Syllabus
Course Program

Security in social networks

Specialty
125 – Cybersecurity and information protection

Institute
Educational and Scientific Institute of Computer Science and Information Technology

Educational program
Cybersecurity

Department
Cybersecurity (328)

Level of education
Bachelor's level

Course type
Profile training, Selective

Semester
8

Language of instruction
English

Lecturers and course developers

Serhii YEVSEIEV

serhii.yevseiev@khpi.edu.ua
Doctor of technical sciences, professor, head of the cyber security department of National Technical University "Kharkiv Polytechnic Institute".

The number of scientific publications: more than 350, including 42 utility model patents, 17 monographs, of which 9 are collective monographs, 31 textbooks, 4 of which bear the seal of the Ministry of Education and Science of Ukraine, 163 articles in foreign publications and specialized publications of Ukraine, with 61 of them are in the Scopus scientometric database. Leading lecturer in the disciplines: "Information security management", "Introduction to networks", "Security of banking systems", "Hybrid warfare and national security", "Audit and monitoring of corporate networks", "Blockchain: basics and application examples", "Fundamentals of smart contracts", "Basics of cyber security" for undergraduate and graduate students, Section "Methods and technologies of information security monitoring and auditing", "Methods of building post-quantum cryptosystems", "Latest technologies for ensuring cyber security based on blockchain technology" for postgraduate students.

More about the lecturer on the department's website

Olha KOROL

olha.korol@khpi.edu.ua
Candidate of technical sciences, associate professor, associate professor of the department of cyber security of National Technical University "Kharkiv Polytechnic Institute".

The number of scientific publications: more than 150, of which 14 are textbooks, 48 articles in foreign publications and specialized publications of Ukraine, 8 patents for a useful model, 9 in the Scopus scientometric database. Leading lecturer in the disciplines: "Information security management",

"State national security", "State information security", "Comprehensive training "Security of web applications"" for undergraduate and graduate students.

More about the lecturer on the department's website

Natalya VOROPAY

voropay.n@gmail.com
Candidate of Technical Sciences, associate professor of the cyber security department of National Technical University "Kharkiv Polytechnic Institute".

The author of more than 30 scientific and educational works. Leading lecturer in the disciplines: "Programming technologies Part 1", "Decentralized systems", "Protection of critical infrastructure objects", "Antivirus protection of information", "Blockchain and smart technologies" in electronic document circulation".
More about the lecturer on the department's website

General information

Summary

The academic discipline "Security in social networks" is an optional academic discipline. The study of this discipline gives the student the opportunity to: become familiar with the legal aspects of ensuring information and cyber security at the state and international level; familiarize yourself with the principles of building social networks, data exchange protocols in cyberspace; familiarize yourself with modern software (software and hardware) applications for ensuring the security of personal data; learn to navigate modern threats, their orientation; learn to analyze the risks of using confidential information in social networks, distinguish fake information in the media space; learn to navigate services and security mechanisms; acquire practical skills in ensuring the security of personal personal data in the conditions of modern threats.

Course objectives and goals

Learning the principles of ensuring the security of personal data (confidential information) in social networks, using the mechanisms of security services in the conditions of modern threats.

Format of classes

Lectures, laboratory classes, consultations, self-study. Final control - exam.

Competencies

GC-2. Knowledge and understanding of the domain and understanding of the profession.
GC-5. Ability to search, process and analyze information.
PC-2. Ability to use information and communication technologies, modern methods and models of information security and/or cyber security.
PC-5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy.
PC-8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment.
PC-10. Ability to apply methods and means of cryptographic and technical protection of information at objects of information activity.
PC-12. Ability to analyze, identify and evaluate possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established policy of information and/or cyber security.

