



NETWORK ARCHITECTURE AND IOT DEVICES SECURITY Syllabus

Details of the academic discipline

Cycle of Higher Education	<i>Second (master's)</i>
Field of Study	<i>F Information technologies</i>
Speciality	<i>F2 Software engineering</i>
Education Program	<i>Software engineering of multimedia and information-search systems</i>
Type of Course	<i>Selective</i>
Mode of Studies	<i>full-time</i>
Year of studies, semester	<i>2nd year of training, 3rd semester</i>
ECTS workload	<i>Lectures: 36 hours, laboratory work: 18 hours, independent work: 66 hours.</i>
Testing and assessment	<i>Final test, modular test, calendar control</i>
Course Schedule	<i>According to the schedule of the current academic year (http://roz.kpi.ua/)</i>
Language of Instruction	<i>English</i>
Course Instructors	Lecturer: Ph.D., associate professor, Liubov Oleshchenko, <i>oleshchenkoliubov@gmail.com</i> Laboratory work: Ph.D., associate professor, Liubov Oleshchenko, <i>oleshchenkoliubov@gmail.com</i>
Access to the course	Google classroom. Access is granted to registered students.

Program of educational discipline

1. Description of the educational discipline, its purpose, subject of study and learning outcomes

The study of the discipline "Network architecture and IoT devices security" allows students of higher education to develop the competencies necessary for solving practical problems of professional and scientific activities related to the design of networks of IoT devices and ensuring security IoT devices.

***The purpose** of studying the discipline "Network architecture and IoT devices security" is to form students' abilities to programmatically configure IoT devices for their safe functioning in a network of a given topology.*

***The subject** of the discipline "Network architecture and IoT devices security" is protocols, technologies and software methods for creating networks of IoT devices.*

*After mastering the discipline "Network architecture and IoT devices security", **the learning outcomes** are:*

knowledge:

- IoT protocols and standards;*
- IoT network architectures;*
- security parameters of IoT networks and their settings.*

skill:

- design networks of IoT devices in the Packet Tracer simulation environment, configure security parameters of IoT networks, and perform testing of programmed IoT devices in a network of a given topology.*

experience:

- designing IoT networks, ensuring security and data integrity of IoT devices;
- development of software for IoT devices for their operation in a given topology network.

The study of the discipline "Network architecture and IoT devices security" helps students of higher education who study under the educational program "Software engineering of multimedia and information-search systems" develop the competencies necessary for solving practical problems of professional activity related to the use wireless network technologies and programming for building IoT systems and ensuring their security:

GC01 Ability to abstract thinking, analysis and synthesis.

GC03 Ability to conduct research at an appropriate level.

PC02 Ability to develop and implement scientific and/or applied projects in the field of software engineering.

2. Pre-requisites and post-requisites of the discipline

(place in the structural and logical scheme of training according to the relevant educational program)

The successful study of the discipline "Network architecture and IoT devices security" is preceded by the study of the disciplines "Operating systems", "Programming" and "Computer Systems and Networks Fundamentals" of the curriculum of bachelor's training in the specialty F2 Software engineering.

The discipline "Network architecture and IoT devices security" ensures the implementation of course projects and master's theses in the specialty F2 "Software engineering".

3. Content of the academic discipline

The discipline "Network architecture and IoT devices security" involves the study of the following topics:

Topic 1. Architectural models of IoT.

Topic 2. Security of IoT devices.

Modular test.

Final test.

4. Educational materials and resources

Basic literature:

1. Finardi A. IoT Simulations with Cisco Packet Tracer // Electronic resource. Access mode: <https://www.theseus.fi/bitstream/handle/10024/150158/Andrea%20Finardi%20%20Master%20of%20Engineering%20%20Information%20technology.pdf?sequence=1&isAllowed=y>
2. Leading the IoT // Electronic resource. Access mode: https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf
3. Junejo A.K., Breza M., McCann J.A. Threat Modeling for Communication Security of IoT-Enabled Digital Logistics. *Sensors* 2023, 23, 9500. <https://doi.org/10.3390/s23239500>
4. Hubert K, Kaledio P. Security and Privacy in IoT: Considerations for securing IoT devices. https://www.researchgate.net/publication/377853082_Security_and_Privacy_in_IoT_Considerations_for_securing_IoT_devices
5. Megan Kay Ryan. A Survey and Analysis of Recent IoT Device Vulnerabilities. A Survey and Analysis of Recent IoT Device Vulnerabilities. March 26th, 2024. DOI: 10.21203/rs.3.rs-3982790/v1

