. 예전의 우리나라와 같이 국가수준의 교과과정이 제시되는 경우, 현장에서 교과과정을 개발한다는 것은 결국 교과과정을 재구성한다는 것과 같은 의미이다. 최근에는 교과과정의 자율성이 학교마다 보장되고 있는 추세이므로 교과과정 개발 모형으로서의 관점도 필요하다. 즉 보다 유연하고 개방적인 교과과정 모델을 개발할 수 있다. 여기에서도 이와 같은 맥락에서 교과과정 개발 모형을 살펴보기로 한다.

교과과정 개발 모형에는 학자에 따라 다양하게 제시하고 있으나, 크게 세 가지 유형으로 나눌 수 있다. 첫째, 1950~60년대에 미국에서 활발히 활용되었던 전통적/고전적 모형으로 대표적인 학자들은 Ralph W. Tyler(1949)와 Hilda Taba(1962)를 들 수 있다. 둘째, 1970년대 영국이나 호주를 중심으로 크게 환영을 받았던 순환적 교과과정 개발 모형으로서 대표적인 학자들은 Audrey Nicholls와 Howard Nicholls(1972, 1978)를 들 수 있다. 셋째, 교과과정 개발에 있어서 숙의(deliberation)의 과정을 강조하면서 1970년대 미국에서 활발하게 논의되었던 자연주의적 모형으로서 대표적인 학자들은 Decker Walker 등을 들 수 있다. 이 외에도 교과과정 학자들의 관심을 끈 Saylor-Alexander-Lewis 모형, Oliva모형 등을 들 수 있다.

1.1 전통적/고전적 교과과정 개발 모형

교과과정 개발에 있어서 가장 많은 관심과 넓게 알려진 모형은 아마 Ralph W. Tyler(1949)의 『교과과정과 수업의 기본원리』(Basic Principles of Curriculum and Instruction)에 있는 전형적인 모형일 것이다. Tyler가 가장 강조한 것은 목표를 명확하게 규정하는 것이라고 주장하였다. 교육과정을 개발할 때 무엇보다도 일반적인 교육 목표를 세 가지 목표 원천에 근거하여 도출하도록 권하였다. 즉, 학습자에 대한 체계적인 연구, 학교 밖의 현대 생활에 관한 연구, 교과의 분석으로부터 학습 목표는 도출되어져야 한다고 했다. 일반적인 많은 목표가 도출되면, 교육과정 개발자는 학교의 교육적 및 사회적 철학과 학습 심리학에 근거하여 이들을 정선하여야 한다. 이렇게 되었을 때 적절한 학습 경험을 선정할 수 있고, 그 경험을 조직하고, 평가를 결정하는 데 있어 효과적인 기초가 되기 때문이다.

Tyler의 기본 모형을 보완한 학자가 Hilda Taba(1962)라고 할 수 있다. Taba는 자신의 저서 『교육과정 개발 : 이론과 실제』(Curriculum Development : Theory and Practice)에서 Tyler의 모형이 현장과 괴리가 있음을 지적하고, 보다 현실적이고, 이론과 실제가 연계될 수 있는 교육과정 개발 체계가 있어야 함을 피력하였다. Taba는 Tyler의 모형을 각 단계마다 보강하여 다음과 같은 7단계 교육과정 개발 모형을 제시하였다.

1단계 : 요구의 진단
2단계 : 목표의 설정
3단계 : 내용의 선정
4단계 : 내용의 조직
5단계 : 학습 경험의 선정
6단계 : 학습 경험의 조직
7단계 : 무엇이 평가되어야하고, 그것을 평가하는 방법과 수단의 결정

1.2 순환적 교과과정 개발 모형

교육과정 개발은 합리적 모형이 제시한 바와 같이 1회에 끝나는 것은 극히 드물다. 새로운 정보나 실제에 따라 항상 변화하는 상황을 지속적으로 반영해야 한다. 특히, 사회 생활의 변화가 급속도로 진행되는 시대는 자칫 교육과정이 사회 변화에 대응하지 못하게 되는 경우도 있다. 이 때는 교육과정 개발도 사회의 필요에 따라 반응하고, 끊임없이 수정되어 간다. 따라서, Audrey Nicholls와 S. Howard Nicholls(1972, 1978)는 순환적 교육과정 개발 모형을 제시하였다. 순환적 교육과정 개발 모형은 교육과정의 요소를 상호 관련적이고 의존적인 것으로 간주한다.

Nicholls와 Nicholls는 『교육과정 개발 지침』(Developing a Curriculum : A Practical Guide)라는 저서에서 상황의 변화에 따라 새로운 교육과정을 필요로 하는 경우에 교육과정 개발의 논리적 접근의 필요성을 인식하고 순환적 교육과정 개발 모형을 제시하였다. 합리적 모형에서 볼 수 없었던, 교육과정 개발의 예비단계라고 할 수 있는 상황 분석 단계를 강조함으로써 Tyler, Taba의 합리적 모형을 더욱 세련시켜 놓았다고 할 수 있다. 교육과

정 개발 과정에서 각 구성요소들로 넘어가기 이전에, 교육과정의 의사결정이 이루어지는 상황분석이 신중하게 이루어져야 함을 주장하였다. 이는 학습자들의 요구에 보다 더 잘 대처할 수 있다.

비록, 앞 단계가 완성되어야 다음 단계가 완성될 수 있는 부분은 본질적으로 합리적 모형을 벗어나지 못하고 있으나, 교육과정의 각 요소들이 상호관련되어 있고, 상호의존적이며 순환적 형태를 유지하고 있음을 간파한 것은 교육과정 개발에 큰 진보라고 할 수 있다.

1.3 자연주의적 교과과정 개발 모형

합리적 교육과정 개발 모형이 미국을 중심으로 발전·확산되었고, 순환적 모형은 주로 영국을 중심으로 발전되었다. 이 두 모형은 교육과정 개발에 있어서 직선형이며, 계열적인 형태를 유지하고 있다. 이에 대해 Decker Walker(1971)는 교육과정 개발은 어떤 교육과정 요소로도 시작할 수 있고, 어떤 순서로 진행되어도 무방하다고 주장했다. 교육과정은 정강(platform), 숙의(deliberation), 설계(design)의 세 가지 요소로 이루어진다고 주장하였다.

Walker의 모형은 숙의과정으로서, 교육과정 개발에 참여한 사람들의 의견이 타협되고 조정되는 과정을 강조한 점이 특징이라 하겠다. 즉, Walker는 결과보다는 의사결정 과정이나 절차에 초점을 두고 있기 때문에 자연주의적(naturalistic) 또는 과정지향적(process-oriented)인 성격을 지닌다. 특히, 교육과정 개발의 출발점이 교육과정 개발을 위한 교육자의 신념체계나 집단 구성원들의 신념, 태도, 아이디어, 이상, 희망 등으로 교육과정 계획에 있어서, 획득해야 할 것으로 미리 결정된 정보보다는 학습자의 흥미, 요구, 관심사를 더 중요하게 생각한다. 또한, 수업 내용과 방법, 수업 절차 등을 보다 현장에 맞게 진술하고 정련시키는 데 많은 시간을 투자하기 때문에 보다 현장에 적절한 교육과정을 개발할 수 있다. 하지만, 어떻게 목표를 구체화할 것인가, 어떤 교육내용을 선정할 것인가, 어떤 방법을 활용할 것인가 등과 같은 문제는 여전히 남아있기 때문에 오히려 Tyler 모형을 더 확장시킨 것으로 볼 수 있다(Posner, 1988).

