

실무중심 정보보안 교육을 위한 셀 기반 입체교육 모델

최 상 용,^{*} 김 정 삼, 이 규 창[†]
영남이공대학교 (교수)

CTD-Edu: Cell-Based Three-Dimensional Education Model for Information Security Education

Sang-Yong Choi,^{*} Jeong-Sahm Kim, Kyu-Chang Lee[†]
Yeungnam University College (Professor)

요 약

최근 정보보안의 중요성이 더욱 커지면서 대학의 정보보안 관련 학과를 포함한 민간 또는 사설 교육기관의 정보보안 관련 학과가 증가하고 있다. 이와 같은 교육기관의 커리큘럼을 분석한 결과 전공과목에 관련하여 NCS에서 언급하고 있는 직무능력과 많은 관련이 있는 것으로 보이며, 이는 직무능력별 표준화된 교육수준을 제공할 수 있는 장점이 있다. 하지만 교과목 기반의 교육과정은 교육 기관별 중복 커리큘럼, 강사의 수준에 따른 교육품질, 필요한 요소기술의 적시 교육 등에 대한 한계점이 발생할 수 있다. 본 논문에서는 대학 및 민간 또는 사설 교육기관의 교육과정을 분석하고, 한계점 해결을 위한 셀 기반 입체교육 모델을 제안한다. 제안하는 모델은 발생 가능한 한계점을 효과적으로 개선할 수 있음을 전문대학 교육과정을 기초로 검증한다.

ABSTRACT

Recently, the importance of information security has become greater. For this reason, the number of departments related to information security at universities and professional educational institutions is increasing. It is analyzed that the curriculum of such educational institutions has a lot to do with the job competency mentioned in NCS in relation to major subjects. This has the advantage of providing a standardized level of education for each job competency. However from the perspective of students there may be limitations on duplicate curriculum quality of education according to the level of teachers and timely acquisition of necessary elemental skills. In this paper we analyze the curriculum of universities and professional educational institutions and propose a cell-based three-dimensional education model to address the limitations of students. We verified based on the college curriculum that the proposed model can effectively improve its limitations.

Keywords: Information Security, Cyber Security, Education, curriculum, Model

1. 서 론

최근 정보보안 분야는 ICBM(IoT, Cloud Computing, Big-Data, Mobile)으로 대표되는 4차산업혁명의 핵심기술의 안전한 구현과 활용을 위

한 필수요소로 그 중요성이 더욱 커지고 있다[1]. 한국인터넷진흥원에서 발표한 2021년 사이버위협 전망에 따르면 표적형 공격 랜섬웨어의 확산, 코로나 19 사이버 공격, 클라우드 서비스공격, 5G를 이용한 IoT 제품에 대한 보안 위협 등으로 4차 산업혁명 기술에 대한 위협이 대부분을 차지하고 있다[2].

정보보안에 대한 중요성이 커지면서 정보보안 인력양성의 필요성 또한 증가하고 있으며, 많은 대학에서는 정보보안관련학과를 신설하거나 기존의 IT 관련 학

Received(08. 17. 2021), Modified(09. 13. 2021),
Accepted(09. 13. 2021)

^{*} 주저자, spikechoi@ync.ac.kr

[†] 교신저자, skynsoul@ync.ac.kr(Corresponding author)

과들을 정보보호 학과로 개편하여 운영하고 있다[3]. 유사한 이유로 정부에서는 정보보안 인재가 갖추어야 할 직무능력을 국가직무능력표준(NCS, National Competency Standards)으로 정의하고 있다[4]. 산업체 등에서 NCS를 활용함으로써 인해 많은 교육기관에서 NCS를 기반으로 교육과정을 구성하게 되어, 인해 어떤 기관에서 교육을 수료하더라도 특정 직무에 대해서는 공통적인 직무능력을 키울 수 있지만 교육 기관별 중복된 커리큘럼으로 인해 유사한 별개 교육과정을 수료할 때, 유사한 과목과 내용을 중복하여 수강해야 하는 현실적인 문제점 또한 존재하는 것이 현실이다. 이에 본 논문에서는 정규 교육기관과 민간 또는 사설 교육기관의 각 교육과정을 분석하여 교육수혜자 입장에서의 한계점을 분석하고, 이를 해결하기 위한 방향을 제안하고자 한다.

이를 위해 2장 관련 연구에서는 국내 대학의 정보보안 관련학과의 커리큘럼 및 민간 또는 사설 교육기관의 커리큘럼을 분석하고, 3장에서는 분석결과 도출된 한계점과 한계점을 해결하기 위한 접근 방향과 새로운 교육모델을 제안하며, 4장에서는 적용모델을

통해 제안하는 교육모델의 적합성을 분석한다.

II. 관련 연구

본 장에서는 정보보안 교육을 진행하고 있는 대학에서의 학과 교과과정과 민간 또는 사설 교육기관에서 진행되는 교육과정에 대해서 분석하고 대학과 기관에서 취하고 있는 교과과정의 방식에 대한 한계와 문제점을 살펴본다.

2.1 정보보안 관련학과의 교육과정

대학의 교과과정 분석을 위해 정보보안 관련 실무중심 교육을 목표로 하는 3개 대학(순천향대학교 정보보호학과, 서울여자대학교 정보보호학과, 아주대학교 사이버보안학과)을 선정하여 학년별 교과목들을 분석한다.

Table 1. The curriculum of the Department of Information Protection at Soonchunhyang University

Grade	Subject	NCS Competency Unit
1	Computer Programming	-
	Discrete Mathematics	-
	Introduction to Information Protection	Planning and Operation of Security Management
	∴	∴
2	Data Communication	Security Equipment Operation
	Cryptology 1	System Security Operations
	Operating System	Digital Forensics
	Assembly language	Planning and Operation of Security Management
	System Programming	Planning and Operation of Security Management
	Computer Network	Security Equipment Operation
	Database Security	Application Security Operations
∴	∴	
3	Cryptology 2	System Security Operations
	Internet Security	Planning and Operation of Security Management
	OS Security	Malware Analysis
	Information Theory	Planning and Operation of Security Management
	Malware Analysis	Malware Analysis
	Design of Management Information System	Establishment of CERT
∴	∴	
4	Technique for Countermeasures against Cyber Terrorism	Digital Forensics
	Practical Information Protection	Security Strategy Establishment Consulting
	Technique for Vulnerability Analysis	Infringement Accident Analysis
	Intrusion Prevention and Detection	Security Event Escalation
	Technique for Countermeasures against Intrusion	Infringement Accident Analysis
	Analysis of Digital Evidence	Cyber Investigation
∴	∴	

2.1.1 순천향대학교 정보보호학과

순천향대학교 정보보호학과는 2001년 한국 최초로 학부과정에 신설된 학과로서 정보보호 관련 기술을 이해하고, 학생과 산업체, 사회가 요구하는 교육 내용을 지속해서 반영하여 창의적인 사고 능력과 공학도로서의 윤리의식과 의사전달능력을 갖춘 글로벌 전문 인재 양성을 교육목표로 하고 있다(5).