Additional literature:

1. Changing the programming paradigm for the embedded in the IoT domain // Electronic resource. Access mode: <http://ieeexplore.ieee.org/document/7389059/?arnumber=7389059>
2. Things and Components available in Packet Tracer 7.2 // Electronic resource. Access mode: <https://www.packettacernetwork.com/internet-of-things/pt7-iot-devices-configuration.html>
3. IOT attacks // Electronic resource. Access mode: <https://www.educative.io/answers/what-are-iot-attacks>

The materials are freely available on the Internet.

Educational content

5. Methodology

№	Type of training session	Description of the lesson	Hours
<i>Topic 1. Architectural models of IoT.</i>			
1	<i>Lecture 1. Basic concepts of IoT (Internet of Things). History of IoT. IoT architecture.</i>	<i>Basic concepts of IoT. Using IoT. History of the Internet of Things. IoT in industry. The IoT ecosystem. IoT architecture.</i>	2
2	<i>Lecture 2. IoT reference model.</i>	<i>IoT compatibility standards. IoT reference model from MSE-T. Reference model from the World IoT Forum. Model NIST Special Publication 800-183. Industrial Internet of Things Reference Architecture model.</i>	2
3	<i>Lecture 3. IoT platforms.</i>	<i>The concept of an IoT platform. The Linux Foundation platform. AggreGate platform. Everywhere Cloud platform.</i>	2
4	<i>Laboratory work 1. Programming of IoT devices using Cisco Packet Tracer.</i>	<i>Lesson 1. Modeling an IoT Home Network in Cisco Packet Tracer. Task: in the Packet Tracer environment, model the topology of a home network according to the given scenario. Add IoT devices, tablets, and servers by connecting them to a wireless router. Make sure that all devices are connected to a single network.</i>	2
		<i>Lesson 2. Configuring a wireless network and DHCP/WLAN services. Task: configure wireless network parameters (SSID, password, standard WLAN settings) for all IoT devices. Enable DHCP on the router to automatically assign IP addresses. Verify that all connected devices receive correct network parameters.</i>	2
		<i>Lesson 3. Configuring a DNS server and testing the operation of IoT devices. Task: create and configure a DNS server to translate the URL of the IoT home page to the IoT server's own IP address. Test the operation of programmed devices: check the availability of IoT services, the correct operation of network services, and the interaction of devices with each other.</i>	2
5	<i>Lecture 4. IoT gateways.</i>	<i>Gateways of the Eurotech company. Intel gateways. Huawei gateways. Cisco gateways. NEXCOM gateways. Dell Edge Gateways. Hewlett Packard Enterprise gateways.</i>	2
6	<i>Laboratory work 2. Protection of IoT cloud services.</i>	<i>Lesson 1. Registering IoT devices and creating interaction conditions. Task: register four IoT devices of the company warehouse in the Packet Tracer environment: a motion detector, a directional light, and a webcam. Add conditions in the registration server: when the motion detector is activated, the light and camera are automatically turned on.</i>	2
		<i>Lesson 2. Configuring secure access and traffic restrictions.</i>	2

