Syllabus
Course Program

Security of Internet things

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
Special (professional), Mandatory

Semester
7

Language of instruction
English

Lecturers and course developers

Serhii POHASII

Serhii.Pohasii@khpi.edu.ua
Candidate of economic sciences, associate professor of the department of cybersecurity of National Technical University "Kharkiv Polytechnic Institute".

The number of scientific publications: more than 95, including 2 utility model patents, 6 monographs, of which 4 are collective monographs, 4 teaching aids, 4 of which bear the seal of the Ministry of Education and Science of Ukraine, 65 articles in foreign publications and specialized publications of Ukraine, with 11 of them are in the Scopus scientometric database. Leading lecturer in the disciplines: "Analog and digital electronic devices", "Internet of things and services", "Security of cloud technologies", "Fundamentals of construction and protection of modern operating systems", "Modeling of critical infrastructure systems", "Fundamentals of construction and protection of microprocessor systems ", "Security of smart technologies and Internet of things", "Information and communication systems in the field of national security" for undergraduate and graduate students, Section "Information security of cloud services", "Modern methods of protection of socio-cyber-physical systems", "Modeling of mechanisms cyber security" for graduate students.

More about the lecturer on the department's website

General information

Summary

The educational discipline "Security of Internet things" is a mandatory educational discipline. The discipline is aimed at studying the main concepts and approaches to the development and implementation of reliable, secure IoT systems, researching models and methods for ensuring reliability and ensuring security and evaluating IoT-based systems, familiarization with the process of testing and finding vulnerabilities in IoT devices.

Course objectives and goals

The formation of the students' knowledge system in the field of the Internet of Things and digital technologies, and a broader category called digital transformation, on the basis of which a qualified specialist will be able to ensure the development, application and operation of such systems in production and in the scientific field. In the discipline, the main emphasis is on understanding the fundamental concepts and mechanisms underlying the functioning of Internet of Things.

Format of classes

Lectures, laboratory classes, consultations, self-study. Final control - credit test.

Competencies

PC-8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment.
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-9. Implement processes based on national and international standards for detection, identification, analysis and response to information and/or cyber security incidents.
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-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-19. Apply theories and methods of protection to ensure information security in information and telecommunication systems.
LO-23. Implement measures to prevent unauthorized access to information resources and processes in information and telecommunication (automated) systems.
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-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-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-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-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.

Student workload

The total volume of the course is 120 hours (4 ECTS credits): lectures - 32 hours, laboratory classes - 16 hours, self-study - 72 hours.

Course prerequisites

Web application development. Fundamentals of construction and protection of microprocessor systems.

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. History of the Internet of Things.
The history of the development of the Internet of Things. Prospects for the development of the Internet of Things. Industry and production. Consumers Retail trade, finance and marketing. Medicine. Transport and logistics. Agriculture and the environment. Energy. A smart city. The government and the army.
Topic 2. History of the Internet of Things.
Architecture and resources of modern operating systems.
Topic 3. Sensors, endpoints and power systems.
Fusion of sensors. Input devices. Output devices. Functional examples (all together). A functional example is the TI SensorTag CC2650. Between the sensor and the controller. Energy sources and power management. Reproduction of electricity. Energy storage.
Topic 4. Theory of communication and information.

Theory of communication. Radio frequency energy and theoretical range. Radio frequency interference. Information theory. Bitrate limits and the Shannon-Hartley theorem. Bit error rate. Narrowband and broadband communication. Radio spectrum. Management structure.

Topic 5: Wireless Personal Area Network (WPAN) is not based on IP.

Wireless personal local area network standards. Standards 802.15. Bluetooth. IEEE 802.15.4. Zigbee. Z-Wave.

Topic 6. IP-based WPAN and WLAN.

Internet Protocol and Transmission Control Protocol. The role of the IP protocol in the Internet of Things. WPAN with IP - 6LoWPAN. WPAN with IP - Thread. Thread architecture and topology. Thread protocol stack Thread routing. Thread addressing. Neighbor detection IEEE 802.11 protocols.

Topic 7. Telecommunication systems and protocols (GVS).

Functional compatibility of cellular communication devices. Standards and management model.Cellular communication access technologies. Categories of subscriber equipment 3GPP. Allocation of spectrum and frequency bands in 4G LTE. 4G LTE network topology and architecture. E-UTRAN 4G LTE network protocol stack. 4G LTE geographic areas, data flows and handover procedures. 4G LTE packet structure. Categories 0, 1, M1 and NB-IoT. 5G LoRa and LoRaWAN. LoRa physical layer. LoRaWAN MAC layer. LoRaWAN topology. Brief description of LoRaWAN. Sigfox. Physical layer of Sigfox. Sigfox MAC layer. Sigfox protocol stack. Sigfox topology.

Topic 8. Router and gateways.

Routing functions. Gateway functions. Routing fault tolerance and out-of-band management. VLAN.VPN. Management of traffic speed and QoS. Security features. Metrics and analytics. Processing on the edge. Software network interaction. SDN architecture. Traditional cross-network interaction. Advantages of SDN.

Topic 9. IoT data transfer protocols from the edge device to the cloud.

Protocols. MQTT. MQTT-SN. Architecture and topology of MQTT-SN. Limited application protocol. CoAP architecture details. Other protocols. STOMP. AMQP. Summary and comparison of protocols.

Topic 10. Topology of cloud and fog computing.

Cloud services model. Public, private and hybrid cloud. OpenStack cloud architecture. Keystone. Limitations of Cloud Architectures for IoT. Fog computing.

Topic 11. Data analysis and machine learning in cloud and fog platforms.

