Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.3, Jun. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.3.527

국내외 정보보안 교육의 현황 및 인공지능의 발전에 따른 청소년 정보보안 정규교육의 중요성에 대한 연구*

정 다 혜,[1†] 전 상 훈[2‡]
[1,2]수원대학교 (학생, 교수)

A Study on the Current Status of Domestic and International Cybersecurity Education and the Importance of Regular Cybersecurity Education for Teenagers according to the Development of AI*

Dahye Jeong,[1†] Sanghoon Jeon[2‡]
[1,2]The University of Suwon (Student, Professor)

요 약

디지털 시대가 도래하면서 인공지능(AI)의 발전과 디지털 기술의 급속한 통합이 일어나고 있다. 이런 변화는 우리 사회에 많은 기회를 제공하지만, 그와 동시에 정보보안에 대한 위협도 증가시키고 있다. 특히 청소년들은 디지털 기술을 손쉽게 받아들이는 '디지털 네이티브'로, 이러한 변화를 선도하는 주역이다. 하지만, 청소년들은 정보보안에 대한 충분한 이해와 지식 없이는 기술을 안전하게 사용하는 데 어려움을 겪을 수 있다. 따라서 본 논문은 영국, 호주, 미국의 청소년 정보보안 교육체계를 살펴보고, 이를 바탕으로 한국에서 청소년 정보보안 교육 도입의 중요성과 효과적인 실행 방안을 제시한다. 이들 국가는 이미 청소년을 대상으로 한 정보보안 교육을 실시하고 있으며, 이는 사이버 위협에 대비하고 미래 사회를 위한 인재를 양성하는 중요한 역할을 하고 있다. 이러한 국제적 추세를 반영하여 한국도 정보보안 교육을 필수적으로 도입하고 청소년들이 기술적, 비기술적 영역을 모두 이해할 수 있도록 교육체계를 마련해야 한다. 이를 통해 청소년들이 디지털 시대의 정보보안에 대비할 수 있는 튼튼한 기반을 마련하고, 미래 사회에서 요구되는 정보보안 역량을 갖출 수 있을 것이다.

ABSTRACT

In the digital age, the growth of AI and digital technologies brings opportunities and cybersecurity risks. At the forefront of this change are teenagers, referred to as 'digital natives'. However, they may have difficulty using technology safely without proper information security knowledge. This paper highlights the need for information security education for teenagers in South Korea by referring to cases in the UK, Australia, and the US. These countries are already providing education that prepares young people for cyber threats and future societal needs. Reflecting this trend, South Korea should also establish comprehensive information security education for teenagers to equip them for the digital age.

Keywords: Adolescents, Cybersecurity, Education, Regular Education

Received(03. 25. 2024), Modified(05. 28. 2024), Accepted(05. 29. 2024)

* 본 연구는 2021년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2021R1I1A1A0104094313)

† 주저자, jts9006@suwon.ac.kr
‡ 교신저자, shjeon@suwon.ac.kr(Corresponding author)

I. 서 론

인공지능(Artificial Intelligence, AI)의 발전은 효율적인 패턴 인식, 자연어 처리, 데이터 분석 등 다양한 분야에서 획기적인 성과를 거두며 눈에 띄는 효과를 보이고 있다[1][2]. AI의 성장은 우리에게 새로운 기회를 제공하며, 고도의 패턴 인식 능력을 통해 사용자에게 맞춤화된 정보를 제공하는 등의 활용 사례를 보여주고 있다[3]. 이는 사용자가 원하는 정보를 더욱 정확하게, 빠르게 얻을 수 있게 해주며, 이는 기회의 폭을 넓히고 있다[4].

그러나, AI의 급속한 발전은 우리 사회의 많은 부분에 영향을 미치는 동시에, 새로운 보안 위협을 야기하고 있다[5]. 이러한 문제는 특히 청소년들에게 중요하다. AI 기술이 우리 생활의 많은 부분에 통합됨에 따라, 청소년들은 더 이상 선택적으로 기술을 사용하는 것이 아니라 필수적으로 사용해야 하는 상황에 놓여 있다[6]. 이로 인해 청소년들이 새로운 사이버 위협에 노출될 위험성은 더욱 높아지고 있다[7]. 특히, 아직 보안 및 윤리 관련 가치관이 형성되지 않은 청소년들은 이러한 위험성이 더욱 높다[8]. 이러한 청소년들은 자신들도 모르게 '사이버 범죄' 활동에 가담하게 될 가능성이 있다[9]. 이는 청소년들이 기술을 사용하는 능력이 그들의 기술에 대한 이해를 뛰어넘을 때 발생하는 문제다.

