Information & Security: An International Journal

Potii and Oliynykov, vol.35, 2016, 11-27 https://doi.org/10.11610/isij.3501

UKRAINIAN EDUCATIONAL SYSTEM IN THE FIELD OF CYBERSECURITY

Oleksandr V. POTII and Roman V. OLIYNYKOV

Abstract: Main threats and challenges to cybersecurity are considered in this article from an educational perspective. The authors analyse the system of higher education in the field of information and cybersecurity, present the standards of education in the field of information security, outline the system of universities in Ukraine, as well as analysis of a number of practical cases.

Keywords: Cybersecurity, information security, educational system.

Introduction

Cybersecurity is an integral part of national security.[1] It depends on many factors. An important factor is the human factor. The individual is the main carrier and the user information. He is the subject and object of information warfare. Therefore, the security of information resource depends on:

- The public awareness of the problems of cyber security of individuals, society and the state;
- The level of specialized training of state and military leadership, of armed forces and special services personnel;
- The level of training of civilian and military experts.

Low level of training, lack of information about new threats in cyberspace, a misunderstanding of using new technologies is threats of cyber security in Ukraine. Another threat is a low level of security culture of the population. Using of electronic services in households is a new trend in Ukraine. But there is a low level of knowledge about threats in cyberspace still.

So, the problem of forming a new system of training is topical and timely for Ukraine. We understand that one of the possible answers to the new challenges of cybersecurity is the transformation of the education system in the field of information security and cybersecurity.

The main goals of transformation are providing training of high qualified specialists and creation of the cybersecurity culture among Ukrainians, understanding the threats of cyber-security and the consequences of their implementation.

Achievement of these objectives will allow Ukraine to modernize the education system in the field of cybersecurity. Cybersecurity education will be modern and meet the new challenges. So, role of educational and scientific research in the field of information security is very important.

Tasks of the Education System

Modernization of the educational system contributes to the implementation of the state policies. The main streams of the government policies are presented on the next slide. As you can see these directions are technological. Without high qualified staff this policy is unrealized. It requires a transformation in the education system.

The educational system in the field of cyber security performs the following tasks:

- to develop and coordinate research work in the field of cyber security;
- to create favourable conditions for young professionals in the field of information technology should facilitate their employment in Ukraine;
- to amend the curriculum and programs of secondary and higher education, training of scientific and pedagogical staff;
- to strengthen state support of major areas of science and technology as the basis for the creation of high information technologies;
- to develop national programs to improve public awareness of cyber threats;
- to support the efforts of civil society and business to increase public awareness on pressing cyber threats;
- to provide continuous training of civil servants and employees involved in key critical infrastructure.

In addition, the education system should be transformed in the context of the Bologna process and the requirements of the new Law on Higher Education.

In the USSR training of specialists on information security was carried out by military and special educational institutions. Programmers, radio engineers, mathematicians graduated from these institutions. They were engaged in security of governmental communication, technical and cryptographic information security, counteraction to foreign intelligence technical services. During independence in Ukraine a system of training specialists in the field of information security was created powerful research teams were organised. Strong training centres for preparation were organized in Kyiv, Kharkiv and Lviv.

In the future, we see such structure of training in cybersecurity:

- training of civilian experts in the field of information security and cyber security (IT-sector, banking, critical infrastructure);
- training military experts and experts for special services (cyberwar, fighting against cybercriminal and cyberterrorism);
- special training and advanced training for public administration and governments;
- common training Ukrainian citizens and their adaptation for the life in the modern information space.

Training is carried out in three areas of expertise:

- Technical experts in security and military science (information security, cybersecurity and so on);
- Technical experts in engineering (computer science, soft engineering, computer engineering and so on);
- Experts in the social sciences, business and law.

Characteristics of Educational Standards in the Field of Information and Cybersecurity

The training of specialists in information security began in 1995. In 1997, the list of specialties, which trains specialists in universities, incorporated specialties 1701 "Information Security," which includes five specialties.

Today, the system training of specialists in the field of information security includes three groups of standards for training.

The first group are standards 1701 "Information Security."[2] This knowledge sphere includes three areas of training and five specialties (Table 1). Training is carried out at the level of bachelors and masters.