학과에서 안내하고 있는 1학년 과정을 살펴보면 기초교양과 더불어 컴퓨터 프로그래밍, 정보보호 개론 등의 기초과목을 교육한다(6). 2학년 과정에서는 데이터통신, 암호학 1, 운영체제 등을 기초과목으로 진행하고 있고, 어셈블리어, 시스템 프로그래밍, 컴퓨터 네트워크, 데이터베이스 보안 등의 정보보호 관련 전공과목을 교육하며, 3학년 과정에서는 암호학 2, 운영체제 보안, 정보이론, 악성코드 분석, 정보보호 시스템 설계 등 심화 과정을 거치고 있다. 마지막으로 4학년 과정에서는 사이버테러 대응기술, 정보보호 실무, 취약점 분석 기술, 침입 차단 및 탐지, 침해대응 기술 등 산업체에서 요구하는 실무 위주의 과목을 교육하고, 인턴십이나 기업연계형 장기현장실습(IPP)을 통해 실무경험을 학생들에게 제공 함으로써 위에서 언급한 학과의 교육목표를 실현하기 위한 충분한 교육과정을 설계하고 있는 것으로 보인다.

위 학과의 전반적인 교과과정을 살펴보면 국가직 무표준(NCS) 정보보안 분야에서 명하시는 대학의 교육 훈련과정의 대부분을 학부기초 형태로 진행하고 있고 전공과목들은 NCS에서 명시하는 직무능력 단위에서 일부 또는 전체를 수행할 수 있도록 설계하고 있는 것으로 보인다. Table 1은 위 학과에서 교육하는 교육과정 일부와 해당 과목을 통해 수행할 수 있는 관련 NCS 직무능력 단위를 보여준다.

2.1.2 서울여자대학교 정보보호학과

서울여자대학교 정보보호학과는 정보보호 전문가로서 갖추어야 할 기초적 이론과 지식, 기술을 습득하는 것은 물론 그에 어울리는 올바른 인성을 함양하고, 정보보호 기술 분야의 전문지식과 실무능력, 사회적 책무성을 겸비한 정보보호 전문가를 양성하는 것을 교육목표로 하고 있다(7).

2021학년도 교과과정 살펴보면 1학년 과정은 컴퓨터 및 정보보호 개론, C/C++ 프로그래밍, 현대 암호학 기초, 이산 수학, 윈도우즈 보안과 운영 실습

등 IT 기반의 기초 학습과 더불어 보안의 기초 이론 위주의 교육이 진행되고 있다. 2학년 과정은 컴퓨터 구조, 데이터통신 및 네트워크, 운영체제 등의 IT 기초과목과 더불어 웹 프로그래밍, 자바프로그래밍, 네트워크 프로그래밍, 모바일 프로그래밍 등 소프트웨어 개발 기초 이론과 보안에 중점을 두고 있는 모양새이다. 3학년 과정에서는 시스템 프로그래밍, 웹 애플리케이션 보안 등의 일부 소프트웨어 관련 수업과 더불어 현대 암호학 응용 및 실습, 침입 탐지와 차단 시스템, 윈도우즈 보안과 악성코드, 클라우드 컴퓨팅 서비스 보안 관리, 인공지능과 정보보호 등 시스템 보안 운영의 수행과 관련된 교과목으로 주 구성을 이루고 있다. 4학년 과정에서는 모바일 보안, 정보보호 관리체계 인증, 디지털 포렌식, 블록체인과 정보보호 등 일부 과목 자체를 NCS의 직무능력 단위로 구성하여 실무능력을 갖춘 정보보호 전문가를 양성하기 위한 과정을 구성하고 있다.

위 학과의 교육과정을 전반적으로 살펴보면 NCS 정보보안 분야에서 명시하고 있는 교육 훈련과정들이 전 학년에 걸쳐 분포되어 있고, 인공지능, 블록체인, 클라우드 등 4차 산업 혁명과 더불어 쟁점이 되는 구체적인 분야를 교과과정으로 구성함으로써 오늘날 빠르게 변화하는 추세에 맞추어 사회가 요구하는 전문지식을 갖춘 인재 양성을 위한 노력으로 보인다. 또한, 전반적인 과목들이 NCS 직무능력 단위의 일부를 수행할 수 있도록 구성되고 있으며, 특히 4학년 과정에서는 NCS 직무능력 단위 자체가 몇몇 과목으로 구성하고 있음을 미루어 볼 때 실무중심의 직무수행 인재 양성을 위한 교육과정 설계임을 보여준다. 위 학과에서 구성하는 학년별 교육과정 일부와 각 교과목의 관련 NCS 직무능력 단위를 Table 2에 정리하였다.

2.1.3 아주대학교 사이버보안학과

아주대학교 사이버보안학과는 회소가치를 인정받는 통섭형 사이버보안 리더 양성이라는 목표 아래 윤리적 사고력과 인간존중 마인드 향상과 현장 실무능력 및 취업 경쟁력 그리고 국제 경쟁력 향상을 교육 목표로 한다. 아주대 사이버보안학과는 정보보호 특성화 트랙별 교육과정 이수 형태를 이루고 있으며, 1, 2학년 과정에서 기초 공통 과목을 진행하고, 3학년부터는 IM (IoT/Mobile) 트랙과 CB (Cloud/Big data) 트랙별로 트랙 심화 과정을 진

Table 2. The curriculum of the Department of Information Protection at Seoul Women's University.