1.4 Saylor, Alexander, Lewis 교과과정 개발 모형

Saylor, Alexander, Lewis(1981)는 교육과정을 "학습자들에게 일련의 학습의 기회를 제공하기 위한 계획"으로 정의하고, 교육과정 개발을 단순한 문서로 여기기보다는 "교육과정의 특정 부분을 위한 많은 작은 계획"이라고 정의하였다. 이들의 교육과정 개발은 다음 그림과 같이 크게 교육과정 설계, 교육과정 이행, 교육과정 평가의 세 과정으로 구분하고 있다.

1. 교육과정 설계 : 특정한 교육기관을 위한 교육과정 개발 담당 그룹에 의해 만들어진 설계안으로서의 결정. 정치적·사회적 기관들에 의한 기존의 다양한 결정들이 최종적인 교육과정 설계안에 대해 제한을 가할 수 있음.
2. 교육과정 이행(교수) : 담당 교사(들)에 의한 교수(敎授) 양식으로서 결정. 교육과정 계획에는 자원, 매체, 조직 등과 같은 대안적인 교수 양식이 들어있어서 교사(들)와 학생들을 위한 보다 융통성과 자율성이 부여되어 있음.
3. 교육과정 평가 : 담당 교사들의 의해 학습자들의 성취 정도를 결정하기 위한 평가 과정으로서의 결정. 교육과정 개발 담당 그룹에 의해 만들어진 교육과정 계획을 평가하기 위한 과정으로서의 결정. 평가 자료는 차후 결정을 위한 기초자료가 됨.

이 모형에 의하면 교육과정 개발은 성취하고자 하는 주요 교육목적과 구체적인 교육목표를 구체화함으로써 시작된다. Saylor, Alexander, Lewis는 교육 목적을 학습 경험이 많이 일어나는 개인적인 발달, 사회적 능력, 지속적인 학습 기능, 특별 영역의 네 영역으로 구분하였다. 교육의 목적, 목표, 영역이 일단 설정되면 교육과정을 설계하는 단계에 접어든다. 교육과정 개발자들은 각 영역의 적절한 학습 기회를 결정하고 언제 어떻게 이런 기회가 주어져야 하는지도 결정한다. 즉, 학문의 순서에 따라 배열할 것인지, 사회 제도의 형태에 따라 배열할 것인지 아니면 학습자들의 흥미와 관심사에 따라 배열할 것인지를 결정하게 된다.

교육과정 설계안들이 만들어지면 교사들은 이 안에 의해 교수·학습 계획을 세워야 한다. 교육과정이 학습자들과 연계될 수 있도록 방법을 모색해야 한다. 교사들은 이 과정에서는 수업목표에 주목한다. 수업의 양식이나 수업 전략을 선정하기 전에 보다 구체적으로 수업목표를 명세화한다.

Saylor, Alexander, Lewis 교육과정 개발 모형의 마지막은 평가에 해당된다. 이때는 교육과정 개발자와 교사가 함께 참여해야 한다. 평가는 학교 교육의 목적, 목표, 수업의 효율성, 학습자들의 성취 등을 포함한 학교 교육 프로그램 전체를 평가하지만 프로그램 자체도 평가해야 한다. 그래야만 학교의 목적이나 수업의 목표들이 성취되었는지를 알 수 있다.

1.5 Oliva 교과과정 개발 모형

Peter F. Oliva(1988)은 자신이 초기(Oliva, 1976)에 제시했던 6단계(교육철학적 진술→교육목적의 진술→교육목표의 진술→교육 계획의 설계→시행→평가)의 교육과정 개발 모형을 확장시켜 12단계(phases)의 보다 종합적이고, 구체적인 모형을 제시하였다. 이들을 열거하면 다음과 같다.

I 1. 일반적인 학생들의 요구(needs) 구체화.
2. 사회의 요구를 구체화.
3. 교육의 철학과 이념 기술.
4. 학습자들의 요구 구체화.
5. 지역사회의 요구 구체화.
II 6. 교과의 요구 구체화.
III 7. 자신들의 학교의 교육과정 목적 구체화.
IV 8. 자신들의 학교의 교육과정 목표 구체화.
V 9. 교육과정을 조직하고 시행.
VI 10. 교수·학습 목적 구체화.
VII 11. 교수·학습 목표를 구체화.
VIII 12. 교수 전략 선정.
IX 13. 평가 전략 선정 시작.
X 14. 교수 전략을 시행.
IX 15. 평가 전략에 대해 최종 선택.
16. 수업을 평가하고 수업 요소를 수정.
17. 교육과정을 평가하고 교육과정 요소를 수정.

Oliva의 모형은 교육과정 원천에서부터 평가에 이르기까지 각 단계별로 그 과정을 종합적으로 제시하고 있다. 하지만, 자세히 살펴보면 Tyler의 모형을 보다 구체적으로 광범위하게 제시했음을 볼 수 있다

2. 외국의 정보보호 교과과정의 목표

NSA등에서는 국가 안보에 미치는 중요성을 인식하여 정보보호 인력 양성에 막대한 투자를 하고 있어, NSA가 인증하는 교육 프로그램을 미국 전역에 걸쳐 7개 대학에서 공히 실시하여 일관성 있고 객관성 있는 교육의 질을 확보하며 전문 인력을 양성하고 있다. 정보통신 분야에서의 역할을 고려하는 효율적인 교육체계를 제시하고, NSTISSC 훈련 기준을 바탕으로 99년 5월, 7개 대학을 CAEIAE (Center of Academic Excellence in Information Assurance Education, James Madison University, George Mason University, Idaho State University, University of California, Davis, Purdue University, University of Idaho, Iowa State University)로 선정하여 미국 정부 보증의 정보보호 전문 인력을 양성하게 되었다[1],[2]. 다양한 분야에 걸쳐 정보보호문제에 대한 다양한 접근법을 제기하고 있으며, 이는 다음과 같은 연구, 개발 및 교육 분야를 포함하고 있다.

- 컴퓨터 및 네트워크 보안
- 통신보안 (communications security)
- 정보시스템 보안 (information system assurance)
- 이동코드(애플릿 등)상에서의 보안 및 신뢰 (security and trust in mobile code (applets, etc))
- 전자시대 상에서의 프라이버시 윤리 (the ethics of privacy in an electronic world)
- 정보보호에 관한 공공정책 (public policy regarding information security)
- 정보 관리 및 정책 개발 (information management and policy development)
- 정보사용, 남용에 관한 사회적, 법적, 윤리적 관점 (social, legal and ethical aspects of information use and abuse)
- 정보보호 경제학 (the economics of information assurance)
- 전자상거래 보호 (electronic commerce security)
- 해킹 심리학 (the psychology of hacking)
- 컴퓨팅 시스템과 네트워크에 대한 위험관리 (risk management for computing systems and networks)
- INFOSEC 전문가들의 인지 및 훈련방법 (awareness and training methods for infosec professionals)

- 컴퓨터 범죄 수사 및 대응 (computer crime investigation and response)
- 정보전 이슈들 (information warfare issues)

영국 정보 보호 교육 과정은 주로 다음과 같은 정보보호 목표를 교육 과정 설치와 내용의 목표로 하고 있다.

- Confidentiality(비밀성)
- Integrity(무결성)
- Availability(유용성)
- Accountability(책임성)
- Reliability(신뢰성)
- Functionality versus Assurance
- Security threats(보안위협)
- Risk analysis(위험성 분석)
- Providing security(보안설비)
- Focus of control(통제의 초점)
- Location of security controls(보안제어구조)

다음과 같은 IT 시스템의 5계층에서 보안을 요구한다고 분류할 수 있다.

