Co-funded by the Erasmus+ Programme of the European Union

lmpi licence master professionnel en protection informatique

LMPI - N°573901-EPP-1-2016-1-IT-EPPKA2-CBHE-JP
"Licence, Master professionnels pour le développement, l'administration, la gestion, la protection des systèmes et réseaux informatiques dans les entreprises en Moldavie, au Kazakhstan, au Vietnam »

Accreditation file

	Licence Pro	Master
Ho Chi Minh	non	création
Hanoi Agriculture	création	rénové
Hanoi Science et technology	rénové	rénové

rentrée 1ere session étudiants: 03/ 2018

Grade: Mention:	*Master of Information Technology*	Domaine:	*Computer Network and Cyber Security*

Université:	*HUST*	**University Chair:**	**Assoc. Prof. Ngo Hong Son, Dean of School of ICT**
Date de conception:	2018		

Author:	**Assoc. Prof. Nguyen Linh Giang**		

Co-funded by the
Erasmus+ Programme
of the European Union

lmpi
licence master professionnel
en protection informatique

LMPI - Licence, Master professionnels pour le développement, l'administration, la gestion, la protection des systèmes et réseaux informatiques dans les entreprises en Moldavie, au Kazakhstan, au Vietnam

Project N° 573901-EPP-1-2016-1-IT-EPPKA2-CBHE-JP

PROTOCOL OF PROJECT DOCUMENT VALIDATION

PROCES VERBAL DE VALIDATION DE DOCUMENT DU PROJET

Work Package/lot	3
Activity/Activité	3.3
Name of the activity/ Nom de l'activité	Les programmes et cours des licence et master et 6 dossiers de demandes d'accréditation.
Name of the document/ nom du document:	Dossiers de demande d'accréditation (Vietnam)
Partner(s) concerne/partenaire(s) concerné(s)	P19, P20, P21
Referent EU University/université UE réferente	P06 University of Vigo
Person validating the document/personne qui valide le document	
Name/nom	Ana Fernández Vilas
Function/fonction	Professor. Local Coordinator at University of Vigo

Date: 14 juin 2019

Signature:

UNIVERSIDADE DE VIGO - 1990
RECTOR

Ana Fernández Vilas

I. Context of the degree

a) In which context you have a project to create the new curricula (aims, motifs...)

This course aims to provide students with advanced knowledge and skills required in the security of computer network & security information systems. This course provides students principles and practical knowledge of computer network & Cyber security, their potential weaknesses and how they can be managed to make system more secure. The course will develop a comprehensive understanding of the underlying technologies and security mechanisms required for security experts, networking experts and provide students with the knowledge and understanding of the threats faced by operating systems, computer applications, network management & administration, and the appropriate countermeasures. Through the understanding and evaluation of new threats to authentication, authorisation, confidentiality and privacy, the course will promote a professional attitude for those wishing to enter employment within the field of Computer Network, Network Security and Cybersecurity. After graduation, students can work in universities, research institutes, companies or at institutions that apply solutions to ensure information security and security in almost all areas of the economy and society. Graduate students may also pursue further Doctoral programs in Computer Network, Network Security, Cyber Security, Information Security.

b) List the potential jobs covered by the new curriculum, refer to the official job classification

After graduation, students have the capacity to involve in project development, design secure software & applications, manage & implement network secure systems, develop & implement products & technical solutions in the field of Computer Network and Cyber Security. The students will acquire following abilities:

- Awareness of the intimate relationship between security and information security solutions with economic, social and environmental factors in the globalized world.
- Capacity to identify problems and form ideas for technical solutions, participate in project development to ensure safety, security information, communication, network and communication projects.
- Capacity to design systems, products, technical solutions to ensure information safety and security.
- Capacity to participate in installation, deployment of systems, products, solutions for computer network, communication network, technology solutions to ensure security and security for computer networks, communication networks and Information systems, secure data transmission, ensuring detection and prevention of network intrusion, information leakage, information and communication system vulnerability detection and detection, application development and security services for information and communication systems, communication projects.
- Capacity to develop and maintain secure systems, software and applications and solutions in the field of information security and communication, communication and computer networks, management and development of epidemics. Security and safety in the network and communications environment.

Therefore, the students likely to have potential jobs such as:

- Network security expert
- System security engineer
- Security managers & information security architects
- Network Manager and Administrator experts

c) Indicate the predictions for the professional integration of young graduates.