Grade	Subject	NCS Competency Unit
1	Intrusion Detection and Prevention System	
	C++ Programming	Information Security Product Evaluations Consulting
	Fundamentals of Modern Cryptology	System Security Operations
	Windows OS Security and Management	System Security Operations
	∴	∴
2	Computer Architecture	
	Data Communication and Network	Security Equipment Operation
	Operating System	Digital Forensics
	Web Programming	Application Security Operations
	Java Programming	Information Security Product Evaluations Consulting
	Software Security	Information Security Product Evaluations Consulting
∴	∴	
3	Applied Modern Cryptology and Practice	System Security Operations
	Intrusion Detection and Prevention System	Infringement Accident Analysis
	Cloud Computing Services and Security Management	Security Equipment Operation
	Artificial Intelligence & Information Security	System Security Operations
	Windows Security and Basics of Malicious Code	Malware Analysis
∴	∴	
4	Current Topics in Information Security Industry Technology	Managed Security Operations
	Mobile Security	System Security Operations
	Information Security Management System	Information Security Management System
	Digital Forensics	Digital Forensic
	Blockchain & Information Security	System Security Operations
∴	∴	

행한다[8].

1학년 과정은 사이버보안 윤리, 이산 수학, 컴퓨터 프로그래밍 및 실습, 자료구조 및 실습 등 전공 진입 및 기초 소양 교육을 진행[9]하고, 2학년 과정에서는 정보 보호법 제도와 정책, 현대 암호 이론 및 응용, 컴퓨터구조, 객체 지향 프로그래밍, 운영체제, 컴퓨터 네트워크 등의 전공기반 및 사이버보안 진입 교육을 진행한다. 3학년부터는 트랙 심화 과정을 진행하지만, 공통으로 시스템 S/W 보안 및 실습, 모바일 응용 보안 및 실습, 네트워크 보안 및 실습 등을 진행하고, IM 트랙에서는 IoT 플랫폼 보안, 기계학습 및 데이터 마이닝 등을 학습, CB 트랙에서는 데이터베이스, 클라우드 서비스 보안 과목을 학습한다. 4학년 과정에서도 트랙 공통과정이 있어서 캡스톤 디자인, 사이버보안 관제 및 실습, 보안 사례특강, 정보보호 제품 평가 등으로 구성하고, IM 트랙은 사이버 플랫폼 보안, 모바일 네트워크 과목이 있고, CB 트랙은 빅데이터 응용 보안, 분산시스템 등으로 구성된다.

교육과정의 전반을 살펴보면 타 학과와 마찬가지로 정보보안 전문가로서의 기초지식을 습득할 수 있

도록 교과과정이 구성되어 있고, 2개 분야로 트랙화가 나누어져 있지만, 공통으로 진행되는 과목들을 통해서 정보보호의 전문지식을 습득할 수 있으며, 해당 과목들은 NCS의 직무능력 단위의 일부를 수행할 수 있도록 구성이 되어있다. 또한, 정보통신 분야의 새로운 먹거리 창출의 장으로 자리매김하기 위한 ICBM(IoT, Cloud, Big data, Mobile) 분야의 정보보안 전문가를 양성하기 위한 트랙 심화 과정을 통하여 경쟁력 있는 실무 인재를 양성하기 위한 구성을 갖추고 있는 것으로 보인다. Table 3에서 공통 과정 및 트랙 심화 과정의 일부 과목과 관련 NCS 직무능력 단위를 확인할 수 있다.

2.2 민간 또는 사설 교육기관 교육과정

정보보안 전문인력 양성을 위한 민간 또는 사설 교육기관에서 진행되는 교육과정으로는 과학기술 정통부가 주최하고 한국인터넷진흥원이 주관하는 케이실드 주니어(K-Shield Jr.)의 정보보호 관리진단 과정 및 보안사고 분석대응 과정과 한국정보기술연구원에서 주관하는 BoB(Best of the Best)의 교육

Table 3. The curriculum of the Department of Cyber Security at Ajou University.

Grade	Subject	NCS Competency Unit
1	Cybersecurity Ethics	-
	Computer Programming and Practice	Consulting on the evaluation of information protection products.
	Data Structure and Practice	-
	⋮	⋮
2	Information Protection Law and Policy	Security Strategy Establishment Consulting
	Modern Cryptology Theory	System Security Operations
	Computer Architecture	-
	Object-oriented Programming	Information Security Product Evaluations Consulting
	Operating System	Digital Forensics
	Computer Network	Security Equipment Operation
	⋮	⋮
3 (Common)	System SW Security and Practice	System Security Operations
	Mobile Security and Practice	System Security Operations
	Network Security and Practice	Information System Diagnostics
	SW Application Security and Practice	Application Security Operations
	⋮	⋮
3 (IM)	Embeded Software	Information Security Product Evaluations Consulting
	IoT Platform Security	Network Security Operations
	Machine Learning and Data Mining	
3 (CB)	Database	Application Security Operations
	Cloud Service Security	Information System Diagnostics
4 (Common)	Special Lecture on Cyber Security Cases	Security Countermeasures and Design Consulting
	Information Security Product Evaluations	Information Security Product Evaluations Consulting
4 (IM)	Cyber Platform Security	System Security Operations
	Mobile Network	Information System Diagnostics
4 (CB)	Cyber Security Management and Practice	Planning and Operation of Security Management
	Design of Web System	Application Security Operations
	Big data Application Security	Application Security Operations

과정을 비교하여 살펴봄으로 민간 또는 사설 교육기관에서 NCS가 얼마나 반영되어 있는지를 분석한다.

2.2.1 케이쉴드 주니어

케이쉴드 주니어교육은 향후 정보보호 분야 취업 시 현장 실무를 즉각 수행할 수 있는 정보보안 전문 주니어 인력양성을 목표로 하는 프로그램이다. 국가 직무 능력표준(NCS)에 맞춘 실습 중심의 교육과정으로 정보보호 관리 과정과 보안사고 분석대응 과정으로 구성되어 있다. 운영기관별 100명씩 총 200명을 선발하여 200시간 이상의 교육과정 이수 후 취업 지원까지 운영되는 취업 지원 실무 맞춤형 교육과정이다[10].

정보보호 관리진단 과정은 보안 이슈를 미리 진단하고 대비할 수 있는 인재를 양성한다. 커리큘럼을 살펴보면 정보보호 개론이나 시스템, 네트워크, 보안 장비에 관련한 정보보안 기초 학습을 진행하고, 보안

업무 프로세스에 대한 기업보안업무기초를 진행[11]한다. 기초 학습 이후 직무능력 수행을 위한 과정으로 진입한다. 관리 보안 운영에서는 관리적 보안과 물리 보안, 개인정보보호 등에 대한 운영에 대해서 교육하고, 기술 보안 운영을 위해 네트워크, 보안 장비, 시스템 등에 대한 보안 운영을 교육한다. 이어서 정보시스템 진단 부분에서 취약점 진단 방법론, 분석 기법, 진단 보고서 작성방법 등을 교육하며, 마지막으로 모의 해킹 부분에서 모의 해킹 수행절차, 시나리오 작성, 모의 해킹 수행, 대책 수립, 보고서 작성 등에 관해 교육한다. Table 4는 케이쉴드 주니어 정보보호 관리진단의 교육과정 일부를 정리한 내용이다.