- Application programs, (응용프로그램)
- Services: DBMS 또는 분류된 파일 시스템에 의해 제공된 서비스
- Operating system: 파일운영, 프린터운영을 수행하는 운영 체제 시스템
- Kernel (of Operation System): 프로세서 및 메모리 접근을 중재하는 커널
- Hardware: 프로세서 및 메모리
  - Other security controls(그밖의 보안통제)
  - Assurance versus complexity(보증성과 복잡성)
  - Bypassing security controls(보안제어침투)
  - Security management (보안관리)
  - Security policies (보안정책)

이와 같은 정보보호 교육의 목적에 따라 미국등에서는 많은 연구가 수행되고 있다. 1996년에 개정된 OMB(Office of Management and Budget) Circular A-130은 NIST가 SP 500-172를 보완할 것을 요구하였다. 그 결과, 1998년에 SP 800-16가 SP 500-172를 대치하고 정보보호 교육 훈련에 대한 새로운 개념적 골격을 제시하였다. 여기에는 오늘날의 컴퓨터/네트웍 환경에 적당한 정보보호 교육 훈련의 필요성과 미래의 기술 발전 추이와 그와 관련된 경영적인 측면들이 두루 포함되어 있다. 특히 역할 기반 개념을 도입하여 체계적인 교육 훈련 교과과정 계발 연구를 지속적으로 행하고 있다. 우리나라에서는 2000년부터 관련 연구들이 처음 시도돼는 실정이다.

3. 정보보호 교과과정의 특징

우리의 현실에 적합한 교과과정 개발을 위하여는 무엇보다도 정보보호 교육/훈련이 가지는 특징과 우리의 현실에 대한 파악이 필요하다. 본 절에서는 이러한 특징을 추출하여 정보보호 교과과정 개발의 전제조건으로 제시한다.

먼저 정보보호 전문 인력을 양성하기 위한 교과과정이 구현될 수 있는 환경에 대하여 고려해보자. 정보보호 전문 인력의 역할, 그리고 이에 따른 전문 인력의 소요 자질들을 감안할 때, 효율적인 정보보호 교과과정이 구현되기 위한 교육 환경은 다음과 같은 방향으로 정립되어야 한다.

첫째, 정보보호 전문 인력으로서의 기본 자질을 교육해야 한다. 이론 교과목에 덧붙여 시스템, 프로토콜 설계 교과목을 필수 과정으로 부과하여 전문가로서의 기본 자질을 키우고, 현실성 있는 문제파악 능력과 창의적인 문제해결 능력을 배양해야 한다. 또, 실험실습 및 정보보호 및 정보통신 산업체 연계 교육을 강화하여 산업과 사회현실에 적용 가능한 전공기반 지식을 두루 갖추도록 해야 한다. 한편, 기술적 문제에 대한 경제적 접근능력도 배양해야 한다.

둘째, 사회 구성원으로서의 기본 자질을 교육해야 한다. 입시준비에 편중된 중등 교육의 결함을 보완하여 인성 및 사회성을 도야시키고 장차 건설적인 민주사회 시민으로 성장할 수 있도록 기본 자질을 함양시켜야 한다. 특히 국가 안보와 개인 사생활 보호, 정보화 역기능 방지등, 정보보호 전문 인력으로서의 바른 가치관과 윤리의식을 갖추고, 협동심과 공동체 의식을 갖추도록 배양해야 한다. 또한 사회적 교양과 기본지식을 갖추고, 국제적 적응능력을 키울 수 있도록 해야 한다.

셋째, 대학의 교육목표에 부합되는 특성화된 전문 자질을 교육해야 한다. 과거의 이론 치중 공학교육

의 틀을 벗어나 대학의 위상과 산업 및 사회의 요구에 맞춰 대학별 교육목표를 설정하고, 이에 부합되는 특성화된 전문자적 자질을 함양시켜 주어야 한다. 이것은 주로 전공심화 교과과정을 특성화 방향에 맞춰 구성하므로서 실천할 수 있다. 한편, 전문분야 내적 능력배양에 덧붙여 산업과 사회 등 주변환경에 대한 폭넓은 안목도 길러주어야 한다.

넷째, 자율적 자기발전을 추구하는 능동적 자질을 교육해야 한다. 누구나 한가지 전문 분야에 대해서 자신감을 갖도록 전문성 있는 교육을 해야 하며, 학생 스스로 교과목 이수계획을 세우고 능동적인 학습을 할 수 있도록 유도해야 한다. 또 장래 진로계획을 스스로 세워서 전공심화과정을 선별적으로 이수하고, 산업과 사회진출에 대비할 수 있도록 해야 한다. 이를 뒷받침하기 위해, 틀에 박힌 교과과정 이수체계와 획일적으로 적용되고 있는 등급 학점 위주 평가방식을 다양하게 개선해야 한다.

다섯째, 시대환경 변화를 선도하는 진취적 자질을 교육해야 한다. 세분화된 교과과정을 큰 단위로 구분하여 종합적 안목을 키워주고, 인근분야간 학제적 학습과 관련 교과목(이론+실험, 분석+합성, 유사과목)간 통합교과목 제공으로 학습동기를 유발하고 학습효과를 높일 수 있도록 해야 한다. 원격교육, 초빙교수제도 등을 통해 산업체와 긴밀한 교육협력을 이루고 협동과정 교육을 강화하여 현실성 있는 교육 프로그램을 제공하며, 한편 교육프로그램과 교육내용에 대해 산업체 및 사회로부터 피드백과 정기적인 평가를 받도록 해야 한다.

이제 우리나라의 교과과장 현황에 대한 조사 분석 결과 정보보호 교육에 대하여 다음과 같은 특징들을 관찰할 수 있었다.

1. 4년제 대학교 중 수학, 컴퓨터, 전자, 정보통신 관련 학과가 설치된 일정 규모 이상인 대학의 학부 과정에는 대부분 정보보호 관련 과목들이 적어도 한 과목은 개설되어 있다. 명시적으로 학과목을 개설한 경우와 특강등의 과목 명으로 개설하는 등 대부분의 자연계 전공과정에서는 강의를 진행하고 있는 실정이다. 이는 정보보호의 필요성이나 수요가 인식된 결과이며 교과과정 개편이 용이하지 않은 대학의 환경으로 보아 이례적인 일로 볼 수 있다. (과목 개설 확산)
2. 대학원에서는 주로 관련 교수들의 연구실 중심으로 연구가 진행되면서 아울러 관련 과목이 설치되어 있는 현상을 보이고 있다. 이는 학과목의 개설이 교과과정이라는 거시적 접근에 의하여 개설되어 지는 것이 아니라 교수 개인들의 연구 관심에 의하여 관련 과목이 설치되고 있음을 의미한다. (교수 중심 개설)
3. 독립 전공으로 교과과정을 개설하기에는 아직 많은 어려움 들이 있는 것으로 분석되었다. 다양한 배경의 교수의 확보가 어렵다는 것이 가장 큰 이유이다. 전문 대학원의 경우도 전담 교수없이 대부분이 겸임 형태로 교수를 확보하고 있는 경우가 대부분이며, 교과과정 및 교육 시설의 확보가 독립적이지 못하다. 특히 학부 정보보호 전공은 대학원과정에 대한 선수 단계로서의 성격을 가질 수 밖에 없다. 즉 학부과정의 정보보호 전공 이수 내용과 그 깊이에 한계가 있으므로 학부 과정에서는 인접 전공에 대한 복수전공이나 2개의 부전공등을 교과과정에 포함함이 타당하다. 그러나 이점은 국가 공인 정보보호 자격증에 관한 정책과도 밀접한 관계가 있다. 즉 자격증을 기사급으로 할 것인지, 기술사 급으로 할 것인지에 따라 학부 과정의 교과목 범위와 깊이가 현격한 차이를 가져올 것이다. (독립전공 한계)
4. 교육 내용의 질적 차이가 극심하다. 동일한 교과목의 경우도 교육의 양이나 질적인 면에서 많은 차이가 있다. 이는 각 학교가 가진 학생의 수준과 교육 환경에 기인하는 바가 크다. 또한 한 대학에서는 한 과목 내용을 다른 대학에서는 3학기 3과목으로 강의하는 경우도 있었다. (교육 내용 상이)
5. 수도권 지역의 편중화와 대도시 집중화 현상이 정보보호 교과목의 개설에도 나타나고 있다. 물론 수요와 졸업생 취업등에 따른 원인이 크지만 관련 지원이 편중되고 있음을 알 수 있다. 물론 효율화를 위한 집중 지원과 무분별한 평등 지원을 배제하여야 함은 사실이지만 일부 지방대학교와 수도권 대학에서는 상대적 박탈감을 느끼고 있는 것 또한 사실이다. 아울러 정보보호 인력양성의 목적이 산업 수요에 부응하는 것 외에 국가적으로 원천 기술을 확보할 수 있는 고급 연구인력의 확보에도 있다고 할 때, 응용 분야에 대한 지원 못지 않은 기초 분야의 지원이 필수적이라 하겠다. (전공별, 지역별 지원 편중 현상)