In the Master of Information Technology, path Computer Network and Cyber Security, the students should acquire professional skills and personal qualities needed following in order to succeed in a security career:

- Analytical and problem-solving techniques in the field of Computer Network and Cyber Security,
- Ability to experiment, research and explore knowledge in Computer Network and Cyber Security,
- Systematic thinking and critical thinking in the field of Computer Network and Cyber Security,
- Ethics and Professional Responsibilities,
- Understanding contemporary issues and lifelong learning.

The students can have a chance to work in Internet Service Providers (ISPs), Bank, e-Commerce companies as network manager, network security experts. They also can be recruited by security companies as audit engineer, security manager and system secuirity to provide security service for other ICT-based companies.

d) Indicate the origin of the students admitted, their number, and the methods of recruitment.

In order to apply Master of Information Technology, track Computer Network and Cyber Security, the students should have a bachelor or engineer degree of following:

- Bachelor or Engineer Degree in Information Technology, Computer Science, Data Communication and Networking, Software Engineering, Information System, Information Security, Computer Engineering, Applied Information Technology, Automation Control Engineering, Electronic & Communication Engineering of Hanoi University of Science & Technology. For the engineer students if continuing to the Master program of Information Technology, track Computer Network and Cyber Security, the students are exempted 18 ECTS for basic mandatory courses, and 18 ECTS for optional courses of master program.
- Bachelor or Engineer Degree of Electronics Engineering, Telecommunication Engineering, Automation Control Engineering, Mechatronics, Industrial Engineering, Applied Mathematics of other Universities. But the students have to study additional mandatory courses in order to study the degree.

Admission is made by taking the University exam with three subjects: Advanced mathematics; English; Specialized subjects in Information Technology. The number of admissions is 60 each academic year. The training program is organized according to the credit system based on the regulation of Organization and Graduation Management & Training of Hanoi University of Technology, issued by decision No. 3341 / QĐ-DHBK-SDH August 21, 2014 by President of Hanoi University of Science & Technology.

(e) Indicate whether the possibility of access to adult learners as part of lifelong learning is offered.

Hanoi University of Science and Technology has set up an E-learning platform that supports well distance learning and blended-learning, therefore, the students have a chance to access E-learning materials and interact with lecturers at lms.hust.edu.vn.

(f) Indicate the possible pursuit of studies.

The students can have a chance to pursuit Doctoral program in Network Security, Cyber Security or related fields. During Master thesis, the students are encouraged to do research on following topics:

- Network Security
- Privacy & Access Control
- Computer Forensics
- Secure Software
- Secure Computing
- Network Management Security

g) Indicate the modalities of composition of differentiated paths if necessary.

In the Master of Information Technology, path Computer Network and Cyber Security provides students not only advanced networking skills but also security kills, therefore, the students can pursuit to work or study more in the field of Networking, or Cyber Security.

II. General description of the curriculum

II.1. Description of training outcomes:

Training outcomes	Description
Disciplinary knowledge	Master of Information Technology, domain Computer Network and Cyber Security
General Competences	GC1. The ability to analyse systems, mechanisms and procedures related to protection of information entities and objects GC2. Problem solving ability, design ability GC3. Critical thinking GC4. Creativity and Reactivity GC5. Ability to apply theoretical knowledge to practice GC6. Ability for self-study GC7. Ability to work in a diversity group and in an international context (teamwork) GC8. Ability to project organization and planning GC9. Time management skill GC10. Representation skill: Ability to represent, illustrate, convince GC11. Skill in conducting trend analysis.
Specific Competences	SC01. To update security systems to meet new demands and latest technologies. SC02. Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). SC03. Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters). SC04. Skill in securing network communications. SC05. Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems. SC06. Skill in performing packet-level analysis. SC07. Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic). SC08. Skill in recognizing and categorizing types of vulnerabilities and associated attacks. SC09. Skill in using incident handling methodologies. SC10. Skill in preserving evidence integrity according to standard operating

