



LMPI – KAZAKHSTAN_P24_ L'Al-Farabi Kazakh National University

INTERIM TECHNICAL REPORT



Index

QUALITY OF THE PROJECT IMPLEMENTATION	3
CURRICULUM DEVELOPMENT	8
ACTIVITIES RELATED TO TEACHING/TRAINING	12
AWARNESS RAISING, DISSEMINATION, SUSTAINABILITY AND EXPLOTATION OF THE PROJECT RESULTS	13



QUALITY OF THE PROJECT IMPLEMENTATION

1. Description of the implemented activities

The role of the KazNU (P24) will be as follows:

Participates in all the work within the framework of the mission entrusted to it within the strategic regional plan. Participation in the regional steering committee, study visits and training courses planned in Bulgaria, training of teachers (curriculum developers, ODL and counseling in employability orientation), and co-facilitation with its European referent of the training of curriculum renovators, co-authoring the specialized fields of work in "development, management, administration and protection of computer systems and networks in companies", and participation at the choice of the bachelor's degree and the associated master's degree, co-authoring of the programs, the courses and the educational resources (license, master and modular device of formation throughout the life), organization of the lessons to welcome the students in the first year of the 2 new curriculum, creation of a diploma (double or joint) with the European partner universities, contributes to the sustainability and dissemination of results.

In May 2017, employers were questioned. The survey involved 600 participants. Of these, 100 respondents from Taraz companies. The greatest need, according to respondents, in IS specialists is felt in the banking sector, telecommunications companies, public administration institutions.

The respondents identified the following main tasks, which should be carried out by IS specialists:

1. Installation of systems for detection, prevention and prevention of intrusions (369/600);
2. Setting up mechanisms for preventing, restoring and maintaining system continuity (264/600);
3. Frequent detection, detection of system vulnerabilities (262/600);
4. Network and system monitoring, incident response (255/600);
5. Implementation of information encoding, authentication and PKI construction (251/600).

Among the most actively used tools (tools) for protecting information were:

1. Opposition to viruses and malware (319/600);
2. Software protection facilities (278/600);
3. Controlled access (265/600);
4. Data encryption (253/600);
5. Means of protection of hardware (213/600).

Based on the results of the questionnaire, the following most important, in the respondents' opinion, competencies were identified:

1. update security systems in response to new threats and new technologies (288/600);
2. ensure the stability of security systems (278/600);
3. provide various solutions for protection (264/600);
4. to carry out diagnostics of the information system (257/600);
5. implement various security processes (254/600).



When asked about the subjects that will allow these specific competences to be obtained, the following answers were received:

1. Security Policy (267/600);
2. Protecting Servers and Client Computers (246/600);
3. Administration system (230/600);
4. Cryptography (222/600);
5. Devices and equipment for security (VPN-firewall, etc.) (214/600)

Based on the responses of the respondents, the following knowledge and skills that an information security specialist must possess:

- knowledge of the legislative framework in the field of information security;
- the ability to design, development and apply technologies and tools and data protection;
- the ability to design, develop and apply information security technologies and tools;
- the ability to apply standard and design new cryptographic algorithms and protocols to protect information in computer systems and networks;
- the ability to apply methods and means of countering unauthorized receipt of information in accordance with the requirements of regulatory documents of the system of technical protection of information.

Based on the identified market needs, the goal was to develop an educational program for the master's program "Computer systems and networks security". This program is a specialization of Information Security. The main objectives of the educational program is the organization of the security of information and communication systems and networks, which implies a development by, embodiments, implementation and management of complex software and hardware systems, and information security in institutions.

In this regard, the classification of the identified competences on clusters was carried out. The following clusters were identified:

- Ensuring information security;
- Network design and cloud computing;
- Security of network devices and mobile solutions;
- Software and hardware data protection.

Based on the results of analysis and synthesis of the survey materials, a map of the specialty of the master's degree program "Safety of computer systems and networks" was compiled.

As part of the project, KazNU (P24) together with TarSU (P29) developed a training trajectory "Security of computer systems and networks".

The website of the project is developed.

11.04.2017 in the KazNU within the framework of the agreement signed by KazNU and Kaspersky Lab, representatives of Kaspersky Lab conducted a training seminar "Kaspersky day".



The key topic of the seminar-training "Kaspersky Day" was cybersecurity. Representatives of Kaspersky Lab conducted a lecture on cyberthreats, the business game Kaspersky Interactive Protection Simulation (KIPS), where, using real business cases, they looked for ways to solve cybersecurity problems and training on "Vulnerability Analysis in Software".