이러한 이유로, 청소년들에게 정보보안의 중요성을 가르치는 정규교육이 필수적이다[10]. 이는 단순히 기술적인 지식을 넘어, 정보보안의 윤리적 가치와 그 중요성에 대한 인식을 높이는 것을 목표로 해야 한다[11]. 이를 통해 청소년들은 안전한 인터넷 사용 방법을 배우고, 사이버 위협을 인식하며, 그리고 이에 적절하게 대응하는 방법을 습득할 수 있어야 한다[12]. 그러나 이러한 교육은 단기간에 이루어질 수 있는 것이 아니다. 교육과정은 청소년들이 정보보안에 대한 중요성을 인식하고, 기술을 책임감 있게 사용하는 방법을 배울 수 있도록 체계적이고 지속적으로 이루어져야 한다[13][14]. 이러한 필요성을 인식하고 교육에 투자하는 대표적인 사례로, 영국의 경우 'Computing Programmes of Study: National Curriculum in England'를 통해 체계적인 정보보안 교육을 실시하고 있다[15]. 이 프로그램은 Key Stage 2에서 학생들에게 안전한 기술 사용법과 개인정보를 보호하는 방법, 그리고 온라인에서 겪을 수 있는 다양한 문제에 대한 도움과 지원을 찾는 방법에 대한 교육을 제공한다[16].

이런 배경 속에서, 본 논문은 국내 청소년들의 체계적인 정보보안 교육을 위해 국내외의 정보보안 교육과정을 비교하며, 체계적인 정보보안 교육의 필요성 및 방안에 대해 다루고자 한다.

본 논문은 Ⅱ장에서 국내외 정보보안 교육 현황 비교분석을 통해 한국의 정보보안 교육이 어떤 방향으로 나아가야 하는지 연구한다. Ⅲ장에서는 국내외 교육체계 분석을 종합적으로 활용하여 청소년 정보보안 정규교육의 필요성을 강조하고, Ⅳ장에서는 이를 실현하기 위한 방안을 제시하며 결론을 맺는다.

II. 국내외 정보보안 교육체계 분석

2.1 국내 정보보안 교육체계

2.1.1 2022 개정 초중등학교 실과(기술・가정)/정보과 교육과정

현재 국내에서 가장 최신에 개정된 2022년 개정 초중등학교 실과(기술・가정)/정보과 교육과정에 대한 내용이다[17]. 해당 교육과정은 21세기 정보화 사회의 구성원으로서 필요한 기본적인 능력 배양을 목표로 하며, 모든 학생이 이수해야 하는 공통 교육과정과 학생 스스로 선택하여 수강할 수 있는 선택중심 교육과정으로 나누어져 있다. 한국에서는 해당 교육과정을 통해 학생들에게 정보보안에 대한 개념을 가르치고 있다. 아래 Table 1에서는 2022년 개정된 초·중학교 실기(기술·가정) 또는 정보과 교육과정의 정보보안 교육을 포함한 과목과 내용을 요약한 것이다.

Table 1. Analysis of domestic information security curricula

Course name	Information
Course Types	Choice-based curriculum
Goals	Understand the development and changes in society brought about by digital technology, and develop attitudes and abilities to recognize and practice the importance of information protection and information security

Content organization	Computing systems	
	Data	
	Algorithms and programming	
	Artificial intelligence	
	Digital culture	
Digital Culture	Core Ideas	Living safely in a digital society requires following the rules of data protection and information security
	Content element	
	Knowledge and understanding	Information privacy and security
	Courses and Features	Identify issues that require the application of information protection and security technologies and apply workarounds
	Values and attitudes	Good privacy and security awareness
Achievement Criteria	Understand the need for information security and leverage security technologies to practice digital ethics	

그러나 이 과목은 학생들이 스스로 선택해야만 수강할 수 있는 선택과목이며, 공통 교과과정에서 정보보안 교육이 이루어지지 않기 때문에 이 과목을 선택하지 않는 학생들은 정보보호의 기본 개념조차 배우지 못한다.