대학 및 대학원의 이러한 특징들, 과목 개설 확산, 교수 중심 개설, 독립전공 한계, 독립전공 한계, 지원 편중 현상등은 정보보호 전문 인력 양성을 위한 정책 뿐 아니라 정보보호 산업 육성책, 기술개발 지원 정책등의 수립에 있어서도 간과할 수 없는 특징이라 할 수 있다.

Ⅲ. 학부에서의 정보보호 교육 교과과정

학부의 교과과정은 교육 관련 법들과 그 시행령등의 규정과 각 학교별 교육 목표 및 환경등에 직접적인 영향을 받고 있다. 따라서 표준적인 교과과정을 개발하여 학교별로 적용하기는 어려우나 다음과 같은 일반적 모델을 제시하고 교과 목표등의 준거를 제시함으로 학부의 정보보호 교육 교과과정 발전에 기여할 수 있다.

정보보호 교과과정은 단순 계층적 교과과정으로 구성될 수 없는 특징을 가졌다. 특히 교양 교과 과정과 인접 전공 교과 과정이 다른 어느 학문 분야보다 필수적인 교과 과정을 구성하여야 한다.

기본교양과정·전공기초과정·전공심화교과 및 인접 전공 교과과정 등의 4가지 요소로 구성되고, 그 중 교양과정과 전공기초과정을 2개의 기둥으로 삼아 그 위에 전공심화교과와 인접 전공 교과를 올려놓은 구조를 가진 교육체계가 필요하다.

1. 교양과정

교양과정은 대학 졸업자가 산업과 사회의 구성원들과 조화롭게 생활하는 가운데 전문성과 공학적 접근 능력을 발휘할 수 있도록 뒷받침 해 주는 기본소양을 쌓는 과정이다. 교양 과정에서는 기존의 인문, 사회, 예술분야 교양교과목들에 사회 교양과 경제적 문제접근 능력을 배양하기 위한 교과목들을 강화시키고, 이에 덧붙여 의사소통 능력 그리고 협동성 및 지도력과 같은 사회적 기본소양을 함양시켜 준다.

장래 산업과 사회의 제반 문제는 기술과 사회 경제적 요소들이 복합적으로 결부되어 있기 때문에, 이를 해결해야 하는 전문인력들에게는 인간·사회·기술로 연결되는 미래사회에 대한 거시적인 안목과 이에 부합된 접근수단이 필요하다. 이를 위하여 기본소양과정에는 인문 예술 교양(어학, 문학, 예술, 역사, 철학, 문화 등), 사회 교양(경제, 경영, 법, 환경 등), 경제적 접근능력(공업경제, 기술경제학, 재무회계 등), 정보처리 및 의사소통능력(컴퓨터 언어, 인터넷, 작문, 발표 등), 협동성 및 지도력(인성, 윤리, 체력, 협동성, 지도력 연마) 등의 교육이 필요하다.

2. 전공기초과정

전공기초 과정이란 정보보호 분야에 대한 기초적인 이론적 요소(학문성)와 실천적 요소(기술성)를 함께 갖추고 이를 종합할 때 이루어지는 공학적 접근능력을 구비하여, 자부심을 가진 전문 인력으로서 산업과 사회에 진출할 수 있는 기반을 쌓는 것을 목표로 하는 과정이다. 이 과정은 기존의 교양과정에 속하는 기초과학 교양 교과목들과 기존의 전공과정에 속하는 전공기초 및 기초 필수과정 교과목과 공학일반 교과목, 공학설계 교과목 및 학제적 통합 교과목들로 구성된다.

특히 정보보호 메카니즘의 시스템, 프로토콜 설계 교과목은 학생 스스로가 엔지니어라는 자기 확신을 갖고, 전문가 정신을 키우며, 거기에 자부심을 느낄 수 있게 할 수 있는 과목이 바로 설계 과목이다. 설계과목은 현실적 문제에 대해 해결방안을 연구하고 이를 실제 기획, 설계, 구현한 후, 그 결과물을 검증하는 과정을 포함하게 되므로, 이러한 일련의 과정을 통해서 정보보호 이론의 필요성을 깨닫고 또 기술성을 연마하여 엔지니어로서의 감각과 자신감을 쌓아 갈 수 있게 된다.

3. 전공심화과정

전공심화과정이란 장차 산업과 사회에 진출하여 정보보호 전문가로서의 역할을 담당하는 데에 직접적인 밑받침이 될 전문능력을 심화 학습시키는 과정이다. 전공심화 과정에서는 대학의 교육목표에 맞추어, 또 학생 각자의 적성과 인생목표에 맞추어, 특정 교과목군(群)이나 세부전공분야를 집중 학습시켜 사회진출에 대비할 수 있도록 전문능력을 심화 학습시켜 준다.

전공심화과정을 위한 교육내용과 교과목구성은 대학별로 해당교육 목표에 맞추어 짜는 것이 중요하다. 예를 들어, 학부제를 실시하여 1-3학년 과정을 전공공통 교과목으로 채우게 되는 경우에는, 4학년 전공심화 교과과정에서 세부전공 과목들을 제공하므

로서 장차 대학원 진학과 산업체 진출에 대비할 수 있도록 하는 것도 바람직하다.

한편, 산업과 사회의 지도자적 전문 인력을 육성하고자 하는 경우라면, 전공심화과정을 연구지향, 산업지향, 사회지향의 교과목군들로 구성하고, 이들 중 한가지를 집중 학습하도록 유도하는 것을 고려할 수 있다.

4. 인접 전공교과 과정

인접 전공 교과 과정이란 정보보호 전문 분야가 가진 특성에 기인한다. 정보의 흐름과 저장이 어느 특정 개체에 머물지 않으며, 기술적 측면으로부터 정책적 측면에 까지의 다양한 구성 요소를 가지고 있으므로 단일 전공을 배경으로 한 정보보호 기술은 효용성을 극대화할 수 없는 실정이다. 따라서 인접 전공 분야 및 차별 전공 분야에 대한 이해가 교양의 수준을 넘어서는 정도까지 확대되어야 할 필요가 있다. 즉 현 대학 교과과정에 비추어 보면 부전공 21학점, 7과목 정도의 수료가 요구되는 것이라 할 수 있다.

