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

lmpi
licence master professionnel
en protection informatique

LMPI – BULGARIA_P5_University of Library Studies and Information Technologies

INTERIM TECHNICAL REPORT

Index

1. Higher education

In LMPI project partners' universities from Kazakhstan are five. There are three Bachelor programmes which will be redesigned under the LMPI project and four new MSc programmes in Cyber security.

For Kazakhstan there is specific set of courses with are mandatory for obtaining the Kazakhstan diploma at any level. These courses are part of new and redesigned programmes. In each programme there are 3 types of courses – **core courses** – one part for professional level and other specific for Kazakhstan and set of **elective courses** which are just few per programme.

- Bachelor programmes are in the area of Information security. They are 4 years programmes and each programme obtain 60 ECTS per year.
    - *Informatics and Software* – this programme correspond to the job description in the Kazakhstan register with same name and number 5B070400. This programme will be implement in three Kazakhstan universities P22-UEEK, P24-KazNU and P29-TarSU. A set of core courses is established as well as the variety of elective courses
    - *Technical and Technology* – this Bachelor programme is oriented to two job profiles: 5B070300 "Information systems", 5B070400 "Computer engineering and software". It is a part of educational set of all 5 universities
    - *Information Systems, Informatics and Software*– this Bachelor programme is oriented to two job profiles: 5B070300 "Information systems", 5B070400 "Computer engineering and software". It is a part of educational set of all 5 universities
- 4 MSc programmes in *Computer Engineering* in domain of *Cyber security* are created with slightly differences for the universities. One similar programme is for P24-KazNU; P29-TarSU. The 120 ECTS credits are set for two years of study.

The development of both programmes level follows:

- the principle of the Bologna process – for quality in higher education
- the emphasizing systems based on internal institutional quality culture –results from TUNING project
- the competence-based path in course creation and strongly related to the e-Competence Framework and the levels of European Qualification Framework.
- the specific competences in area of Information Security are based on the developed by NATO competence framework for cyber security. P05-ULSIT is part of the NATO project MN CD E&T;
- the curriculum for both level is based on Association for Computing Machinery (ACM) IEEE Computer Society (IEEE-CS) standards in the area:
    - Bachelor programme corresponds on Curriculum Guidelines for Baccalaureate Degree Programs in Information Technology 2017
    - MSc programmes relates to the Computer Engineering Curricula 2016

The accreditation files are on not completely finished. Additional work is required in next month. We expect to have a final version in May, 2018 and these accreditation files to be introduced to the Kazakhstan Ministry Education for validation.

2. New/ updated courses

Title	ECTS	Modules	Core / elective	HEIs curricular	degree part of	level of development from 1 to 10
Algorithms and programming	3	1. Introduction 2. Algorithms Principles of algorithmic analysis 3. Types and structure of data 4. Algorithms of succession. Algorithms for sorting 5. Solicitation algorithms 6. Principles of analysis of algorithms 7. Programming methods and technology	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	Bachelor	5
Basic principles of cryptanalysis	7	1. Cryptanalysis of block ciphers and hash functions 2. Cryptanalysis of flow ciphers 3. Non-standard approaches to cryptanalysis 4. Quantum cryptography	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	Bachelor	5
Cloud Computing Protection		M1. Methods of monitoring the user's system environment and information processed by the information being processed. M2. Introduction to the concepts of cloud computing. Advantages and disadvantages of cloud computing. M3. Overview of existing services. Review of existing platforms. Cloud computing technologies	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	Bachelor	5
Cryptographic analysis using software	3	M1. Cryptographic Encryption Algorithms. Complexity and cryptographic strength M2. Software and hardware cryptographic tools and tools for cryptanalysis. Practical problems of the development of cryptographic applications and means of cryptanalysis	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	Bachelor	5

Title	ECTS	Modules	Core / elective	HEIs curricular	degree part of	level of development from 1 to 10
		M3. Methods of cryptographic analysis of symmetric ciphers. M4. Methods of cryptographic analysis of asymmetric ciphers. Search cryptoatak publications of modern encryption algorithms				
Cryptography	6	1. Introduction to cryptography 2. Classic cryptography 3. Symmetric cryptosystems 4. Cryptosystems with public key 5. Asymmetric cryptosites 6. Modern cryptography	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	Bachelor	5
Database security	4	1. Methods of protection of databases 2. Principles for designing secure databases 3. Distributed database architecture 4. Methods of protecting distributed databases	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	Bachelor	5
Information security assessment methods	5	1. Characteristics of information security 2. Modern means of protecting information against unauthorized access 3. Criteria for assessing the security of computer networks and systems 4. Assessment of Information Security Risks	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	Bachelor	5
Information security standards		1. Basic concepts Classification of standards. General criteria, terms and definitions 2. Evaluation standards for information technology security. 3. Audit of the information security system for compliance with the requirements of ISO / IEC 27000	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	Bachelor	5