The second group are standards are relative with 1701 "Information Security" speciality. The group includes such standards as:

- 0501 "Informatics and Computer Science (Computer Science, Computer engineering, software engineering)";
- 0502 "Automation and Control (Systems Engineering)";
- 0509 "Radio, Radio and communication devices (radio, telecommunication)";

Table 1: Standards of higher education 1701 “Information Security.”

Bachelor	Master
6.170101 Security of information and communication systems	8.17010101 Security of information and communication systems
	8.17010102 Security of the state information resources
6.170102 Systems of technical information security	8.17010201 Systems of technical information security and Automation of its processing
6.170103 Information Security Management	8.17010301 Information Security Management
	8.17010302 Administrative management in the sphere of information security

- 0403 “System Sciences and Cybernetics (Computer Science, applied mathematics, cryptology)”;

The third group are standards for social sciences, business and law:

- 0302 “International Relations” (international relations, international information);
- 0303 “Journalism and information (journalism, advertising, public relations)”;
- 0304 “Law”;
- 0301 “Social and Political Sciences” (sociology, practical psychology, political science);
- 0201 “Culture” (Documentation and Information);
- 1601 “Military science, national security” and others.

In 2015, as a result of the reform, it was decided to introduce a new training direction – cybersecurity. In 2016 to begin training new specialists.

Let’s consider the requirements of educational and professional training programs for *bachelor’s degree*.[4] Table 2 shows the structure of the Bachelor program. The program contains three groups of subjects − education regulatory discipline, the discipline that a student chooses on their own and practice. Normative period of bachelor study − 4 years.

Table 2: Structure of the Bachelor's programme.

Cycle training	The maximum time for training cycles (semester hours / credits ECTS)
1. NORMATIVE TRAINING COURSE	
1.1 The cycle of humanitarian and socio-economic disciplines	480/16
1.2 Cycle of disciplines of natural science (fundamental) training	1560/52
1.3 Cycle of disciplines of general training	3360/112
2. STUDENT DISCIPLINE OF FREE CHOICE	
2.1 The cycle of humanitarian and socio-economic disciplines	270/9
2.2 The cycle of general professional disciplines and professional-practical training	1530/51
2.3 Military training	870/29
3. PRACTICE	
Industrial practice	150/5
Pre-diploma practice	180/6
State qualification work	90/3
Total number:	**7200/240**

Kharkiv Karazin National University offers a list of subjects for the implementation of Bachelors (presented in Table 3).

Table 3: Disciplines in the Bachelor's programme.

Subject	**ECTS**
1. The cycle of humanitarian and socio-economic disciplines	
Philosophy	3
Foreign Language	6
Foreign language Professional oriented	3
History of Ukraine	3
Science of law	1
Physical Training	11

2. Cycle of disciplines of natural science (fundamental) training	
Higher mathematics	19
Physics	13
Computer basics	3
Application Programming Packages	5
Discrete mathematics	6
Probability Theory, probabilistic processes	6
3. Cycle of disciplines of general training and the cycle of general professional disciplines and professional-practical training	
Introduction to the profession	4
Information Theory and Coding	5
Fundamentals of information security	2
Number theory	2
Theory of groups, fields, rings	3
Microprocessors and their applications	3
Metrology and measurement	3
Fundamentals of the theory circles, and processes signals in electronics	5
Electrical engineering and electronics	5
Computer circuitry and architecture of computers	5
Information and Communication Systems	12
Operating Systems	4
Algorithmic and Programming	5
Cross-platform programming	4
The theory of algorithms	4
Object-oriented programming	6
Parallel systems and computing	5
Optoinformatics	4
Computer Graphics	3
Steganography	6
Specialized programming language	5
Life Safety	3
Systems of technical protection of information	5
Regulatory information security	2
Applied Cryptology	8
Information protection in information and communication systems	19
Complex systems of information protection: design, implementation and maintenance	10
Information Security Management	3
Components of complex computer networks	4

Let’s consider the requirements for educational and professional training programs for a *master’s degree*. Table 4 shows the structure of the Master’s programme. The programme contains three groups of subjects − education regulatory discipline, the discipline that a student chooses on their own and practice. Normative period of master’s study is 1,5 or 2 years.

Table 4: Master’s Preparation Structure.