보안사고 분석진단 과정은 보안사고 발생 시 문제 원인을 파악하고 조치할 수 있는 인재를 양성한다. 해당 과정에서도 마찬가지로 직무능력 단위로 교육과정이 구성되어 있다. 먼저 보안이벤트 대응에서는 운영체제, 네트워크, 웹 애플리케이션의 취약점에 대해

Table 4. The curriculum of Information Protection Management Diagnostics of K-Shield junior.

Division	Subject
Fundamentals of Information Security	Introduction to Information Protection
	Introduction to Personal Information Protection
	Fundamentals of System
	⋮
Fundamentals of Corporate Security Operations	Keyword for Security Operations
	Keyword for Information Security-related Cities and News
	A taste of Security Operations
	⋮
Management Security Operations	Managed Security Operations
	Physical Security Operations
	Personal Information Protection Operations
	⋮
Technical Security Operations	Network Security Operations
	Security Equipment Operation
	System Security Operations
	⋮
Information System Diagnostics	Criteria of Information System Diagnostic
	Vulnerability Diagnosis Methodology
	Techniques of Information System Analysis
	⋮
Mock Hacking	Execution Process
	Scenario Writing
	Scenario-based Mock Hacking Execution
	⋮

이해하고 대응하는 방법을 학습[12]한다. 이어서 보안 로그 분석을 위해 분석 방법론, 시스템 및 보안 장비 로그 분석 등을 교육하고, 디지털 포렌식 및 디지털 데이터 분석에 대해서도 학습[12]한다. 사이버 수사 직무수행을 위한 인터넷 추적 및 디지털증거 압수 등을 교육하고 악성코드 분석을 위해 리버스 엔지니어링, 예셈블러, 악성코드 분석, 윈도우 프로그래밍 등을 학습한다. 이어서 침해사고 분석을 수행하기 위해 침해 감염 서버와 PC 분석 등에 대해 교육하며 그 외 보안관제 기획/운영, 침해대응팀(CERT) 구축에 대해서도 교육과정에 포함[12]되어 있다.

Table 5는 보안사고 분석대응 과정에 대해 일부를 정리하고 있다.

케이쉴드 주니어에서 운영하는 두 가지 과정을 모두 살펴보면 앞서 언급하였다시피 NCS 중심의 교육

Table 5. The curriculum of Security Incident Analysis and Response of K-Shield junior.

Division	Subject
Security Event Escalation	Understand and Respond to OS Vulnerabilities
	Understand and Respond to Network Vulnerabilities
	Understand and Respond to Web Vulnerabilities
	⋮
Security Log Analysis	Overview and Analysis Methodology
	Advanced Log Analysis
	Log Analysis for Systems Security Equipment
	⋮
Digital Forensics	Digital Forensics and Evidence Collection
	Digital Data Analysis
	Report Generation
Cyber Investigation	Understanding Cyber Investigation Perspectives
	Internet Tracking and Confiscation of Digital Evidence
Malware Analysis	Fundamentals of Reverse Engineering & Assembly
	Malware Analysis
	Window Programming
	⋮
Infringement Accident Analysis	Outline
	Analysis of Infringement Infection Server
	Analysis of Infringement Infection PC
	⋮
Security Management Planning & Application	Security Management Planning & Application
Establishment of CERT	Establishment of CERT

과정이다 보니 몇몇 기초 분야를 제외하고는 교육과정이 명확하게 NCS 직무능력 단위와 일치하는 것을 볼 수 있다. 따라서 하나의 직무능력을 완전히 수행할 수 있도록 관련된 교육들을 모아서 연속된 교육으로 분산도를 낮추고 교육수요자들의 집중도를 높이는 이점이 있는 것으로 보인다.

2.2.2 Best of the Best 프로그램

BoB는 2012년 정보보안 인재 양성을 통한 국가적 보안 난제 해소라는 가치 아래 한국정보기술연구원(KITRI)에서 주관하여 시행되고 있는 차세대 보안 리더 양성 프로그램이다[13]. BoB의 교육과정은 취약점 분석, 디지털 포렌식, 보안컨설팅, 보안제품 개발 등 4가지 트랙으로 구성된다.

취약점 분석 트랙은 보안취약점이 발생하는 원인을 이해하고, 사고를 미리 방지하기 위한 정보보안 기술 동향을 학습[14]한다. 리버스 엔지니어링 기법, 취약점 이해, 네트워크, 운영체제 원리 등을 학습한다. 디지털 포렌식 트랙은 디지털 포렌식 기초 개념을 이해하고, 실 사례연구를 통해 활용방안을 익힌다. 디지털 포렌식 기초, 침해사고 시스템 분석, 시스템 분석 절차 연구 등을 학습한다. 보안컨설팅 트랙은 최신 정보보안 정책과 관리체계에 대해 학습하고 컨설팅 기법 및 법 제도에 대한 이해를 통해 컨설팅 기초 소양을 배양[14]한다. 보안컨설팅 기법, 보안 인증체계 및 법/제도, 감사 및 산업보안 등을 학습한다. 마지막으로 보안 제품 개발 트랙은 보안 통제 기능의 SW를 구현함으로써 정보보안 위협에 대응하고 잠재적인 보안취약점을 제거하고, 보안을 고려하여 기능을 설계 및 구현[14]한다. 개발 보안 방법론, 소프트웨어 개발 보안, 개발 보안 구현 등을 학습한다. Table 6은 BoB의 4가지 트랙에 대해 정리하고 있다.

2.3 현재 교육과정의 한계

지금까지 대학과 민간 또는 사설 교육기관의 교육 과정을 살펴보고 각 기관에서 설계하고 있는 교육과정 전반에 대해 특징들을 분석하였다.

대학의 경우 일반적으로 NCS 정보보호 분야에서 명시하고 있는 교육 훈련과정의 대부분을 기초 학습 형태로 1~2학년 사이 진행을 하고 있다. 2학년 이후 정보보호 관련 전공과목과 심화 과정을 교육하고

Table 6. Four tracks of Best of the Best.