	procedures or national standards. SC11. Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort). SC12. Skill in conducting vulnerability scans, recognizing and categorizing vulnerabilities in security systems. SC13. To understand and to apply the up-to-date methods, tools, software and techniques to analyze risks, threats and protect the system. SC14. Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes. SC15. The ability to know, understand and apply code analysis techniques. SC16. Skill in developing, testing, and implementing network infrastructure contingency and recovery plans. SC17. Skill in analysing and predicting trends in security aspects. SC18. Skill in analyzing anomalous code as malicious or benign. SC19. The ability to know, understand and apply binary analysis techniques and tools (e.g., Hexedit, command code xxd, hexdump). SC20. Skill in performing damage assessments. SC21. Ability to evaluate risks (risk assessment) SC22. To design/establish security policies, privacy policies and standards SC23. To make employees aware about corporate security policies and standards SC24. To design, develop and report monitoring indicators according to policies and standards SC25. Ability to describe and illustrate the risks, threats and solutions SC26. The ability to know, understand and apply database security techniques. SC27. The ability to know, understand and apply cloud computing security solutions. SC28. The ability to know, understand and apply the methods of cryptography and cryptoanalysis, the digital identity fundamentals and the protocols of secure communications. SC29. The ability to know, understand and apply privacy principles to organizational requirements. SC30. The ability to understand security demands and design and implement software/hardware security solutions. SC31. The ability to know, understand and apply the methods of networking protection (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters, securing network communications, intrusion detection, VPN). SC32. Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.). SC33. Skill in assessing security systems designs. SC34. Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.). SC35. Skill in creating policies that reflect system security objectives. SC36. Skill to identify cybersecurity and privacy issues that stem from connections with internal and external customers and partner organizations. SC37. Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience). SC38. Skill in negotiating vendor agreements and evaluating vendor privacy practices. SC39. Skill to extract information from available tools and applications associated with collection requirements and collection operations management. SC40. Skill to develop a collection plan that clearly shows the discipline that can be used to collect the information needed. SC41. Skill to analyze target or threat sources of strength and morale. SC42. Skill in technical writing. SC43. Skill in target network anomaly identification (e.g., intrusions, dataflow or processing, target implementation of new technologies). SC44. Skill in target development in direct support of collection operations. SC45. Skill in reviewing and editing assessment products. SC46. Skill in providing analysis to aid writing phased after action reports. SC47. Skill in knowledge management, including technical documentation

	techniques (e.g., Wiki page). SC48. Skill in developing and deploying signatures. SC49. Skill in applying host/network access controls (e.g., access control list). SC50. Skill in analyzing network traffic capacity and performance characteristics. SC51. Skill of identifying, capturing, containing, and reporting malware. SC52. Skill to design incident response for cloud service models. SC53. Skill to develop insights about the context of an organization's threat environment

II.2. Decomposition of curricula in semesters

Fr/ bachelor = 3 years (180 ECTS) – Master = 2 years (138 ECTS)
VN bachelor = 4 years, Engineer = 5 years, Master = 1,5 years (123 ECTS)

1. Short description of proposed subjects

CONTENT	CODE/ VN Code	SUBJECTS	ECTS	Hours
General	UE1 / SS6010	Philosophy	9	180
Mandatory subjects (48 ECTS)				
Basic mandatory subjects (18 ECTS)	UE2 / IT5670	Network Performance Evaluation	6	120
	UE3 / IT5570	Wireless Networks and Mobile Communication	6	120
	UE4 / IT5432	Security Evaluation of Information System	6	120
Advanced mandatory subjects (30 ECTS)	UE5 / IT6560	Advanced computer network	6	120
	UE6 / IT6600	Pattern Recognition	6	120
	UE7 / IT6580	Network Security Solutions and Policies	6	120
	UE8 / IT6570	Digital Communications	6	120
	UE9 / IT6575	Principles and Paradigms of Distributed Systems	6	120
OPTIONAL (36 ECTS)				
Optional (36 ECTS)	UE10 / IT5404	Cloud Computing	9	180
	UE11 / IT5434	Satellite information systems	6	120
	UE12 / IT5435	Fundamentals of Digital Forensics	6	120
	UE13 / IT5436	Data Mining	6	120
	UE14 / IT5409	Computer Vision	9	180
	UE15 / IT6610	Enterprise Network Administration	6	120
	UE16 / IT6826	Blockchain and Cryptocurrency	6	120
	UE17 / IT6596	Web 3.0 and Next generation of Internet Services	6	120
	UE18 / IT6605	Next generation of Mobile Networks	6	120
	UE19 / IT6827	Biometrics	6	120
	UE20 / IT6828	Digital Watermarking and Digital Rights Protection	6	120
	UE21 / IT5437	Secure software and system	6	120
Thesis	UE22 / IT6002	THESIS	30	600