2.1.2 사이버 10만 인재 양성 방안

국내 교육과정 이외에도 정부에서는 최정예 사이버 인력 양성을 위해 2022년 7월에 발표된 '사이버 10만 인재 양성 방안'을 추진하고 있다[18]. 해당 방안의 목표는 실전형 사이버 인력 10만 양성, 최정예 전문 인재 2,000명 육성, 우수 보안 스타트업 25개의 창업 지원하는 것이다. 인재 양성 인력의 분포는 아래 Fig. 1과 같다.

이러한 정책의 추진 방향은 누구나 사이버 보안 교육을 받고 성장할 수 있도록 교육 저변(온라인, 지역, 글로벌)을 확장하는 것에 있다. 이를 위해 Fig. 2는 사이버 인재 양성을 위한 두 가지 교육과정을 보여준다. 첫째, 화이트해커에 대한 진입장벽을 낮추고 잠재력 있는 보안 인재에 재능 사다리 제공을 위한 '화이트햇 스쿨' 과정을 신설한다. 둘째, 정보기술(IT) 개발 인력을 선발하여 보안 교육·창업을 지원하는'S-개발자' 과정 신설한다.

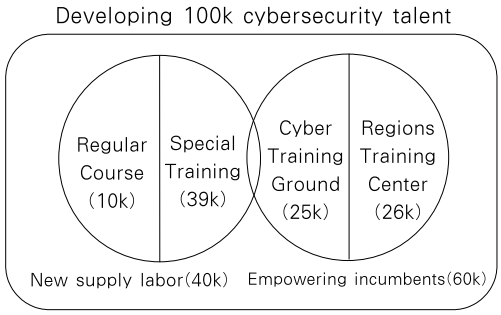

Fig. 1. Cybersecurity 100K talent distribution

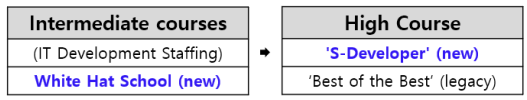

Fig. 2. Curriculum

이 밖에도 K-Shield Jr, Security Academy 등 다양한 프로그램이 있으며, Table 2는 **학교**에서 공부하는 **학생**들이 참여할 수 있는 프로그램을 정리하였다. 그 중, '청소년'들이 참여할 수 있는 프로그램은 유일하게 신설된 '화이트햇 스쿨' 과정 한가지로 매우 제한되어 있음을 알 수 있다.

Table 2. State of Information Security Education Programs in Korea

S-Developers	Organization	KISIA, Ministry of Science and ICT
	Period	2023~present
	Target	Information Security Development SW Development Ability and personality
	Contents	Network ,Systems, Cryptography, Devops, Project

	Training Duration	24.3 ~ 24.12 (10 months)
AI Security	Organization	KISIA, Ministry of Science and ICT
	Period	2023~present
	Target	College Student, Graduate (Expected) Information Security Advancement Hee 75 dead
	Contents	Malware, Network, Privacy, Project
	Training Duration	23.5 ~ 23.10 (6 monthes)
Ontact Converged Security	Organization	KISIA, Ministry of Science and ICT
	Period	2023~present
	Target	Job seekers, information security professionals, students, researchers, and others who want to improve their information security skills and are interested in the field. interested in
	Contents	Malware analysis and technology trends using AI, IoT security incident analysis and response, Cloud security, OT security
	Period	23.7 ~ 23.11 (4 months)
Best of the Best (BoB)	Organization	KITRI, Ministry of Science and ICT
	Period	2012~present
	Target	16 years of age or older
	Contents	Vulnerability analysis, digital forensics, security consulting, security product development, Project
	Training Duration	23.7 ~ 24.3 (9 months)
White Hat	Organization	KITRI, Ministry of Science and ICT
School	Period	2023~present
	Target	24 years old or younger
	Contents	background, system hacking, web hacking, forensics, cloud, project
	Training Duration	24.3 ~ 24.9 (7months)

