Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Department of Applied Radio Electronics

# [RE-281] COMPUTER NETWORKS AND SECURITY USING CISCO TECHNOLOGIES

## Curriculum of the academic discipline (Syllabus)

## Course details

| | |
|---|---|
| Level of higher education | First (bachelor's) |
| Field of knowledge | 17 - Electronics, automation, and electronic communications |
| Specialization | 172 - Electronic communications and radio engineering |
| Educational program | All |
| Discipline status | Elective (F-catalog) |
| Form of higher education | Full-time |
| Year of training, semester | Available for selection starting from the 2nd year, fall semester |
| Scope of the discipline | 4 credits (Lectures 18 hours, Practical 36 hours, Lab 0 hours, Independent work 66 hours) |
| Semester Control/control measures | Credit |
| Class schedule | https://schedule.kpi.ua |
| Language of instruction | Ukrainian |
| Information about the course leader/teachers | Lecturer: Nikitchuk A. V.,<br>Practical: Nikitchuk A. V., |
| Course location | https://do.ipo.kpi.ua/course/view.php?id=5928 |

## Curriculum

### 1. Description of the course, its purpose, subject matter, and learning outcomes

Modern information technologies are heavily dependent on computer networks consisting of billions of interconnected devices. This creates unique challenges in management, scaling, and security. For reliable and efficient data exchange,

a variety of network equipment, technologies, and protocols for collecting, storing, transmitting, processing, and protecting information are used.
Studying this discipline will be useful for anyone who works with computers, data, and information, and will help develop and implement security strategies and measures to prevent cyberattacks, assess network vulnerabilities and related risks, and respond appropriately to cyber incidents.

Students will gain knowledge/skills in:

- the basics of cybersecurity and the biggest problems facing cyberspace today;
- the basics of networks and network equipment, as well as the rules governing data exchange on the network;
- configuration of network equipment and end nodes;
- the main threats, attacks, and vulnerabilities that exist in cyberspace; •
basic means of protecting end nodes and networks;
- assessing network vulnerabilities and related risks;
- responding to cyber incidents, restoring and collecting data for examination.

Studying this discipline will increase personal security in cyberspace and provide a competitive advantage in the labor market in various fields and roles. It will be especially useful for:

- IT specialists, network administrators, system administrators, and network security engineers who are responsible for setting up and managing network infrastructure, ensuring data security, and protecting networks from potential threats.
- Information security specialists who will be involved in identifying and analyzing security threats, implementing measures to prevent cyberattacks, performing penetration testing, and developing security policies.
- Network security consultants who will advise companies and organizations on network security issues, audit their infrastructure, and develop strategies to protect against cyberattacks.

## 2. Prerequisites and post-requisites of the discipline (place in the structural-logical scheme of training under the relevant educational program)

For successful mastery of the discipline, students must have: •

knowledge of computer science and PC skills;
- English language skills or skills in using online translators.

Related disciplines:

- Programming of embedded Internet of Things systems (application of communication protocols in programming network nodes/equipment).

- .NET technologies for software development (development of web applications for use in computer networks).

## 3. Course content

### Chapter 1. Fundamentals of Computer Networks and Cybersecurity

- Topic 1. Fundamentals of cybersecurity and computer networks •
Topic 2. Networks and their characteristics. Network equipment
- Topic 3. Network organization and the OSI reference model. Principles of global computer network construction
- Topic 4. Network-level protocols and their vulnerabilities

- Topic 5. Transport and application layer protocols and their vulnerabilities

**Section 2. Endpoint security, network protection, and cyber threat management**

- Topic 6. Types of cybersecurity threats and ways to protect against them
- Topic 7. Characteristics of computer networks. Security devices, services, and data •

Topic 8. Deep protection, firewalls, access control lists, and security policies

## 4. Learning materials and resources

*Basic:*

1. *Organization of computer networks: laboratory workshop [Electronic resource]: textbook for students majoring in 121 "Software Engineering," specializing in "Software for computer and information retrieval systems" / L.M. Oleshchenko; Igor Sikorsky KPI. – Electronic text data (1 file: 4.68 MB). – Kyiv: Igor Sikorsky KPI, 2018. – 137 p. (Can be found on the Internet; students should familiarize themselves with it and answer the test questions)*
2. *A. O. Azarova, N. V. Lysak. Computer Networks and Telecommunications/Textbook Vinnytsia VNTU 2012. (Available online, students should familiarize themselves with it)*

*Additional:*

1. Grubb, Sam. How Cybersecurity Really Works: A Hands-On Guide for Total Beginners. United States: No Starch Press, 2021.
2. Zach, Coding. Computer Programming and Cybersecurity for Beginners: This Book Includes: Python Machine Learning, SQL, Linux, Hacking with Kali Linux, Ethical Hacking. Coding and Cyber Security Fundamentals. N.p.: Rdf Publishing Limited, 2021.
3. Lewis, Elijah. Ethical Hacking: 3 in 1- Beginner's Guide+ Tips and Tricks+ Advanced and Effective Measures of Ethical Hacking. N.p.: Amazon Digital Services LLC - KDP Print US, 2020.
4. Morgan, Kevin. Computer Networking Beginners Guide: The Complete Basic Guide to Master Network Security, Computer Architecture, Wireless Technology, and Communications Systems Including Cisco, CCNA and the OSI Model. N.p.: Tommaso Sammartano, 2021.
5. White, Michael B.. Computer Networking: The Complete Guide to Understanding Wireless Technology, Network Security, Computer Architecture and Communications Systems (Including Cisco, CCNA and CCENT). N.p.: CreateSpace Independent Publishing Platform, 2018.
6. Kiser, Quinn. Cybersecurity: A Simple Beginner's Guide to Cybersecurity, Computer Networks and Protecting Oneself from Hacking in the Form of Phishing, Malware, Ransomware, and Social Engineering. United States: Primasta, 2020.