2. Decomposition of curricula in semesters

Year	Semester	Title of semester (*)	EU Educational units
Year 1	S1	Fundamental Courses of Computer Network and Cyber Security (45 ECTS)	UE1. Philosophy (9) UE2. Wireless Networks and Mobile Communication (6) UE3. Security Evaluation of Information System (6) UE4. Network Performance Evaluation (6) UE10. Cloud Computing (O) UE11. Satellite Information Systems (O) UE12. Fundamentals of Digital Forensics (O) UE13. Data Mining (O) UE14. Computer Vision (O) UE15. Enterprise Network Administration (O) UE16. Blockchain and Crypto Currency (O) UE17. Web 3.0 and Next generation of Internet Services (O) UE18. Next Generation of Mobile Networks (O) UE19. Biometrics (O) UE20. Digital Watermarking and Digital Rights Protection (O) UE21. Secure software and system (O)
	S2	Advanced Courses of Computer Network and Cyber Security (48 ECTS)	UE5. Advanced Computer Network (6) UE6. Pattern Recognition (6) UE7. Network Security Solutions and Policies (6) UE8. Digital Communications (6) UE9. Principles and Paradigms of Distributed Systems (6) UE10. Cloud Computing (O) UE11. Satellite Communication Systems (O) UE12. Fundamentals of Digital Forensics (O) UE13. Data Mining (O) UE14. Computer Vision (O) UE15. Enterprise Network Administration (O) UE16. Blockchain and Crypto Currency (O) UE17. Web 3.0 and Next generation of Internet Services (O) UE18. Next Generation of Mobile Networks (O) UE19. Biometrics (O) UE20. Digital Watermarking and Digital Rights Protection (O) UE21. Secure software and system (O)
Year 2	S3	Thesis	UE22. Graduation Thesis (30 ECTS)

II.3 Description of EU (educational units)

Distribution of the study plan measured in ECTS credits by type of subject. General outline of the study plan is described as following

Type of subjects/ courses	Credits to undertake	Credit offered
Basic mandatory courses	27	27
Advanced mandatory courses	30	30
Optional	36	36
Master Thesis	30	30
Total	123	123

PROGRAM SCHEDULE

1st Semester		45 ECTS	2nd Semester		48 ECTS
UE2/ IT5670	Network Performance Evaluation	6 ECTS	UE5/ IT6560	Advanced computer network	6 ECTS
UE3/ IT5570	Wireless Networks and Mobile Communication	6 ECTS	UE6/ IT6600	Pattern Recognition	6 ECTS
UE4/ IT5432	Security Evaluation of Information System	6 ECTS	UE7/ IT6580	Network Security Solutions and Policies	6 ECTS
Optional Courses (18 ECTS)			UE8/ IT6570	Digital Communications	6 ECTS
			UE9/ IT6575	Principles and Paradigms of Distributed Systems	6 ECTS
UE1/ SS6010	Philosophy	9 ECTS	Optional Courses (18 ECTS)		
3rd Semester		30 ECTS			
IT6002	Thesis	30 ECTS			

EU semester 1 (1 semester = 45 ECTS)

EU	Objectif	Modules	ECTS	Lectures (hours)	TP (h.)	TL (h.)	Pers. work	Total
UE1	Philosophy (9 ECTS)	Module 1: Philosophy & Its Impact in Society Module 2: Eastern Philosophy Module 3: Mac-Le Philosophy Module 4: Materialism and idealism Module 5: Dialectical method and metaphysical method Module 6: Ho Chi Minh Philosophy	9	60	30	30	60	180h
UE2	Network Performance Evaluation (6)	Module 1: Basic knowledge and concept relating analytical modelling technique Module 2: Basic knowledge and concept relating simulative modelling technique Module 3: Performance evaluation methods and	6	45	15	30	30	120h

		simulation technique Module 4: Queueing theory Module 5: Simulation tools						
UE3	Wireless Networks and Mobile Communication (6)	Module 1: Fundamental knowledge on data transmissions Module 2: Wireless Networks Module 3: Mobile and Cellular communication Module 4: Coding Theory Module 5: MIMO Technology Module 6: Fundamentals of satellite communication	6	45	15	30	30	120h
UE4	Security Evaluation of Information System (6)	Module 1: Introduction to Security Evaluation Module 2: Vulnerability assessment fundamentals Module 3: Vulnerability Assessment Frameworks Module 4: Security tools for information system evaluation, management Module 5: Vulnerability mitigation.	9	45	30	15	90	180h
UE10	Cloud Computing (O)	Module 1: Cloud Computing Overview Module 2: Infrastructure as a Service Module 3: Platform as a Service (PaaS) Module 4: Software as a Service Module 5: Business Process as a Service Module 6: Cloud Computing Security	9	45	30	15	90	180h
UE11	Satellite Communication Systems (O)	Module 1: Overview of satellite, orbit and satellite launching methods Module 2: Space component, ground component, transmission line, and typical transmission access methods of the satellite information system Module 3: Broadcast satellite services Module 4: Application services such as IMMARSAT, GPS, etc. Module 5: Advanced topics on Satellite Information Systems	6	30	30	30	30	120h
UE12	Fundamentals of Digital Forensics (O)	Module 1: Introduction and Digital Forensic Process and Methodologies Module 2: Evidence Preservation Techniques Module 3: Forensic Software Packages Module 4: Forensic Reports and Legal Concerns Module 5: Windows Forensic Techniques Module 6: Macintosh & Unix Forensics	6	30	30	30	30	120h
UE13	Data Mining (O)	Module 1: Introduction to Data	6	30	30	30	30	120h