Learning outcomes

LO-1. Apply knowledge of state and foreign languages in order to ensure the effectiveness of professional communication;
LO-2. Organize own professional activity, choose optimal methods and ways of solving complex specialized tasks and practical problems in professional activity, evaluate their effectiveness;
LO-3. Use the results of independent search, analysis and synthesis of information from various sources for the effective solution of specialized tasks of professional activity.
LO-4. Analyze, argue, make decisions when solving complex specialized tasks and practical problems in professional activity, which are characterized by complexity and incomplete determination of conditions, be responsible for the decisions made.
LO-5. Adapt under the conditions of frequent changes in the technologies of professional activity, to predict the final result.
LO-6. Critically understand the main theories, principles, methods and concepts in education and professional activity.
LO-7. Act on the basis of the legislative and regulatory framework of Ukraine and the requirements of relevant standards, including international ones in the field of information and/or cyber security.
LO-8. Prepare proposals for regulatory acts on ensuring information and/or cyber security.
LO-9. Implement processes based on national and international standards for detection, identification, analysis and response to information and/or cyber security incidents.
LO-10. Perform analysis and decomposition of information and telecommunication systems.
LO-11. Perform analysis of connections between information processes on remote computer systems.
LO-12. Develop threat and intruder models.
LO-13. Analyze projects of information and telecommunication systems based on standardized technologies and data transmission protocols.
LO-14. Solve the task of protecting programs and information processed in information and telecommunication systems by hardware and software tools and evaluate the effectiveness of the quality of the decisions made.
LO-15. Use modern hardware and software of information and communication technologies.
LO-16. Implement complex information security systems in the automated systems (AS) of the organization (enterprise) in accordance with the requirements of regulatory and legal documents.
LO-17. Ensure the processes of security and functioning of information and telecommunication (automated) systems based on practices, skills and knowledge, regarding structural (structural-logical) schemes, network topology, modern architectures and models of security of electronic information resources with a reflection of relationships and information flows, processes for internal and remote components.
LO-18. Use software and software-hardware complexes for the security of information resources.
LO-19. Apply theories and methods of protection to ensure information security in information and telecommunication systems.
LO-20. Ensure the functioning of special software to protect information from destructive software influences, destructive codes in information and telecommunication systems.
LO-21. Solve tasks of provision and support (including: review, testing, accountability) of the access control system according to the stated security policy in information and telecommunication (automated) systems.
LO-22. Solve the management procedures of identification, authentication, authorization of processes and users in information and telecommunication systems according to the established policy of information and/or cyber security.
LO-23. Implement measures to prevent unauthorized access to information resources and processes in information and telecommunication (automated) systems.
LO-24. Solve the problems of managing access to information resources and processes in information and telecommunication (automated) systems based on access management models (mandatory, discretionary, role-based).
LO-25. Ensure the introduction of accountability of the access management system to electronic information resources and processes in information and telecommunication (automated) systems using event registration logs, their analysis and stated protection procedures.

LO-26. Implement measures and ensure the implementation of processes of prevention of unauthorized access and protection of information, information and telecommunication (automated) systems based on the reference model of interaction of open systems.
LO-27. Solve problems of data flow protection in information and telecommunication (automated) systems.
LO-28. Analyze and evaluate the effectiveness and level of security of resources of various classes in information and telecommunication (automated) systems during tests in accordance with the established policy of information and/or cyber security.
LO-29. Evaluate the possibility of realization of potential threats of information processed in information and telecommunication systems and the effectiveness of the use of complexes of protection means under the conditions of realization of threats of various classes.
LO-30. Assess the possibility of unauthorized access to elements of information and telecommunication systems.
LO-31. Apply protection theories and methods to ensure the security of elements of information and telecommunication systems.
LO-32. Solve the tasks of managing the processes of restoring the regular functioning of information and telecommunication systems using backup procedures in accordance with the stated security policy.
LO-33. Solve the problems of ensuring the continuity of business processes of the organization on the basis of risk management theory.
LO-34. Participate in the development and implementation of an information security and/or cyber security strategy in accordance with the goals and objectives of the organization.
LO-35. Solve the tasks of providing and supporting complex information security systems, as well as countering unauthorized access to information resources and processes in information and information-telecommunication (automated) systems in accordance with the stated policy of information and/or cyber security.
LO-36. Detect dangerous signals of technical means.
LO-37. Measure the parameters of dangerous and interfering signals during the instrumental control of information security processes and determine the effectiveness of information security against leakage through technical channels in accordance with the requirements of regulatory documents of the technical information security system.
LO-38. Interpret the results of special measurements using technical means, monitoring the characteristics of information and telecommunication systems in accordance with the requirements of regulatory documents of the technical information security system.
LO-39. Carry out attestation (based on accounting and survey) of regime territories (zones), premises, etc. under the conditions of compliance with the secrecy regime, recording the results in the relevant documents.
LO–40. Interpret the results of special measurements using technical means, control of ITS characteristics in accordance with the requirements of regulatory documents of the technical information security system.
LO-41. Ensure the continuity of the event and incident logging process based on automated procedures.
LO-42. Implement processes of detection, identification, analysis and response to information and/or cyber security incidents.
LO-43. Apply national and international regulatory acts in the field of information security and/or cyber security to investigate incidents.
LO-44. Solve the problems of ensuring the continuity of the organization's business processes on the basis of risk management theory and the stated information security management system, in accordance with national and international requirements and standards.
LO-45. Apply early classes of information security and/or cyber security policies based on risk-based access control to information assets.
LO-46. Analyze and minimize the risks of information processing in information and telecommunication systems.
LO-47. Solve the problems of protection of information processed in information and telecommunication systems using modern methods and means of cryptographic protection of information.
LO-48. Implement and maintain intrusion detection systems and use cryptographic protection components to ensure the required level of information security in information and telecommunications systems.