Division	Subject
Vulnerability Analysis	Reverse Engineering Techniques
	Understanding Vulnerabilities
	Principles of Network Operating System
Digital Forensics	Fundamentals of Digital Forensics
	Analysis of Infringement Accident Systems
	System Analysis Procedure Research
	Application Example Research
Security Consulting	Security Consulting Techniques
	Security Certification System and Laws / Institution
	Audit and Industrial Security
	Trend of Security Market
Security Product Development	Development Security Methodology
	Software Development Security
	Enhancement Activities of Development Security
	Implementation of Evelopment Security

있고, 전공 교과목들 대부분이 NCS 직무능력 수행을 위한 근거가 될 수 있어 현 대학 기관의 정보보호 학과들이 실무중심의 교육을 위해 큰 노력을 하고 있다고 보인다. 하지만 이러한 노력에도 불구하고 대학이라는 특성상 교과목 기반으로 교육과정을 편성하고 있고 각 과목은 직무능력 단위의 수행 준거로서 일부만을 차지하고 있어, 학과의 모든 교육과정을 조합한다고 하여도 하나의 능력 단위 전체를 수행하기에는 다소 부족한 부분이 아쉬움을 남긴다.

반면, 민간 또는 사설 교육기관의 경우 교육의 목표 자체가 NCS 기반의 실습 중심 교육을 표방하고 있기에 교육과정의 분류 자체가 직무능력 단위로 구성되어 있고, 명시되어 있는 직무능력 모두를 수행하기 위한 학습들로 구성이 되어있어서 하나의 직무를 수행에 필요한 교육을 집중하여 효율적으로 학습할 수 있다는 장점이 있다.

하지만 대학 기관과 민간 또는 사설 교육기관의 교과과정을 비교하였을 때 중복되는 과정들이 다수

존재한다. 물론 대학과 같은 정규 교육기관과 민간 또는 사설 교육기관의 교육목적이 상이하므로 단순히 과목명과 NCS를 기준으로만 비교하는 것에는 한계가 있는 것이 사실이지만, 이것은 편성된 교육과정에서 특정 수준의 학습을 받기 위해서 이미 다른 기관에서 습득하고 있는 지식을 중복하여 교육받아야 할 수 있으며, 이는 학생을 포함한 교육수요자의 관점에서 그만큼 불필요한 시간 낭비가 될 수 있을 가능성이 있음을 절대 간과해서는 안 된다. 교육수요자는 내가 원하는 수준의 교육을 적시에 수강한다면 그만큼 시간의 효율성과 만족도를 높일 수 있을 것으로 판단된다.

또한, 각 기관에서 교과목을 수업을 진행하기 위해서 한 명의 강사가 꽤 오랫동안 많은 범위를 담당하여 강의하는 것이 매우 일반적이다. 통상적으로 대학의 경우 15주, 교육기관은 수십 시간을 할당받아 강의가 진행된다. 대다수 이 부분에 대하여 전통적 관레이자 매우 당연한 방식이라고 생각할 수 있지만 다르게 말하면 한 과목 질이 강사의 역량에 따라 강의 품질이 정해질 수 있다. 즉, 같은 과목이지만 강의 품질의 일관성을 보장하는 것에 한계가 있다.

따라서, 오늘날 교육과정에서는 각 기관에서 구성하는 중복된 커리큘럼 문제와 원하는 수준의 교육을 적절한 시기에 수강할 수 없는 문제, 그리고 강의 품질의 일관성 유지에 대한 새로운 고찰과 방향성 제시가 요구된다.

III. 셀 기반 입체교육 모델

3.1 기존 교육모델 개선 방향

관련 연구에서 분석한 바와 같이 기존의 교육모델은 교육 기관별 중복된 커리큘럼, 강사의 강의 품질 일관성 확보 한계, 필요한 지식과 기술을 적시에 습득할 수 없는 한계 등 크게 3가지의 한계를 가지고 있다. 또한, 부가적으로 효과적인 정보보안 전문인력 양성을 위해서는 중등교육과를 포함한 중등교육과정과 고등교육과정이 충분한 연계성을 가지고 이루어져야 한다. 이와 같은 한계점을 개선하기 위한 방향으로서는 중복된 커리큘럼을 최소화하고, 필요한 지식과 기술을 교육수요자가 필요한 시점에 적시에 선택할 수 있는 방향으로 모델이 개발되어야 한다. 또한, 강사의 수준에 따른 최소한의 품질 확보를 위해서는 교육의 단위를 세부적이고 최소화된 단위로 나누어 강사의 수준에 따른 교육품질 저하에 대한 대응력을 높일 수 있는 모델이 개발되어야 한다. 이와 유사한 한계점 해결을 위한 방안으로 나노 디그리, 마이크로 디그리[15]와 같은 학점기반학위 제도가 연구되고 있으나, 기존의 디그리 시스템은 교과목 기반 시스템으로 언급한 한계점을 모두 해결하기에는 한계가 있다. 본 논문에서는 이와 같은 한계점을 개선하기 위해 셀(CELL) 기반 입체 교육모델인 CTD-Edu(Cell-based Three-Dimensional Education) 모

