FUNDAMENTALS OF CYBERSECURITY

COURSE SYLLABUS

Code and name of specialty	122 Computer Science	**Institute / faculty**	Faculty of Computer Science and Software Engineering
Program name	"Computer Science and Intelligent Systems"	**Department**	Software Engineering and Management Information Technologies
Type of program	Educational and Professional	**Language of instruction**	Ukrainian

LECTURER

Serhii Yevseiev — ***Serhii.Yevseiev@hneu.net***

Doctor of Technical Sciences, Professor, Professor of the Department of Software Engineering and Information Technologies of NTU "KhPI". Prepared and published more than 295 scientific and educational works (Google Scholar: (Google Scholar: https://scholar.google.com/citations?hl=ru&user=Y4kNr38AAAAJ&view_op=list_works&sortby=pubdate; ORCID https://orcid.org/0000-0003-1647-644; Scopus: https://www.scopus.com/authid/detail.uri?authorId=57190440690; Publons: https://publons.com/researcher/1527869/serhii-yevseiev/).
Leading lecturer of the courses: *Fundamentals of Cybersecurity (in Ukrainian)*

GENERAL DESCRIPTION OF THE COURSE

Summary	The course "Fundamentals of Cybersecurity" is a discipline in the cycle of special compulsory training in the specialty 126 "Information Systems and Technologies". It is taught in the sixth semester in the amount of 90 hours (3 ECTS credits), in particular: lectures - 16 hours, laboratory classes - 32 hours, independent work - 42 hours. There are no individual tasks. The study of the discipline ends with an exam
Course objectives	Teaching students the principles of building information security systems, research and use of modern procedures for providing basic information security services in cyberspace, auditing the current state of information security.
Types of classes and control	Lectures, laboratory classes. Current control - laboratory work, intermediate modular control. Final control - exam.
Term	6

Student workload (credits) / Type of course	3 / Mandatory (elective)	**Lectures (hours)**	16	**Laboratory classes (hours)**	32	**Self-study (hours)**	42

Program competences	GK1. Ability to abstract thinking, analysis and synthesis. GK2. Ability to apply knowledge in practical situations. GK3. Knowledge and understanding of the subject area and understanding of professional activity. GK6. Ability to learn and master modern knowledge. SK14. Ability to apply methods and means of information security, to develop and operate special software for protection of information resources of critical information infrastructure

Learning outcomes	**Teaching and learning methods**	**Forms of assessment (continuous assessment CAS, final assessment FAS)**

PR15. Understand the concept of information security, the principles of secure software design, ensure the security of computer networks in conditions of incomplete and uncertain source data	Interactive lectures with presentations, discussions, laboratory classes, teamwork, case method, method of feedback from students, problem-based learning	Written individual assignments for laboratory work (CAS), assessment of knowledge in laboratory classes (CAS), final / semester control in the form of a semester exam, according to the schedule of the educational process (FAS)

ASSESSMENT AND GRADING

Ranges of points corresponding to grades	core (points) for all types of learning activities	ECTS grading scale	The national grading scale
	90-100	A	excellent
	82-89	B	good
	74-81	C	
	64-73	D	satisfactory
	60-63	E	
	35-59	FX	Unsatisfactory (with the exam retake option)
	0-34	F	Unsatisfactory (with mandatory repetition of the course)

Allocation of grade points	
	100% final assessment in the form of exam (36%) and current assessment (64%). **36% exam** **64% current rating:** Module №1 (12%) Module №2 (12%) Laboratory work (40%) Laboratory work № 1 (5%) Laboratory work № 2 (5%) Laboratory work № 3 (5%) Laboratory work № 4 (5%) Laboratory work № 5 (5%) Laboratory work № 6 (5%) Laboratory work № 7 (5%) Laboratory work № 8 (5%)

Course policy	Students must attend all classes according to the study schedule and adhere to the norms of academic ethics. To study the course, students need to have their personal computer and (or) use computers of the computer center at the department. Students must work with compulsory and recommended reading, including Internet resources. Students must complete and submit all laboratory works during the semester in which the course is taught, before the examination session. The final assessment is not carried out without the personal presence of students.

COURSE STRUCTURE AND CONTENT

Topic 1	The concept of cybersecurity of the state and components of national interests of Ukraine in cybersecurity	**Laboratory work 1**	Deploy an operating system to audit the information security of computer networks and information systems	**Self-study**	The main stages of internal audit on information security
Topic 2	Cybersecurity risk analysis. Classification of cyber threats. Practical models of delimitation of access rights	**Laboratory work 2**	Tools for covertly collecting technical information from an information system or computer network		Acquaintance with the main channels of information leakage. Basic principles of forming classifiers of computer incidents, cyber threats
Topic 3	Mechanisms for ensuring the confidentiality and integrity of data	**Laboratory work 3**	Research of modern block symmetric ciphers and encryption modes.		Basic mechanisms for ensuring integrity in information systems