		Mining Module 2: Overview of different methods to explore and visualise large amounts of data Module 3: Classification methods Module 4: Clustering methods Module 5: Introduction to association analysis Module 6: Security in the area of data mining						
UE14	Computer Vision (O)	Module 1: Introduction to Computer Vision Module 2: Fundamentals of image processing, grouping, and multiple views Module 3: Introduction of Machine learning in Computer Vision Module 4: Supervised learning and classification Module 5: Practical vision problems Module 6: AI and beyond in Computer Vision	9	45	30	15	90	180h
UE15	Enterprise Network Administration (O)	Module 1: Introduction to Network Management Module 2: Internet administration with SNMP, Syslog Module 3: Network Administration Tools and Utilities Module 4: Network Security Tools Module 5: Advanced Topics	6	30	30	30	30	120h
UE16	Blockchain and Crypto Currency (O)	Module 1: Introduction to Blockchain Module 2: Decentralized peer-to-peer network architecture Module 3: Cryptocurrency Module 4: Smart Contracts Module 5: Advanced Decentralized Applications	6	30	30	30	30	120h
UE17	Web 3.0 and Next generation of Internet Services (O)	Module 1: Introduction to Web – Web 3.0 Module 2: Advanced Web services Module 3: Web models of user cooperation and information sharing Module 4: Web services applications and the next generation of Internet. Module 5: Web service security	6	30	30	30	30	120h
UE18	Next Generation of Mobile Networks (O)	Module 1: Fundamental of Wireless Networking Module 2: Mobile and wearable sensing Module 3: Multi-gigabit wireless networks Module 4: Indoor localization	6	30	30	30	30	120h

		and RF sensing Module 5: Low-power networking Module 6: Future mobile networking						
UE19	Biometric (O)	Module 1: Introduction to biometrics, principles, classification theory Module 2: Face recognition Module 3: Speaker recognition Module 4: Iris and Fingerprint recognition Module 5: Vein recognition, multi-modal and soft-biometrics Module 6: Security of biometrics (spoofing and anti-spoofing)	6	30	30	30	30	120h
UE20	Digital Watermarking and Digital Rights Protection (O)	Module 1: Applied cryptography to steganography and watermarking Module 2: Steganography vs. watermarking Module 3: Classification of watermarking algorithms Module 4: Steganalysis and attacks on Digital watermarking Module 5: Digital rights management and intellectual property protection Module 6: Digital signatures and authentication	6	30	30	30	30	120h
UE21	Secure software and system (O)	Module 1: Introduction to Secure Programming Module 2: Secure Programming with Memory Corruption Module 3: Buffer Overflow & SQL Injection Attacks Module 4: Secure Programming Techniques Module 5: Secure Programming with Static Analysis Module 6: Secure flow programming techniques	6	30	30	30	30	120h

Legend:
TL: Laboratory work or supervised practical work
TP: practical work in small groups
W pers: personal work (library, home, internship, etc.)

