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

lmpi
licence master professionnel
en protection informatique

LMPI – GREECE_P4_ Piraeus University of Applied Sciences (University of West Attica)

INTERIM TECHNICAL REPORT

Index

1. Higher education

Moldova is a country which adopted ECTS since 2005. There are 16 public HEIs accredited by the Moldovan Ministry of Education. Higher education in Republic of Moldova, is realized in three cycles. In our case we do consider only the first two cycles. 1st Cycle – License, with a duration of 4 years or sometimes 5 years (in accordance with the current system in Greece), corresponding to 60 Credits per study year. The 2nd Cycle – Master, has a duration of 1 to 2 years, corresponding to 90 - 120 ECTS. (http://www.erasmusplus.md/en/article/higher-education-system-moldova) The adoption of ECTS ensures the comparability in the standards and quality of higher-education qualifications. Moldova usually uses 4-6 ECTS per course and has less than 30 ECTS for the dissertation according to the country regulations. The only side effect is that the students must attend more than 8-9 courses to obtain their MSc degrees. Of course as the studies are 4-5 years it is possible to diminish the ECTS to the minimum of 60 ECTS for the MSc (one year) courses.

The Double degree MSc program we propose/design through the LMPI program promotes Internationalisation and offers the opportunity to those persons involved in Cyber Security to examine similar curricula in partner country(ies). Also they have the opportunity to visit EU Companies with a major role in the area of Cyber Security as well as in EU partner Countries.

The possible approval of the ERASMUS +ICM program can promote staff and student mobility. The program was submitted last January and we are expecting the results from the National Agency. This option will increase the feedback as both students and staff can visit for a short period MD and vice versa GR within the frame of our common programs (BSc and MSc) currently run under LMPI.

Application of student-centred approaches. These can be summarised into the following:

- Reliance on active learning;
- Emphasis on critical and analytical learning and understanding;
- Increased responsibility on the part of the student;
- Increased autonomy of the student;

Compatibility with ECTS

According to the country regulations for a programme with 240 ECTS, depending on the role of the discipline in professional formation, courses are divided into: − fundamental (50-80 ECTS); − general skills and abilities (up to 15 ECTS); − socio-humanistic orientation (25-35 ECTS); − specialization oriented (50-95 ECTS); − orientated towards the second cycle (25 ECTS);

Indicative number of hours of student workload corresponding to 1 ECTS = 30 – 40 hours. The common European standard is 25-30 hours. So here is a point that must be taken into consideration for the work load allocated per ECTS. (http://eacea.ec.europa.eu/tempus/participating_countries/overview/moldova_tempus_country_fiche_final.pdf). Most of the participating countries in the LMPI use the 1ECTS = 25 hours mode.

Compatibility with the ESG standards for QA

Internal Quality assurance. The criteria set by the EU are:

1.1 Policy and procedures for quality assurance

The relationship between teaching and research in the institution;

- *the institution's strategy for quality and standards;*
- *the responsibilities of departments, schools, faculties and other organisational* units *and individuals for the assurance of quality;*
- *the involvement of students in quality assurance;*
- *the ways in which the policy is implemented, monitored and revised.*

1.2 Approval, monitoring and periodic review of programmes and awards

- *development and publication of explicit intended learning outcomes;*
- *careful attention to curriculum and programme design and content;*
- *specific needs of different modes of delivery (e.g. full time, part-time, distance learning, e-learning)*
- *availability of appropriate learning resources;*
- *formal programme approval procedures by a body other than that teaching the programme;*
- *monitoring of the progress and achievements of students;*
- *regular periodic reviews of programmes (including external panel members);*
- *regular feedback from employers, labour market representatives and other relevant organisations;*
- *participation of students in quality assurance activities.*

1.3 Assessment of students

Student assessment procedures are expected to:

- *be designed to measure the achievement of the intended learning outcomes* and *other programme objectives;*
- *be appropriate for their purpose, whether diagnostic, formative or summative;*
- *have clear and published criteria for marking;*
- *be undertaken by people who understand the role of assessment in the progression of students towards the achievement of the knowledge and skills associated with their intended qualification;*
- *where possible, not rely on the judgements of single examiners;*
- *take account of all the possible consequences of examination regulations;*
- *have clear regulations covering student absence, illness and other mitigating circumstances;*

- *ensure that assessments are conducted securely in accordance with the institution's stated procedures;*

1.4 Quality assurance of teaching staff

Tutors are the most important learning resource available to students. They must have a full knowledge and understanding of the subject they are teaching, have the necessary skills and experience to transmit their knowledge and understanding effectively to students in a range of teaching contexts, and can access feedback on their own performance. Include a means of making certain that all new staff have at least the minimum necessary level of competence. Teaching staff should be given opportunities to develop and extend their teaching capacity and should be encouraged to value their skills.