2.2 국외 정보보안 교육체계 분석

2.2.1 영국 교육체계

영국은 국가에서 의무적으로 컴퓨터 프로그래밍 정규 커리큘럼(Computing programmes of study)을 운영하고 있다. 영국의 교육부인 UK Department for Education 기관에 따르면 전체적인 교육체계는 Key Stage 1부터 4까지 나뉘며, 만 5세에서 만 16세까지의 학생들이 교육을 받는다[19]. 해당 정규 커리큘럼의 목적은 학생들이 컴퓨터가 작동하는 방식과 프로그래밍에 컴퓨터를 활용하는 방법을 배우는 것이다. 교육과정에서 각 Stage마다 정보보안에 대해 다루고 있기 때문에 영국의 모든 학생은 전반적으로 정보보안 교육을 받고 있다. 이는 정보 과목을 선택한 학생 일부만이 정보보안 교육을 듣는 국내 교육방식과는 매우 다른 방식이다. Table 3은 이러한 영국의 정규교육 과정 중 각 Key stage별 정보보안 강의 내용이 담겨있다.

Table 3. Information security lessons by key stage in the UK

Key stage 1
Use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies
Key stage 2
Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact
Key stage 3
Understand a range of ways to use technology safely, respectfully, responsibly

and securely, including protecting their online identity and privacy; recognise inappropriate content, contact and conduct and know how to report concerns
Key stage 4
Understand how changes in technology affect safety, including new ways to protect their online privacy and identity, and how to identify and report a range of concerns

교육 내용을 간략히 요약하면, 정보보안의 기술적인 내용(안전 및 보안성 기술 사용, 개인정보보호, 기술 변화에 따른 안전성 고려 등)보다는 학생들이 쉽게 배울 수 있는 비기술적인 내용들이 중점을 두고 있다.

2.2.2 호주 교육체계

호주의 국가 교육 커리큘럼을 개발하는 호주 표준 및 평가 공단 ACARA(Australian Curriculum, Assessment and Reporting Authority)은 F-10이라는 명칭의 교육체계를 가지고 있다[20]. Table 4는 호주의 F-10 교육과정 중 학년별 정보보안 강의 내용이다. 만 5세에서 만 15세 사이 학생들을 교육하며, 정보 시스템에 대한 깊은 이해를 통해 학생들이 데이터와 디지털 시스템을 효과적으로 선택, 활용, 관리함으로써 학생들이 자신의 미래를 설계할 수 있도록 하는 것을 목표로 하는 정규교육이다. 1학년부터 10학년까지는 정보보안과 관련된 교육을 다수 진행하고 있으며 주로 디지털 윤리, 개인정보보호, 데이터 보안에 대해 배운다. 호주도 영국과 마찬가지로 정규교육을 통해 정보보안을 가르치고 있는데, 이는 일부 학생만이 선택과목을 통해 정보보안 교육을 받는 국내 교육 방식과 크게 다르다.

Table 4. Information security course content by grade level in Australia

Foundation to 2
Emphasize on using technology in a safe and respectful manner, ensuring personal information remains private. It's critical to identify resources for help and support when encountering concerns about the content or contact on the internet or other online technologies
Years 3 and 4
Encourage the use of technology in a responsible, safe, and respectful manner. Recognize what constitutes acceptable and unacceptable behavior when using technology, and identify a variety of ways to report any concerns about content and contact
Years 5 and 6
Understand a variety of methods to use technology in a safe, respectful, responsible, and secure manner. This includes protecting online identity and privacy, recognizing inappropriate content, contact, and conduct, and knowing the procedure to report such concerns
Years 9 and 10
Comprehend how technological changes can affect safety, including new strategies to protect online privacy and identity. It is also important to understand how to identify a range of concerns and know the appropriate channels for reporting them