		<i>Task: configure complex authentication on the router for logging in to the console and for remote access. Additionally, configure an ACL (Access Control List) to limit traffic between the registration server and the company warehouse. Test the operation of the restrictions.</i>	
		<i>Lesson 3. Configuring a cloud web server for data security. Task: create and configure a web server in the cloud service provider's network. Ensure secure data transfer between the server and the company warehouse (encryption, secure access). Check the availability of the server and the operation of the IoT system, taking into account security.</i>	2
7	<i>Lecture 5. Intelligent sensors.</i>	<i>Simple sensors. Active and passive sensors. Sensor-computer systems. Intelligent sensors. Types of mechanical sensors. Microsystem technologies. Deformation intelligent sensors. Principles of operation of the global orientation system. Sensors of linear and angular movement. Intelligent acoustic sensors. Electric sensors.</i>	2
8	<i>Lecture 6. IoT technologies.</i>	<i>Industry 4.0. Industrial Internet of Things. Smart Factory - intelligent production.</i>	2
9	<i>Lecture 7. Data transmission technologies and protocols in IoT networks.</i>	<i>Long-distance data transmission technologies in IoT networks. LoRaWAN technology. SigFox technology. NB-IoT standard. Weightless-P technology. Short-distance data transmission technologies in IoT networks. Z-Wave technology. NFC technology. RFID. Bluetooth Low Energy. Wi-Fi HaLow. Sensor networks.</i>	2
10	<i>Lecture 8. IoT protocols.</i>	<i>Infrastructure protocols. Service detection protocols. Application layer protocols. MQTT. CoAP.</i>	2
11	<i>Lecture 9. Smart Home technologies. Security threats of the "smart home".</i>	<i>Elements of a "smart house". Threats of the "smart house". Attacks on the "smart house".</i>	2
12	<i>Lecture 10. Smart City technologies.</i>	<i>Smart City classification. Smart city concepts. The main components of the Smart City. Technologies of smart cities. Smart city standards. Information technologies and information technology platforms.</i>	2
13	<i>Lecture 11. Smart Grid technologies.</i>	<i>History of development of energy systems. Possibilities of modernization. Systems based on the Smart Grid technological platform. Properties of smart energy systems. Technologies of smart energy systems. Research in Smart Grid. Modeling of smart energy systems.</i>	2
<i>Topic 2. Security of IoT devices.</i>			
14	<i>Lecture 12. IoT security challenges. Threat model analysis for IoT system.</i>	<i>Anatomy of an IoT Attack. Mirai software. IoT security model. IoT health monitoring. Security in the IoT reference model. Standardized ETSI M2M architecture. Modeling IoT threats. NICE Cybersecurity Workforce Framework.</i>	2
15	<i>Laboratory work 3. Configuring the security of IoT devices.</i>	<i>Lesson 1. Creating a topology and connecting IoT devices. Task: in the Packet Tracer environment, simulate the topology of a given network and connect IoT devices to it using a wireless router. Check the availability of devices on the network.</i>	2

		<i>Lesson 2. Configuring basic security settings. Task: configure security settings on the wireless router: change the SSID, enable WPA2 encryption, set a complex password. Make sure that only authorized IoT devices can connect to the network.</i>	2
		<i>Lesson 3. Additional mechanisms for protecting IoT devices. Task: improve network security: configure access filtering by MAC addresses of IoT devices, create a separate VLAN for the IoT network. Check the operation of the protection by attempting an unauthorized connection.</i>	2
16	<i>Lecture 13. Vulnerabilities and attacks at the hardware level.</i>	<i>Physical vulnerabilities of IoT devices. Security of the physical device. Hardware vulnerabilities. Firmware vulnerabilities. Embedded software vulnerabilities. Access control models. IoT device identity management. Encryption in constrained systems.</i>	2
17	<i>Lecture 14. Vulnerabilities of the communication level.</i>	<i>IoT communication scenarios. Roles of IEEE 802.15.4 devices. IEEE 802.15.4 topologies. IEEE 802.15.4 security. Mesh protocols that use 802.15.4.</i>	2
18	<i>Lecture 15. TCP/IP vulnerabilities in IoT networks.</i>	<i>Common IP vulnerabilities. DoS attacks. Boost and bounce attacks. ICMP attacks. IP address forgery attacks. TCP vulnerabilities. TCP SYN Flood attack. UDP vulnerabilities. Security for IoT communication protocols. A threat model for IoT communication technologies. IoT Communications Checklist.</i>	2
19	<i>Lecture 16. Application-level attacks of IoT systems.</i>	<i>OWASP Web and Cloud Application Vulnerabilities. Device management and data programs. Guidelines for secure web and cloud applications. Web interface vulnerabilities. Application-level threat modeling. IoT messaging protocols. MQTT protection. CoAP protection.</i>	2
20	<i>Lecture 17. Vulnerability and risk assessment in IoT systems.</i>	<i>IoT Risk Assessment. General vulnerability assessment system. CVSS indicator groups. CVSS base metric group. Components of IoT Data Flow Diagrams. Risk management strategies. IoT and blockchain.</i>	2
21	<i>Lecture 18. Final lecture.</i>	<i>Review of the studied material. Modular control work.</i>	2

6. Independent work of student

The discipline "Network architecture and IoT devices security" is based on independent preparation for classroom classes on theoretical topics.