EU semester 2 (1 semester = 48 ECTS)

EU	Objectif	Modules	ECTS	Lectures (hours)	TP (h.)	TL (h.)	Pers. work	Total
UE5	Advanced computer network	Module 1: Next generation of Internet Architecture Module 2: Advanced Routing Protocols Module 3: High speed Internet Technologies Module 4: Data Center and Cloud Computing Architecture	6	30	30	30	30	120h

		Module 5: Software Defined Networking Module 6: Content Delivery Networking						
UE6	Pattern recognition	Module 1: Basic knowledge and concepts of Pattern recognition Module 2: Feature Extraction and Selection Module 3: Statistical Pattern Recognition Module 4: Unsupervised Learning and Clustering Module 5: Neural Networks, Syntactical and Structural Pattern Recognition Methods	6	30	30	30	30	120h
UE7	Network Security Solution and Policies	Module 1: Fundamental knowledge on information and network security Module 2: Information and system security services Module 3: Policies and Law of Cyber Security Module 4: Secure network services and transactions Module 5: Intrusion detection methods Module 6: Security in Cloud Computing and Internet of Things Security	6	30	30	30	30	120h
UE8	Digital Communications	Module 1: Introduction to Digital Communications System Module 2: , Probability and Stochastic Process in Digital Communications Module 3: Data transmission and reception Module 4: Structure of optimal receiver, efficiency of the optimal receiver Module 5: Synchronization, Equalizing and Spread Spectrum Module 6: Security in Digital Communications	6	30	30	30	30	120h
UE9	Principles and Paradigms of Distributed Systems	Module 1: Introduction to Distributed Systems Module 2: Principles of Distributed Systems Module 3: Paradigms of Distributed Systems Module 4: New models of Distributed Systems Module 5: Security in Distributed System	6	30	30	30	30	120h
UE10	Cloud Computing (O)	Module 1: Cloud Computing Overview Module 2: Infrastructure as a Service Module 3: Platform as a Service (PaaS) Module 4: Software as Service Module 5: Business Process as a Service	9	45	30	15	90	180h

		Module 6: Cloud Computing Security						
UE11	Satellite Communication Systems (O)	Module 1: Overview of satellite, orbit and satellite launching methods Module 2: Space component, ground component, transmission line, and typical transmission access methods of the satellite information system Module 3: Broadcast satellite services Module 4: Application services such as IMMARSAT, GPS, etc. Module 5: Advanced topics on Satellite Information Systems	6	30	30	30	30	120h
UE12	Fundamentals of Digital Forensics (O)	Module 1: Introduction and Digital Forensic Process and Methodologies Module 2: Evidence Preservation Techniques Module 3: Forensic Software Packages Module 4: Forensic Reports and Legal Concerns Module 5: Windows Forensic Techniques Module 6: Macintosh & Unix Forensics	6	30	30	30	30	120h
UE13	Data Mining (O)	Module 1: Introduction to Data Mining Module 2: Overview of different methods to explore and visualise large amounts of data Module 3: Classification methods Module 4: Clustering methods Module 5: Introduction to association analysis Module 6: Security in the area of data mining	6	30	30	30	30	120h
UE14	Computer Vision (O)	Module 1: Introduction to Computer Vision Module 2: Fundamentals of image processing, grouping, and multiple views Module 3: Introduction of Machine learning in Computer Vision Module 4: Supervised learning and classification Module 5: Practical vision problems Module 6: AI and beyond in Computer Vision	9	45	30	15	90	180h
UE15	Enterprise Network Administration (O)	Module 1: Introduction to Network Management Module 2: Internet administration with SNMP, Syslog Module 3: Network Administration Tools and	6	30	30	30	30	120h

		Utilities Module 4: Network Security Tools Module 5: Advanced Topics						
UE16	Blockchain and Crypto Currency (O)	Module 1: Introduction to Blockchain Module 2: Decentralized peer-to-peer network architecture Module 3: Cryptocurrency Module 4: Smart Contracts Module 5: Advanced Decentralized Applications	6	30	30	30	30	120h
UE17	Web 3.0 and Next generation of Internet Services (O)	Module 1: Introduction to Web – Web 3.0 Module 2: Advanced Web services Module 3: Web models of user cooperation and information sharing Module 4: Web services applications and the next generation of Internet. Module 5: Web service security	6	30	30	30	30	120h
UE18	Next Generation of Mobile Networks (O)	Module 1: Fundamental of Wireless Networking Module 2: Mobile and wearable sensing Module 3: Multi-gigabit wireless networks Module 4: Indoor localization and RF sensing Module 5: Low-power networking Module 6: Future mobile networking	6	30	30	30	30	120h
UE19	Biometric (O)	Module 1: Introduction to biometrics, principles, classification theory Module 2: Face recognition Module 3: Speaker recognition Module 4: Iris and Fingerprint recognition Module 5: Vein recognition, multi-modal and soft-biometrics Module 6: Security of biometrics (spoofing and anti-spoofing)	6	30	30	30	30	120h
UE20	Digital Watermarking and Digital Rights Protection (O)	Module 1: Applied cryptography to steganography and watermarking Module 2: Steganography vs. watermarking Module 3: Classification of watermarking algorithms Module 4: Steganalysis and attacks on Digital watermarking Module 5: Digital rights management and intellectual property protection Module 6: Digital signatures and authentication	6	30	30	30	30	120h
UE21	Secure software and system (O)	Module 1: Introduction to Secure Programming	6	30	30	30	30	120h

