TEST Engineering & Management

March - April 2020
ISSN: 0193-4120 Page No. 4322 - 4333

Conformity of Information Security Curriculum and Task Technology of Security System Design and Analysis

Jin-Keun Hong[*1], Jung-Soo Han[2]

[*1]Professor, Div. of Information Communication Technology, Baekseok University, 76 Munamro Dongnamgu Cheonansi, 330-704, Republic of Korea

[2]Professor, Div. of Information Communication Technology, Baekseok University, 76 Munamro Dongnamgu Cheonansi, 330-704, Republic of Korea

jkhong@bu.ac.kr[*1], jshan@bu.ac.kr[2]

Article Info
Volume 83
Page Number: 4322 - 4333
Publication Issue:
March - April 2020

Abstract

Background/Objectives: The National Initiative for Cybersecurity Education (NICE) recommends the skills and capabilities required by cybersecurity officers in connection with the staffing framework for cybersecurity. However, college education programs that train information protection personnel lack discussion and reflection on them. Therefore, in this paper, we analyzed the information protection curriculum of five universities in the Seoul metropolitan area of Korea and studied whether this process is suitable for the job requirements technology presented in the Framework for the Training of Cybersecurity Personnel.

Methods/Statistical analysis: In this paper, the security techniques and security capabilities to be retained by the task force responsible for designing and analyzing the security system presented by NICE criteria were analyzed first. At that time, the security technologies required by the officer were classified into core and specialized technologies. The reason why NICE criteria are applied is because they are classified as most objective and reasonable internationally. In this paper, the curriculum of the major information protection departments in Korea and their relevance to the security technologies and technologies that should be equipped by those in charge were analyzed.

Findings: The reason for this analysis is to see if information security curricula in 5 universities of the Seoul metropolitan area appropriate education system for conducting security system design and analysis. To analyze this, we classified requirements and capabilities of job skill of NICE framework. And the required skills and capabilities were mapped to security education subjects in the department of information protection. Studies show that the information security curriculum of five universities in the Seoul metropolitan area should be supplemented to acquire the skills required for the design and analysis tasks of security systems. In this study, what we found that the curriculum of the relevant university has features and advantages in each curriculum. However, if the departments concerned want to train the personnel responsible for designing and analyzing security systems, there are many more subjects to be added to the current curriculum.

Improvements/Applications: The results of this paper were understandable about the security requirements and capabilities required to perform the tasks of design and analysis of security systems. It can also be used as a reference model when preparing and designing of future security curricula.

Keywords: Cyber Security, Security Education, Security Workforce, Curriculum, Security Competency

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 26 March 2020*

1. Introduction

It is the fourth industrial revolution era. The rapid development of Internet-based technologies increases the threat of cybersecurity, which is why countries are interested in fostering information protection workers. Recently, the Program Committee of the NICE Workforce Framework hosted a program for the development of cybersecurity education and manpower capabilities in Garmisch Partenkircend of Germany. The program sought cross-country collaboration on cybersecurity staff. But This NICE framework, however, classifies and describes cyber security personnel that apply to the public, private and academic sectors. NICE describes information about cybersecurity tasks and personnel, training and training, and the knowledge, skills, and capabilities required to complete cybersecurity tasks and responsibilities. The curriculum guideline of cybersecurity degree course was presented by Joint Task Force, which is formed by Association for computing machinery (ACM), IEEE-Computer society (CS), Association for Information systems special interest group on information security and privacy (AIS SIGSEC), International federation for information processing technical committee on information security education (IFIP) Working group 11.8 [1].