Education and Training Cycle	The maximum time for training cycles (semester hours / credits ECTS)
1. NORMATIVE TRAINING COURSE	
1.1 The cycle of humanitarian and socio-economic disciplines	150/5
1.2 Cycle of disciplines of mathematical and natural-science training	420/14
1.3 Cycle of disciplines of professional and practical training	1200/40
2. STUDENT DISCIPLINE OF FREE CHOICE	
2.1 The cycle of general professional disciplines and professional-practical training	900/30
3. PRACTICE	
Research practice	240/8
Pre-diploma practice	180/6
Qualifying exam	60/2
Execution of the master's work	450/15
Total number	**3600/120**

Master training includes such disciplines (in parentheses are the amount of hours in ECTS): Mathematical modelling and process optimization (14); Basics of Patent (2); Technologies for information security management communication systems (8); Methods of analysis and cryptosystems (14); Modelling and evaluation of information security (10); Information Security in Banking (6); Research practice (8); Basic research and organization science (3); Technology design, analysis and use of symmetric cryptosystems (8); Monitoring and auditing information and communication systems (6); Wireless Security (2); The theory of distributed information resources, protection of data and knowledge bases (7); Standardization in the field of security of information systems and technologies (6).

According to the results of study the student has to acquire certain competencies. The standard specifies such competence: social and personal (e.g., the ability to work in a team); the general scientific (e.g., the ability to conduct their own analysis, classification, comparison, abstraction, the willingness to generate new ideas); professional (for example, the ability to use basic methods, principles and means of communication in the construction of systems of information protection).

Analysis of training programs and learning outcomes allows us make to the following conclusions.

1. Education in Ukraine is aimed to training technical specialists with technical information security and cryptography;
2. Basic special educational disciplines provide technical skills and do not provide such skills as leadership, resource management, human resource, business processes, risks, etc.;
3. Attention fayed to the skills of information security management is not satisfactory.

The industrial base for the production of national information security tools has been developed. The good results were obtained in the development of technical and cryptographic protection in Ukraine. The national cryptographic standards are developed. PKI is developing actively. In this case, all CAs use only national facilities of information protection. Nowadays national facilities of information security are used in educational process.

Where to Educate Information Security Specialists in Ukraine?

The specialist training system in Ukraine is based on scientific and pedagogical schools, which exist at universities. To create a scientific and pedagogical school it is necessary to spend 10-15 years. For a partial change of their tasks within the traditional orientation and the formation of a contingent of students it is necessary to spend to 4-8 years. Today the eighteen Ukrainian universities carry out training of specialists in the field of information security. The quantity of universities which train experts in different specialties and levels is given in Table 5.

Table 5: Number of universities providing education and training in the field of information security.

Specialties	Bachelor	Master
170101 Security of information and communication systems (SICS)	18	12
170102 Systems of technical information security (STIS)	17	12
170103 Information Security Management (ISM)	12	4
17010302 Administrative management in the sphere of information security	-	4
17010102 Security of the state information resources	-	1

Leading universities for education and training in information security, and their websites, are as follows:

1. National Aviation University (NAU), http://nau.edu.ua/en
2. Military Institute of Telecommunications and Information of the State University of Telecommunications, http://viti.edu.ua/en
3. State University of Telecommunications (SUT), http://www.dut.edu.ua/en/pages/7
4. Taras Shevchenko National University of Kyiv, http://univ.kiev.ua/en/
5. National Technical University of Ukraine “Kiev Polytechnic Institute” (NTUU “KPI”), http://kpi.ua/en/
6. N. Zukovsky National Aerospace University “KhAI,” http://www.khai.edu/
7. Kharkiv National University of Radio Electronics (KhNURE), http://nure.ua/
8. Kharkiv V. N. Karazin National University (KhNU), http://www.univer.kharkov.ua/en
9. National University Lviv Polytechnic, http://lp.edu.ua/en
10. Odessa O.S.Popov National Academy of Telecommunications, http://onat.edu.ua/en.

The number of students who entered at universities for Information Security specialty in 2014 is provided in Table 6. Over the past four years, this figure did not change. Note that this is less than one percent of the total number of students who entered universities.

Table 6: Results of the entrance campaign in 2014.