		Module 2: Secure Programming with Memory Corruption Module 3: Buffer Overflow & SQL Injection Attacks Module 4: Secure Programming Techniques Module 5: Secure Programming with Static Analysis Module 6: Secure flow programming techniques						

EU semester 3 (1 semester = 30 ECTS)

EU	Objectif	Modules	ECTS	Lectures (hours)	TP (h.)	TL (h.)	Pers. work	Total
UE22	Master Thesis	The thesis is where the student must demonstrate proficiency in making use of methodologies and theories in an analysis of an issue relevant to Cyber Security or Network Security Management. Through the work on the thesis, students must show an ability to use theories and methods within program to produce a major, written academic assignment on an individually chosen topic provided by supervisor.	30	0	120	120	360	600h

GRADING

The grading in word (A, B, C, D, F) and the corresponding 4-point scale are used to evaluate the official learning results. 10-point scale is used for component/ progress points of the module.

Status	Level of 10			Level of 4	
				In word	In number
Pass*	from 8,5	To	10	A	4
	from 7,0	To	8,4	B	3
	from 5,5	To	6,9	C	2
	from 4,0	To	5,4	D	1
Fail	Dưới 4,0			F	0

II.3. Tableau de mise en corrélation entre compétences et unités d'enseignement:

	GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	GC9	GC10	GC11
UE1		X	X						X		
UE2	X				X						X
UE3		X			X					X	
UE4				X	X	X					
UE5					X			X		X	
UE6					X	X				X	
UE7			X				X	X			
UE8	X				X						X

UE9		X		X						X	
UE10	X		X								X
UE11					X					X	X
UE12		X	X			X					
UE13	X	X			X						
UE14						X				X	X
UE15	X						X				X
UE16					X					X	X
UE17		X						X	X		
UE18	X	X						X			
UE19	X				X						X
UE20				X			X			X	
UE21	X		X	X							
UE22	X				X				X		

II.4. The final dissertation

a) What will be asked from students for the dissertation (When? Number of pages? Relationship with the curriculum.

The final dissertation is in 4th semester and has 18 ECTS. The students being asked to do or being given a Cyber Security topic by advisor. There is no rule for number of pages which will be decided by the advisor. The dissertation's name and content, and format have to follow the general template of University. The final disertation topic should be well following Cyber Security path.

b) Describe the role of the two types of tutors, the university tutor, the company tutor

The students have one mandatory advisor from the University staff who have at least a Ph. D. degree. The students may do the Master thesis with company tutor but the advisors in the company may be secondary or complementary advisors, or co-advisors, but it's optional.

c) Describe the expected results of the final dissertation

The final dissertation is expected to be an original, unpublished and significant contribution to the field of digital security and cybersecurity, in any of its possible domains of application (industry, manufacturing, administration, public services, societal services, baseline & fundamental technologies, applied products and services, etc.)

d) Describe the modalities of defense of final dissertation

The students have to defend before a committee or jury formed by 5 members from different universities. Thesis reviewed by an internal reviewer and an external reviewer. The jury does not include the thesis advisor. Students must submit final dissertation to the jury after approval by the advisor and the two reviewers. Publication of research papers in conferences or journals is optional, not a requirement.

e) Indicate the timetable for the realization of the final dissertation

Students should prepare their dissertation since 3rd semester. The lecturers will post their topic in Cyber Security on their website, and the students are freely to choose. The 3rd semester for students to choose advisor and defining topic with advisor. The 4th semester is for doing

technical work and prepare dissertation. The final disertation have to be submitted to the University committe at least 2 months before the defense of final disertation. The defense of final disertation for studetns can be organized 2-3 times per academic year.

f) Indicate the number of ECTS granted to the final dissertation

30 ECTS

II.5. Internship in company

The internship to industrial organizations is not mandatory. The students can deal with the supervisors and have an internship to a company during their thesis under the supervision of their thesis co-supervisors (company advisors).

II.6. Internship in a company abroad

The internship to industrial organizations is not mandatory. The students can deal with the supervisors and have an internship to a company during their thesis under the supervision of their thesis co-supervisors (company advisors).