Also in parallel with the training was a round table "Information Security: Educational Programs", where faculty of the Faculty of Mechanics and Mathematics and representatives of the Kaspersky Lab discussed the content and timing of educational courses for students and refresher courses for teachers in the field of information security for 2017-2018 academic year. More than 80 students and teachers took part in the event.

04.2017-05.2017 Study of the professional standard of the Russian Federation "Computer Systems and Networks Security Specialist", European e-Competence Framework 3.0, Cisco CCNA, Cisco CCNP Security, HP ATA, educational programs of partner universities in the field of security systems and networks.

09.06.2017 a meeting of the KazNU team with the project coordinator Pachoud Jean-Noel, coordinator of the ERASMUS+ national office Sh. Tasbulatova, partners from TarSU.

12.06-20.06.2017 Analysis of the results of the questionnaire. Conducting meetings with experts in the field of information security. Based on the information received about the needs of the labor market, compiling a list of generalized labor functions of a specialist in the field of system and network security.

06.2017 A textbook on the course "Information and Communication Technologies" was published, in which modern trends of ICT are consecrated: mobile platforms, cybersecurity, network technologies. One of the authors of the textbook is the head. Department of Informatics Urmashhev B.A. The Department of Informatics of KazNU is the developer of TUP on the cycle of general educational disciplines "Information and Communication Technologies" (for all specialties and areas of bachelor's training) ICT.

2. Visibility

Within the framework of the project, a website is developed, the website address is <http://lmpi.kaznu.kz>. The purpose of the website is to disseminate information about the LMPI project and highlight important events during the project implementation. The website is supported in three languages: Kazakh, Russian and English. The website consists of sections: Home, About, Partners, News, Contact. The website 's database is located on the server of KazNU. The website was developed by the participants of the project from KazNU Salimhanova Assem and Mambetniyazov Murat. Below are screenshots of the website:



Partners	Website	Country
UNINETTUNO	(Web)	Italy
ASEM - Academia de Studii Economice a Moldovei	(Web)	Republica di Moldavia
Centrul de Telecomunicati Speciale	(Web)	Republica di Moldavia
Centrulul pentru Combaterea Crimelor Informatice	(Web)	Republica di Moldavia
CESE - Centro Studi ed iniziative Europeo	(Web)	Italy
City Scientific Research Center for New Technologies in Education - Almaty	(Web)	Kazakhstan
CORPORATE FUND FUND ZHAS OTAN IN AKMOLA REGION	(Web)	Kazakhstan
ENU - L.N Gumilyov Eurasian National University	(Web)	Kazakhstan
GIP FIPAG - Académie Grenoble - GIP Formation et Insertion Professionnelle	(Web)	France
HCMUT - Ho Chi Minh City University of Technology	(Web)	Vietnam
HTWK - Hochschule für Technik, Wirtschaft und Kultur Leipzig	(Web)	Germany
HVN - Vietnam National University of Agriculture	(Web)	Vietnam
Intreprinderea mixta «EFES VITANTA MOLDOVA BREWERY» SA	(Web)	Republica di Moldavia

Summary

The LMPI project seeks to establish e-learning Bachelor's and Master's degrees for the protection of computer systems and networks in three Partner Countries, Vietnam, Moldova and Kazakhstan. In order to bridge skills gaps at both technician and engineering levels, the partners will develop a lifelong learning program in this area for employers. The curriculum to be developed will meet the needs of private companies which are seeking specialists to protect themselves against cybercrime.