재 정보보호 교과목으로 제안하는 16개 학과목에 대한 종류 및 내용을 살펴본다. 먼저 20개 학과목을 제안하여 그중 16개를 선택하는 체계를 가지도록 한다. 다만 학부 교과과정이라는 특성상 일반적 과목명을 설정하며, 교과 내용 역시 각 학교의 현황을 무시할 수 없으므로 최소 내용만을 설정한다. 특히 수강 학생들의 수학적 능력이나 컴퓨터 통신 관련 능력의 차이 및 교육환경의 차이로 동일한 명칭의 과목과 최소 내용을 규정한다 해도 학습의 깊이를 동일하게 보장할 수 있는 것은 아니다.

필수 교과목 (2)
- 정보통신 윤리
- 정보보호 표준

전공 기초 (5)

〔표 1〕 학부 과정을 위한 교과과정 모델

과정	교과목	이수학점				
		1년	2년	3년	4년	계
		1 2	3 4	5 6	7 8	
기 본 교 양	인문사회교양12 인문학, 사회과학 등 정보보호 전문가 기본소양 8 기술과 사회 관련교과목 공업경제, 기술경제학 등 논문 및 보고서 작성법 기타(정보통신윤리)	3 3	3 3	2	3 3	20
정보보호 전공기초 및 인접전공	기초과학 32 수학 물리 통계, 확률등	4 4 4 4 3	4 3 3	3		80
	정보보호입문 8 정보처리입문 시스템 설계입문 컴퓨터 프로그램	3 3 2				
	정보보호 및 복수전공 기초 40 정보보호 기초 (20) 복수 전공 기초 (20)		6 6 6 6	4 4 4 4		
정보보호 전공심화	정보보호 및 복수전공 심화 40 복수전공 심화 (15) 정보보호 심화 (25)			3 6 6	6 6 8 5	40
계		16 17	19 21	17 19	17 14	140

정보보호 개론
암호 프로토콜
정보이론 및 계산이론
정수론 및 대수학
확률.통계

전공심화 I (9)
운영체제 보안
인터넷보안
시스템보안
해킹 및 바이러스
스마트카드 보안
데이터베이스 보안
침입차단 및 탐지 기술
전자상거래 보안
스테가노그라피

전공 심화 II (4)
정보보호 산업 제품 분석
정보보호법, 정책
정보보호 프로젝트 수행
정보보호 특강

위와 같은 교과목들은 그 여건에 따라 시수 조정 및 내용의 폭과 깊이를 조절할 수 있을 뿐 아니라 필요한 경우 과목 I, II제도를 도입하여 과목 내용의 폭을 확대할 수 있다. 따라서 위의 20개 교과목을 중심으로 약 25개의 교과목을 확보할 수 있기는 하다. 또한 보안 감사, 사이버 수사 기법, 생체인식, 무선 인터넷 보안, 라우터.게이트웨이 보안등의 과목을 더 개발할 수 있으므로 정보보호 전공으로 약 30개 교과목을 개설할 수 있다.

아울러 정보보호 전공 자체적으로 관련 부전공 혹은 복수 전공 대체로서 정보보호 전공과 밀접한 관련 과목들을 설정한다면, 다음과 같은 과목들을 그 대상 교과목으로 설정할 수 있다.

자료구조, 컴퓨터구조,
객체지향 프로그래밍, 웹 프로그래밍,
시스템 프로그래밍, 네트웍 프로그래밍,

학기	제안학점	개 설 과목수	필수 과목	정보보호 과목			수리 과목	개별 과목	비고
2/1	6	2	정보통신윤리		정보보호개론				
2/2	6	2			암호프로토콜		정수론 대수학		
3/1	10	3		운영 체계		DB 보안	정보 이론		
3/2	10	4		시스템	인터넷	전자 상거래	확률 통계		
4/1	8	5	해킹바이러스	스마트카드	침입차단		스테가노그라	법제도	
4/2	5	4	표준	특강	제품			프로젝트	
계	45	20	(학과목명은 약칭 사용)						

정보보호 전공 과목 연계도

운영체제, 데이터 베이스, 네트웍,
데이터 통신, 마이크로프로세서,
네트웍 관리,

이러한 과목들외에 개설할 수 있는 교과목들을 나열하면 다음과 같다. 물론 이들 과목들은 학교의 특성 혹은 정보보호 기술 발전 방향에 맞추어 교과과정에 포함할 수 있다. 대부분의 대학들이 교과과정의 유연성을 확보하려는 추세에 있으므로 모든 과목을 일단 교과과정에 넣어야 한다는 과거와 같은 생각은 불필요 하다고 본다.

보안 감사 및 정보통신 감리,
사이버 수사 기법과 사이버 범죄,
생체인식의 기법 및 제품 동향,
무선 인터넷 보안과 무선 단말기 보안,
라우터,게이트웨이 보안
양자 암호시스템등 차세대 암호 시스템
계산 복잡도 이론과 암호 알고리즘 분석
암호 해독 기법

IV. 대학원에서의 정보보호 교육 교과과정

대학원의 정보보호 전공은 다른 전공과 비교하여 다음과 같은 차이가 있다.

먼저 일반적으로 교과과정 개발 및 적용 학교에 따른 차이가 있다. 즉 그 차별성으로 인하여 초중고교의 교과과정처럼 일률적 교과과정을 적용하기가 학부 과정보다 더욱 어렵다. 아울러 석박사 과정 개설 학교와 일반 대학원 및 특수대학원의 경우가 차이가 있을 수 있다.

둘째로 또한 정보보호 전공이 학제간 전공 영역이라는 특성을 가지고 있으므로 다양한 학부 전공을 고려하여야 한다. 즉 정보보호 전공을 암호학이라 단정지을 수도 없으며, 네트워 보안 전공이라 한정지을 수도 없다. 앞서도 언급하였던 것처럼 이것은 학생이 자신의 논문을 어느 영역으로 하였는가 정의하는 것과는 다른 것으로 여기서는 정보보호 전공의 대학원과정을 위한 교과과정 관점의 전공을 이르는 것이다.

셋째로 정보보호 전공 영역은 일부분의 이론적 면을 제외하고는 급변하는 정보기술에 신속히 적응하여야 하는 시의적절한 교과과정 개설이 필요한 영역이다. 신제품 개발과 원천기술을 확보하기 위한 연구등 유연한 교과과정을 가져야함을 특징으로 하고 있다. 정보보호 전문가의 역할이 변하고 새롭게 정의됨에 따라 연구, 개발등의 직무를 만족하기 위한 교과과정이 되어야 한다. 넷째로 정보보호 교과과정은 다른 대학원 교과과정과 마찬가지로 학위수여자의 다양한 진로에 공통적으로 적용 가능한 범용성을 확보하여야 한다.

위와 같은 특징, 차별성, 학제간 성격, 유연성, 공통적용성을 가지는 대학원 교과과정의 이란 모델을 개발하기 위하여 먼저 학부 전공 영역을 다음과 같이 구별한다.

계산이론, 통계, 확률등 수리 관련 영역(Th)
법, 행정, 무역등 경영, 경제 영역(Ma)
전자, 전파등 HW 영역(Pr)
정보통신, 통신등의 네트웍 통신 영역(Ne)
컴퓨터 과학 및 공학 영역(Cs)

어느 영역을 학부 전공하였든지 정보보호 전공의 대학원 교과과정은 다양한 배경을 수용하여 정보보호 전문인력을 교육 훈련 시켜야 함은 물론이다. 따라서 공통 필수과목을 설정한 후, 자신의 학부 전공 영역이 아닌 영역의 과목에 대한 이해를 필수적으로 부과하여 교과과정을 구성한다. 즉 영역별로 연계된 교과목 집합을 만들고 자신의 학부 전공 외의 영역에 대한 이해와 과목 이수를 요구한다. 학부 전공이 부전공(6과목) 혹은 복수전공(12과목)을 포함할 경우 그 영역의 학과목은 면제가 되는 등 정해진 학기안에 학위를 마칠 수 있도록 교과과정이 구성되어야 함은 물론이다.