Simple data analysis in the Internet of Things. Machine learning in the Internet of Things. Machine learning models.

Topic 12. Security of the Internet of Things.

Commonly used concepts of cyber security are related to attack. Anatomy of cyberattacks on IoT devices. Physical and hardware security. Cryptography. Architecture of software-based perimeter. Recommendations for securing IoT devices.

Topic 13. Consortia and communities.

Consortia with personal networks. Bluetooth SIG. Thread Group. Zigbee Alliance Consortiums based on Open Connectivity Foundation and Allseen Alliance protocols. Consortia on global computing networks. Weightless SIG. LoRa Alliance. Internet Engineering Council. Wi-Fi Alliance Consortiums with fuzzy and edge computing. OpenFog. EdgeX Foundry. Specialized organizations Industrial Internet Consortium. Institute of Electrical and Electronics Engineers IoT (IEEE IoT).

Topics of the workshops

Not provided for in the curriculum

Topics of the laboratory classes

Topic 1. Packet Tracer - Deployment and connection of devices.

Topic 2. Creating a simple network using Packet Tracer.

Topic 3. Connecting and monitoring IoT devices.

Topic 4. Smart room based on Raspberry Pi and PL-App.

Topic 5. Converged network and interconnection of things, security issues and main pillars of Cisco IoT, automation technologies.

Topic 6. Building a project to create an Internet of Things solution, starting from planning and ending with prototyping the solution.

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.
In particular, certain topics of this component can be taken into account in case of successful completion of the following CISCO courses:
Introduction to IoT and Digital Transformation, Exploring Networking with Cisco Packet Tracer https://www.netacad.com/catalogs/learn?category=course.

Course materials and recommended reading

Basic literature:

1. David Rose, David Rose, The Future of Things. How fairy tales and fiction become reality, ISBN: 978-5-91671-394-7, 2015.
https://responsiveobjects.wordpress.com/wp-content/uploads/2016/01/enchanted-objects_-design-human-desire-and-the-internet-of-things-rose-david.pdf
2. Baranov A.A., Internet of things: theoretical and methodological foundations of legal regulation. Volume I. Fields of application, risks and barriers, problems of legal regulation, ISBN: 978-966-937-513-1, 2018, 344p.
https://jurkniga.ua/nternet-rechey-teoretiko-metodologchn-osnovi-pravovogo-regulyuvannya-tom--sferi-zastosuvannya-riziki--barri-problemi-pravovogo-regulyuvannya/
3. Samuel Greengard, The Internet of Things (MIT Press Essential Knowledge series), ASIN: B00VB7I9VS, 2015, 230 P.
https://ru.scribd.com/document/441966460/the-internet-of-things-the-mit-press-essential-knowledge-series-by-samuel-greengard
4. Cuno Pfister, Getting Started with the Internet of Things: Connecting Sensors and Microcontrollers to the Cloud (Make: Projects) 1st Edition, ASIN: B00COVJUGI, 2011, 194 P.
https://www.openhacks.com/uploadsproductos/getting_started_with_the_internet_of_things_pachube_client.pdf
5. Erik Brynjolfsson and Andrew McAfee, The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies 1st Edition, ASIN: B00D97HPQI, 2014, 320 P.
http://digamo.free.fr/brynmacafee2.pdf
6. Thomas M. Siebel, Digital Transformation: Survive and Thrive in an Era of Mass Extinction, ASIN: B07SPDT74L, 2019, 253P.
https://www.perlego.com/book/2433384/digital-transformation-survive-and-thrive-in-an-era-of-mass-extinction-pdf
7. Information protection technologies./ S.E. Ostapov, S.P. Yevseiev, O.G. Korol. – Chernivtsi: Chernivtsi National University, 2013. – 471 p.
http://kist.ntu.edu.ua/textPhD/tzi.pdf.
8. Yevseiev S.P. Cyber security: basics of coding and cryptography/ S.P. Yevseiev, O.V. Milov, S.E. Ostapov, O.V. Severinov. - Kharkiv: Ed. "New World-2000", 2023. - 657 p.
https://acrobat.adobe.com/id/urn%3Aaaid%3Asc%3AEU%3A3c427761-01ab-4365-88f6-37f76ca508c5/?x_api_client_id=chrome_extension_viewer&bookmarkAcrobat=true&x_api_client_location=bookmark&filetype=application%2Fpdf&viewer%21megaVerb=group-discover

Additional literature:

9. Ethem Alpaydin, Machine Learning: The New AI (MIT Press Essential Knowledge series), ASIN: B01M60Y1T7, 2016, 232P.

https://pdfcoffee.com/machine-learning-the-new-ai-alpaydin-2016pdf-pdf-free.html
10. Nayan B. Ruparelia, Cloud Computing (MIT Press Essential Knowledge series), ASIN: B01FLE5JH8, 2016, 258 P.
https://s3.amazonaws.com/arena-attachments/911381/0ea8a9793158a95d9b91911e49240a43.pdf
11. Synergy of building cybersecurity systems: monograph / S. Yevseyev, V. Ponomarenko, O. Laptiev, O. Milov and others. - Kharkiv: PC TECHNOLOGY CENTER, 2021. - 188 p. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
12. 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. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
13. 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. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.
14. Ethernet technology: laboratory workshop / M. O. Bilova, S. P. Yevseiev, O. S. Zhuchenko, I. S. Ivanchenko, O. V. Shmatko.– Lviv: "Novyi Svit-2000", 2020. - 196 p.
http://library.hneu.edu.ua/storage/new-arrivals-books/December2020/.pdf2.pdf

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;
- credit test: 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