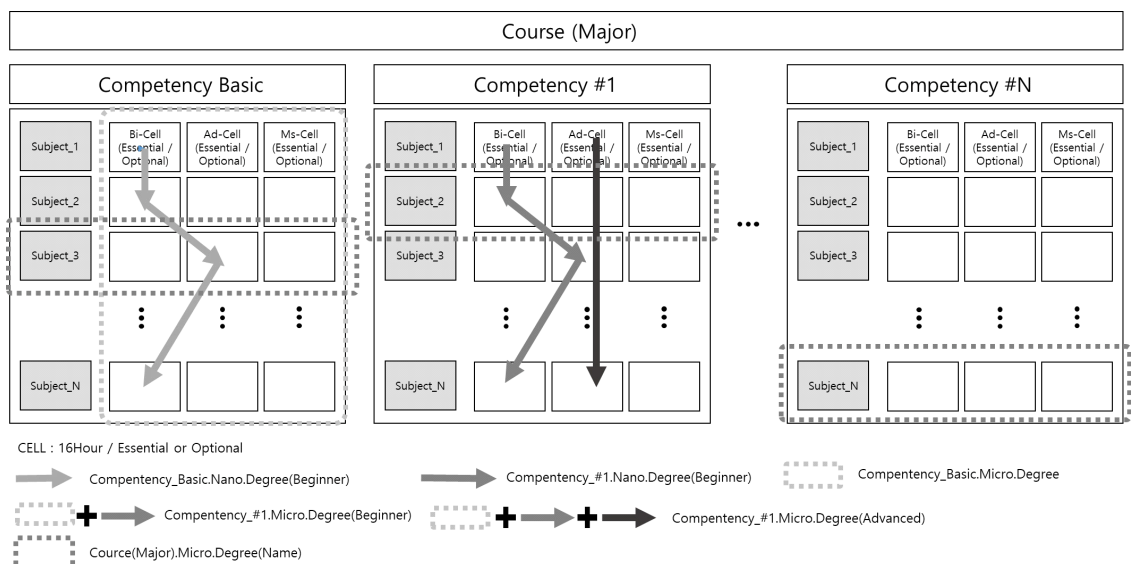


Fig. 1. Cell-based Three-Dimensional Education Model

델을 제안한다. 제안하는 모델은 과목보다 세분화된 학습단위를 셀로 정의하고, 셀을 유기적으로 연계하여 과목과 학습 과정을 설계하는 방법이다.

3.2 CTD-Edu 모델

제안하는 CTD-Edu 모델은 통상적인 대학교육의 1과목(3학점, 15주)을 3개 또는 4개의 단위 셀로 나눈다. 각 커리큘럼의 셀은 Bi-Cell(Beginner Cell), Ad-Cell(Advanced Cell), Ms-Cell(Master Cell)로 구성되어 한 과목의 학습을 목적에 따라 단계별로 수강할 수 있도록 지원한다. 수 개의 셀로 구성된 과목을 직무에 필요한 유사/연계 과목을 통합하여 전공을 구성한다. 각 과목을 구성하는 셀은 필수 셀과 선택 셀로 구성하여, 수준과 직무에 따라 마이크로 디그리, 나노 디그리로 코스를 구성한다.

이러한 교육모델의 전체 구성은 Fig. 1과 같다.

3.2.1 CTD-Edu 모델의 세부구조

제안하는 모델에서 수여하는 디그리는 기본적으로 셀의 수준에 따라 특정 직무의 Bi-Cell 중 필수 셀과 선택 셀 중 활용하고자 하는 교육기관에서 설계하고 결정한 기준을 충족하는 경우 “직무.Nano.Degree(Beginner)”와 같은 나노 디그리를 수여할 수 있다. 또한, 특정 직무에 포함된 CELL의 수료조건을 만족하는 경우 “직무.Micro.Degree”를 수여할 수 있다. 또한, 각 직무의 특정 과목들로 구성된 마이크로 디그리 과정을 구성할 수도 있다. 이처럼 제안하는 모델은 활용하고자 하는 교육기관에서 각 셀 단위로 교육과정을 유기적으로 연계하여 나노 디그리와 마이크로 디그리를 교육수요자에게 제공할 수 있다. 교육수요자 입장에서는 본인이 직무를 위해 필요한 셀 만큼 학습함으로써 불필요한 학습의 시간을 단축할 수 있고 실제적인 교육의 효과를 나타낼 수 있는 장점이 있다.

3.2.2 CTD-Edu 모델 적용 통한 한계점 개선

제안하는 모델을 활용한다면, 먼저 셀이 세분화됨으로 인해 교육품질에 대한 교육 강사의 의존도가 낮아진다. 즉, 기존 전체 한 과목을 한 명의 강사가 교육한다고 가정하면 강사의 수준에 따라 전체적인

교육의 품질이 결정되는데, 한 과목을 셀로 나누어 셀별 최적의 강사들로 구성한다면, 한 강사의 수준이 상대적으로 낮다고 하더라도, 다른 셀 강의를 통해 보완할 수 있다. 또한, 각 과목이 셀 단위로 세분화됨으로 인해 교육생의 관점에서 기존에 수강한 과목을 중복해서 수강해야 할 필요성이 줄어들고, 한 과목 전체라 하더라도 교육생이 필요에 따라 요구되는 셀만 수강할 수 있도록 지원함으로써 필요한 교육을 적시에 지원할 수 있다. 물론 세 번째 적시적 교육 제공의 경우 상시적으로 과정이 개설되어 있어야 한다는 전제가 있지만, 기존과 같은 과목 기반의 교육과정 대비 상대적으로 적시성이 높아질 수 있다.

또한, 셀을 효과적으로 구성한다면 학습 나이에 따라 초등학교, 중학교, 고등학교, 대학교, 재직자 등 선행학습의 수준 및 기초교육의 수준에 따라 필요한 셀을 추출하여 정보보안에 대한 인식 제고, 공통 기초과정, 초·중급 과정을 유기적으로 연계할 수 있고, 만약 대학의 학사관리체계에서 이러한 선수학습을 인정할 수 있는 학사제도가 마련된다면 진정한 평생교육의 모델로 성장할 수 있을 것으로 예상된다.

3.2.3 CTD-Edu 모델 적용을 위한 기준체계 개선

제안하는 CTD-Edu 모델의 안정적인 정착을 위해서는 먼저 정규교육과정의 학사운영 체계가 변화될 필요가 있다. 지금과 같은 학점 위주의 학사정책은 제안하는 셀 단위의 학습모델을 그대로 적용하기에는 한계가 있다. 제안하는 교육모델을 효과적으로 적용하기 위해서는 제안모델에서 제시하는 디그리 단위의 학습모델에서 일정 디그리 이상을 수료한 경우 학위를 수여하는 방향으로 학사운영이 유연하게 변화되어야 한다. 또한, 다양한 교육수요자의 요구를 충족시키기 위해 선행학습인정제도(RPL, Recognition of Prior Learning)가 보다 폭넓게 적용되어야 한다. 예를 들어 재직자의 경우 선이수가 반드시 해당 디그리의 선수과정을 이수하는 것뿐만 아니라 선수과정을 이수한 것과 같은 동등한 자격을 갖춰있음을 평가하고 검증할 수 있는 경력 및 직무 기반의 다양한 기준이 마련되어야 할 필요가 있다. 이를 위해 교육모델을 설계하는 교육기관에서는 셀, 과목구성, 전공 구성 등이 유기적으로 연계될 수 있는 다양한 디그리 코스를 정의하고, 필요에 따라 교육수요자가 수강한 셀을 연계하여 일정 수준에 도달할 경우 수요자가 디그리를 제안할 수 있는 시스템으로까지 확장되어야 할 것

이다. 물론, 현재의 정규교육 시스템에서 학기나 학점체계를 단기간에 변화시키는 것을 쉽지 않은 부분이 있지만, 장기적인 측면에서 충분히 검토되고 시범 적용과 같은 방법으로 순차적으로 검증할 방안이 필요하다.

