The syllabus of the discipline

Security of infocommunication networks

V.A. Zolotaryov,
Associate Professor of INE dept, 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	First (bachelor'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 infocommunication networks
Number of ECTS credits	5
Discipline structure (distribution by types andhours of study)	28 hours - 18 lectures, 8 hours - 3 practical classes, 20 hours - 5 laboratory classes, 8 hours - 7 consultations, 71 hours - homework, **type of control**: credit
Schedule (terms) of studying the discipline	4th year, VII semester
Prerequisites for studyingthe discipline	Previously, the disciplines "Fundamentals of information communication technologies"; «Fundamentals of circuitry»; «Higher mathematics» (special sections); «Guiding systems for electrical and optical communication»; «Data processing technologies in IR»; «Local area networks»; «Mobile communication systems»
Competences, knowledge, skills, understanding, whichis acquired by the applicantin higher education in the learning process	be able to ensure the confidentiality of personal and professional information through 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. To 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.
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 universityAnnual 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, anti-virus software, etc.; acquisition of special knowledge and practical skills in the use of modern information technologies in professional activities.

Content

Content module 1. Theoretical foundations of information security of telecommunication systems

Topic 1. Information security of telecommunication systems: essence, factors, criteria

Topic 2. Methods of information protection in telecommunication systems

Topic 3. Regulatory framework for information protection in telecommunications systems.

Content module 2. Cryptographic protection of information

Topic 1. Cryptography: basic concepts and definitions

Topic 2. Classical cryptography: substitution codes, simple and complex replacement codes

Topic 3. Block symmetric encryption methods

Topic 4. Asymmetric encryption methods

Topic 5. Methods of information authentication in telecommunication systems

Topic 6. Electronic digital signature

Content module 3. Information protection systems in telecommunication systems

Topic1. Protection of information from leakage through technical channels in telecommunications systems

Topic 2. Protection of information in fixed telephone lines

Topic 3. Methods and means of information protection in mobile communication systems

Topic 4. Hardware and technical means of protection of telecommunication systems

Topic 5. Software methods of information protection in telecommunication systems

Topic 6. Steganography

Learning outcomes of higher education

As a result of studying the discipline, students must:

KNOW: the main trends in the development of information and telecommunications, threats to information; opportunities for information leakage in communication channels; application of information protection technologies in telecommunications; regulatory framework for the use of technical and software means

of information protection in telecommunications, fixed and mobile communications; 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.

To have in the process of practical activities in the field of infocommunications skills to ensure information security of the network; selection 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 assess the work of a student during the semester, the final rating score Q_{sem} is calculated as the sum of marks for different types of classes and control activities

Type of lesson / control measure	Rating
Lb № 1, 2	(6…10) x 2 = 12….20
Pr № 1, 2,3	(3…5) x 3 = 9….15
Control testing 1	(3…5) = 3…5
Checkpoint 1	**24…40**
Lb № 3, 4, 5	(6….10)x3 = 18….30
Pr № 1, 2,3	(3…5) x 2 = 6….10
Control testing 2	(3…5) = 3…5
Practice Control testing 1№ 1, 2, 3	(3…5) x 3 = 9...15
Checkpoint 2	**36…60**
Total for the semester	**60…100**

A written (combined) exam is used as a form of final control for the discipline ZITKS. With this type of control, the final score Q is calculated by the formula:

$$Q = 0{,}6\ Q_{sem} + 0{,}4\ Q_{ex},$$

where

Q_{sem} - semester score in a 100-point system,

Q_{ex} - score for the exam in a 100-point system.

The ticket for the exam consists of 2 theoretical questions and one task. The theoretical question is evaluated in 30 points, and the task - in 30 points (in total - 100 points).

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.

Well, 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.
3. Horbenko I.D. Zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh: Navch. posib. dlia stud. Ch. 1. Kryptohrafichnyi zakhyst informatsii . – Kharkiv, KhNURE, 2004.
4. Maksymenko V.N., Afanasev V.V.,Volkov N.V. Zashchyta ynformatsyy v setiakh sotovoi podvyzhnoi sviazy. – M.: Horiachaia lynyia – Telekom, 2007. 5. Yemets V., Melnyk A., Popovych R. Suchasna kryptohrafiia. Osnovni poniattia. – Lviv: BaK, 2003.
6. Romanets Yu.V., Tymofeev P.A., Shanhyn V.F. Zashchyta ynformatsyy v komputernykh systemakh y setiakh. – M:Radyo y sviaz, 1999. – 328 s.

Supporting literature

1. Buzov H.A., Kalynyn S.V., Kondratev A.V. Zashchyta ot utechky ynformatsyy po tekhnycheskym kanalam: Uchebnoe posobye. – M.: Horiachaia lynyia-Telekom, 2005.
2. Fylyn S.A. Ynformatsyonnaia bezopasnost. Uchebnoe posobye.–M., Alfa-Pres, 2006.
3. Tarasiuk M.V. Zashchyshchennыe ynformatsyonnыe tekhnolohyy. Proektyrovanye y prymenenye. – M.: Solon-Press, 2004.
4. Kuznetsov O. O. , Yevseiev S.P., Korol O.H. Zakhyst informatsii v informatsiinykh systemakh – Kharkiv: Vyd. KhNEU, 2010.

Methodical instructions 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

Original software