II.7. Mobility to foreign companies (if any)

a) List universities abroad with a partnership with your university and the chairs (or department, or institute) concerned

b) Indicate the areas, diplomas for which a period of mobility is possible

III Modalities for the control of knowledge

a) For each EU, indicate the methods of checking knowledge

- There are several forms of examination (written, oral, practical, defense, etc.) which is depending on lecturers, but there are two mandatory evaluation which are mid-term and final examination.
- Duration of the control: 50-70 minutes for mid-term exams; 70-120 minutes for final exams - Test coefficient (if applicable)
- The maximum score is 10.

b) Indicate the rules of obtaining a EU (UE)

- Rules for the allocation of EU: In order to finish a course, the students must pass the exams, exercises, attendance, course project, etc. which are required by lecturers
- Compensation rule between units (if applicable): The students must pass all mandatory and fundamental courses. For optional course, students can choose and finish some of courses from the list to get at least the number of credits required for optional courses.
- Period of validity of a EU obtained (UE)
- Eliminary scores: No

IV Composition of pedagogical team

a) The general pedagogical responsible of the new curriculum

Name : NGO
First name : HONG SON
Function : Dean of School of Information & Communication Technology
University : Hanoi University of Science and Technology

b) Pedagogical responsibles by EU Educational units (Teachers by EU)

EU	Responsible of EU	University of attachment
2,3	Prof. Trinh Van Loan	HUST
4	Dr. La The Vinh	HUST
5	Prof. Nguyen Thi Hoang Lan	HUST
6,7	Dr. Tran Hoang Hai	HUST
8, 10	Prof. Nguyen Linh Giang	HUST
9, 17	Prof. Nguyen Khanh Van	HUST
11	Dr. Nguyen Thanh Hung	HUST
12, 15	Dr. Tran Quang Duc	HUST
13	Dr. Pham Huy Hoang	HUST
14	Dr. Tran Vinh Duc	HUST
16	Prof. Ngo Hong Son	HUST

c) Teachers involved in the curriculum (= renovators)

Name	University	Disciplines taught	Number of hours of intervention	Concerned EU
Ngo Hong Son	HUST			
Nguyen Linh Giang	HUST			
Tran Quang Duc	HUST			
Tran Hoang Hai	HUST			

d) Professionals involved in the curriculum
(=professionals animating a training course/a lecture on a professional theme)

Name	Company	Disciplines taught	Number of hours of intervention	Concerned EU

NB: the number of hours of intervention of professionals must be 30% of the total hours.

V Professional Insertion

a) Indicate the methods used to support the professional integration of young graduates

- International Department will provide information for students to do internship abroad. In School of ICT, the students also are encouraged to contact with companies to do internship with support from Industry Sector.

- The university has a center that supports students in seeking jobs during their study and after graduation. Moreover, many job advertisements are also shown on the website of HUST and School of ICT.
- Creation of corporate databases

(b) Indicate the composition and role of the employment office of the university

Student Supporting Department will provide all of information for students about scholarship & internship opportunities. They also organize several events with companies to promote collaboration between University & Industry, and in those events, the students have a chance to interact with companies for job, internship, etc.

VI The Diploma Supplement

See Examples in the section "Lot2 / 2.1.1. Common methodological guide / E. Other Europass documents'.

Annex 1 : Partnership with training institutions

1.1. Universities implied in the training

Universities	Role in the training course
Ho Chi Minh University of Technology	Joint teaching and sharing of E-learning contents
Vietnam National University of Agriculture	Joint teaching and sharing of E-learning contents
University of Vigo	Double degree

Join contracts.

1.2. Other training institutions implied

Institution	Role in the training course
BKIS – Bachkhoa Cyber Security Center	Practical work, internship, co-training and teaching
VNCert - Vietnam Computer Emergency Response Team	internship, co-training on specific topics on Cyber Security

Join contracts.

Annex 2 : Cooperation with companies

2.1. Companies implied in the training

Company	Role in the training course
BKAV Corporation	Internship, co-training on specific topics on Cyber Security
VCCorp	Internship, co-training on specific topics on Cyber Security
CMC Security	Internship, co-training on specific topics on Cyber Security

Join contracts.

2.2. Other companies supporting the training course

Companies	Adress
BKAV Corporation	Internship, co-training on specific topics on Cyber Security
CMC Security	Internship, co-training on specific topics on Cyber Security

Join support letter

Annexe 3 : Job description profile (fiche métier)

Join job description profiles which resulted from the survey