	Eastern region			Central region			Western region	Sum
	KhNU	KhAI	KhNURE	NTUU “KPI”	NAU	SUT	Lviv Poly-technic	
SICS	28	22	40	54	74	23	24	265
STIS	-	-	30	32	32	27	33	153
ISM	-	-	2	-	46	16	30	94
							Total:	**512**

The student’s competitions in the field of information security are carried out every year. It supports high training of students. High level is demonstrated by students from Kharkiv National University of Radio electronics, National Technical University of Ukraine “KPI”, Institute of Special Communication and Security Information, Kharkiv Karazin National University. After leaving a university termination students are ready to work at various positions (Table 7).

Table 7: Characteristics of jobs.

Bachelor	**Qualification**	**First positions**
6.170101 Security of information and communication systems	Specialist in information security in information and telecommunication systems	- inspector; - specialist of public service.
6.170102 Systems of technical information security	Specialist in technical information security	- engineer; - specialist of public service; - specialist of technical expertise; - operator of radio engineering control; - inspector of telecommunication.

6.170103 Information Security Management	Expert in the organization of information security	- expert in the information security organization with limited access; - specialist in a privacy mode; - specialist in supervision and protection; - specialist on the organization of information security.

Besides Ukraine has specialized training centers: InformSecurity, Domina Security, Academy «АйТі», Network Academy "Lanit," etc.

A big achievement of Ukraine is building of a postgraduate education: philosophy doctor and doctor of science theses (Table 8). The main scientific schools preparing information security staff are in Kyiv, Kharkiv and Lviv. There are two postgraduate programs in Ukraine. (Table 4).

Table 8: Postgraduate programmes in Ukraine.

Code	Science area, group of specialties, specialty	Science area
05.13.21	System of Information Security. The theoretical, scientific, technical and technological issues related to organization, creation of methods and tools to protect information during its storage, processing and transmission using modern mathematical methods, information technology and facilities.[3]	Technical science
21.05.01	Information security of the state. Information security state - the branch of science that studies the problem of information security of national interests of Ukraine, studying and justifying forms and methods of protection of man, society and the state from external and internal threats in the information sphere, as well as ways to improve the efficiency of information systems in modern conditions.[4]	Technical science

Practical case

When training specialists much attention is paid to practical training. Let’s demonstrate following two examples of lab activities that are carried out in academic disciplines.

The first example is series of laboratory works on certification authority (CA) for public key infrastructure (PKI) support. During this activity students master issuing and maintenance of users' public key digital certificates, time-stamping service, means of digital signature and encryption. Laboratories at Kharkiv V.N. Karazin National University (Ukraine) are equipped with modern hardware and software means also deployed in several government-certified Ukrainian CA. Functional scheme of the laboratory equipment is given in Figure 1.

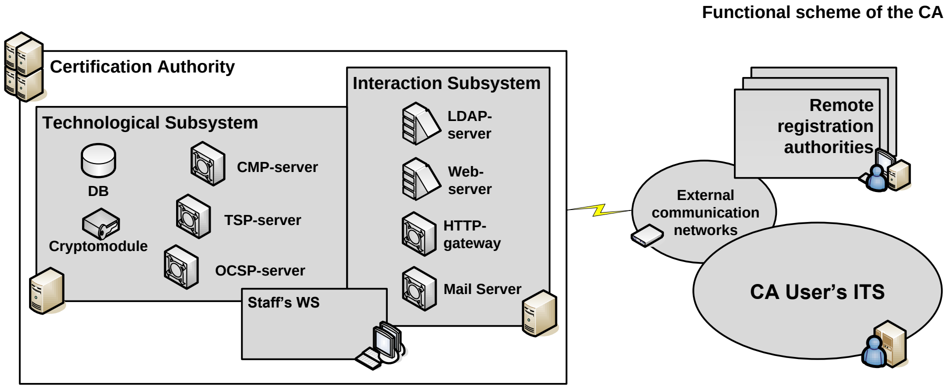

Figure 1: Functional scheme of the system.

During the laboratory works students master the following functions of CA (Table 9).

Table 9: Functions of CA.