IV. 모델 적용 설계 및 분석

CTD-Edu 모델의 실효성을 검증하기 위해 현재 영남이공대학교 사이버보안계열의 교육과정을 기초로 하여 모델 적용을 설계하고, 학습 과정을 분석하였다. 현재 영남이공대학교 사이버보안계열의 교육과정은 Table. 7과 같다. 사이버보안계열의 교육목표에 따른 세부직무는 보안사고 분석 및 대응, 정보보호 관리 및 운영, 정보보호 진단 및 분석, 인공지능 보안 등의 4가지 직무와 직무수행을 위한 공통과정으로 직업(군)공통 과목이 학기별로 배치되어 있다. 대부분 교과목은 NCS를 기준으로 3학점 45시간 기준으로 작성되어 있으며 이는 대부분의 정규대학 교육과정과 같다. 계열의 세부 전공은 정보보안전공과 인공지능보안전공 두 가지로 분류되며, 두 전공은 직업

(군)공통 직무에 해당하는 과목과 보안사고 분석 및 대응, 정보보호 관리 및 운영 등의 직무에 대해서는 대동소이하게 수강하여야 하며, 두 전공에 따라 정보보안전공의 경우 정보보호 진단 및 분석 직무에 해당하는 교과목을 인공지능보안전공은 인공지능보안 직무에 해당하는 교과목을 이수하여야 한다. 그리고 학과에서 비교과 과정으로 진행하고 있는 과정의 경우 6개월 코스의 “쿠버네틱스 기반의 클라우드 시스템 개발자 양성 과정(이하 클라우드 과정)”을 운영하고 있으며, 학생들의 경우 한국인터넷진흥원(정보보호지원센터), BoB 과정 등에 개별적으로 참여할 수 있다.

이러한 교육체계는 기존 교육체계의 한계점인 중복된 커리큘럼이 존재한다. 예를 들어 클라우드 과정의 경우 6개월 중 1개월 이상을 리눅스 시스템, 네트워크, 웹 개발, 파이썬 등의 기초과목을 수강하여야 한다. 하지만 클라우드 과정에 참여하는 학생의 대부분은 학과 교과목을 수강하는 과정에서 이와 같은 기초직무는 모두 이수한 경우가 대부분이다. 따라서 교육수요자 측면에서는 중복과목을 다시 수강해야 하는 문제점이 있을 수 있으며, 이로 인해 수업의 집

Table 7. The curriculum of the Department of Cyber Security at YeungNam University College

Grade	Core job	Subject
1	Analysis and response to security incidents.	Python Programming
	Information protection management and operation.	Linux System Operation
		Web Programming
	Information protection management and operation.	Networking
	Artificial intelligence security.	Introduction and practice of Artificial Intelligence.
∴	∴	
2	Analysis and response to security incidents.	Firewall
		Secure Programming
		Intrusion Detection System
	Information protection management and operation.	Database Security
		Operation System Security
		Hacking and Cracking
		Secure Script
Artificial intelligence security	Penetration Test	
	Artificial Intelligence Programming	
∴	AI and Big-data Analysis	
∴	∴	
3	Analysis and response to security incidents.	Security System Operation
		Reversing Engineering
		Security Event Analysis
		Security Accident Response
	Information protection management and operation.	Network Analysis
		Vulnerability analysis.
Artificial intelligence security.	Deep Learning	
∴	∴	

중도와 몰입도가 하락하는 요소가 발생할 수 있다. 물론, 학과 정규 교과목에서 배우는 기초과목과 클라우드 과정에서 필요한 기초과목에 대한 지식수준이 다를 수 있어 후자에서 추가적인 교육이 필요할 수는 있지만, 그럼에도 불구하고 만약 클라우드 과정에 선행학습이수제도에 대한 평가와 인증 기준이 있다면 기존 학과에서 학습한 정규 교과목의 같은 과목을 이수하지 않아도 되어 교육수요자 입장에서의 비용 절감과 사회적 비용 절감의 효과가 있을 것으로 예상된다.

현재 사이버보안계열의 파이썬 프로그래밍 교과목을 대상으로 분석해 보면, 파이썬 프로그래밍의 학습 수준은 파이썬 문법, 파이썬 라이브러리, 파이썬 응용 등 파이썬의 공통적인 내용을 학습하게 된다. 하지만 클라우드 과정에서 필요로 하는 파이썬의 내용은 파이썬 라이브러리 중 데이터 분석에 활용되는 Pandas, Numpy 등과 같은 응용 라이브러리 활용 능력이 필요하다. 이를 위해 교육과정에서 파이썬 기초문법부터 응용까지를 모두 다루게 된다. 따라서 이 두 과정을 모두 수강하는 학생의 경우 파이썬 정규과목 45시간(3시간/15주)을 수강하고, 클라우드 과정에서 파이썬 과목을 32시간 정도를 수강하게 된다. 이 32시간 중 약 12시간 이상은 파이썬 기초문법과 응용을 수강하는데 이 두 과정을 모두 수강하는 학생의 경우 최소 12시간의 중복 커리큘럼이 발생한다. 한 과목으로는 이 시간이 커 보이지 않지만 중복된 4과목을 합산하게 되면 최소 48시간 이상의 시간을 더 투입해야 하는 문제가 발생할 수 있다. 만약 정규 과목을 셀 단위로 구성하고, 클라우드 과정도 셀 단위로 구성하게 되면 선행학습인증과정을 거쳐 후자의 과정을 신청한 학생은 후자 교육과정의 셀 중 1개 셀 이상을 선이수로 인정할 수 있게 되어 실제적인 교육의 효과 및 실제 필요한 수강생의 수업 집중도 및 질 제고가 가능한 것으로 판단된다. 만약, 직무별 다양한 교육기관의 다양한 커리큘럼을 셀 단위로 세부적으로 구성하고 각 셀의 교육목표를 명확히 한다면 개별 교육기관의 디그리 이수를 인정할 수 있게 되고, 이를 통해 교육수요자의 만족도 향상과 교육기관의 교육 효과를 높일 수 있을 것이다.