LO-49. Ensure the proper functioning of the monitoring system of information resources and processes in information and telecommunication systems.
LO-50. Ensure the functioning of software and software-hardware complexes for detecting intrusions of various levels and classes (statistical, signature, statistical-signature).
LO-51. Maintain operational efficiency and ensure configuration of intrusion detection systems in information and telecommunication systems.
LO-52. Use tools for monitoring processes in information and telecommunication systems.
LO-53. Solve problems of software code analysis for the presence of possible threats.
LO-54. Be aware of the values of a civil (free democratic) society and the need for its sustainable development, the rule of law, the rights and freedoms of a person and a citizen in Ukraine.

Student workload

The total volume of the course is 90 hours (3 ECTS credits): lectures - 24 hours, laboratory classes - 12 hours, self-study - 54 hours.

Course prerequisites

Information security of the state.

Features of the course, teaching and learning methods, and technologies

In the course of teaching the discipline, the teacher uses explanatory-illustrative (informational-receptive) and reproductive teaching methods. Presentations, conversations, and master classes are used as teaching methods aimed at activating and stimulating the educational and cognitive activities of applicants.

Program of the course

Topics of the lectures

Topic 1. Overview of system security.
Basic concepts and definitions of security. The role of information protection in cyberspace, conditions of functioning of the security subsystem in social (computer) networks and systems. System security requirements, security risks. Security components and services: confidentiality, integrity, availability, involvement, observability. Distribution of security services according to the levels of the ISO/OSI model. Security criteria of computer systems. National regulatory acts and international safety system regulators.
Topic 2. Modern threats in social (computer) networks.
A formal definition of a cryptosystem. Performance criteria and indicators. Analysis of the main types of attacks, risks and vulnerable elements of information systems in cyberspace. Synergy and hybridity of modern threats, main trends of direction.
Topic 3. Mechanisms for ensuring confidentiality and integrity.
Principles of building symmetric and asymmetric encryption. The main criteria for their use. Block symmetric ciphers, DES block symmetric encryption algorithms, GOST-28147, Rijndael, Kalina-256. Asymmetric cryptosystems of RSA, El Gamal and Diffie-Gellman. The principles of their use with social networks.
Topic 4. Mechanisms for ensuring authenticity.
Classification of authentication mechanisms: MDC codes, MAC codes, digital signature. Basic standards of digital signature. Classification of authentication mechanisms based on two-factor authentication methods. Classification of threats for two-factor authentication procedures. Basic requirements for two-factor authentication protocols. Basic procedures that ensure security in two-factor authentication protocols.
Topic 5. Fundamentals of digital steganography.
Classification of public key digital steganography methods. Basic methods of hiding confidential information.
Topic 6. Network information protection protocols.

Information protection at the network level. Security and integrity protocols IPSec, SSL, TLS, their essence. PGP and CS MIME security systems. Cryptographic functions. Compatibility at the email level. Secure email.
Topic 7. Key management mechanisms and protocols in IVC in social networks.
Components and services of public key infrastructure. PKI architecture and topology. Basic requirements of the public key standard, certificate management. PKI systems. Basic PKI policy requirements.
Topic 8. Software and hardware means of information protection on the Internet.
Basic principles of information protection when connecting to the Internet. Use of passwords and control mechanisms.
Topic 9. Software and hardware (software) means of protecting information in the Wi-Fi network.
Basic principles of information protection when connecting to a Wi-Fi network. Use of passwords.
Topic 10. Software and hardware (software) means of information protection in cloud technologies.
Basic principles of information protection when using cloud networks (technologies).

Topics of the workshops

Not provided for in the curriculum.