Description

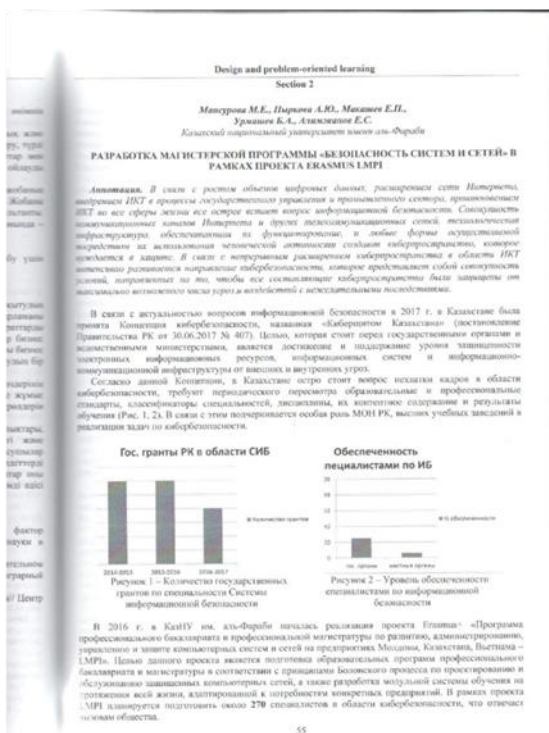
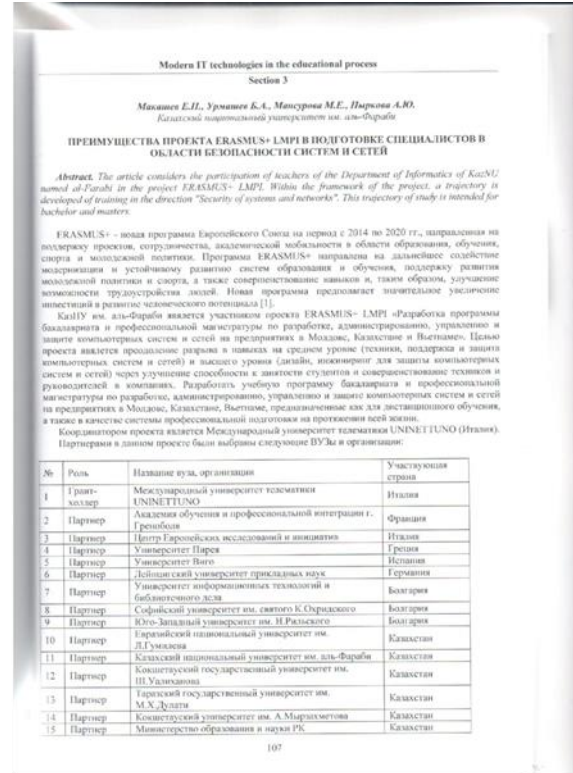
Cybercrime affects almost all countries. In order to face it, well-trained specialists in advanced computer technologies are needed. The three participating Partner Countries suffer from a shortage of managers, technicians and engineers to address this major problem. The need for the project which develops university education in this sector is, thus, quite evident. Highly-qualified graduates with vocational or professional background are needed, as are academic and professional staff to train them. Continuing education to keep them abreast of the latest developments in this advanced area is an imperative. The project focuses on curriculum development in the area of computer sciences or, more specifically, security services.

A survey of 500 companies will analyse the needs in basic and specific skills in businesses and therefore the training needs and specialization required for the Bachelor's and Master's degrees. It will then list them, break them down into semester's curriculum and different teaching units. The teaching units would be practical work, work laboratory, personal work and allocation of ECTS credits. It will then be possible to design the courses contents and educational resources in each of the three countries and to set up a center of excellence in each of the three leading universities (resource center and technology platform equipped by the project).

The project envisages training courses that can be accessed online as well. Each partner university will build or adapt a didactic cyberspace in which all activities will take place. In order to respond flexibly to the businesses' needs the project will also build a modular system covering all fields of network administration and security of computer systems (10 modules). In particular, they cover the following fields: cryptographic mechanisms and applications, administration and network security system, software engineering, UML and network protocol and service development, security, cryptographic mechanisms, data security, information and security, both systems IT development, information and security, both systems IT development, information and security, both systems IT development.



International scientific-practical conference "Active teachings methods" was held on 23-24 November 2017 in Almaty. The conference is organized jointly by Kazakh National University named after Al-Farabi with Newcastle University upon Tyne with partners participation – British Council, Newton Fund, Royal Academy of Engineering, Nazarbayev University, JSC Almaty Power Stations, TOO Crystal Spring and others. At this conference, project participants made presentations and two articles were published. Article in the collection of the international scientific conference "Active methods of teaching":





CURRICULUM DEVELOPMENT

1. New/updated courses

As part of the project, KazNU (P24) together with TarSU (R29) developed a training trajectory «Security of computer systems and networks»:

- in 2018 for the undergraduate specialty «5B070400-Computer Engineering»
- in 2018 for the master's degree in the specialty «6M070400-Computer Engineering», with the clarification and addition of 2018.