Also, in the related research, Wonhyung Park and Seongjin Ahn analyzed the educational curriculum of private educational institutions and researched improvement of the NICE-based cyber security education curriculum[2]. The study calls for a curriculum that takes into account the needs of education consumers and suppliers, and researchers point out that this is not enough. Thus, in this paper, the security education curriculum needed to foster cybersecurity workforce in the field of attack response is developed and improvements are presented. But this approach is a meaningful one. Hong Soon-jwa studied the policy comparison framework for training new cybersecurity workforce based on the U.S. ATE policy[3]. The paper emphasizes that security technology is one of the high-tech education fields among STEMs. The study also reviewed five detailed operational programs supported by ATE. It is analyzing this by comparing it with the development of cyber security personnel in Korea. This study is meaningful as it identifies problems in cybersecurity education, draws improvements, and presents implementation measures. Shoemaker explains why understanding of the importance of NICE Cybersecurity Human Resources Development Framework is necessary[4-9]. Conklin et al were studied in terms of re-engineering US cybersecurity education. In this paper, the focus is on the results of NICE research[10]. Alsmadi studied Saudi Arabia's cyber security program. In this paper, the NICE framework is analyzed around the cyber security program of Arab and Saudi countries, and recommendations are proposed[11]. Caulkins Bruce D. et al. conducted research on the development of cyber manpower using the behavioral cybersecurity paradigm[12]. The study suggests a practical training strategy and argues that it contributes in terms of cybersecurity community efforts to strengthen cyber workforce development. In this paper, the National Cyber Security Workforce Framework, the Department of Homeland Security, and the National Initiative for Cybersecurity Careers and Studies education framework are discussed. Miloslavskaya et. al. focused on job competency in IoT and cloud information security environments[13]. The competences of interest in the paper are about competence and functional framework for the development of IT security personnel. The focus of the study is the mapping of information security manual roles and the cybersecurity capabilities framework. The EU is also interested in the e-Competence framework.

In this paper, we looked at NICE Cybersecurity Personnel Training Framework standards and various related research analyses on cybersecurity education. In the paper, given the job skills and competencies presented by NICE framework, it was concluded that it was necessary to identify whether the workforce training program at domestic universities was suitable. Therefore, in this paper, we analyzed what skills are required in the design analysis tasks of the security system among tasks classified by NICE. Then we looked at what capabilities the technology needed. From this point on, the researchers felt the need to analyze the relevance of the skills and skills required by NICE to the security curriculum currently being conducted by the university. Therefore, if we look at the subjects taught by the university's information protection department, it was judged that most subjects were being opened based on the experience of professors who were engaged in the information protection practice field. However, I would like to mention the need to discuss the curriculum and suitability required for job developers related to design and analysis of real security systems. The researchers needed a basis for objective judgment on what criteria the relevant departments opened and how the related subjects were required for their duties. The researchers concluded that it was reasonable and appropriate to apply the NICE staffing framework, which is the most objective criterion to date. Therefore, in this paper, we have identified the necessary competencies and skills required by the design analysis tasks of the security system presented by NICE. They also judged that this technology and capability could be objective criteria applicable to working-level sites that design and analyze information protection systems. The reason is that no other objective standard has been proposed yet. Therefore, the composition of this paper is as follows. First, Chapter 2 looked at NICE Information Protection Task Classification. Among these categories, the required skills for the analysis and design tasks of the information system were analyzed, as well as the skills required for the tasks. The required capabilities were classified into IT and security technologies. In addition, job descriptions related to security systems were classified into core and specialized skills to be completed by the task force. Chapter 3 analyzed the information security curriculum (security technology area) of five universities located in the nation's capital area. The necessary skills and capabilities required by the tasks involved in the design and analysis of security systems were compared with the curriculum of universities. We analyzed whether the subjects opened and operated by universities matched the skills and capabilities of the staff for design analysis of security systems presented by NICE. From this, we presented the necessary training skills and capabilities that should be supplemented for the education of security system design analysis tasks in universities. And I concluded in Chapter 4.

2. Task Classification of Information Security based on NICE framework

2.1 Needs Task of Security System

For tasks related to security systems, they can be classified into system design and analysis technologies. Tasks related to security systems include information assurance security architects, information guarantee security technicians, network security analysts, security engineers, security solutions designers, and system security analysts.