1.5 Learning resources and student support

In addition to their teachers, students rely on a range of resources to assist their learning. These vary from physical resources such as libraries or computing facilities to human support in the form of tutors, counsellors, and other advisers. The Learning resources and other support mechanisms are accessible by the students, designed with their needs in mind and responsive to feedback from those who use the services provided. Institutions monitor, review and improve the effectiveness of the support services available to their students.

1.6 Information systems

The quality-related information systems required by individual institutions will depend to some extent on local circumstances, but it is at least expected to cover:

- *student progression and success rates;*
- *employability of graduates;*
- *students' satisfaction with their program;*
- *learning resources available and their costs;*

The Universities using some funds from the program purchased needed equipment for the realization of the program.

During our extensive discussions with the program leaders, the Deans of the Schools and the Higher Academic Administration of the Universities all the above criteria(1.1-1.6) are fulfilled.

Continuing Professional Development (CPD) is increasingly recognised to be essential for those working in regulated professions and it is perceived by the professionals as lifelong learning. Also elements of the CPD may be converted into 2nd cycle (MSc) qualifications. (in our case the MSc program the Universities offer, including the new Cyber Security courses). LMPI program offers this opportunity to the perspective students.

2. New/updated courses

The purposes of the standards and guidelines are:
• to improve the education available to students;
• to assist Universities in managing and enhancing their quality and,
to help to justify the institutional autonomy;

Quality assurance takes into account the needs and expectations of students, and the society. Quality assurance responds to the diversity of higher education systems, institutions, programs and students.

The Programs designed under the LMPI needs respect the requirements. They:

- *are designed with overall program objectives that are in line with the institutional strategy and have explicit intended learning outcomes;*
- *are designed by involving students' and society needs*
- *benefit from external expertise and reference points;*
- *are designed so that they enable smooth student progression;*
- *define the expected student workload,*
- *are subject to a formal institutional approval process.*

fulfilling the guidelines paying attention to the careful consideration of the design and delivery of study program of each University and the assessment of outcomes.

The implementation of student-centred learning and teaching - respects and attends to the diversity of students and their needs, enabling flexible learning paths; - considers and uses different modes of delivery, where appropriate; (physical presence or using e-platforms) - regularly evaluates and adjusts the modes of delivery and pedagogical methods; - encourages a sense of autonomy in the learner, while ensuring guidance and support from the teacher; - has appropriate procedures for dealing with students' complaints.

Considering the importance of assessment for the students' progression and their future careers, quality assurance processes for assessment take into account the following: - The criteria for and method of assessment as well as criteria for marking are published in advance;

The assessment allows students to demonstrate the extent to which the intended learning outcomes have been achieved. Students are given feedback, which, if necessary, is linked to advice on the learning process; - Where possible, assessment is carried out by more than one examiner and moist of the times the exam paper is set by a group of tutors; - The regulations for assessment take into account mitigating circumstances;

Universities have primary responsibility for the quality of their staff and for providing them the environment that allows them to carry out their work effectively. So, there exist a clear, transparent and fair processes for staff recruitment and conditions of employment that recognise the importance of teaching; - encourages scholarly activity to strengthen the link between education and research; - encourages innovation in teaching methods and the use of new technologies. There exist in Moldova State University, examples of tutors, who participate in LMPI, that gain grants for their excellent achievement in topics related to their expertise.

The agreed 8 courses among all the Moldovan Universities and Piraeus University of Applied Sciences (University of West Attica) are: four for the BSc program and four for the MSc program degree.

Some of developed/renewed courses will be fully implemented in the new curricular offered by the Universities, some of them will be used inside an existing training offers as shown in the table below as well as the level of achievement of each course.