Bachelor

Security of computer systems and networks			
Course name	Credit	ECTS	Semester
Operating system security	3	5	6
Intelligent Data Analysis	3	5	7
Technical means and methods of information protection	3	5	7
Information Security Standards	3	5	6
Network Security	3	5	7
Cryptography	3	5	6
Database Security	3	5	7
Web application Security	3	5	7
Development of secure software	3	5	6
Fundamentals of cryptanalysis	3	5	6

For the undergraduate specialty «5B070400-Computer Engineering», the training trajectory «Security of computer systems and networks», the above-mentioned elective disciplines, is being introduced into the curriculum since the academic year 2018 (only elective disciplines!). Obligatory disciplines of the specialty remained unchanged. In the undergraduate curriculum, students can choose one of the two trajectory of choice. In the existing curriculum of the specialty "5B070400-Computer Engineering", the third training trajectory «Security of computer systems and networks» was developed and added, developed within the ERASMUS + LMPI project. Since the academic year of 2018, bachelors have been given the choice to study in one of three directions. In percentage terms, the level of achievement compared with the final product at the bachelor's degree:

- Development / update tasks in% - 20.4% (10 of 49).

After graduation, the student is awarded the «Bachelor of Engineering and Technology» degree in specialty 5B070400-Computer Engineering.

The undergraduate curriculum was accredited by ASIN:



EQANIE ACCREDITATION CERTIFICATE

ASIIN e.V.

has accredited the

**Bachelor's Programme Computer Engineering
(formerly Computer Science and Software)**

provided by

Al-Farabi Kazakh National University

on September 26th, 2014 until September 30th, 2019.

The programme satisfies the outcomes of First Cycle Programmes specified by the

**Euro-Inf Framework Standards and Accreditation Criteria for
Informatics Degree Programmes.**

Therefore for the above period of accreditation is awarded the

Euro-Inf Bachelor Quality Label.

EQANIE

For the European Quality Assurance Network
for Informatics Education e.V. (EQANIE)

The President, Eduardo Vendrell Vidal
Düsseldorf, July 25th, 2016

ASIIN

For ASIIN e.V.

The Managing Director, Dr. Iring Wasser
Düsseldorf, July 25th, 2016



Master

Security of computer systems and networks			
Course name	Credit	ECTS	Semester
Malware analysis	2	4	1
Applied Cryptography	3	5	2
Mobile Security	2	4	3
Architecture of Cybersecurity Systems	2	4	2
Fundamentals of Cybersecurity	3	5	1
Cyber Security & Network Protection	3	5	2
Java for Security purpose	3	5	3
Design Cybersecurity of Database	3	5	3
Industrial Cybersecurity	2	4	3

The training trajectory «Security of computer systems and networks» for the master's degree in the specialty «6M070400- Computer Engineering» was launched in 2017. 2017-2018 academic year, the first set of 10 undergraduates for the specialty «6M070400- Computer Engineering» on the trajectory «Security of computer systems and networks» was implemented. The above mentioned elective disciplines are introduced into the curriculum from the academic year 2018 with the addition (only disciplines of choice!). Obligatory disciplines of the specialty remained unchanged. In the curriculum of a master's program, trainees can choose 1 out of 5 trajectories of choice. One of them is the trajectory «Security of computer systems and networks» developed within the ERASMUS + LMPI project. In percentage terms, the level of achievement compared to the final product at the master's level:

- Development / update tasks in% - 25.9% (7 of 27).

After graduation, the undergraduate is awarded the "Master of Engineering" degree in specialty 6M070400- «Computer Engineering»

The Master's program was accredited by ASIIN:



EQANIE ACCREDITATION CERTIFICATE

ASIIN e.V.

has accredited the

**Master's Programme Computer Engineering
(formerly Computer Science and Software)**

provided by

Al-Farabi Kazakh National University

on September 26th, 2014 until September 30th, 2019.

The programme satisfies the outcomes of Second Cycle Programmes specified by the

**Euro-Inf Framework Standards and Accreditation Criteria for
Informatics Degree Programmes.**

Therefore for the above period of accreditation is awarded the

Euro-Inf Master Quality Label.

EQANIE

For the European Quality Assurance Network
for Informatics Education e.V. (EQANIE)

The President, Eduardo Vendrell Vidal
Düsseldorf, July 25th, 2016



ASIIN
For ASIIN e.V.