2.2.3 미국 교육체계

미국의 경우 주마다 다른 교육제도와 구조로 인해 아직 정규교육이 활성화되지 않았으나, 2010년에 발표된 국가 사이버보안 교육 추진 프로그램 NICE(National Initiative for Cybersecurity Education)를 통해 정보보안 정규교육에 관심이 있음을 확인할 수 있다. NICE는 혁신적인 21세기 사이버 보안 교육, 훈련 및 인식을 통해 미국의 경제적 번영을 촉진하고 국가 안보를 보장하며 사이버 보안을 개선하는 것을 목표로 한다[21]. 교육은 초등학교부터 대학교, 그리고 직장까지 다양한 단계에서 시행되며, 정보보안에 대한 중요성을 인식하고 이를 실제로 적용할 수 있는 능력을 배양하는 데 초점을 맞추고 있다. NICE 프로그램 내에는 K-12 교육 프로그램을 포함한다. K-12는 미국 교육 시스템을 대표하는 용어로 유치원부터 고등학교 졸업까지의 교육을 의미하며, 공개된 로드맵을 통해 정보보안 교육을 어떻게 실행해 나갈지 정의하고 있다[22].

미국의 각 주마다 다른 교육커리큘럼을 가지고 있지만, 미국도 NICE 프로그램을 통해 정보보안에 대한 중요성을 인식하기 위한 정규교육 실시에 관심을

갖고 있음을 확인할 수 있다. Table 5는 미국의 K-12 교육체계에 따른 Cyber Security 교육 로드맵을 나타낸다.

Table 5. US National K12 Cybersecurity Education Roadmap

1	Increase Cybersecurity Career Awareness
	Grow and sustain youth and public engagement in promoting cybersecurity career awareness and exploration
2	Engage Students Where Disciplines Converge
	Identify, design, and share cybersecurity resources for the future STEM and cybersecurity workforce
3	Stimulate Innovative Educational Approaches
	Enrich K12 cybersecurity education instruction and learning
4	Promote Cybersecurity Career Pathways
	Cultivate youth pursuing cybersecurity or cybersecurity-related credentials (e.g., diplomas, degrees, certificates, certifications, badges)
5	Prioritize Research
	Enhance efficiency and effectiveness of K12 cybersecurity education programs and instructional practices

III. 청소년 정보보안 정규교육 도입의 필요성

현재 우리는 초지능(Super-intelligence)으로 대표되는 4차 산업혁명 시대를 경험하고 있으며, 이는 우리 생활 방식과 근무 환경에 극적인 변화를 불러오고 있다[23]. 글로벌 연구 및 자문 회사인 Gartner는 정보 기술 관련 연구와 컨설팅 서비스를 제공하는 기업으로, 기술 관련 통찰, 연구, 분석 및 자문 서비스를 통해 기업 리더들이 중요한 결정을 내릴 수 있도록 객관적이고 심층적인 정보를 제공한다. 이러한 Gartner의 발표에 따르면, AI 소프트웨어 시장은 2021년까지 620억 달러에 이를 것으로 예상되는데, 이는 AI 기술의 급속한 성장을 의미한다(Fig. 3.)[24].

이러한 변화는 우리 사회에 많은 기회를 제공하지만, 그와 동시에 여러 가지 새로운 보안 위협도 안고 온다. 특히, 청소년들은 디지털 기술의 발달로 인해 더 큰 영향을 받는데, 통계청 자료에 따르면, 코로나 펜데믹 이후 대한민국의 전체 인터넷 이용률 및 청소년 인터넷 사용률이 지속적으로 증가하고 있음을 아래 Fig. 4를 통해 확인할 수 있다.

이는 청소년들이 인터넷과 디지털 기술을 더 많이 사용함에 따라, 정보보안에 대한 이해와 교육의 중요성이 더욱 강조된다는 것을 의미한다.

따라서, 4차 산업혁명 시대에 맞는 새로운 기술 및 정보보안에 대한 체계적인 교육을 통해 청소년들이 기술을 안전하고 책임감 있게 사용할 수 있도록 준비시키는 것이 필요하다[25]. 청소년들이 이러한 교육을 통해 사이버 보안의 중요성을 인식하고, 위협을 식별하며, 적절한 대응 방법을 배우게 된다면, 그들은 기술의 발전을 활용하여 좀 더 안전하게 성장하고 발전할 수 있을 것이다[26].