Topic 4	Authentication mechanisms	**Laboratory work 4**	Research of electronic digital signature. El Gamal CPU, DSTU 4145, ECDSA. Investigation of system or network vulnerabilities using a specialized vulnerability scanner - Nessus		Basic special hash functions. Digital signature standards, their classification
Topic 5	The main directions of development of modern cryptography	**Laboratory work 5**	Steganography methods of information protection		Methods of steganography in the spatial and frequency domain
Topic 6	Mechanisms and protocols of key management in PKI	**Laboratory work 6**	Statistical studies of random and pseudorandom sequence generators according to the NIST method		Basic PKI protocols based on symmetric and asymmetric cryptography
Topic 7	Risk analysis technologies	**Laboratory work 7**	Identify vulnerabilities in web resources and web applications. Vulnerability scanner - Vega		Methods of risk analysis
Topic 8	Risk analysis in non-information security management	**Laboratory work 8**	Collection of technical and sensory information with the help of class software - sniffers. A tool to study the vulnerabilities of wireless Wi-Fi networks - Aircrack-ng		Methods of risk analysis

RECOMMENDED READING

1. Єvseєv S.P, Ostapov S.E., Korol' O.G. (2019) Kiberbezpeka: suchasni tehnologiï zahistu. Navchal'nij posibnik dlja studentiv vishhih navchal'nih zakladiv. L'viv: “Novij Svit- 2000”
2. R. V. Grishhuk, ta Ju. G. Danik. (2016) Osnovi kibernetichnoï bezpeki: Monografija Zhitomir: ZhNAEU,.
3. Lenkov S.V., Peregudov, D. A., Horoshko. V. A. (2008) Metody i sredstva zashhity informacii. V 2-h tomah Kiev: Arij, T.II. Informacionnaja bezopasnost'.

Recommended

4. Baranov A.A., Internet rechej: teoretiko-metodologichni osnovi pravovogo reguljuvannja. Tom I. Sferi zastosuvannja, riziki i bar'єri, problemi pravovogo reguljuvannja.
5. ISO/IEC 27001:2013. Information technology – Security techniques Information security management systems Requirements. [Online]. Available: Retrieved from: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534.
6. Gorbenko I. D., Gorbenko Ju. I. (2012) Prikladna kriptologija. Kharkov, Vidavnictvo: Fort
7. Popovskij V.V., Persikov. A. V. (2006) Zashhita informacii v telekommunikacionnyh sistemah: Uchebnik: V 2 t. Khar'kov: OOO “Kompanija SMIT”
8. Popovskij V.V., Persikov. A. V. (2006) Zashhita informacii v telekommunikacionnyh sistemah: Uchebnik: V 2 t. Khar'kov: OOO “Kompanija SMIT”,
9. Strategija kiberbezpeki Ukraïni” (Vvedeno v diju Ukazom Prezidenta Ukraïni vid 15 bereznja 2016 roku №96/2016).
Єvseєv S.P. Laboratornij praktikum z disciplini “Tehnologiï zahistu informaciï”

INTERNET RESOURCES

10. DSTU ISO/IEC TR 13335-1:2003 Informacijni tehnologiï. Nastanovi z keruvannja bezpekoju informacijnih tehnologij. Chastina 1. Koncepciï ta modeli bezpeki informacijnih tehnologij. [Jelektronnyj resurs]. Dostupno: http://lindex.net.ua/ua/shop/bibl/500/doc/11423.
11. DSTU ISO/IEC TR 13335-2:2003 Informacijni tehnologiï. Chastina 2. Nastanovi z keruvannja bezpekoju informacijnih tehnologij. [Elektronnij resurs]. Dostupno: http://www.premier-hs.com.ua/ru/content/dstu-isoiec-tr-13335-22003-nastanovi-z-kieruvannia-biezpiekoiu-informatsiinikh-tiekhnologhii.
12. DSTU ISO/IEC TR 13335-3:2003 Informacijni tehnologiï. Nastanovi z keruvannja bezpekoju informacijnih tehnologij. Chastina 3. Metodi keruvannja zahistom informacijnih tehnologij. [Elektronnij resurs]. Dostupno: http://lindex.net.ua/ua/shop/bibl/500/doc/11425
13. DSTU ISO/IEC TR 13335-4:2005 Informacijni tehnologiï. Nastanovi z upravlinnja bezpekoju informacijnih tehnologij. Chastina 4. Vibirannja zasobiv zahistu. [Elektronnij resurs]. Dostupno: http://metrology.com.ua/download/iso-iec-ohsas-i-dr/61-iso/290-dstu-iso-iec-tr-13335-4-2005
14. DSTU ISO/IEC TR 13335-5:2005 Informacijni tehnologiï. Nastanovi z upravlinnja bezpekoju informacijnih tehnologij. Chastina 5. Nastanova z upravlinnja merezhnoju bezpekoju. [Elektronnij resurs]. dostupno: http://lindex.net.ua/ua/shop/bibl/500/doc/11427
15. http://dstszi.gov.ua.

Academic integrity

Graduate students are expected to adhere to the Code of Ethics of Academic Relations and Integrity” of NTU “KhPI”.

The content of this syllabus is consistent with the course program.