*Descriptions of protocols, standards, terms, etc. can be found on the Internet, for example on Wikipedia (https://www.wikipedia.org) or on the official websites of network equipment manufacturers and standards developers.*

## Educational content

## 5. Methodology for mastering the academic discipline (educational component)

| **Section 1. Fundamentals of computer networks and cybersecurity** | |
|---|---|
| Lecture 1 | Fundamentals of cybersecurity and computer networks |
| Lecture 2 | Networks and their characteristics. Network equipment |
| Lecture 3 | Network organization and the OSI reference model. Principles of global computer network construction |
| Lecture 4 | Network-level protocols and their vulnerabilities |
| Lecture 5 | Transport and application layer protocols and their vulnerabilities |

| | |
|---|---|
| PR 1 | Getting Started with Cisco Packet Tracer |
| PR 2 | Channel, network, and transport layer functions |
| PR 3 | Cisco IOS network operating system |
| PR 4 | Configuring network equipment |

**Section 2. Endpoint security, network protection, and cyber threat management**

| | |
|---|---|
| Lecture 6 | Types of cybersecurity threats and ways to protect against them |
| Lecture 7 | Characteristics of computer networks. Security devices, services, and data |
| Lecture 8 | Deep protection, firewalls, access control lists, and security policies |

| | |
|---|---|
| PR 5 | Researching threats to endpoints |
| PR 6 | Improving security in Windows: research, monitoring, management, and configuration |
| PR 7 | Investigating data flows in a local network using Wireshark |
| PR 8 | Configuring basic WLAN security features |
| PR 9 | Configuring access control and authentication |
| PR 10 | Security monitoring data |
| PR 11 | Access control lists. Configuring standard ACLs |
| PR 12 | Access control lists. Configuring advanced ACLs |
| PR 13 | Security and risk management |
| PR 14 | Cyber threat analysis |
| PR 15 | Incident response |

### 6. Independent student work

*1. Throughout the semester:*

- *Study of materials assigned for independent study at the end of each lecture.* • *Working through literary sources.*
- *Answering questions for self-assessment and taking tests.*

*2. During the week before the planned activity:*

- *Preparation for practical work.*
- *Preparation for writing a test.*
- *Preparation and completion of homework assignments.* • *Prepare for the exam.*

## Policy and control

### 7. Academic discipline policy (educational component)

*<u>Rules for attending classes</u>:*

- *for lectures and practical classes - attending classes (Zoom video conferences) according to the schedule;*
- *independent study of the material using lecture recordings and other materials posted in the relevant distance learning course is permitted;*
- *asynchronous completion of practical assignments is permitted.*

*Rules of conduct in class:*

- *during classes, you must use the Internet to: complete assignments in the distance learning course; familiarize yourself with the links provided; access modern, organized sources of information;*
- *The use of mobile phones, laptops, and other devices is permitted.*

*Rules for performing practical work:*

- *if the teacher has questions about the results obtained, it is necessary to verbally* *go through the defense procedure (answer questions);*

- *The defense procedure is considered timely if it is completed during the class dedicated to the work or the next class according to the schedule.*

*Rules for awarding bonus points:*

- *bonus points are awarded for completing additional tasks specified in the assignments.*

*Rules for assigning penalty points:*

- *Penalty points may be assigned for late submission/defense of practical work.*

*Deadline and retake policy:*

- *tests, exams, and practical work must be completed by the last class of the semester.*

## 8. Types of assessment and the learning outcomes assessment rating system (LOAS)

- *Ongoing assessment: completion of practical work (64 points), quizzes on the topic of the class (16 points), Module Control Work (10 points), Home Control Work (10 points).*
- *Calendar assessment: conducted twice per semester as monitoring of the current status of syllabus requirements.*
- *Semester assessment: test.*
- *Conditions for admission to semester control: semester rating of more than 60 points.*

***Table of correspondence between rating points and grades on the university scale***

| Number of points | Rating |
|---|---|
| 100-95 | Excellent |
| 94 | Very good |
| 84 | Good |
| 74-65 | Satisfactory |
| 64-60 | Sufficient |
| Less than 60 | Unsatisfactory |
| Admission requirements not met | Not admitted |

## 9. Additional information on the discipline (educational component)

***Description of material, technical, and informational support for the discipline***

The discipline includes practical work on PCs using *Cisco Packet Tracer*, *Wireshark*, and *Windows* software.

Classes are held online using the Zoom platform. Practical work is carried out on personal computers or on computers in the department's computer labs.

Assignments, tests (quizzes), and links to lecture recordings are posted on the Sikorsky distance learning platform.

The working program of the academic discipline (syllabus):
**Compiled by** Nikitchuk A. V.;

**Approved by** the PRE Department (Minutes No. 06/2024 dated 06/27/2024)
**Approved by** the methodological commission of the faculty/research institute (protocol No. 06/2024 dated 28.06.2024)