Topics of the laboratory classes

Topic 1. Protection mechanisms of the Windows 10 operating system.
Topic 2. Studying the protection capabilities of the Windows 10 Encrypted File System (EFS), the Security and Service Center, and the Windows 10 Firewall.
Topic 3. Means of user authentication and system security analysis.
Topic 4. Security analysis tools.
Topic 5. Study of the stability of password protection.

Self-study

A student's independent work is one of the forms of organization of learning, the main form of mastering educational material in free time from classroom training. During independent work, students study lecture material, do individual homework, prepare for tests, tests and exams. Students are also recommended additional materials (videos, articles) for self-study and analysis.

Non-formal education

Within the framework of non-formal education, according to the relevant Regulation (http://surl.li/pxssv), the educational component or its individual topics may be taken into account in the case of independent completion of professional courses/trainings, civic education, online education, vocational training, etc.
Subjects are not considered for this component in case of successful completion of the courses.

Course materials and recommended reading

Basic literature:

1. Cyber security: modern protection technologies. Study guide for students of higher educational institutions. Lviv: "New World-2000", 2019. - 678 p.
https://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf
2. Cyber security: modern protection technologies. Study guide for students of higher educational institutions. / S.E. Ostapov, S.P. Yevseev, O.G. King. – Lviv: "New World-2000", 2020. - 678 p.
https://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf
3. Danyk Yu.G. Fundamentals of cyber security and cyber defense: a textbook / Yu.G. Danyk, P.P. Vorobienko, V.M. Chernega - [Second edition, revision. and additional]. – Odesa.: ONAZ named after O.S. Popova, 2019. - 320 p.
https://kr-labs.com.ua/books/%D0%9E%D1%81%D0%BD%D0%BE%D0%B2%D0%B8+%D0%BA%D1%96%D0%B1

%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8+%D1%82%D0%B0+%D0%BA%D1
%96%D0%B1%D0%B5%D1%80%D0%BE%D0%B1%D0%BE%D1%80%D0%BE%D0%BD%D0%B8_+%D0%BF%D1% 96%D0%B4%D1%80%D1%83%D1%87%D0%BD%D0%B8%D0%BA..PDF.
4. Stallings V. Cryptography and Network Security: Principles and Practice, 2nd ed.: Trans. from English - K.: "Williams" Publishing House, 2001. - 672 p.: illustrations. - Paral. title English
https://www.cs.vsb.cz/ochodkova/courses/kpb/cryptography-and-network-security_-principles-and-practice-7th-global-edition.pdf
5. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
http://monograph.com.ua/pctc/catalog/view/64/52/231-1
6. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p.
http://monograph.com.ua/pctc/catalog/view/978-617-7319-72-5/978-617-7319-72-5/746-2
7. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p. http://monograph.com.ua/pctc/catalog/view/978-617-7319-57-2/117/419-2.

Additional literature:

8. "Cybersecurity in Social Networks" – Ricardo Jorge Girante Gonçalves
https://run.unl.pt/bitstream/10362/133016/1/TGI0504.pdf
9. "Security and Privacy in Social Networks" – Rajaraman, R.
https://books.google.com.ua/books/about/Security_and_Privacy_in_Social_Networks.html?id=rpIYSxjfV7wC&redir_esc=y.

Assessment and grading

Criteria for assessment of student performance, and the final score structure

Points are awarded according to the following ratio:
- laboratory work: 40% of the semester grade;
- independent work: 10% of the semester grade;
- control work: 10% of the semester grade;
- exam: 40% of the semester grade.

Grading scale

Total points	National	ECTS
90–100	Excellent	A
82–89	Good	B
75–81	Good	C
64–74	Satisfactory	D
60–63	Satisfactory	E
35–59	Unsatisfactory (requires additional learning)	FX
1–34	Unsatisfactory (requires repetition of the course)	F

Norms of academic integrity and course policy

The student must adhere to the Code of Ethics of Academic Relations and Integrity of NTU "KhPI": to demonstrate discipline, good manners, kindness, honesty, and responsibility. Conflict situations should be openly discussed in academic groups with a lecturer, and if it is impossible to resolve the conflict, they should be brought to the attention of the Institute's management.
Regulatory and legal documents related to the implementation of the principles of academic integrity at NTU "KhPI" are available on the website: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Approval

Approved by

28.08.2024 

Head of the department
Serhii YEVSEIEV

28.08.2024 

Guarantor of the educational program
Serhii YEVSEIEV