이와 같은 배경을 바탕으로, 한국에서 청소년을 대상으로 한 정보보안 정규교육의 도입은 단순히 청소년을 보호하는 차원을 넘어, 미래 사회에서 요구되는 기술적 역량과 보안 의식을 갖춘 인재를 양성하는

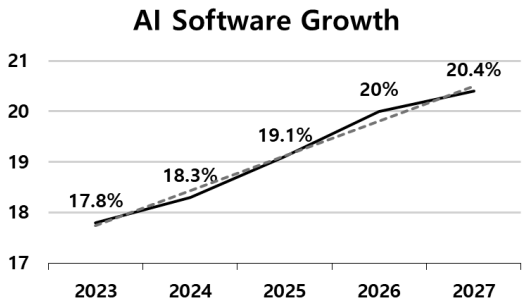

Fig. 3. AI Software Growth by Gartner

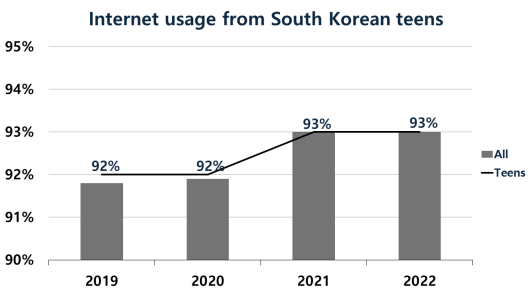

Fig. 4. Internet usage from South Korean teens

데 중요한 역할을 할 것이다. AI 기술의 급속한 발전과 그에 따른 보안 위협의 증가는, 청소년들이 기술을 두려워하지 않고, 오히려 적극적으로 그 기술을 활용하여 성장할 수 있는 환경을 조성하는 데 중요한 동기가 될 것이다.

IV. 정보보안 정규교육 실행방안

본론에서 조사한 바를 바탕으로 영국과 호주 사례를 살펴보면, 이들 국가는 각각의 교육 체계에 적합한 형태로 프로그래밍 정규교육을 실시하고 있으며, 여기에 정보보안 교육도 포함하고 있음을 확인할 수 있다. 이러한 선진국의 사례는 한국에서 청소년 대상의 정보보안 정규교육 도입과 실행 방안을 모색하는 데 중요한 참고 자료로 활용될 수 있다.

따라서 아래 Table 6을 포함해 한국 교육 체제에 정보보안 교육을 새롭게 추가하는 것을 제안한다. 구체적으로는 2022년 개정 초중등학교 실과/정보 교육과정의 공통 교육 내용 체계 중 주요 세 가지 항목인 기술적 문제해결과 혁신, 지속가능한 기술과 융합, 디지털 사회와 인공지능에 정보보안 교육 내용을 포함시키는 것이다. 이를 통해 학생들이 디지털 시대에 필요한 보안 인식과 기술을 배울 수 있도록 각 항목에 적절한 정보보안 교육 내용을 통합한다는 것이 핵심이다.

기술적 문제해결과 혁신 항목의 경우 기술을 활용하여 창의적인 해결을 통해 지식재산을 보호하며, 친환경 에너지 사용으로 자원 및 환경 문제를 해결하는 것이 목표이며 **지속가능한 기술과 융합**의 경우 건설, 로봇, 정보통신, 생명기술 분야에서의 다양한 기술적 융합을 통해 인류의 쾌적하고 지속 가능한 미래 생활을 실현하는 것을 목표로, **디지털 사회와 인공지능** 항목은 디지털 사회의 다양한 문제를 해결하고 인간의 생활을 향상시키기 위해 프로그래밍과 인공지능 기술을 활용하는 것을 목표로 한다.

아래 Table 6은 각 내용 체계 항목별 목표와 적합한 정보보안 정규교육 실행방안을 제시하고 있다.

이와 같은 정보보안 교육의 도입과 실행은 한국의 정보보안 인식과 역량을 향상시키고, 미래 사회에 대비한 우수한 인재를 양성하는 데 크게 기여할 것으로 기대된다.