Functions	Sub-functions
User registration	– feeding user registration data into the users’ register; – maintaining the users’ registry and access to the registration data; – backing up and archiving users’ registry; – changing the user registration data in the registry; – deleting the user registration data from the register;

Certification of user's public keys	– reception and registration of user queries on the digital certificate generation; – storage of queries received from users in a database query; – archiving database queries; – formation of user digital certificates; – storing generated digital certificates in the digital certificates registry; – storing digital certificates registry; – backing up digital certificates registry.
User's public key digital certificates distribution	– publication digital certificates registry in public directories (LDAP-directory) and CA information resource (web-page) – providing user access to the digital certificates registry in public directories (LDAP-directory) and information resource CA (web-page) dispatch digital certificates registry to users by electronic mail.
User's public key digital certificates status management and information on the status of digital certificates distribution	– reception and registration of user requests for revocation, blocking or renewal of digital certificates; – storage of queries received from users in a queries database; – archiving queries database; – revocation, blocking or renewal of digital certificates based on requests; – adding information about the current status of the digital certificate in the register of digital certificates; – CRLs creation; – publication of revoked digital certificates lists in public directories (LDAP-directory) and CA information resource (web-page); – providing the user access to the CRLs in public directories (LDAP-directory) and CA information resource (web-page); – providing the user access to information on the digital certificate status using the OCSP protocol; – alerting users about changing status of digital certificates by e-mail.
Time stamping services	– reception and registration users queries of time stamp generation; – timestamps generation; – transfer of generated timestamps to users; – storing of generated timestamps in the database; – archiving timestamps database.

For CA user side students works with the following software (Table 10).

Table 10: Function of software module.

Software module	**Function**
User’s private and public key generation	– user's private and public key generation; – user’s digital certificate request generation and its transfer to the CA; – receipt, validation, storage and use of the generated digital certificate; – blocking, cancellation and renewal requests formation and transmission to CA
User’s data Digital Signature (DS) and encryption	– access and application of the user private key; – interactive validation of certificates status via the OCSP protocol; – search for digital certificates in the CA LDAP-directory; – obtaining time stamps from the CA; – digital signature generation and verification, e-mail encryption, electronic documents workflow, etc.

After successful completion of the laboratory work series students have enough skills to work as service personnel in the Ukrainian certification authorities.

The second example is Laboratory work on packet filtering for providing the basic network security level. This work is intended for students training on practical network packet filtering with the Linux iptables firewall. Each student is equipped by two computers. One of them (client) is running windows and the basic network utilities such as web-browser, telnet, e-mail agent, etc. Another one is a Linux server running network daemons for *e-mail*, *http*, *dns*, *ftp*, *telnet* services. As a variant, it is possible to use a single PC with virtual machine (VM) running another OS with corresponding software.

On theoretical part students learn the basic filtering chains in the ip tables (Figure 2).

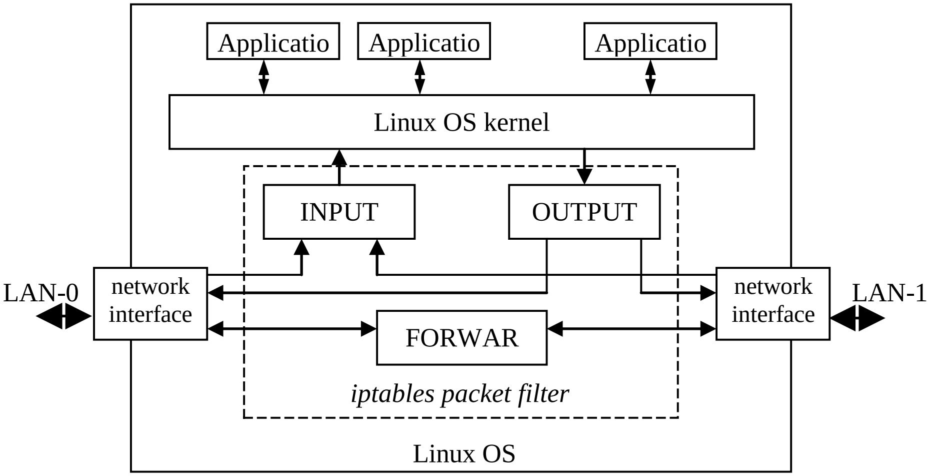

Figure 2: iptables filtering chains in Linux.