No	The name of the topic submitted for independent processing	Hours of study	References
1	Preparation for the lecture 1	2	[1], pp. 5-9
2	Preparation for lecture 2	2	[1], pp. 11-16
3	Preparation for the lecture 3	2	[2]
4	Preparation for laboratory work 1	4	[1], pp. 17-25, [2 add.]
5	Preparation for the lecture 4	2	[2], [1 add.]
6	Preparation for laboratory work 2	4	[1], pp. 25-37
7	Preparation for the lecture 5	2	[1], pp. 38-46
8	Preparation for the lecture 6	2	[1], pp. 47-57

9	Preparation for the lecture 7	2	[1], pp. 68-79
10	Preparation for the lecture 8	2	[2]
11	Preparation for the lecture 9	2	[2]
12	Preparation for lecture 10	2	[2]
13	Preparation for lecture 11	2	[2]
14	Preparation for lecture 12	2	[2]
15	Preparation for laboratory work 3	4	[4]
16	Preparation for lecture 13	2	[2]
17	Preparation for lecture 14	2	[3]
18	Preparation for lecture 15	2	[5]
19	Preparation for lecture 16	2	[5]
20	Preparation for lecture 17	2	[2], [3 add.]
21	Preparation for modular control work	20	[1-5], [1-3 add.]

Policy and Assessment

7. Course policy

Forms of organizing the educational process, types of training sessions and assessment of learning outcomes are regulated by the Regulations on the Organization of the Educational Process at the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".

Class attendance policy. Attendance at lecture classes is mandatory. Attendance at laboratory classes may be occasional and required for the defense of laboratory work. The presence or absence of a student at a class is not assessed by awarding or deducting points. If a student cannot attend classes, he or she is still responsible for studying the theoretical material and completing practical assignments.

Policy on ethical norms in the classroom: discipline; compliance with subordination; honesty; responsibility; respect for those present, turning off phones.

Policy on assessing learning outcomes. The policy on assessing learning outcomes is regulated by the Regulations on the system of assessing learning outcomes at Igor Sikorsky Kyiv Polytechnic Institute. According to the Regulations, each grade is given in accordance with the criteria developed by the teacher and announced to students in advance. If a student fails to complete all four laboratory tests, he/she will not be allowed to take the test. Failure to pass the current control measure (modular test) without good reason is assessed as 0 points.

The policy and principles of academic integrity are regulated by the norms set of the Code of Honor of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" (https://kpi.ua/files/honorcode_en.pdf); Regulations on the Organization of the Educational Process, Regulations on the System for Preventing Academic Plagiarism, Regulations on the Commission on Ethics and Academic Integrity. Plagiarism and other forms of violation of the principles of academic integrity are unacceptable. The student must complete all laboratory practical tasks independently using open sources of information and acquired knowledge and skills.

Plagiarism and other forms of violation of the principles of academic integrity are unacceptable. All work for current and semester tests must be completed independently by the student using open sources of information and the acquired knowledge and skills.

All works that violate the principles of academic integrity (the program code does not match the assignment option, the identity of the program code among different works, etc.) are evaluated at 0 points. To gain access to the test, the student must independently complete the laboratory work (without

changing the current rating). In the case of semester control work that violates the principles of academic integrity, the semester control report is marked "Eliminate".

Policy on appealing the results of assessment of control measures. According to the "Regulations on resolving conflict situations at Igor Sikorsky Kyiv Polytechnic Institute" (https://osvita.kpi.ua/sites/default/files/downloads/regulations_resolving_conflict_situations_2020.pdf), students have the right to appeal the results of control measures with arguments, explaining which criterion they disagree with according to the assessment. A student can raise any issue related to the procedure of control measures and expect that it will be considered in accordance with predetermined procedures.

Policy on assigning incentive points. According to the "Regulations on the system of assessing learning outcomes at Igor Sikorsky Kyiv Polytechnic Institute", incentive points are not included in the main RSO scale, and their sum cannot exceed 10 points.

Incentive points are awarded for a creative approach in performing laboratory work (the maximum number of points for all work is 10 points), as well as for participation in scientific projects and conferences related to the topic of this course.

8. Monitoring and grading policy

During the semester, students perform **3 laboratory works**.

The maximum number of points for each laboratory work: 20 points.

Points are awarded for:

- quality of performance of the laboratory work: 0-8 points;
- answer during the defense of the laboratory work: 0-8 points;
- timely submission of work for defense: 0-4 points.