All courses (100%) have been designed but not yet taught to the students. This procedure will start next September. The courses have been submitted for accreditation by the Ministry of Education after their approval form the Departments involved in all Universities.

The courses intended to be developed (/updated) under the LMPI project for the Moldovan Universities according to the propositions made by them for the LMPI project requirements and by the industrial partners who participated in the questionnaires are listed below.

All courses will be delivered during 60 hours (30 hours for courses and 30 hours for practical activities), each one being equal to 5 ECTS.

Course	**Full implementation in curricular offer**	**Partial implementation in existing courses**	**Development**	**Recognition (waiting final approval)**	**Delivered**
L1 **Cryptographic Methods of Information Protection**	UTM ASEM	USM USARB	75%	50%	30%
L2 **Information Systems Security**	UTM, USM ASEM, USARB		75%	50%	0%
L3 **Administration and security of computer networks**	UTM USM ASEM	USARB	50%	50%	15%
L4 **Technical means of information protection**	UTM USM ASEM	USARB	50%	50%	15%

M1 **Information security management**	UTM ASEM	USM USARB	50%	50%	30%
M2 **Information Security Audit**	UTM USM ASEM	USARB	75%	50%	15%
M3 **Enterprise Information Security**	UTM USM ASEM	USARB	75%	50%	15%
M4 **Security of electronic transactions**	UTM USM ASEM	USARB	50%	50%	15%

BSc level

L1 Cryptographic Methods for Information Protection
L2 Information Systems Security
L3 Network administration and security
L4 Technical means of information protection

Each course is developed/renewed by a team including members from each partner university.

Courses' outlines for developed courses:

L1. Cryptographic Methods for Information Protection

- Introduction to Cryptography
- Classical ciphers
- Modern stream ciphers
- Modern block ciphers
- Hash Functions
- Message Authentication Codes
- Basic public key encryption algorithms
- Signature schemes
- Security issues of encryption algorithms
- Steganographic methods for information protection

L2. Information Systems Security

- Introduction to Information Systems Security;
- Legal aspects of information security;
- Access control to computer systems.
- Forms of hazard manifestation in information systems (threats, attacks, malicious software);
- Information protection in information systems;
- Basic software security of information system;
- Insecurity in Software;
- Detecting and preventing intrusions in information systems;
- Security Policy of the Information System;
- Ensuring the confidentiality, integrity and availability of the information system.

L3. Network administration and security

- Computer networks security: specific issues, treats and vulnerabilities, attacks, security solutions and strategies, security policies;
- Network management as a security technique for computer networks. Local networks: protocols, structure, network equipment, virtual networks.
- Vulnerabilities in local networks and security techniques; Basic security in an IP network. Network addressing and IP protocol. Network structure and routing as a method of enhancing network security;
- Network perimeter security. Secure Network Design. Firewalls: principles, functionalities, strategies, types, configuration.
- Cryptographic methods for information protection in computer networks. Elements of cryptography: symmetrical and asymmetric cryptography. Encryption algorithms RSA, DES, IDEA, RC4, AES.
- Confidentiality of communication sessions, session key concept and Diffie-Hellman protocol.
- Data integrity control protocols: public key cryptography, digital signature;
- Authentication methods. Single Sign On (SSO) authentication, RADIUS, TACACS, KERBEROS and LDAP protocols;
- Public Key Infrastructure (PKI): services, actors, operation. X.509 certificate;
- Pretty Good Privacy (PGP) encryption system. OpenPGP standard and its GNU Privacy Guard (GPG) software implementation.
- E-mail securing; Network layer securing, IPSec protocol: principles, services, working modes, authentication, header format;
- Transport layer securing, SSL and TLS/SSL protocols. Web security with HTTPS protocol. SSH protocol;
- Virtual private networks (VPNs): architectures and technologies. IPSec, PPTP, TLS/SSL tunnel*s*.

L4. Technical means of information protection

- Introduction to technical means of information protection. Structure of information protection technical means.
- Methods and techniques for detecting and correcting errors.
- Information protection provided by processor / computer architecture.
- Information protection provided by the technical means of data storage. Technical means of data management.
- Addressing techniques in computer systems and computer networks and information protection methods. Pre- and post-identification of intrusions.
- Information protection techniques in communication channels.
- Technical means for the protection of information carriers.
- Numerical accelerators for information protection.
- Methods and techniques for controlling access to information.
- Methods and techniques for destroying the information.