The task for laboratory work is to create rules for iptables chains for allowing traffic for accessing e-mail, *http*, *dns*, *ftp*, *telnet* services implementing prohibiting policy (disabling all network traffic and adding separate rules for allowing necessary services). Each firewall rule should be tested, as well as access to specified network services.

After successful completion of the laboratory work series students are able to use the basic network utilities for controlling and filtering network traffic.

Conclusion

Today the priority task is to organize the process of national information security system and cybersecurity system highly skilled experts, subject to certain features of this field, namely:

- information security and cybersecurity – a specific subject area that requires an integrated approach to the training, i.e. teaching different sections of basic and applied knowledge as engineering and humanities;
- the education system in the field of information security should ensure the compliance level of training pace of scientific and technological progress and national legislation in the sphere of information relations;
- general training on information security should have all the subjects of information activity, especially management staff of enterprises, institutions and organizations;

- the training of all categories of information security should be based on a single methodological and legal basis;
- system of training IT professionals require of mandatory monitoring by the state.

To point out the problems in cyber security education in Ukraine:

- insufficient training and timely training of teaching staff, providing educational process;
- insufficient level of modernization of teaching and laboratory facilities Universities;
- insufficient involvement in the course of training (re-training) on information security for civil servants;
- insufficient level of cooperation between ministries and agencies for training specialists in information security;
- excessive commercialization courses in information security. A large part of the commercial segment of the training is actually representative offices of foreign companies. This increases the dependence of Ukraine and reduces the degree of foreign control of information technologies, which are implemented in the public and commercial sector.

Several positive aspects of Ukrainian market of training in the field of information security can be identified, including:

- a rather “powerful” centres for IT professionals in the leading government technical schools recognized today not only in Ukraine but also abroad;
- use in educational process of advanced credit-modular technology of the educational process;
- use in educational process industrial design information security and software systems;
- expansion of international relations with foreign training centres.

Ukraine completed a certain stage of the creation of a system of training of specialists in information security. But in the context of international experience, current and future threats in the sphere of information and cyberspace, this system requires further development.

Bibliography

1. Law of Ukraine “On the basic principles to ensure cyber security of Ukraine,” Draft. Accessed September 17, 2014. http://www.dstszi.gov.ua/dstszi/control/uk/publish/article.

[2.] Y. Grycuk and V. Girman. *Training of Information Security in Educational Institutions of Ukraine*. Accessed October 15, 2015. http://ubgd.lviv.ua/moodle/pluginfile.php/14209/mod_folder/content/0/КафедраУІБ/ГрицюкЮ.I/2012/5.pdf.

[3.] The list of specialties in higher educational institutions of Ukraine on the educational and skill levels of specialist and master levels, www.abiturient.in.ua/ua/napriamki_magistr_1_ua.

[4.] Standards of Higher Education 1701 “Information Security.” Accessed November 10, 2014. http://iszzi.kpi.ua/index.php/ua/biblioteka/normativno-pravova-baza/nmk-informatsijna-bezpeka.html.

[5.] List of Public Higher Education Institutions Licensed in the Areas of 1601, 1701 in the Field of Knowledge “Information Security.” Accessed November 15, 2014. http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article.

[6.] Passport of Specialty 05.13.21 “System of Information Security.” Accessed November 15, 2014. http://search.ligazakon.ua/l_doc2.nsf/link1/MUS969.html.

[7.] Passport of Specialty 21.05 “Information Security of the State.” Accessed November 15, 2014. http://search.ligazakon.ua/l_doc2.nsf/link1/MUS969.html.

About the Authors

Oleksandr V. POTII is colonel, Doctor of Technical Science, Professor of Department of information systems and technologies security of V. N. Karazin Kharkiv National University. He graduated from the Kharkov Higher Military School of Rocket Forces as an Engineer in Radioelectronics in 1993. In 1996, he received a PhD degree in Automatic Control Systems for Armed Forces. In 2008, he was awarded a doctoral degree in Information Security Systems. He has published more than 90 articles dealing with issues of information security, cryptography, PKI and e-services. He took part in the development of national standards and legal documents related to information security. He is a guest lecturer at the Kharkiv National Aerospace University and Kharkiv National University of Radioelectronics.

Roman V. OLIYNYKOV is Professor at Information Systems and Technologies Security Department, V.N.Karazin Kharkiv National University.