The syllabus of the discipline

Information security of e-business

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	Information security of e-business
Number of ECTS credits	3
Discipline structure (distribution by types andhours of study)	22 hours - 11 lectures, 20 hours - 5 laboratory classes, 6 hours - 3 consultations, 57 hours - homework, **type of control**: credit
Schedule (terms) of studying the discipline	3rd year, V semester
Prerequisites for studyingthe discipline	Basic knowledge of disciplines: e-commerce information systems, information security in TCS, Electronic payment systems
Competences, knowledge, skills, understanding, whichis acquired by the applicantin higher education in the learning process	The discipline is used to form the following competencies: skills to ensure information security of e-business.
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 for working with software and hardware information security in e-business, such as cryptographic packages, software and hardware network protection, anti-virus software, etc.; acquisition of special knowledge and practical skills in the use of modern infocommunication systems of electronic business technologies in professional activities.

Content

Content module 1 E-business information security paradigm

Topic 1. Regulatory framework for information security in e-business

Topic 2. Authentication protocols

Topic 3. Problems of ensuring the confidentiality and authenticity of information in e-business

Topic 4. Special digital signature schemes

Content module 2. Information protection in electronic payment systems

Topic 1. Non-anonymous real-time EPS

Topic 2. Non-anonymous autonomous EPS

Topic 3. Anonymous EPS working in real time

Topic 4. Anonymous standalone EPS

Content module 3 Cryptographic protocols in e-commerce

Topic 1. The main tasks of information security in e-commerce.

Topic 2. Secure channels for information transmission in the EC

Topic 3. Fair exchange of digital signatures and its applications

Topic 4. Multilateral transactions, commercial agreements, legal relations

Learning outcomes of higher education

As a result of studying the discipline, students must:

know: components of cryptographic electronic payment systems, cryptographic protocols used in the field of e-commerce and business; general requirements for the organization of secure payment systems; cryptographic protocols for the distribution of cryptographic keys used in e-business.

be able to: investigate the infrastructure of cryptosystems, including cryptographic key management procedures; use regulatory framework in the field of information security of e-business; implement and use selected information security measures; use their theoretical knowledge and practical skills to identify information threats in e-business; analyze information risks of e-business; to choose the means of protection.

to possess (list of competencies) in the process of practical activities in the field of infocommunications skills to ensure information security of e-business.

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
Control testing №1	(6…10) = 6…10
Control testing №2	(6…10) = 6…10
Checkpoint 1	**24…40**
Lb № 3, 4,5	(6….10)x3 = 18….30
Control testing № 3	(6…10) = 6…10
Control testing №4	(6…10) = 6…10
Checkpoint 2	**30…50**
Practice Control testing	6…10
Total for the semester	**60…100**

As a form of final control for the discipline, a test is used, during which the individual homework is defended.

Qualitative evaluation criteria in the national scale and ECTS

Satisfactory, D, E (60-74). Have a minimum of knowledge and skills. Work out and defend all laboratory work and IDPs.

Well, C (75-89). Know the main topics of the discipline. Work out and defend all laboratory work and ID.

Excellent, A, B (90-100). Know all the topics of the discipline. Work out and defend all laboratory work and IDPs. Prepare essays on each of the content modules.

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. Zapechkyn S.V. Kryptohrafycheskye protokoly y ykh prymenenye v fynansovoi y kommercheskoi deiatelnosty. – M., Horiachaia lynyiaTelekom, 2007.- 320 s.
2. 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.
3. Klymash M.M., Luntovskyi A.O. Informatsiina bezpeka rozpodilenykh system. Monohrafiia.- Lviv: Natsionalnyi universytet «Lvivska politekhnika», 2014. – 480 s.
4. Horbenko I.D. Zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh: Navch. posib. dlia stud. Ch. 1. Kryptohrafichnyi zakhyst informatsii . – Kharkiv, KhNURE,2004.

Support literature

1. CUA-14-01ARekomendatsii CERT-UA dlia usunennia vrazlyvostei, poviazanykh z nekorektnym nalashtuvanniam DNSserveriv. – 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-14-03ARekomendatsii 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 NTPserveriv/ - K., DSTZI, 2014. – 8 s.
6. CUA-15-01MOpys 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 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 с. 3. Poliakov N.L., Tyshchenko A.V. Matematycheskye osnovy kryptohrafyy. Zadachy y reshenyia. – M.: Fynansoвыi unyversytet, 2015. – 25 s.
3. Pravovyi zakhyst informatsii. Navchalnyi posibnyk. / N.I.Lohinova, R.R.Dorozhbur – Odesa, Feniks, 2015 – 264 s.

Information support

Original software