따라서 일반체계는 대학원 필수 교과목과 그 필수 교과목을 이수하기 위한 학부 전공 연계 과목, 그리고 인접 영역에 대한 이수 과목으로 구성될 수 있다. 대학원의 경우 석사과정은 3학기, 박사과정은 6학기의 코스웍, 특수대학원의 경우 시수는 적지만 약 4학기의 교과과정 개설이 필요하다. 공통적으로 약 8과목(24학점) 을 석사학위 과정의 필요과목으로, 14과목(42학점)을 박사과정의 필요과목으로 설정할 수 있다. 추가적으로 석사논문을 위한 6학점등의 논문 준비학점이 필요하다. 물론 특강등의 과목 개설을 할 수 있다.

그 일반 체계를 그림으로 보면 다음과 같다.

학부전공	Th	Ma	Pr	Ne	Cs
기초과목B	1	1	1	1	1
심화과목A	2	2	2	2	2
근사과목O					
박사과목D	3	3	3	3	3
필수(3)+학부 영역 심화(2)+인접영역기초(1)+인접영역심화(3) + 학위논문 : 박사과정의 경우 박사심화(6)					
ReQ 필수과목 3과목					

〔그림 1〕 대학원 교과과정 일반체계도

예를 들어 A 영역의 학부 전공 학생은 필수 3과목과 자신 영역의 심화과목 2과목, 자신의 관심분야 혹은 학교의 특성화 분야의 인접 영역 B 영역 3 과목등 모두 8과목을 교과과정으로 선택할 수 있다. 아울러 학부 전공영역의 기초과목을 위하여 학부 과정 과목을 수강하게 함으로 필요학습량을 확보하도록 한다. 아울러 학교의 특성화가 되어 있는 경우 근사 과목에 해당하는 과목을 설정함으로 좀더 심도 있는 내용을 학위과정에 구현 할 수 있다. 여기서 근사 과목이란 기초 및 심화 과목 외에 해당 대학원에서 개설이 가능한 과목을 말한다. 본 교과과정에서는 2과목 정도를 적시하도록 한다.

이와 같은 일반적 체계는 모든 대학원이 모두 같은 정보보호 전공 과목을 개설하는 것을 방지하여 교육의 내실화를 기할 수 있다. 즉 A 대학원은 위의 다섯 영역 중 3영역으로 특성화하고 B 대학원은 다른 조합의 3영역으로 특성화함으로 학과목의 백화점식 나열을 방지하고 지원의 집중화를 이루어 효율적인 인력 양성을 꾀할 수 있다. 이는 또한 학부 전공 특성화 분야와도 연계되어 대학원 학부의 연계성을 높이고 효율적인 교과과정을 운영하도록 할 수 있다. 즉 특정 대학원이 모든 정보보호 전문인력을 집중 배출하는 것을 방지하여 균형적인 인력 양성이 가능하도록 한다.

학과목 코드를 설명하면 다음과 같다. 처음 두자는 학부 및 배경 전공 영역을 나타내는 것으로 Th, Ma, Pr, Ne, Cs가 있다. 다음 한개 영문자는 기초과목 B,심화과목A, 근사과목O, 박사과목D, 필수과목 R을 나타내면 뒤 한 개의 숫자는 영역내의 과목 순번을 나타낸다. 예를 들어 ThO2 는 수리 영역의 근사 과목중 2번째 과목이라는 의미이다. 예외는 ReQ#인데 이는 필수 과목 #을 나타낸다.

위의 일반체계에 필요한 교과과목을 나열하도록 한다. 현재 우리나라의 경우 정보보호 전공 대학원 석사 박사과정에서 개설되어 있는 학과목의 수나 내용은 학교간 큰 차이가 있다. 특수대학원 경우를 고려하더라도 교과과정상 과목 수나 학기 개설과목의 수는 현격한 차이가 있다. 이는 물론 교수진의 구성과 교육 환경에 따라 다른 것으로 이러한 조건을 모두 고려하는 교과과정을 개발하기는 어렵다. 따라서 본 절에서는 대학원의 정보보호 전공에서 최소한 개설할 수 있는 교과과목을 중심으로 나열한다. 제 1 절에서 언급된 일반체계에 의하면 대학원의 특성화나 관심 영역에 따라 다음 교과 과목들 중 선별적으로 교과과정을 구성할 수 있다. 아울러 학교의 특성상 과목을 I, II로 구분하여 확장할 수 있으며 다른 영역의 과목들도 필요에 의하여 교과과정에 조합할 수 있음은 물론이다.

ReQ1 정보통신보안 수학
ReQ2 네트워, 프로토콜 이해
ReQ3 시스템 프로그래밍과 데이터 구조

ThB1 계산 정수론
ThA1 계산이론과 정보이론
ThA2 암호학
ThO1 확률론
ThO2 스테가노그라피
ThD1 현대암호이론
ThD2 암호분석론
ThD3 계산대수학

MaB1 전자상거래보안
MaA1 전자지불 방법론
MaA2 정보시스템 감리
MaO1 정보통신 윤리
MaO2 해킹 및 바이러스
MaD1 정보보호 정책
MaD2 정보보호 표준 및 평가
MaD3 정보시스템 위험 분석

PrB1 프로세서 기본 구조와 설계
PrA1 OS 보안
PrA2 암호 프로세서 설계
PrO1 스마트 카드 보안
PrO2 Tamper-Resistant 설계
PrD1 COS, 무선 emulator들과 보안 메카니즘
PrD2 보안 장비의 설계
PrD3 무선 보안 장비 설계

NeB1 데이터 통신
NeA1 네트워 보안
NeA2 인터넷 보안
NeO1 침입탐지 및 차단
NeO2 유무선 LAN 보안
NeD1 VPN 이해
NeD2 이동통신보안
NeD3 안전한 네트워 프로그래밍

CsB1 암호 프로토콜
CsA1 DB 보안
CsA2 유무선 PKI
CsO1 키 관리 프로토콜
CsO2 Language Security
CsD1 접근통제
CsD2 바이러스 방비
CsD3 차세대 컴퓨터, 시스템 보안

이제 이들 과목들의 내용을 키워드 중심으로 기술한다. 여기서 간과하지 말아야 할 것은 같은 명칭의 과목이며, 같은 키워드를 학습하였다 하여도 그 깊이가 다르다는 것이다. 정보보호 전문 인력의 질적 균등화와 정보보호 기술의 원천 기술확보를 위하여 깊이 있는 교과 운영과 학습이 필요하다. 이점이 바로 교육내용에 대한 인증이 정책적으로 필요한 이유 중의 하나이다.

ReQ1 정보통신보안 수학 : 정보보호에 관련된 이론 연구에 필요한 기초적인 수학 지식, 즉 이산 수학, 정수론, 대수학, 확률론 등의 주요 개념 소개.
ReQ2 네트워, 프로토콜 이해 : 프로토콜에 대한 일반적 구조와 여러 종류의 네트워에 대한 내용.
ReQ3 시스템 프로그래밍과 데이터 구조 : 컴퓨터에서 프로그램을 효율적으로 처리하기 위하여, 여러 가지 데이터의 구조에 대하여 학습. 또한 이를 응용한 기본적인 알고리즘을 설계하기 위한 방법 및 이의 프로그래밍.