V. 결 론

최근 4차산업혁명과 IT 기술의 발전으로 인해 정보보안의 중요성은 그 무엇보다 커지고 있으며, 대학

및 민간 또는 사설 교육기관의 정보보안 관련 과정이 증가하고 있다. 이러한 현상은 정보보안 인력수급이라는 측면에서는 긍정적인 요소가 분명하지만, 교육수요자 입장에서는 중복 커리큘럼, 적시에 필요한 교육을 받을 수 없는 점 및 강의 품질의 일관성 확보 문제 등 문제점 또한 내포하고 있다. 이런 측면에서 본 논문에서는 현재 정규 교육기관과 민간 또는 사설 교육기관의 교육과정을 분석하여 교육수요자 관점에서 개선해야 할 한계점을 분석하고, 한계점을 개선하는 방향으로 새로운 교육모델인 셀 기반 입체교육 모델(CTD-Edu)을 제안하였다. 제안한 모델은 교육단위를 보다 세분화한 셀로 나누고 각 셀을 종과 횡으로 입체적으로 구성하여 나노 디그리, 마이크로 디그리와 같은 형태로 그룹화하는 교육과정으로 교육수요자 입장에서는 중복된 수강을 최소화하고 필요한 교육을 적시에 받을 수 있는 모델이다. 또한, 셀을 세분화함으로써 강사의 수준에 따른 강의의 질에 대한 영향을 최소화할 수 있다. 하지만, 제안하는 모델을 현재의 교육과정에 적용하기 위해서는 현재의 학사운영시스템이 유연하게 개선되어야 하며, 일률적인 학점 위주의 학위부여 체계를 탈피하여 디그리와 학위를 연계하는 방향으로 개선되어야 할 것이다. 따라서 앞으로는 제안하는 셀 기반 입체교육 모델을 적용하기 위해 세부적으로 학사운영체계가 어떻게 변해야 하는지를 지속적으로 연구할 계획이다.

References

- [1] The Presidential Committee on the 4th industrial revolution, "Technology, and the Fourth Industrial Revolution," <https://www.4th-ir.go.kr/4ir/detail/8?boardName=code1>, Accessed: Jun, 2021[Online]
- [2] Krcert, "The Trend of Cyver Threats at 2021", https://krcert.or.kr/data/reportView.do?bulletin_writing_sequence=35878, Accessed: Jun, 2021[Online]
- [3] Higher Education in Korea, "Information Security", <https://www.academyinfo.go.kr/mjrinfo/mjrinfo0450/doInit.do>, Accessed: Jun, 2021[Online]
- [4] National competency Standards, <http://ncs.go.kr/unity/th03/ncsSearchMai>

- n.do, Accessd: Jun. 2021[Online]
- [5] The Department of Information Protection(Soonchunhyang Univ.), "The educational objective," <https://homepage.sch.ac.kr/security/01/03.jsp>, Accessd: Jun. 2021[Online]
- [6] The Department of Information Protection(Soonchunhyang Univ.), "The curriculum," https://www.swu.ac.kr/www/futured_1.html, Accessd: Jun. 2021[Online]
- [7] Seoul Women's Univ., "Department of Information Security," https://www.swu.ac.kr/www/s-pdf/2021_futured.pdf, Accessd: Jun. 2021[Online]
- [8] The Department of Cyber Security(Ajou Univ), "The educational objective," <http://security.ajou.ac.kr/security/edu/edu01.jsp>, Accessd: Jun. 2021[Online]
- [9] The Department of Cyber Security (Ajou Univ), "The curriculum," <http://security.ajou.ac.kr/security/edu/edu02.jsp>, Accessd: Jun. 2021[Online]
- [10] K-Shield Jr., "Trainees Recruitment," <http://kshieldjr.org/hr/home?custom=&year=2021&lastLoginTime=&isCmpt=false>, Accessd: Jun. 2021[Online]
- [11] K-Shield Jr., "The curriculum - Information Protection Management Diagnostics," http://kshieldjr.org/tlnt_mu01_001.do, Accessd: Jun. 2021[Online]
- [12] K-Shield Jr., "The curriculum - Security Incident Analysis and Response," http://kshieldjr.org/tlnt_mu01_002.do, Accessd: Jun. 2021[Online]
- [13] BEST OF THE BEST, "Greetings," <https://www.kitribob.kr/intro/about>, Accessd: Jun. 2021[Online]
- [14] BEST OF THE BEST, "Guidance of Track," <https://www.kitribob.kr/learn/curriculum>, Accessd: Jun. 2021[Online]
- [15] Sumii Park, Ahn Jeongmin, "Analysis of Domestic Application Cases of Micro-Degree as Competency-Based Education," *Journal of Lifelong Learning Society (JLLS)*, 17(1), pp. 173-197, Feb. 2021

 <저자소개>



최 상 용 (Sang-Yong Choi) 정회원

2000년 2월: 한남대학교 수학과 졸업

2003년 2월: 한남대학교 컴퓨터공학과 석사

2014년 2월: 전남대학교 정보보안협동과정 박사

2012년 2월~2015년 12월: 한국과학기술원 사이버보안연구센터 책임연구원

2015년 12월~2017년 9월: 한국폴리텍대학 정보보안과 조교수

2017년 10월~2019년 2월: 한국과학기술원 사이버보안연구센터 연구교수

2019년 3월~현재: 영남이공대학교 사이버보안계열 조교수

<관심분야> 네트워크 보안, 웹보안, 악성코드 분석, 정보보호 교육



김 정 삼 (Jeong-Sahm Kim) 정회원

1987년 2월: 경북대학교 전자공학과 졸업

1990년 2월: 경북대학교 컴퓨터공학과 석사

2011년 2월: 경북대학교 컴퓨터공학과 박사

1990년 3월~1995년 3월: 국방과학연구소 연구원

2002년 3월~현재: 영남이공대학교 사이버보안계열 교수

<관심분야> 정보보호교육, 정보보호컨설팅, 모빌리티보안



이 규 창 (Kyu-Chang Lee) 정회원

2009년 2월: 영남이공대학교 컴퓨터정보계열 졸업

2010년 2월: 학점은행제 컴퓨터공학 학사

2013년 2월: 경북대학교 모바일통신공학과 석사

2020년 8월: 경북대학교 컴퓨터학부 박사

2013년 3월 ~ 2018년 6월 : (주)사람과세상 IoT솔루션팀 팀장

2020년 3월~현재: 영남이공대학교 사이버보안계열 조교수

<관심분야> 인공지능 보안, 웹 보안, IoT 보안, 클라우드 컴퓨팅