The syllabus of the discipline

Security of transactions in open systems

V.A. Zolotarev,
Associate Professor of INE, Ph.D., Associate Professor
E-mail: vadym.zolotarov@nure.ua

Field name	**Detailed content, comments**
Name of the faculty	Faculty of Infocommunications
Level of higher education	Second (master's)
Code and name of the specialty	172 Telecommunications and radio engineering
Type and name of educational program	EPP "Information and Network Engineering"
Name of the discipline	Security of transactions in open systems
Number of ECTS credits	4
Discipline structure (distribution by types and hours of study)	24 hours - 12 lectures, 16 hours - 4 laboratory classes, 8 hours - 4 consultations, 72 hours - homework, type of control: credit
Schedule (terms) of studying the discipline	1-st year, I semester
Prerequisites for studying the discipline	Previously, the disciplines for the first (bachelor's) level of education in the specialty 172 Telecommunications and Radio Engineering should be studied.
Competences, knowledge, skills, understanding, which is acquired by the applicant in higher education in the learning process	The discipline is used to form the following competencies: in the process of practical activities in the field of infocommunications skills to ensure information security of the network; choice of hardware, cryptographic and software for a specific network; be able to detect and block technical channels of information leakage
The quality of the educational process	Educational-methodical and material-technical resource provision of the educational program, within the framework of which the discipline is studied, meets the licensing requirements and accreditation conditions of the educational activity of the university. Annual monitoring and revision of the curriculum of the discipline in accordance with the requirements and recommendations of the Ministry of Education and Science, state certification of acquired competencies of graduates, standards of cooperation with employers to ensure a competitive level of training. Adherence to the principles of academic integrity (https://lib.nure.ua/plagiat). Contains public information on the requirements, competencies, level of education within the current educational program.

Description and content of the discipline

The purpose of the discipline is to acquire knowledge, skills and techniques of working with software and hardware means of information protection, such as cryptographic packages, software and hardware systems of network protection, antivirus software, etc.; acquisition of special knowledge and practical skills in the use of modern information technologies in professional activities.

Content

Content module 1. Paradigm of information security of open systems

Topic 1. International criteria for assessing the information security of open systems

Topic 2. Potential attackers on open systems, hacking, forensic science

Topic 3. Remote attacks on open systems

Topic 4. Classification and characterization of methods and means of obtaining information from open systems

Content module 2. Protection against remote attacks on open networks

Topic 1. Protection against remote attacks aimed at intercepting user data and detecting open network data

Topic 2. Protection against remote attacks aimed at detecting data on an open system

Topic 3. Protection against remote attacks aimed at denial of service

Topic 4. Protection against remote attacks "Spoofing"

Topic 5. Protection against remote attacks aimed at gaining access to the operating environment

Topic 6. Protection against remote attacks such as injections

Content module 3. Hardware and software means of information protection in open systems

Topic 1. Firewalls and VPNs

Topic 2. Network protocols for data protection

Topic 3. Data backup strategies

Topic 4. Computer viruses and MALWARE, antivirus programs, passwords

Learning outcomes of higher education

As a result of studying the discipline, students must:

know: the main trends in the development of open information systems, cyber threats to information; application of technologies to protect information in infocommunications from remote attacks; regulatory framework for the use of technical and software means of information protection in open information systems; types of security software and their purpose; cryptographic means of information protection; the possibility of using

software to restrict access to electronic documents both on the local PC and through the information and communication network, using standard means of encrypting information;

be able to: ensure the confidentiality of personal and official information by obtaining theoretical knowledge and practical skills; use the regulatory framework in the field of information security; determine the information to be protected; implement and use selected information security measures; use their theoretical knowledge and practical skills to identify information threats; analyze information risks; to choose the means of protection.

have: in the process of practical activities in the field of infocommunications skills to ensure information security of the network; choice of hardware, cryptographic and software for a specific network; be able to detect and block technical channels of information leakage.

Assessment system according to each task for passing the test / exam.

To evaluate the student's work during the semester, the final $O_{сем}$ is calculated as the sum of grades for different types of classes and control activities.

Types of classes / control event	Rating
Laboratory works № 1, 2	(6…10) x 2 = 12….20
Test work №1	(6…10) = 6…10
Test work №2	(6…10) = 6…10
Checkpoint № 1	**24…40**
Laboratory works № 3, 4	(6….10)x2 = 12….20
Test work № 3	(6…10) = 6…10
Test work № 4	(6…10) = 6…10
Checkpoint № 2	**24…40**
Individual homework	12…20
Total result	**60…100**

As a form of final control for the discipline used offset, during which the defense of individual homework.