1) Needed Technology

This task should have an understanding of computer networks and network protocols. It should have an understanding of security principles such as network security methodologies, network protection requirements, network security structures, firewalls or DMZ encryption. it should have an understanding of the risk management process, the ethics of the legal regulations policy. It should have an understanding of cybersecurity principles, cyberthreats and vulnerabilities. an understanding of the authentication authorization and access control techniques, security models (Bel lafadula and Viva models, etc.). It should have an understanding of the cryptographic algorithms (IPSec, AES, GRE, IKE, MD5, SHA, 3DES). It must have an understanding of password and password key management, an understanding of enterprise security structures, and an understanding of security assessments and authorization. Confidentiality integrity, availability, reliability, and reliability should be understood. It should have an understanding of network access and identity management in an open-key infrastructure. It should have an understanding of patch management and security management. It must have an understanding of the security system design tools and methods, and an understanding of the information system. Personal Identification Data Security standards should be understood, supply chain security and risk management policies understood.

2) Competence required for the task

Common capabilities required for security system-related tasks include infrastructure design, risk management, law-regulatory ethics, information system security and network security, and vulnerability assessment capabilities.

Other competencies include information management, data management system, cryptography, information assurance, system test assessment, embedded computing, system integration, hardware engineering, information technology structure, operating system, configuration management, SW engineering, logic system design, system integration, communication, information technology structure, enterprise structure, system lifecycle, recognition, modeling & simulation, computer language, security, network management, process control.

The following table 1 classifies the capabilities of the security system which classifies the IT general technologies and security technologies.

Table 1. Ability to hold task related to security system

Capacity classification	Content
IT General technology	Infrastructure design, information management, data management system, system test evaluation, embedded computing, system integration, hardware engineering, information technology architecture, operating system, configuration management, SW engineering, logic system design, system integration, communication, information technology structure, enterprise structure, system lifecycle, technology recognition, modeling, computer language, process control, network management
Security Technology	cryptography, risk management, legal ethics, information system security, network security, vulnerability assessment, information assurance, security

2.2 Task Needs for Security Systems

1) Core technology of task related of security system

Personnel performing security system-related tasks should have computing network and protocol technologies, network security technologies, security development methodology, risk management, law policy ethics, cybersecurity principles, cybersecurity threat technologies, and vulnerability technologies.

2) Specialization technology of security system tasks

Personnel performing security system-related tasks should have an understanding of authentication technology, authorization technology, security model technology, network access and access management technologies for public key infrastructure, security principles in firewalls or DMZ, network protection requirements, network security structures, enterprise security structures, encryption algorithms (3DES, IPSec, AES, GRE, IKE, SHA, MD5), and key management.

They also require understanding of security system design tools and methods, security assessment and authorization, information assurance, security and patch management, understanding of personal identification information, understanding of data security standards, and understanding of supply chain security and risk management policies.

3. Analysis of security education courses at five universities in Seoul of Korea

The information protection curriculum of five universities in the Seoul metropolitan area was compared and analyzed with the required technology based on NICE workforce classification (security system related tasks). The results of this analysis are intended to determine whether the organized curriculum is appropriate from the correlation between the goals of the workforce training programs set by each university and the classification of NICE workforce.

3.1 Comparison of opened curriculum vs. Task needs of security systems

1) Department of Information Security Cryptography at Korea University

Comparing subjects opened by K. University against the capacity required by NICE related to security systems can be shown in Table 2. The subject opened by the major is network security among the core education subjects. Therefore, it is necessary to supplement other subjects. For example, the current curriculum does not include education on accreditation, authorization, security model, access control, security assessment, information assurance, security management, personal identification information and privacy, supply chain, and risk management policies.