ThB1 계산 정수론 : 소인수 분해문제, 이산대수 문제등 암호학의 기반이 돼는 계산적 정수론에 대한 포괄적 학습.
ThA1 계산이론과 정보이론 :정보전송에 영향을 미치는 요소들에 관한 수학적 이론 및 응용. 알고리즘의 복잡도를 분석하고 P, NP-class와 각 class의 completeness, 문제간의 reduction.
ThA2 암호학 : 암호 메카니즘의 실현 및 응용, 암호학의 이론적 실무적 측면, 암호 알고리듬의 선택과 응용과의 관계, 각종 암호 시스템, 키관리, 인증 및 신분확인, 전자서명, 해쉬 함수.
ThO1 확률론 : 네트워, 암호 분석을 위한 확률의 성질과 계산. 통계적 자료 처리 이론 및 방법론.
ThO2 스테가노그라피 : 정상적인 데이터 내부에 정보를 은닉하는 기법. 저작권 보호, 불법 사용자 추적 기법, DOI.
ThD1 현대암호이론 : 암호학의 수학적 기반, 영지식 증명, 비밀공유방식, 스트림 암호(선형 복잡도), 인증 기법, 블라인드 서명, 공정한 서명 기술, 차세대 암호 기술, 블록, 공개키 암호 알고리듬등 핵심 암호 알고리듬 설계 기술 및 복잡도 이론.
ThD2 암호분석론 : DC/LC 해독기술, 블록 암호에 대한 차분 공격, 선형 공격, 연관키 공격, 보간 다항식 공격, 난수의 통계 평가 방법, 난수열의 각종 복잡도 개념 및 스트림 암호의 각종 공격 방법.
ThD3 계산대수학 : 타원곡선, Number Field, Lattice, Group Action등 대수학적인 이론.
MaB1 전자상거래보안 : 전자상거래 시스템의 보안 요구사항 분석, 필요 메카니즘의 정의, 전자상거래를 위한 각종 보안 응용 프로토콜 제시, 예를들면, SET, SSL/TLS, IPSEC등.
MaA1 전자지불 방법론 : 전자상거래를 위한 각종 온라인 전자화폐, 오프라인 전자화폐, 전자수표를 이용하는 각종 지불 수단, 전자지불 시스템의 장단점과 보안상의 문제.
MaA2 정보시스템 감리 : 정보시스템의 Risk와 통제의 기본 개념 파악, 통제 요소 발굴, 운영상의 감리 요소 파악, CISA 자격증
MaO1 정보통신 윤리 : 정보통신의 역기능 방지를 위한 각종 대책 및 솔루션 파악
MaO2 해킹 및 바이러스 : 해킹 수단에 대한 조사 및 방지 방안, 바이러스 및 해킹 방지를 위한 정책적 지침
MaD1 정보보호 정책 : 암호관련 법과 제도의 개요 파악, 암호 정책의 설정 원칙 제시, 암호 사용/규제 정책, 암호키 위탁 및 복구 정책등 법적, 제도적인 문제와 각종 정책 수행에 따른 사회적 문제점을 분석, 정보보호 서비스가 사용되기 위한 법적, 제도적 요구사항.
MaD2 정보보호 표준 및 평가 : 각종 단체의 표

준화 활동 및 평가 기법과 활동 조사, 표준 알고리즘 및 프로토콜 개발.

MaD3 정보시스템 위험 분석 : 대용량 정보시스템, 교통, 원자력, 항공등 국가 기반구조의 위험 분석 및 대처 방안

PrB1 프로세서 기본 구조와 설계 : 각종 디지털 기본 게이트 및 Flip-flop등의 설계 및 구성 방법.

PrA1 OS 보안 : Win, Unix, Linux, NT등의 보안 요구 조건들을 살펴보고 OS가 가진 취약성을 논함.

PrA2 암호 프로세서 설계 : FPGA등을 이용하여 암호 알고리즘의 칩 구현 실습 및 필요한 몽고메리 알고리즘등 연산 알고리즘.

PrO1 스마트 카드 보안 : ISO 7816, 스마트 카드 파일, 명령어 구조 및 신분확인 카드, SET 카드등의 응용.

PrO2 Tamper-Resistant 설계 : FIPS 140-1의 Tamper-Resistantfmf fdnl한 구축 방법론과 적용.

PrD1 COS, 무선 emulator들과 보안 메카니즘 : 각종 에뮬레이터에서의 암호 알고리즘과 프로토콜 구현.

PrD2 보안 장비의 설계 : 보안 장비의 설계를 위한 요구 조건 분석 및 요소 메카니즘의 정의, case study.

PrD3 무선 환경 보안 메카니즘 설계 : 무선 단말등을 위한 보안 메카니즘의 정의와 알고리즘, 프로토콜 개발

NeB1 데이터 통신 : 데이터 통신 구조 및 모델, 단말 장치, 통신망 관련 소프트웨어 개발.

NeA1 네트웍 보안 : 기존 통신망 분석 및 암호 기술과의 결합, 근거리 통신망 보안 및 네트웍 상의 인증 및 키 관리

NeA2 인터넷 보안 : IPsec등의 인터넷 보안 프로토콜을 통한 인터넷 보안 기술 습득, www 보안.

NeO1 침입탐지 및 차단 : 침입 차단 및 탐지 기술의 구현과 관련 상용 제품 분석 및 효율성 평가 방법론.

NeO2 유무선 LAN 보안 : IEEE 802.10과 Bluetooth 중심의 LAN 보안 메카니즘 파악.

NeD1 VPN 이해 : 넷트웍 보안 제품의 총합으로서의 VPN의 이해와 구현 및 작동 메카니즘 파악.

NeD2 이동통신보안 : 이동 통신망에서의 보안 요구사항 분석, 키 관리 기법, CDMA, IMT2000 보안.

NeD3 안전한 네트웍 프로그래밍 : 정보통신용 보안 SW 개발을 위한 프로그래밍 기법, 프로세스 관리 및 프로세스간 통신등.

CsB1 암호 프로토콜 : 정보보호 프로토콜 개념과 종류, 키 분배, ID, 비밀분산, 영지식 증명.

CsA1 DB 보안 : DB 보안의 엑세스 제어 기법, concurrency 및 그 control, 분산 DB 보안등.

CsA2 유무선 PKI : 인증 기술의 개요, 인증 서버의 구성, RA등 주변 시스템 요소, 인증서 활용 기술

CsO1 키 관리 프로토콜 : 키복구 및 관리 기법, 각국의 기 위탁, 관리 체계, 키 생성 관리에 따른 방법론.

CsO2 Language Security : 객체 지향언어의 보안, 자바 프로그래밍 및 보안, Encapsulation 기법

CsD1 접근통제 : 생체인식, OPT(One Time Password), SSO(Single Sign On) 등의 접근 통제 기법 연구

CsD2 바이러스 해킹 대항 : 시스템 버그, hole 등에 의한 시스템 해킹 방지 및 바이러스 대항 기술, 국가 기반 구조 보호 일환.

CsD3 차세대 컴퓨터, 시스템 보안 : 양자 컴퓨터등의 차세대 컴퓨터 이론 수립, 새로운 시스템에 대한 취약성 분석.

위와 같은 학과 과목 외에도 다음과 같은 과목들이 개설될 수 있다.

사이버 수사 기법과 사이버 범죄,
생체인식의 기법 및 제품 동향,
라우터,게이트웨이 보안
DNA 계산등 미래지향적 계산 알고리즘

본 교과과정은 학생들의 배경과 요구에도 유연하게 적용될 수 있을 뿐 아니라 정보보호 전문가의 역할 기반 직무 분석등에도 유용하게 활용될 수 있다.