Table 6. Implementation plan for regular information security education according to domestic curriculum

<table>
<tr><td rowspan="2">Separation</td><td colspan="2">Content element</td></tr>
<tr><td>Elementary school</td><td>Middle School</td></tr>
<tr><td></td><td>Grades 5 - 6</td><td>Grades 1 - 3</td></tr>
<tr><td rowspan="2">Technical problem solving and innovation</td><td>The concept of copyright</td><td>Copyright law</td></tr>
<tr><td colspan="2">Explore ways to protect your intellectual property through copyright infringement cases</td></tr>
<tr><td rowspan="2">Converging with sustainable technologies</td><td rowspan="2">Basic programming training</td><td>IoT Security Concepts</td></tr>
<tr><td>IoT Security Hands-on with Component Utilization</td></tr>
<tr><td rowspan="2">Digital society and artificial intelligence</td><td>Basic programming training</td><td>Secure Coding</td></tr>
<tr><td colspan="2">Learn security concepts and defense measures through real-life hacking cases (social engineering techniques, keyloggers, etc...)</td></tr>
</table>

V. 결 론

인공지능의 발전과 디지털 기술의 급속한 통합으로 인해 우리 사회가 변화하고 있는 가운데, 청소년들은 프로그래밍 능력뿐만 아니라 정보보안에 대한 이해도 필요하게 되었다. 이에 본 논문에서는 국내 청소년 정보보안 교육의 현황을 살펴보고, 호주, 영국, 미국 등 다른 국가의 정보보안 교육 체계 및 현황과 비교 분석하여 국내 청소년 정보보안 교육 도입의 중요성을 제기하였다. 해외 주요 국가들은 청소년 대상 정보보안 교육을 초등학교부터 청소년기까지 지속적으로 실시하고 있는 반면, 한국은 선택 과목으로 제한되어 있어 청소년들이 정보보안을 깊이 있게 이해하는 데 제약이 있음이 나타났다.

청소년 정보보안 교육은 단순히 청소년을 사이버 위협에서 보호하는 것을 넘어, 미래 사회를 위한 인재를 양성하는 중요한 역할을 한다. 따라서, 한국에서도 청소년 정보보안 정규교육을 도입하고, 이를 효

과적으로 실행하는 방안을 집중적으로 모색하는 것이 필요하다. 이를 통해, 청소년들이 사이버 위협에 대비할 수 있는 기반을 마련하고, 미래 사회에서 요구되는 정보보안 역량을 갖추는 데 기여할 수 있을 것이다.

또한, 청소년 정보보호 교육의 효율적인 방법론과 커리큘럼 개발, 실행 및 평가에 대한 체계적인 연구가 필요하며 교육의 장기적 효과와 영향에 대한 심도 있는 후속 연구가 필요하다.

결론적으로, 본 논문은 청소년 정보보안 교육의 중요성을 강조하며, 한국의 교육 체계 변화를 주장한다. 이를 통해 청소년들이 디지털 시대의 정보보안 위협에 대비하고, 미래 사회의 요구를 충족하는 정보보안 역량을 갖출 수 있도록 기대한다.

References

[1] S. Russell and P. Norvig, Artificial Intelligence: a modern approach, 3rd ed., Pearson, pp. 695-714, 937-978, Apr. 2016.

[2] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning, MIT Press, pp. 326-372, 373-422, Dec. 2016.

[3] M. Chui, J. Manyika, M. Miremadi, N. Henke, R. Chung, P. Nel, and S. Malhotra, "Notes from the AI frontier: Insights from hundreds of use cases," McKinsey Global Institute, pp. 12-18, Apr. 2018.

[4] I. Sutskever, O. Vinyals, and Q. V. Le, "Sequence to sequence learning with neural networks," Advances in Neural Information Processing Systems, vol. 27, pp. 3104-3112, Dec. 2014.

[5] S. Russell and P. Norvig, Artificial Intelligence: a modern approach, 3rd ed., Pearson, pp. 695-714, 937-978, Apr. 2016.

[6] S. Livingstone and E. Helsper, "Gradations in digital inclusion: Children, young people and the digital divide," New Media & Society, vol. 9, no. 4, pp. 671-696, Aug. 2007.

[7] U. Hasebrink, S. Livingstone, and L. Haddon, and K. Ólafsson, "Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU Kids Online," EU Kids Online, pp. 5-50, July 2009.

[8] J. Wolak, K. Mitchell, and D. Finkelhor, "Online victimization of youth: 5 years later," National Center for Missing & Exploited Children Bulletin, pp. 9-14, 2006.