Table 2. Ability to hold task related to security systems (Korea university)

	NICE	Opened Subject
Core Technology	Network security	Network security
	Security development method	
	Risk management	
	Law policy ethics	
	Cyber security principle	
	Cyber security threat	
	Vulnerability	
Specialized Technology	Authentication	Introduction of Cryptology
	Authorization	
	Security model	
	Access based on PKI	
	Security principle – F/W, DMS	Introduction of IS, Network Security
	Network-architecture, requirement	Crypto protocol
	Enterprise Security Architecture	
	Crypto algorithm &	Crypto

	key management	algorithm
	Designed tool and method of Sec. Sys.	
	Security evaluation	
	Information Assurance	
	Security management	
	Individual Identification Information, Individual Information Security	
	Data Security Standard	
	Supply Network Security	
	Risk management policy	
	Security(etc)	Information Sec. project
Needed Capacities	Risk management	
	Law Policy Ethics	
	Information Sys. Sec.	
	Network Sec.	Crypto protocol, Network sec.
	Vulnerability Evaluation	
	Cryptology	Introduction of Cryptology, Crypto Alg.
	Information Assurance	
	Security(etc)	Introduction of Information Sec.

Where sec. is security and sys. is system, F/W is firewall and DMS is data management security. IS. is information security.

2) Convergence Security Department at Dongguk University

Comparing subjects opened by D. University against the capacity required by NICE related to security systems can be shown in Table 3. Subjects opened by the major need to supplement security development methods and risk management courses among the core education subjects. For example, the current curriculum is devoid of training on authentication, authorization, security model, access control, network structure and requirements, enterprise security structure, cryptographic algorithm and key management, design tools and methods of security systems, information assurance, security management, personal identification information and privacy, data security standards, supply chain security, and risk management policies.

Table 3. Ability to hold task related to security systems (Dongguk university)

	NICE	Opened subjects
Core Technology	Network security	Security log analysis, Security event response
	Security Develop. Method	
	Risk Management	
	Law Policy Ethics	Cyber crime, Cyber investigation, Private Security
	Cyber security principle	Cyber War
	Cyber security threat	Malicious code Security event response
	Vulnerability	Digital forensic
Specialized Technology	Authentication	
	Authorization	
	Security model	
	Access based on PKI	
	Security principle – F/W, DMS	Security log analysis
	Network-architecture, requirement	
	Enterprise Sec. Arch.	
	Crypto algorithm & key management	
	Designed tool and method of Sec. Sys.	
	Security evaluation	Sec. consultant

	Information Assurance	
	Sec. management	
	Individual Identification Information, Individual Information Security	
	Data Security Standard	
	Supply Network Security	
	Risk management policy	
Needed Capacities	Risk management	
	Law Policy Ethics	Cyber Crime, Cyber investigation, Private security
	Information Sys. Sec.	
	Network Sec.	Sec. log analysis, Sec. event response
	Vulnerability Evaluation	Digital forensic
	Cryptology	Cryptology
	Information Assurance	
	Security(etc)	Introduction of Information Sec., Industrial Sec.

3) Department of Information Security at Sejong University

Comparing subjects opened by S. University against the capacity required by NICE related security systems can be shown in the following table 4. Subjects opened by this major require supplementation of network security, security development methods and risk management subjects among the core education subjects. The major, in particular, is strengthening education on cyber security threats. For example, it provides training on network and system hacking, web hacking, mobile system security, cyber control and cyber response, and cyber warfare training. However, the current curriculum does not include training on authentication, authorization, security model, access control, network structure and requirements, enterprise security structure, key management, design tools and methods of security systems, information assurance, security management, personal identification information and privacy, data security standards, supply chain security, and risk management policies for task of design and analysis of security system.