M.Sc. level

M1 Information security management
M2 Information Security Audit
M3 Enterprise Information Security
M4 Security of electronic transactions

Each course was developed/renewed by a team including members from each partner university.

M1. Information security management

- The information security management framework. Basic concepts and concepts. International standards about ISM: ISO 27000 family of standards, NIST, PCI DSS. The relationship between standards and their applicability.

- The information security management system (ISMS). Components and mechanisms of an ISMS. Stages of the ISMS implementation process according to ISO 27001. Establishment of objectives and definitions of the ISMS. Declaration of applicability.

- Analysis and assessment of the security risks. General concepts on information security risk management. Inventory of assets. Threats and vulnerabilities. Stages of the risk analysis and assessment process according to ISO 27005 standard. Quantitative and qualitative assessment.

- Methodologies and tools for the informational risk analysis. Microsoft methodology. CRAMM methodology. METHARI methodology. Ebios methodology. Octave methodology. IT methodology - Grundschutz. Ebios, GSTool, Grif, RiskWatch, Cramm.

- The current legal framework. Information security management at the state level: general principles. Information risk management methodologies used by local infrastructure.

- Policies, models, and security programs. Multilevel and multilateral security models. Security policy models. Examples of security policies. Practical aspects of the security policy.

M2. Information Security Audit

- Definition, purpose, destination, types and location of ISA ;
- International reference normative framework. International Standard of Auditing ISO 27001. COBIT. ITIL. ISACA.
- Audit legislation of the Republic of Moldova. Internal regulations and instructions.
- Methods and tools for an information security audit.
- Security audit procedures for equipment, data carriers, data, IT applications, internal networks/communications, web security and external Internet attacks
- Audit/assessment of the compliance with the requirements of the national legislation on the security of personal data.
- Analysis of organization, information security management and human factor.

- Security auditing of companies operating systems and database management systems
- Audit of technical and technological infrastructure in company information systems and IT-based confidential information.
- Analysis of scan reports and suggestions for capitalizing on the findings
- Evaluating security controls for the Information Security Management System (ISMS).
- Structure of the audit report. Elaboration of the audit report and proposals for capitalizing the recorded findings. Revision of security system audit
- Computer Assisted Audit Techniques (CAATs)
- Professional Auditor Requirements. Code of Ethics of the Auditor. CISA, CISM Certification (ISACA)
- Future and perspectives of ISA

M3. Enterprise Information Security

- Modern Enterprise Foundations of
- Legal framework of the microeconomic information environment
- Enterprise Information System threats
- Enterprise information resources risk assessment principles and methods
- Enterprise security policies design
- Personal data management and administration in the enterprise information system
- Enterprise information system protection methods
- Enterprise information security system design and implementation
- Enterprise information security system management and audit particularities
- Crisis (malicious attack) management in the enterprise information security
- Best practices in enterprise information security ensuring

M4. Security of electronic transactions

- E-Commerce. Four E-Commerce Business Models. Digital e-commerce cycle.
- E-Commerce Applications. Classification of e-commerce systems
- Payment systems in Internet. Stages of development of payment systems on the Internet
- Classification and characterization of existing payment systems on the Internet
- Means of protection of electronic messages. Use GPG to encrypt and sign messages.
- Activation and deactivation of keys. Key Certification.
- CRM system.
- Types and sources of threats to e-commerce security.
- E-commerce security tools.
- Communication channel. Protecting communication channel.
- Ensuring transaction integrity.
- Security for client computers. Protecting the web server.