Qualitative evaluation criteria in the national scale and ECTS

Satisfactory, D, E (60-74). Show the required minimum of theoretical knowledge. Know the ways and methods of solving practical problems and be able to use them in practice.

Good, C (75-89). Firmly know a minimum of theoretical knowledge. Demonstrate the ability to solve a practical problem and justify all stages of the proposed solution.

Excellent, A, B (90-100). Show complete knowledge of basic and additional theoretical material. Unmistakably solve a practical problem, explain and justify the chosen method of solution.

Assessment scale: national and ECTS

The sum of points for all types of educational activities	ECTS assessment	Score on a national scale	
		for exam, course project (work), practice	for offset
90 – 100	**A**	perfectly	credited
82-89	**B**	fine	
74-81	**C**		
64-73	**D**	satisfactorily	
60-63	**E**		
35-59	**FX**	unsatisfactory with the possibility of reassembly	not credited with the possibility of re-assembly
0-34	**F**	unsatisfactory with mandatory re-examination	not credited with compulsory re-study of the discipline

Methodical support

Basic literature

1. Zolotarov V. Zakhyst informatsii v telekomunikatsiinykh systemakh // Informatsiini merezhi zviazku. Ch.4 Tekhnolohii nadannia informatsiinykh posluh: navch. Posibnyk / Bezruk V.M., Korolov V.M., Zolotarov V.A., Botsman P.D., Kostromytskyi A.I., Astrakhantsev A.A., Kapusta S.O. . – Kharkiv:KhNURE,2011. – s.324-391.
2. Klymash M.M., Luntovskyi A.O. Informatsiina bezpeka rozpodilenykh system. Monohrafiia.- Lviv: Natsionalnyi universytet «Lvivska politekhnika», 2014. – 480 s.

Supporting literature

1. CUA-14-01A Rekomendatsii CERT-UA dlia usunennia vrazlyvostei, poviazanykh z nekorektnym nalashtuvanniam DNS- serveriv. – K., DSTZI, 2014. – 12 s.
2. CUA-14-02A Rekomendatsii CERT-UA dlia usunennia vrazlyvostei, poviazanykh z vykorystanniam protokolu SNMP. - K., DSTZI, 2014. – 10 s.
3. CUA-14-03A Rekomendatsii CERT-UA dlia usunennia vrazlyvostei, poviazanykh z vykorystanniam protokolu SSDP. - K., DSTZI, 2014. – 10 s.
4. CUA-14-04A Rekomendatsii CERT-UA dlia usunennia vrazlyvostei, poviazanykh z vykorystanniam protokolu NetBIOS - K., DSTZI, 2014. – 10 s.
5. CUA-14-05A Rekomendatsii CERT-UA dlia usunennia vrazlyvostei, poviazanykh z nekorektnym nalashtuvanniam NTP- serveriv/ - K., DSTZI, 2014. – 8 s.
6. CUA-15-01M Opys shkidlyvoho prohramnoho zabezpechennia Regin. - K., DSTZI, 2015. – 13 s.
7. CUA-15-04R Rekomendatsii CERT-UA z protydii zahrozi insaidera. - K., DSTZI, 2015. – 13 s.
8. CUA-15-05R BEZPEKA POShTOVOHO SERVISU. - K., DSTZI, 2015. – 9 s.

Methodical instructions and literature for different types of classes

1. Metodychni vkazivky do laboratornykh robit z dystsypliny «Zakhyst informatsii v telekomunikatsiinykh systemakh» dlia studentiv napriamu «Telekomunikatsii» spetsialnosti 8.092402 – Informatsiini merezhi zviazku. Uporiad.: V.A.Zolotarov, A.A.Astrakhantsev, O.V.Fedorov,. – Kharkiv, KhNURE, 2008. – 108 s.
2. Kryptolohiia u prykladakh, testakh i zadachakh: navch. posibnyk / T.V. Babenko, H.M. Hulak, S.O. Sushko, L.Ia. Fomychova. -Dnipropetrovsk.: Natsionalnyi hirnychyi universytet, 2013. - 318 c.
3. Poliakov N.L., Tyshchenko A.V. Matematycheskye osnovы kryptohrafyy. Zadachy y reshenyia. – M.: Fynansovыi unyversytet, 2015. – 25 s.
4. Pravovyi zakhyst informatsii. Navchalnyi posibnyk. / N.I.Lohinova, R.R.Dorozhbur – Odesa, Feniks, 2015 – 264 s.

Information support

1. Original software