Table 4. Ability to hold task related to security systems(Sejong university)

	NICE	Opened subject
Core Technology	Network security	
	Security Develop. Method	
	Risk Management	
	Law Policy Ethics	Security policy and Law
	Cyber security principle	Information security
	Cyber security threat	Network hacking, System hacking, Web hacking, Mobile sys. sec. Cyber control and response Cyber Warfare train
	Vulnerability	Digital forensic, Malicious code analysis
Specialized Technology	Authentication	
	Authorization	
	Security model	
	Access based on PKI	
	Security principle – F/W, DMS	
	Network-architecture, requirement	
	Enterprise Sec. Arch.	
	Crypto algorithm & key management	Symmetric Cryptology
	Designed tool and method of Sec. Sys.	
	Security evaluation	
	Information Assurance	
	Sec. management	
	Individual Identification Information, Individual	

	Information Security	
	Data Security Standard	
	Supply Network Security	
	Risk management policy	
Needed Capacities	Risk management	
	Law Policy Ethics	
	Information Sys. Sec.	Web hacking, System security, Embedded system security, Mobile system security
	Network Sec.	
	Vulnerability Evaluation	Digital forensic
	Cryptology	
	Information Assurance	
	Security(etc)	Information sec. and basics, Information sec. industrial tech. trend, Sec. programming, Information sec. lecture Sec. Training for Sec. competitions

4) Department of Information Protection at Jongang University

Comparing subjects opened by J. University against the capacity required by NICE related to security systems can be shown in Table 5. Subjects opened by this major require supplementation of core subjects such as network security, security development methods and risk management among the core education subjects. However, the current curriculum does not include education on authentication, authorization, security model, access control, security principle, network structure and requirements, encryption algorithm and key management, design tools and methods of security systems, information assurance, data security standards, supply chain security, and risk management policies.

Table 5. Ability to hold task related to security systems(Jongang university)

	NICE	Opened subject
Core Technology	Network security	
	Security Development Method	
	Risk Management	
	Law Policy Ethics	Industrial sec. crime
	Cyber security principle	Industrial sec.
	Cyber security threat	Industrial terror and infrastructure security., Cyber infringement incidents and response
	Vulnerability	Industrial sec. survey and forensic
Specialized Technology	Authentication	
	Authorization	
	Security model	
	Access based on PKI	
	Security principle – F/W, DMS	
	Network-architecture, requirement	
	Enterprise Sec. Arch.	Digital business and sec.
	Crypto algorithm & key management	
	Designed tool and method of Sec. sys.	
	Security evaluation	
	Information Assurance	
	Sec. management	Industrial sec. management
	Individual Identification Information, Individual Information Security	Consent to the use of personal information
	Data Security Standard	
	Supply Network	

	Security	
	Risk management policy	
Needed Capacities	Risk management	
	Law Policy Ethics	Industrial security management, Technology management and sec., Industrial Sec. Law Sys. Cyber Criminal law Industrial sec. crime
	Information Sys. sec.	Sec. sys. operation and utilization, Cyber physical sys. sec. Electronics Information sec. tech.
	Network sec.	
	Vulnerability Evaluation	Industrial sec. survey and forensic
	Cryptology	
	Information Assurance	
	Security(etc)	Industrial Sec. Psychology, Sec. statistics Sec. Communications Industry Sec. Consulting Sec. data analysis Software sec. Industrial Convergence Sec. Convergence Sec. and Start-up Latest ICT and Sec.

Where tech. is technology.

5) Department of Information Security at Seoul Woman University

Comparing subjects opened by SW. University against the capacity required by NICE related to security systems can be shown in Table 6. Subjects opened by the major need to be supplemented among core education subjects such as network security, risk management, law policy ethics and cyber security ethics. However, the current curriculum does not include education on authentication, authorization, security model, access control, network structure and requirements, cryptographic algorithm and key management, design tools and methods of security systems, information assurance, data security standards, supply chain security, and risk management policies.