List of courses and renovators

Course	University	Participant	e-mail	mob. phone
L1 **Cryptographic Methods of Information Protection**	UTM	Dohotaru Leonid	leonid.dohotaru@mate.utm.md	
	USM	Capcelea Titu	tcapcelea@yahoo.com	069468000
	ASEM (leader)	Zgureanu Aureliu	aurelzgureanu@gmail.com	079234829
	USARB	Gorea Adela	adelagorea@mail.ru	079957878
L2 **Information Systems Security**	UTM	Bulai Rodica	rodica.bulai@ati.utm.md	079701187
	USM (leader)	Novac Ludmila	novacludmila@gmail.com	069791936
	ASEM	Zgureanu Aureliu	aurelzgureanu@gmail.com	079234829
	USARB	Negara Corina	corina.negara@gmail.com	069238884
L3 **Administration and security of computer networks**	UTM	Moraru Victor	victor.moraru@calc.utm.md	060609604
	USM	Băţ Ion	1i2o1n3b@gmail.com	
	ASEM (leader)	Andronatiev Victor	androvic@ase.md	068234488
	USARB	Cabac Eugeniu	eugeniu.cabac@gmail.com	079008201
L4 **Technical means of information protection**	**UTM (leader)**	Ababii Victor	victor.ababii@calc.utm.md	
	USM	Arnăut Vsevolod	arnaut_s@yahoo.com	069272057
	ASEM	Prisăcaru Adrian	prisaandrian@gmail.com	079819615
	USARB	Plohotniuc Eugeniu	eugenplohotniuc@yahoo.com	079825818
M1 **Information security management**	**UTM (leader)**	Bulai Rodica	rodica.bulai@ati.utm.md	079701187
	USM	Brăgaru Tudor	theosnume@gmail.com	062043684
	ASEM	Ohrimenco Serghei	osa@ase.md	079359405
	USARB	Negara Corina	corina.negara@gmail.com	069238884
M2 **Information Security Audit**	UTM	Bulai Rodica	rodica.bulai@ati.utm.md	079701187
	USM (leader)	Brăgaru Tudor	theosnume@gmail.com	062043684
	ASEM	Ohrimenco Serghei	osa@ase.md	079359405
	USARB	Petic Mircea	petic.mircea@gmail.com	079502977
M3 **Enterprise Information Security**	UTM	Moraru Victor	victor.moraru@calc.utm.md	060609604
	USM	Paşa Tatiana	pasa.tatiana@yahoo.com	079406452
	ASEM (leader)	Delimarschi Boris	stud2me@gmail.com	079519406
	USARB	Petic Mircea	petic.mircea@gmail.com	079502977
M4 **Security of electronic transactions**	UTM	Călin Rostislav	rostislav.calin@ati.utm.md	068010143
	USM	Pleşca Natalia	natalia-plesca@yandex.com	079733257
	ASEM	Prisăcaru Adrian	prisaandrian@gmail.com	079819615
	USARB (leader)	Cabac Eugeniu	eugeniu.cabac@gmail.com	079008201

3. Activities related to Teaching / Training

Study visit in Europe no.1

Date: 12-18.06.2017, Place: Athens, Greece

List of Participants from Moldova:

Andronic Serghei	Vice-rector for Didactic Activities	Technical University of Moldova
Besliu Victor	National Coordinator	Technical University of Moldova
Gasitoi Natalia	Vice-rector for Didactic Activities	Alecu Russo State University of Bălţi
Niculită Angela	Vice-rector for International Relations	Moldova State University
Rusu Galina	Dean of the Faculty of Mathematics and Computer Science	Moldova State University
Bolun Ion	Chief of Department Cybernetic and Economic Informatics	Academy of Economic Studies of Moldova
Marina Vasile	Vice-minister	The Ministry of Education, Science and Research
Meico Dmitri	Chief of Department	The Centre of special telecommunications
Putere Alexandru	Chief of Department	The Centre of fighting with the Cyber Criminality

Selection criteria:

The participants to the Strategic study visit were selected to represent all the Moldovan partners of the LMPI project: Ministry of Education, State Centers, Universities. At the institutional level the most appropriate to the subject of the project representatives of administration were selected - the persons who would guide the activities in the project into a better direction. The responsibilities of the selected persons from the Universities are: Implementation of ECTS, implementation of the Bologna Process, Academic Affairs, University courses restructure. Previous experience on Effective Leadership, representation of the University to external bodies, coordination in the strategic planning and curricula development, excellence in instruction, selection and overseeing the processes of faculty and staff selection experience on reviewing, the policies, and procedures, were taken into account.