V. 결 론

본 논문에서는 학부 및 대학원 학위 과정의 교육과정 모델을 제시하였다. 먼저 학부 과정의 경우는 현재 4년제 대학의 교과과정 중 학사 학위 취득 최소 전공 학점수는 35학점이다. 심화 전공의 경우 70학점까지 개설할 수 있으나, 현재 교육 인적자원부의 권고나 대학의 추세로 볼 때, 부전공 혹은 복수 전공으로 다양한 학문 분야를 학사 학위과정에서 이수하도록 하고 있는 바, 본 연구에서도 45학점 20과목의 교과 내용을 학부 과정의 교과 과정으로 제시할 수 있었다. 다만 70학점의 경우도 필요하다고 이에 대한 제안도 학과목 위주로 기술하였다. 이 경우는 아래에서 언급할 영역 전공 과목과 연계되는 경우를 말한다. 언급한 대로 45학점의 교육과정을 제안하되 다음과 같은 분류를 하여 대학원 과정과의 체계적 연계성을 담보하도록 하였다. 즉 정보보호 전문 인력의 그동안 출신 전공등을 고려하고 추후 기술 발전 방향을 예측하여 학부의 전공 과정을 다음 5개 분야로 대별하였다.

1. 법, 경영, 행정
2. 컴퓨터과학, 공학
3. 전자공학
4. 통신공학
5. 수학,물리

이러한 구분이 절대적인 것은 아님은 물론이며, 현재 학사과정에서 많은 교과목들은 중복되어 나타나고 있다. 예를 들어 수학 전공의 학생들이 컴퓨터 과학 학과목을 몇 과목 수강할 수 있으며, 나아가 부전공, 복수전공을 할 수 있기 때문이다. 또한 학교에 따라서는 전자공학과 통신공학의 융화가 있는 교육과정이 있을 수 있는 등 위의 분류가 절대적인 것은 아니다.

대학원 학위과정은 정보 보호 석사 박사 학위과정이 타전공과 독립적으로 개설되는 경우 전공자의 학사 학위 전공을 무시할 수 없는 바, 이의 배경을 고려한 교과과정 모델을 제시하였으며, 이 경우 6과목을 핵심 과목으로 나머지 6과목을 교차 과목으로 설정하였다. 현재 석사 박사 학위 과정을 연계시키고 있는 추세에 비추어 석사 박사 학위 과정 간의 교과목의 구분은 하지 않았다. 또한 야간에 개설되는 특수 대학원 석사학위 과정은 그 성격으로 보아 보수 교육의 범위에 들어가야 하는 경우도 있으나 교육의 주체를 고려한 결과 이 영역에서 다루고 있다. 특수 대학원은 과목당 2학점 체계로 되어있음을 고려하여 교과과정을 구성하려하였으나, 정규 과정과의 내용상 차이만을 둘 수 있었을 뿐이다.

최근 활성화되고 있는 정보보호교육에 대한 정책 설정 시 고려되어야 할 교과과정 및 그 운영 요구사항들에 대해 확인할 수 있다. 이러한 요구사항들은 국내 정보보호 전문 인력 양성 정책 수립 시 중요한 참고 자료로 활용 가능할 것이다. 즉 실용적 현장 적용 기술 인력과 연구 인력에 대한 체계적 교육 내용을 기업 및 대학에 권고할 수 있으며, 국가 공인 자격증 제도 및 교육 인증제등을 통한 정보보호 교육 내용의 견실화를 정책적으로 유도할 수 있으며, 또한 국가 공공 기관 수요 인력 및 정보전 대응 인력을 양성함에 있어서 전문 기관 설립등 정책적인 관점을 설정하는데 활용할 수 있으리라 예견된다. 더 나아가 본 연구결과를 통해 빠른 기간 안에 구체적 정보보호 인력 양성체계, 예를 들면 국가적 정보보호 교육 전문 기관 설립, 정보보호 교육 인증제 도입등을 검토 시행함으로써 국내 정보보호 인력 확보와 기술 축척을 도모할 수 있으며, 이는 고용 창출과 수출 증대등의 산업적 측면과 직결되는 등 그 파급효과가 상당할 것으로 예상된다.

정보보호 산업은 미래의 큰 산업분야로 자리 매김을 할 것으로 기대된다. 이러한 정보보호 산업에 필요한 인력과 대학이나 기타 연구기관에서 양성하는 인력과의 수급을 맞춤으로써 정보보호 산업의 보다 효율적인 발전을 기대할 수 있을 것이다. 또한 전문 인력을 양성하기 위해서, 현재 각 기관과 학교에 산재해 있는 교육 과정을 체계적이고 연계성 있게 수행하여야 하며, 교육 과정의 균형과 교육 과목의 유연한 합리적 구성을 이룩해야만 한다.

아울러 본 논문은 정보보안 교육 과정을 개설하는 대학과 대학원에 참고자료로 활용될 수 있다. 각 대학등에서의 교수 경험과 문제점등을 비교할 수 있으며, 표준적인 교과 내용으로 지속적인 향상을 도모할 수 있는 파급효과를 예견할 수 있다. 그리고 산업체에서 활발히 개설하고 있는 정보보호 과정에 대한 질적 향상을 도모할 수 있는 파급효과가 있다. 현재의 자의적 교과 과정 개설과 상이한 교과 과정을 이수하였음에도 같은 역할을 수행하도록 하는 중대한 결함을 보정할 수 있는 파급효과가 있다.

감사의 글

본 논문은 정보통신부 학술진흥 사업의 연구 결과로 이루어진 것입니다[3][4][5]. 국내에서는 이와 같은 정보보호 교육 관련 연구에 관심을 기울이지 않을 때인데도 연구 수행을 적극 지원하여주신 정보통신부 이 헌 사무관, 한국정보보호센터 교육 홍보팀께 감사드립니다.

참 고 문 헌

[1] Mark Wilson, "NIST Special Pub. 800-16", US Dept of Commerce, NIST, 1998

[2] 이경애, 김 철, "NIST SP 800-16소개", 1999 한국통신정보보호학회 종합학술발표회 논문집 Vol. 9, No. 1, pp 219-227

[3] 김 철, "정보보호 교육과정 개발 연구"2000 정보통신 학술진흥사업 연구보고서, 지정연구 15, 2001.4, 정보통신부

[4] 김 철, "정보보호 인력 수급 및 활용방안 연구" 한국정보보호센터 최종연구보고서, 기술지원연구 99-4, 1999.12 한국정보보호센터

[5] 김 철, "정보통신 보안 전문인력 양성 방안" 제5회 정보보호 심포지움(SIS 2000) 발표집 pp. 573-582, 2000.6

〈著者紹介〉

김 철 (Chul Kim)

84년 2월 : 연세대학교 이과대학 수학과 학사

89년 12월 : 미국 North Carolina 주립대 대학원 수학과 석·박사

1989년 1월 ~ 89년 6월 : 미국 North Carolina 주립대 수학과 강의조교

1988년 8월 ~ 90년 6월 : 미국 Shaw University 수학/정보학과 전임강사

1989년 8월 ~ 90년 6월 : 미국 North Carolina 주립대 수학과 Post Dr.(강사)

1990년 8월 ~ 91년 2월 : 미국 University of South Dakota 수학과 조교수

1991년 3월 ~ 현재 : 광운대학교 자연과학대학 수학과 교수

1997년 1월 ~ 1년간 : 한국학술진흥재단 지원 국비 해외파견 교수로 University of British Columbia 수학과 연구 방문 Visiting Scholar

연구 분야 : 암호학 및 암호해독론, 정보통신보호 이론 및 응용, 정보통신 보안 관리, 감리, 정책, 모의실험 이론(Simulation Theory), Symbolic and Algebraic Computation, 응용 대수학