[9] T. Heiman and D. Olenik-Shemesh, "Cyberbullying experience and gender differences among adolescents in different educational settings," Journal of Learning Disabilities, vol. 48, no. 2, pp. 146-155, 2015.

[10] R. M. Kowalski, G. W. Giumetti, A. N. Schroeder, and M. R. Lattanner, "Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth," Psychological Bulletin, vol. 140, no. 4, pp. 1100-1104, 2014.

[11] S. Livingstone and E. Helsper, "Gradations in digital inclusion: Children, young people and the digital divide," New Media & Society, vol. 9, no. 4, pp. 671-696, 2007.

[12] J. Wolak, K. Mitchell, and D. Finkelhor, "Online victimization of youth: 5 years later," National Center for Missing & Exploited Children Bulletin, pp. 9-14, 2006.

[13] T. Heiman and D. Olenik-Shemesh, "Cyberbullying experience and gender differences among adolescents in different educational settings," Journal of Learning Disabilities, vol. 48, no. 2, pp. 146-155, 2015.

[14] P. K. Smith, J. Mahdavi, M. Carvalho, S. Fisher, S. Russell, and N. Tippett, "Cyberbullying: Its nature

and impact in secondary school pupils," Journal of Child Psychology and Psychiatry, vol. 49, no. 4, pp. 376-385, 2008.
[15] B. De Paula, J. A. Valente, and A. Burn, "Game-Making as a means to deliver the new computing curriculum in England," Journal of Currículo sem Fronteiras, pp. 52-54, 2014.
[16] M. Berry, "Computing in the national curriculum: A guide for primary teachers," British Computer Society, pp. 23-25, 2013.
[17] Ministry of Education, Republic of Korea, "Curriculum for Practical Arts (Technology and Home Economics)/ Information," 2022(33), Dec. 2022.
[18] Ministry of Science and ICT, Republic of Korea, "Plan for Cultivating 100,000 Cyber Talents," Jul. 2022.
[19] Department for Education, "National curriculum in England: framework for key stages 1 to 4," Feb. 2024.
[20] L. Galloway, "A study of the impact of the Australian Curriculum: History on pedagogical practices of rural New South Wales primary teachers," pp. 15-19, Mar. 2023.
[21] National Initiative for Cybersecurity Education (NICE), "Strategic Plan," Aug. 2011.
[22] National Initiative for Cybersecurity Education, "National K12 Cybersecurity Education Roadmap," Dec. 2021.
[23] Jong-wook Jo, "Suggestion on the Need for Socialized AI for the Coexistence of Homo Sapiens and Super Intelligence," Korea Policy Monographs, 19(2), pp. 53-63, 2019.
[24] Gartner, Inc., "Gartner Forecasts Worldwide Artificial Intelligence Software Market to Reach $62 Billion in 2021," Jul. 2021.
[25] K. Schwab, "The Fourth Industrial Revolution," World Economic Forum, 2016.
[26] S. Hinduja and J. W. Patchin, "Cyberbullying: An exploratory analysis of factors related to offending and victimization," Deviant Behavior, vol. 29, no. 2, pp. 129-156, 2008.

〈저자소개〉

정 다 혜 (Dahye Jeong) 학생회원
2021년 3월~현재: 수원대학교 정보보호학과 학부과정
2024년 3월~현재: 수원대학교 정보보안 동아리 Write-Up 회장
〈관심분야〉 정보보안 교육, 웹 보안, 클라우드 보안

전 상 훈 (Sanghoon Jeon) 정회원
2012년 2월: 경북대학교 IT대학 심화 전자공학 공학사
2014년 2월: 대구경북과학기술원 정보통신융합공학전공 공학석사
2020년 8월: 대구경북과학기술원 정보통신융합전공 공학박사
2020년 3월~8월: 한양대학교 산학협력단 선임연구원
2020년 9월~2022 9월: 한양대학교 의과대학 응급의학과 포닥연구원
2022년 10월~2023 9월: 한양대학교 의과대학 응급의학과 연구조교수
2023년 10월~현재: 수원대학교 지능형SW융합대학 정보보호학과 조교수
〈관심분야〉 웨어러블컴퓨팅, 의료인공지능, CPS보안