Title	ECTS	Modules	Core / elective	HEIs curricular	degree part of	level of development from 1 to 10
Introduction of the Information Security	3	1. Introduction 2. Basic Concepts and Information Transformation 3. Discrete information measures 4. Alphabetical coding of information 5. Representation of digital information in digital devices 6. Effective coding 7. Transfer of information 8. Encoding and encrypting information	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	Bachelor	5
IT protection technologies		1. Introduction 2. Basic Concepts of Information Protection Technology 3. The main components of the protection. The main types of threats to computer information 4. Virus protection technologies 5. Program against piracy tools 6. Technologies against software and hardware tabs, protection against the interception of information due to electromagnetic radiation 7. Information protection technologies against interception due to electromagnetic radiation through telecommunication networks 8. Technologies for identifying and authenticating users and processes 9. Information access control technologies 10. Cryptographic protection technologies for programs and data 11. Conclusion	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	Bachelor	5

Title	ECTS	Modules	Core / elective	HEIs curricular	degree part of	level of development from 1 to 10
Mathematical modeling of information security	4	M1. Introduction to mathematical modeling M2. The classification of modeling. M3. Methods and models of information security.	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	Bachelor	5
Network security	4	1. Introduction to network security 2. Multilevel OSI models 3. Current issues of ensuring network security 4. Types of network security measures 5. Characteristics of information security in networks and systems	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	Bachelor	5
Operating system security		1. Introduction 2. Basic concepts and provisions for the protection of information in information systems 3. Security Threats in the Computer and Computer System 4. Software and technical level of information security 5. Operating system security models 6. Windows operating system security 7. The operating system security system of the Unix family 8. Software protection systems 9. Analysis of the security of modern operating systems	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	Bachelor	5
Practical Virology	7	M1. Introduction to virology M2. Technologies for the detection, classification and neutralization of viruses. M3. Methods for diagnosing viruses in network applications.	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	Bachelor	5

Title	ECTS	Modules	Core / elective	HEIs curricular	degree part of	level of development from 1 to 10
Secure software development	5	1. Recommendations for Java application security 2. Recommendations for Java programming 3. Recommendations to improve the reliability and security of Java applications 4. Using the SonarLint static analyzer for secure and secure programming in the Eclipse IDE 5. Dynamic software testing and analysis	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	Bachelor	5
Technical means and methods of protection of information	5	1. The concept of technical protection of information 2. Leakage of information through technical channels 3. Basic principles of the technical protection of information 4. Organizational basis of the technical protection of information 5. Technical means of obtaining information 6. Methods of fighting against leakage and obtaining information 7. Modeling the process of technical protection of information	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	Bachelor	5
Audit of information	5	M1. Basic Concepts and Role of Informational Risk Analysis and Management M2. Audit of information security in the company. M3. International and Russian standards of information security. M4. Methodological basis for the application of standards for the evaluation and management of IT security.	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	MSc	3

Title	ECTS	Modules	Core / elective	HEIs curricular	degree part of	level of development from 1 to 10
		M5. Software used in the audit of information security.				
Cryptographic analysis using software		M1. Cryptographic Encryption Algorithms. Complexity and cryptographic strength M2. Software and hardware cryptographic tools and tools for cryptanalysis. Practical problems of the development of cryptographic applications and means of cryptanalysis M3. Methods of cryptographic analysis of symmetric ciphers. M4. Methods of cryptographic analysis of asymmetric ciphers. Search cryptoatak publications of modern encryption algorithms	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	MSc	3
Cybersecurity and Protection Network		M1. Development of requirements for the cybersecurity system. M2. Development of the cybersecurity system structure for the proposed case. M3. Development of work descriptions for the implementation and operation of software providing cybersecurity.	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	MSc	3
Forensics		M1. Basics of forensic science. Objects of forensic science. M2. Computer information and computer expertise. M3. Theoretical basis of computer forensics	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	MSc	3
Fundamentals of Cybersecurity		M1. The paradigms of building a cybersecurity system. M2. Cybersecurity risk analysis. M3. Engineering and software methods of information protection.	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	MSc	3