The participants were selected by the Country Head of the Program together with at least one of the partners' ministries involved in the program. The experience in curriculum renovation, mastering of tuning tools, academic or professional experience in business on the fields of computer science etc. (as stated above) were taken in consideration.

The main objectives:

- Analysis of the strategies of European universities and their implementation;
- To gain from the experience of prominent companies related to the thematic topics of the program.
- Observation of links between European universities and the economic world;
- Study of Bachelor and Master courses related to information security;
- Observation of the functioning of resource centers and technological platforms, didactic cybernetic spaces;
- Analysis of double diploma practices.

The activities during the Strategic study visit:

- Meeting with the Administration of Piraeus University of Applied Sciences
- Discussions with the personnel of Piraeus University of Applied Sciences involved in the LMPI
- Meeting with the representative of the NOC (Network Operating Center) of Piraeus University of Applied Sciences
- Meetings and description of the tools used for distance learning (synchronous and asynchronous). Presentation of all the tools used by the students of the GR-NET (GU-NET)(Greek National Research & Technology Network) - University of Athens (Professor L. Merakos GUNET director, Dr. Spyros Bolis Head of the Network Operation Center of the University of Athens)
- Visit to the Oracle Hellas. Meeting with the ORACLE responsible of the implementation of GDPR Katerina Kalimeri and Dimitris Theodoropoulos.
- Tour of premises of Lamda Hellix Data Center. Presentation of Lamda Hellix activities by the Kantaros Dimitris, Data Center Facilities Operations Director and Zagoras Nikitas.
- Meeting with and presentations from the Head of the Cyber Crime Unit of the Hellenic Police Dr. Georgios Papaprodromou and Spyros Papageorgiou Director of the Directorate General of the National Defense.
- Visit to CISCO Hellas, connection with CISCO Ukraine and discussions with them as Ukraine is responsible for Moldova about possible collaboration for the needs of the program
- Visit of OTE-COSMOTE main building in Amaroussion. (Discussions and presentation of the organisations’ Policy. Meeting with Michael Tsamaz, Chairman and Chief Executive Officer of OTE and Konstantinos Megas responsible of Situation Center and of Security Operation Center.

Professional stage in Europe no. 2

Date: 12-26.11.2017, Place: Aigaleo, Greece

Participants:

1. Tatiana Pasa, Moldova State University
2. Ludmila Novac, Moldova State University
3. Victor Moraru, Technical University of Moldova
4. Rodica Bulai, Technical University of Moldova
5. Mircea Petic, Alecu Russo State University of Bălţi
6. Eugeniu Cabac, Alecu Russo State University of Bălţi
7. Victor Andronatiev, Academy of Economic Studies of Moldova
8. Aurelin Zgureanu, Academy of Economic Studies of Moldova

Selection criteria:

1. The courses' renovators were selected according to the criteria
2. Courses already delivered to the University
3. The interest in studying a new direction and developing a new course
4. Scientific research Papers related to LMPI
5. Experience from previous course syllabus design
6. Scientific interests in Cyber Security and related topics
7. The competences in the related to the LMPI project topics;
8. The strategies of department, including the age, gender and qualification balance;
9. The inter-partners/universities balance;
10. The inter-groups/new courses balance.

Objectives:

- Professionalization of the teachers on the specific topics in view of the implementation of new programs;
- Deepening scientific knowledge of the renovators of the cursus concerning the Cyber Security;
- Participation in seminars and conferences on sensitive topics concerning the safety of systems and networks, proposed by the partners of the Piraeus University of Applied Sciences (Internet of Things security, Networks, Web application security, The politics of community safety, etc.);
- Collection of associated educational resources, educational sequences (objective, content, duration, teaching methods, etc.);
- Establishment of contacts with educational teams and department professors involved in the project;
- Knowledge of the organization of the teaching and research process in the Piraeus University of Applied Sciences, visits to the operational center of the network academic laboratories, meetings and discussions with the participation of professors.

The activities during the professionals' study visit:

- Meeting with the Administration of the involved Department for LMPI
- Discussions with the staff of Piraeus University of Applied Sciences involved in the LMPI program.
- Class attendance with various tutors presenting the main topics of the course contents and IoT security, GDPR norms.
- Moodle Synchronous platform design procedure
- Visits to sites with Archaeological and Scientific interest.