The syllabus of the discipline

Information security of innovation

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	Information security of innovation
Number of ECTS credits	3
Discipline structure (distribution by types and hours of study)	14 hours - 7 lectures, 16 hours - 4 laboratory classes, 4 hours - 2 practical classes, 6 hours - 3 consultations, 48 hours - homework, type of control: credit
Schedule (terms) of studying the discipline	1-st year, II 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: 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; carry out organizational and administrative measures to protect trade secrets.
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 studying the discipline is to acquire knowledge, skills and techniques of working with information that is a trade secret in an innovative enterprise.

Content

Content module 1. Information risks of innovation

Topic 1. Information security of innovation: the essence and main factors

Topic 2. Methods and means of unauthorized obtaining information about the innovative activities of the enterprise

Topic 3. Information risks of innovative activity of the enterprise

Content module 2. Information protection at an innovative enterprise

Topic 1. Secret information about the innovative activity of the enterprise

Topic 2. Information protection system at the innovative enterprise

Topic 3. Organizational and administrative protection of information in an innovative enterprise

Topic 4. Information protection in the infocommunication network of innovative enterprises

Learning outcomes of higher education

As a result of studying the discipline, students must:

know: basic organizational and administrative methods of protecting trade secrets; application of technologies for protection of confidential information in telecommunications; the possibility of using software to restrict access to electronic documents both on the local PC and through the information and communication network.

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.

list of competencies: 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; carry out organizational and administrative measures to protect trade secrets.

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	(12…20) = 12…20
Checkpoint № 1	**24…40**
Laboratory works № 3, 4,	(6….10) x 2 = 12….20
Test work №1	(12…20) = 12…20
Control task	(12…20) = 12...20
Checkpoint № 2	**36…60**
Total result	**60…100**

As a form of final control for the discipline is used credit.

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. Fylyn S.A. Ynformatsyonnaia bezopasnost. Uchebnoe posobye. – M., Alfa-Pres, 2006.
3. Klymash M.M., Luntovskyi A.O. Informatsiina bezpeka rozpodilenykh system. Monohrafiia.- Lviv: Natsionalnyi universytet «Lvivska politekhnika», 2014.

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. Tarasiuk M.V. Zashchyshchennые ynformatsyonnые tekhnolohyy. Proektyrovanye y prymenenye. – M.: Solon-Press, 2004.
3. Kuznetsov O. O. , Yevseiev S.P., Korol O.H. Zakhyst informatsii v informatsiinykh systemakh – Kharkiv: Vyd. KhNEU, 2010.

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. Pravovyi zakhyst informatsii. Navchalnyi posibnyk. / N.I.Lohinova, R.R.Dorozhbur – Odesa, Feniks, 2015 – 264 s.

Information support

1. Original software