Title	ECTS	Modules	Core / elective	HEIs curricular	degree part of	level of development from 1 to 10
Industrial Cybersecurity		M1. Cyberprotection of industrial infrastructures, basis of risk management and enterprise security M2. Practical safety recommendations for IoT industrial scenarios. M3. Industrial Cybersecurity: Preserving Technological Progress	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	MSc	3
Information Security Management Standards		M1. General information on international standards for ISO 27000 information security management systems. M2. Russian Register of Certificates for ISO 27001. M2. International Register of ISMS Certificates.	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	MSc	3
Intelligent Information Security Platforms		M1. Intellectual information systems based on the representation and processing of knowledge. M2. Logic programming M3. Models and algorithms for decision making and knowledge processing.	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	MSc	3
Java for security reasons		M1. Fundamentals of technologies for building the simplest distributed information systems and security. M2. Java security model. Principles of organization and evolution of the security model in Java. SecurityManager. Initialization and functions. Access rights Manage and verify access rights. M3. Java Cryptography Extension. Key Encryption Algorithms and Digital Signatures ..	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	MSc	3
Practical Virology	7	M1. Introduction to virology M2. Technologies for the detection, classification and neutralization of viruses.	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	MSc	3

Title	ECTS	Modules	Core / elective	HEIs curricular	degree part of	level of development from 1 to 10
		M3. Methods for diagnosing viruses in network applications.				
Reliability and efficiency of information security systems		M1. Principles of reliability and prevention. The principle of the evolution of the structure of the system in the face of real threats of information. M2. Analysis and evaluation of the reliability and effectiveness of the applied protection system. M3. Methodological basis of the company's security system (enterprise).	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	MSc	3
Risk Management in Information Technology Systems	6	M1. Analysis of the security risks of the information system. M2. Development of the documentation for the cybersecurity system. M3. Development of the cryptographic protection program of the communication channel	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	MSc	3
Strategic Analysis of Commercial and Administrative Technologies and Communications		M1. Legal regulation of open information resources. M2. Organizational basis for the protection of information. M3. The main business lines of the company's security service (company) in the protection of information resources.	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	MSc	3
The architecture of cybersecurity systems		M1. Architecture of security systems. Typical files of the information system. Types of data processing: batch, batch online, online. M2. Expert systems. Classification of cybersecurity architecture architectures, characteristics and areas of use of the perspective.	core	P22-UEEK P23-UEKO P24-KazNU P25-UPK P29-TarSU	MSc	3

Title	ECTS	Modules	Core / elective	HEIs curricular	degree part of	level of development from 1 to 10
		M3. Data warehouse and the principles of its organization.				

Express in percentage the level of achievement so far concerning

Programme	The development/ update tasks (%)	The recognition/ accreditation tasks (%)	The % of courses already implemented/ delivered to the target group(s)
Bachelor *Informatics and Software*	75	50	some of the courses from the existing programmes 0% from updated programmes
Bachelor *Technical and Technology*	75	50	
Bachelor *Information Systems, Informatics and Software*	75	50	
4 MSc *Computer Engineering*	85	25	0

3. Activities related to Teaching / Training

According the LMPI schedule two training visits have been passed in Sofia (Bulgaria) first one with the managerial staff – one week and second with faculty – two weeks. Both sessions was very later because of the late financial support for the trips:

- first session was planned for May 2017 and managed for July, 2017
- Second – for November 2017 and was established end of January – beginning of February 2018

These delay affected very much to the project results.
Both sessions was focus on the challenge for Kazakhstan partners with updating and creating of new university programmes. The scope of training was from establishment of the competence-based approach to the specific area of Information Security.

Activities in Chronological way

GPR 1 – May 2017

The goal of the first regional meeting was focus on the project goals, schedule, teachings and products. The competence-based learning was introduced

First visit in Bulgaria– July 2017

Introduction of P05-ULSIT courses, programme, organization on management level
Tasks distribution
First announcement of the agreements wit P05-ULSIT

GPR 2 – November 2017

The cross matrixes for Bachelor and Master levels (competencies / programmes – courses) was established
Further tasks was discussed.

Second visit – training session – January – February 2018

The goals of the second training session was to be developed the accreditation documents

GPR 3 – February 2018

The round trip to each Kazakhstan region:

- problems solving
- final version of the accreditation documents

The results of all sessions with Kazakhstan partners is to be transferred the achievements of P05-ULSIT to them and to be widespread in the partners' universities.
The communication with the Kazakhstan partners is a weak point. The email culture is different. They prefer telephone calls which is not appropriate sometimes.

The team member in the LMPI project from all Kazakhstan partners are selected according their expertise and CVs. All people involved in the projects are from the departments related to the Information technologies, Computer Science and Security as follow:

LMPI partner	Department
P22-UEEK	Information Technology and Security
P23-UEKO	Information Systems and Informatics
P24-KazNU	Computer Science
P25-UPK	Information Systems and Computer Science
P29-TarSU	Information Systems