Performance evaluation criteria:

7-8 points – the work is done qualitatively, in full;

5-6 points - the work is done qualitatively, in full, but has shortcomings;

3-4 points - the work is done qualitatively, but not in full, has flaws;

1-2 points – the work is not done well, not in full, has flaws;

0 points – the work is incomplete or contains significant errors.

Answer evaluation criteria:

7-8 points – the answer is complete, well-argued;

5-6 points – the answer is incomplete, but well argued;

3-4 points – there are minor errors in the answer;

1-2 points – there are significant errors in the answer;

0 points - there is no answer or the answer is incorrect.

Criteria for evaluating the timeliness of work submission for defense:

4 points – the work is presented for defense no later than the specified deadline;

0 points – the work is submitted for defense later than the specified deadline.

The maximum number of points for performing and defending laboratory works:

20 points × 3 lab. = 60 points.

The assignment for **the modular test** consists of 5 questions - 3 theoretical and 2 practical.

The answer to each theoretical/practical question is evaluated by 8 points.

Evaluation criteria for each theoretical/practical question of the modular test:

7-8 points – the answer is correct, complete, well-argued;

5-6 points – the answer is correct, but incomplete or poorly argued;

3-4 points – there are minor errors in the answer;

1-2 points – there are significant errors in the answer;

0 points - there is no answer or the answer is incorrect.

The maximum number of points for a modular control work:

8 points × 3 theoretical questions + 8 points × 2 practical questions = 40 points.

The rating scale for the discipline is equal to:

$$R = R_S = 60 \text{ points} + 40 \text{ points} = 100 \text{ points.}$$

According to the description: $R = R_{lab.} + R_{MKR.} = 60+40 \text{ points} = 100 \text{ points}$

Calendar control: is carried out twice a semester as a monitoring of the current state of fulfillment of the syllabus requirements.

At the first certification (8th week), the student receives "credited" if his current rating is at least 50% of the maximum number of points that the student can receive before the first certification (20 points).

At the second certification (14th week), the student receives "passed" if his current rating is at least 50% of the maximum number of points that the student can receive before the second certification (30 points).

Semester control: **Final test.**

Conditions for admission to semester control:

With a semester rating (r_s) of not less than 60% (60 points) and the inclusion of all the works of the computer workshop.

Completion and defense of a computer workshop is a necessary condition for admission to the credit.

Table of correspondence of rating points to grades on the university scale:

Score	Grade
100-95	Excellent
94-85	Very good
84-75	Good
74-65	Satisfactory
64-60	Sufficient
Below 60	Fail
Course requirements are not met	Not Graded

9. Additional information about the course

A certificate of completion of a similar course is valued at 10 points (if the course topic matches the lab topic), writing articles or participating in conferences/projects on the relevant topic of the discipline is also valued at an additional 5 points. For example, a lab can be automatically credited as 10 points by sending a certificate of completion of a Coursera course on the topic of the relevant lab to the classroom, for example:

An Introduction to Programming the Internet of Things (IoT) Specialization — UC Irvine

A six-course series teaching the design, creation, and deployment of IoT devices using Arduino and Raspberry Pi platforms. Covers embedded systems, networking, programming, and culminates in a hands-on capstone project.

<https://www.coursera.org/specializations/iot>

Introduction to the Internet of Things and Embedded Systems — UC Irvine (part of the specialization)

A focused standalone course introducing IoT fundamentals, components, networking, and embedded systems interactions. Suitable for auditing and provides foundational knowledge in IoT systems.

<https://www.coursera.org/learn/iot>

IoT Communications

Explores programming IoT devices with Arduino/Raspberry Pi, sensor technologies, communication protocols (e.g., MQTT), and foundational networking—all essential for IoT-focused education.

<https://www.coursera.org/learn/iot-communications>

IoT Systems and Industrial Applications with Design Thinking Specialization — LearnQuest

Focuses on designing IoT solutions for industrial automation using design-thinking methodologies, edge computing, IoT security, and robotics integration.

<https://www.coursera.org/specializations/iot-systems-and-industrial-applications-with-design-thinking>

etc.

The student must inform the teacher about the course taken or planned to be taken and clarify the results and prospects for crediting the learning outcomes obtained in non-formal/informal education.

Syllabus of the course

Is designed by teacher PhD, Associate Professor, Liubov Oleshchenko

Adopted by Computer Systems Software Department (protocol № 3, 29.09.2025)

Approved by the Faculty Board of Methodology (protocol № 2, 16.10.2025)