Table 6. Ability to hold task related to security systems(Seoul Woman university)

	NICE	Opened subject
Core Technology	Network security	
	Security Develop. Method	Information security software development capability cert.
	Risk Management	
	Law Policy Ethics	
	Cyber security principle	
	Cyber security threat	Cyber terror and Information War
	Vulnerability	Windows sec. Malicious code basic, Malicious code, Digital forensic
Specialized Technology	Authentication	
	Authorization	
	Security model	
	Access based on PKI	
	Security principle – F/W, DMS	Intrusion detection and Fire Wall
	Network-architecture, requirement	
	Enterprise Sec. Architecture	
	Crypto algorithm & key management	
	Designed tool and method of Sec. Sys.	
	Security evaluation	Information sec. management sys. certificate
	Information Assurance	
	Sec. management	
	Individual	

	Identification Information, Individual Information Security	
	Data Security Standard	
	Supply Network Security	
	Risk management policy	
Needed Capacities	Risk management	
	Law Policy Ethics	
	Information Sys. Sec.	Introduction of Computer and Information Security, Web application sec., Windows sec. management, Windows sec. and operation practices, Mobile sec., Sys. sec. and operation practices
	Network Sec.	Network sec. and programing practices
	Vulnerability Evaluation	Windows sec., Malicious basics, Malicious code
	Cryptology	Modern Cryptology Fundamentals, Application and Practice of Modern Cryptography
	Information Assurance	
	Security(etc)	Software sec., AI and Information sec., New trend of Information sec. technology

3.2 Subjects Design for task matching of design and analysis of security systems

1) Department of Information Security Cryptography at Korea University

For the cryptography department, if it wants to train its workforce as a task developer for security systems, it will have to be secured in the curriculum on security development methodology, risk management, legal policy ethics, cyber security principle, cybersecurity threat technology, and vulnerability technologies among the core technologies proposed by NICE. For specialized technologies, training on authorization or security model, PKI-based access control, enterprise security structure, security system design tools and methods, security assessment, information assurance, personal identification information, data security standards, supply network security, and risk management policies should be complemented. When considered in terms of the capacity to hold system functions, education programs should be presented for the university to enhance its competence in risk management, legal ethics, information system security, vulnerability assessment and information assurance.

2) Convergence Security Department at Dongguk University

The department should complement the security development methodology and risk management technology education, which are core technologies for system development tasks, in the security technology curriculum. If it wants to train its security system task developers, the university should supplement its certification technology, authorization, security model, PKI access management, network protection requirements and security structure, enterprise security structure, cryptographic algorithm and key management, security system design tools and methods, information assurance, security and patch management, personal information, data security standards, security, and risk management policies. For the task of developing a security system, this department requires training in capacity building for information assurance and risk management.

3) Department of Information Security at Sejong University

This department should complement the curriculum of security technology, the training of network security technology, security development methodology and risk management technology, which are core technologies of system development tasks. If the security system task developers are to be nurtured, the department should supplement the education and training of the authentication technology, authorization, security model, PKI access management, security principle, network protection requirements and security structure, cryptographic algorithm and key management, security system design tools and methods, security assessment, information security standards, supply chain, and risk management technologies among the specialized technologies for security system developers. The department should also complement competency training in information assurance, cryptography, network security and risk management for the task of developing security systems.

4) Department of Information Security at Jongang University

This department should complement the curriculum of security technology, the training of network security technology, security development methodology and risk management technology, which are core technologies of system development tasks. If a security system task developer is to be trained, the department should supplement technical training on authentication technology, authorization, security model, PKI access management, network protection requirements and security structure, cryptographic algorithm and key management, security system design tools and methods, information assurance, data security standards, supply network security, and risk management policies among the specialized technologies for security system developers. For the task of developing security systems, the department needs to strengthen capacity-building education on information assurance, cryptography, network security and risk management. The department, however, is characterized by the opening of classes for industrial security and managed psychology, statistics, consulting, analysis and start-up.

5) Department of Information Security at Seoul Woman University

The department should complement technical training in network security technology, risk management, law policy ethics and cyber security principles, which are key technologies for system development tasks in the curriculum of security technology. If a security system task developer is to be trained, the department should supplement technical training on authentication technology, authorization, security model, PKI access management, network protection requirements and security structure, cryptographic algorithm and key management, security system design tools and methods, information assurance, data security standards, supply network security, and risk management policies among the specialized technologies for security system developers. For the task of developing security systems, the department needs to strengthen training for capacity building on risk management, legal ethics and information assurance. The department has a wide range of appropriate subjects for its job in developing security systems.