The Managing Director, Dr. Iring Wasser
Düsseldorf, July 25th, 2016



ACTIVITIES RELATED TO TEACHING/TRAINING

From January 29, 2018 to February 9, 2018 at the University of Library and Information Technologies, ULSIT (Sofia, Bulgaria), according to the project ERASMUS + Project - EPP2016-1JT-EPPKA2-CBHE-JP-LMPI "Bachelor's and professional master's degree in the development, administration, management and protection of computer networks in enterprises ", a training seminar on cybersecurity was held with the participation of project partners from Kazakhstan: L.N. Gumilev, Kazakh National University. al-Farabi, Taraz State University. M.H. Dulati, Kokshetau State University. Sh. Ualikhanova, Kokshetau University A.Myrzakhmetova, Branch of JSC "NTSPK" Orleu "Institute of advanced training of pedagogical workers in Akmola region, and teachers and specialists of the University of Library Science and Information Technologies, BIT (Sofia, Bulgaria). During the meeting, courses on the cybersecurity of personal data and data at enterprises were heard, a curriculum for undergraduate and graduate programs in the area of protection of the information security system was developed. During meeting with the pro-rector for academic work at the University of BIT, professor, Dr. Vanya Pavlova signed an agreement on cooperation between the universities of BIT and TarSU. In the future, a two-diploma education with BIT under the Master's program is planned. Based on the results of the two-week course of the training seminar, the certificates "Development of a curriculum on the basis of the European standard" and "Research in Europe and the development of a curriculum on cybersecurity" were issued.



AWARNESS RAISING, DISSEMINATION, SUSTAINABILITY AND EXPLOTATION OF THE PROJECT RESULTS

The existing Kazakhstan model of school, secondary special, higher and postgraduate education in the field of information and communication technologies (ICT), including specialization in information security, requires constant and careful analysis by all stakeholders (including the Ministry of Education and Science of the Republic of Kazakhstan, higher education institutions educational institutions and potential employers) for compliance with the current needs of the society and trends in ensuring the safe development of information ion technology in mind the dynamic development of this area. In particular, educational and professional standards, classifiers of specialties, disciplines, their content and learning outcomes require periodic revision. There is a need to develop a mechanism that allows more flexible response to modern challenges in the field of ICT. In view of the fact that knowledge in this field is rapidly becoming obsolete, periodic qualification of specialists is required. In the field of ICT there is a shortage of information security specialists, both in the public and private sectors. So in the central state bodies the security is only 25%, in the local - 6%.

Resolution of the Government of the Republic of Kazakhstan dated October 28, 2017 No. 676 approved the Action Plan for the implementation of the Cybersecurity Concept ("Cybershield of Kazakhstan") until 2022. The concept of cybersecurity (CyberSpace of Kazakhstan) was developed in accordance with the Message of the President of the Republic of Kazakhstan "The Third Modernization of Kazakhstan: Global Competitiveness", taking into account the approaches of the Kazakhstan-2050 Strategy on Kazakhstan's entry into the list of 30 most developed countries of the world. The Concept defines the main directions for implementing state policy in the field of protection of electronic information resources, information systems and telecommunications networks, ensuring the safe use of information and communication technologies. The implementation period of the Concept includes two stages:

- 1) the first stage of 2017-2018;
- 2) the second stage of 2019-2022.

At the first stage will be:

- developed a comprehensive enforcement practice of compliance with the already established requirements in the field of information security, which will result in the necessary changes in the legislation;
- the revision of educational programs and professional standards was carried out, the number and quality of trained specialists in the field of information security was increased, and the qualification of existing employees engaged in this field was improved.

Expected results of the concept of cybersecurity:

- 1) the global cybersecurity index of Kazakhstan by 2017 will be 0,200, by 2018 - 0,300, by 2019 - 0,400, by 2020 - 0,500, by 2021 - 0,550, by 2022 - 0,600;
- 2) increase of awareness of information security threats to the base period of 2018 in 2019 - by 5%, in 2020 - by 10%, in 2021 - by 15%, in 2022 - by 20%;
- 3) the number of retrained specialists in the field of information security in 2018 - 300, in 2019 - 500, in 2020 - 600, in 2021 - 700, in 2022 - 800;

Proceeding from the foregoing, in order to understand and build a model of a methodical system for training information security tools, it is necessary:



- develop a work program and content of disciplines on information security disciplines, work programs and content of disciplines (sections of disciplines) of the information cycle for students of various training profiles;
- to improve traditional and innovative forms of education, methods and training programs on the basis of integrated information and the educational environment in accordance with the theoretical essences of the interrelationships of fundamental, professionally directed and informational education;
- to improve such types of training as a professionally directed lecture, practical lesson and laboratory work for the disciplines from the "Information Security" cycle, and also for the information cycle disciplines, including information security issues in the educational process and the field of scientific research;
- to develop distance learning courses for methodical maintenance and improvement of students' education in information security.

All these actions confirm the sustainability of the results of the project after the completion of the project.