4. Conclusion

This paper analyzed the necessary skills and capabilities that the Cybersecurity Task Force recommends in NICE Cybersecurity's Human Resources Development Framework. This paper is an analysis of what security technology is needed for the design analysis tasks of security systems and whether they should have security capabilities. The focus of the research is to find out whether the security technologies (core and specialized technologies) and capabilities of the relevant personnel are being developed through security training of major information protection departments in Korea. To this end, the technologies and capabilities presented by NICE were mapped to the curriculum of the information protection department to analyze their relevance. Based on the results, five universities in the Seoul metropolitan area analyzed security subjects of departments related to information protection. The research and analysis procedures first classified NICE Framework job requirements skills and capabilities. And the required skills and capabilities were mapped to security education subjects in the department of information protection. The analysis conclusion confirmed that the departments concerned have many subjects to be added to the current curriculum if they want to train their staff for designing and analyzing security systems.

Acknowledgment

This paper is supported of project funding of Baekseok University.

References

[1] JTF on cybersecurity education. Curriculum guidelines for post secondary degree programs in cybersecurity. Cybersecurity(CSEC) 2017; Ver.1.0: 1-123.
https://cybered.hosting.acm.org/wp/wp-content /uploads/2018/02/csec2017_web.pdf

[2] Wonhyung Pakr, Seongjin Ahn. Enhancing Education Curriculum of Cyber Security Based on NICE. KIPS Tr. Comp. and Comm. Sys. 2017; 6(1): 321-328.
DOI: doi.org/10.3745/KTCCS.2017.6.7.321

[3] Hong Soonjwa. A Study on the Framework of Comparing New Cybersecurity Workforce Development Policy Based on the ATE Programs of U.S. KIISC Journal. 2018; 28(1): 249-267.
DOI:http://dx.doi.org/10.13089/JKIISC.2018.28.1.249

[4] Cybersecurity Competency Model
https://www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx

[5] DoD cyber workforce framework(DCWF)
https://dodcio.defense.gov/CyberWorkforce/DCWF.aspx

[6] William Newhouse, Stephanie Keith, Benjamin Scribner, Greg Witte. NICE Cybersecurity Workforce Framework. NIST SP 800-181.

[7] NICE Webinar Series「How You can influence an updates to the NICE framework」
https://www.nist.gov/system/files/documents/2019/12/04/NICEFramework_Webinar_FINAL.pdf

[8] Kim, Kevin, Smith, Justin, Yang, T. Andrew, Kom, Dan J. An Exploratory Analysis on Cybersecurity Ecosystem Utilizing the NICE Framework. Cyber Summit NCS. 2018; 1-7.

[9] Gonzalez Manzano, lorena, de Fuentes, Jose M. Design recommendation for online cybersecurity courses. Computers and security. 2019; 80:238-256.

[10] Caulkins Bruce D., Badilo Urquiola Karla, Bockelman Patricia, Leis Rebecca. Cyber workforce development using a behavioral cybersecurity paradigm. Cyber Conflict (CyCon U.S.), International conference on 2016 Oct.; 1-6.

[11] Alsmadi Izzat, Zarour Mohammad. Cybersecurity programs in Saudi Arabia: Issues and Recommendations. Computer Applications and Information Security ICCAIS conference. 2018; 1-5.

[12] Conklin Wm Arthur, Cline Raymond E, Roosa Tiffany. Re engineering cyberseucirty educationin the US : An analysis of the critical factors」(System Sciences (HICCS) 47th Hawaii International Conference. 2014; 2006-2014.

[13] Miloslavskaya natalia, Tolstoy Alexander. State level views on professional competencies in the field of IoT and cloud information security. FiCloudW IEEE conference 2016; 83-90.