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

Department of Computing Engineering

Networks and network information technologies

Syllabus

Requisites of the Course

Cycle of Higher Education	**First cycle of higher education (Bachelor's degree)**
Field of Study	12 Information Technologies
Specialty	121 Software engineering
Education Program	Computer Systems Software Engineering
Type of Course	Normative
Mode of Studies	full-time
Year of studies, semester	Second year, second semester
ECTS workload	4 credits (ECTS). Time allotment - 120 hours, including 54 hours of classroom work, and 66 hours of self-study.
Testing and assessment	Exam
Course Schedule	2 classes per week by the timetable https://schedule.kpi.ua
Language of Instruction	English
Course Instructors	Lecturer and lab teacher: PhD, Associate Professor, Oleksandr Rokovyi, email: rokovyi@comsys.kpi.ua
Access to the course	https://cloud.comsys.kpi.ua/s/o4EGfQ4Ny7kETx4

Outline of the Course

1. Course description, goals, objectives, and learning outcomes

Modern information technologies are closely related to computer networks. The efficiency of many elements of various computer systems depends on the quality of computer networks. The development of high-quality software is impossible without taking into account the characteristics of data transmission in computer networks. The correct choice of technologies, protocols and services will ensure reliable and safe functioning of computer systems. The course "Networks and network information technologies" in addition to theoretical issues of architecture and principles of building computer networks also pays a lot of attention to practical aspects of their use. That is why this course can be useful for future information technology specialists.

The purpose of this course is to train specialists who have knowledge of the architecture and principles of operating computer networks based on the TCP/IP protocol suite, as well as practical skills in using network technologies to solve various tasks.

The subject of the course is the theoretical and practical foundations of data transmission in computer networks, which ensure the necessary level of speed, reliability and security.

The course "Networks and network information technologies" provides the following program competencies and program results of the educational and professional program: FK06, FK15, PRN18, PRN25, PRN26:

- the ability to analyze, choose and apply methods and tools to ensure information security (including cyber security);

- the ability to develop and use network technologies;

- to know and be able to apply information technologies for data processing, storage and transmission;

- to know the software of high-performance computer systems;

- to know the principles of building and functioning of high-performance computer systems.

According to the program of the course, after learning this course, students must demonstrate the following educational results.

Knowledge:

- purpose and functions of the open system interconnection reference model levels;
- the main protocols of the TCP/IP protocol suite and their functions;
- secure data transfer mechanisms in computer networks;
- architecture and features of the DNS domain name system;
- architecture and features of email services;
- architecture and features of file services;
- architecture and features of Web-services;
- architecture and features of IM services.

Skills:

- configure parameters of network interfaces in the GNU/Linux operating system;
- install and configure network services in the GNU/Linux operating system;
- debugging network services;
- to ensure the required level of security during data transmission in computer networks;
- perform calculations of network parameters in TCP/IP protocol suite.

Experience:

- working with network traffic analyzers and generators;
- work in the command line of the GNU/Linux operating system.

2. Prerequisites and post-requisites of the course (the place of the course in the scheme of studies in accordance with curriculum)

In order to successfully master the course "Networks and network information technologies" in accordance with the educational program, it is necessary to master the knowledge of the courses: "Linux workshop", "Basics of computer systems and networks".

Competences, knowledge and skills acquired in the study of the course "Networks and network information technologies" can be used to study the courses: "Operating systems", "Software security".

3. Content of the course

Chapter 1. Domain name system.

Topic 1.1. Structure and Namespace of DNS.

Topic 1.2. Operating modes and format of DNS messages.

Chapter 2. Email services.

Topic 2.1. SMTP protocol.

Topic 2.2. Security in the SMTP protocol.

Topic 2.3. POP3 and IMAP protocols.

Chapter 3. Network data storage.

Topic 3.1. FTP protocol.

Topic 3.2. NFS network file system.

Topic 3.3. SMB/CIFS protocols.

Chapter 4. Web-services.

Topic 4.1. HTTP protocol.

Topic 4.2. Sessions in the HTTP protocol.

Topic 4.3. Caching in the HTTP protocol.

Topic 4.4. Load balancing for Web services.

Topic 4.5. SSL/TLS protocols.

Chapter 5. Instant messaging services.

Topic 5.1. XMPP protocol.

Topic 5.2. Matrix instant messaging services.

4. Coursebooks and teaching resources

Main literature.

1. Larry Peterson, Bruce Davie. Computer Networks: A Systems Approach, 2019. – 489 p. URL: https://github.com/SystemsApproach/book/releases/download/v6.1/book.pdf

2. Evi Nemeth, Garth Snyder, Trent Hein, Ben Whaley, Dan Mackin. UNIX and Linux System Administration Handbook, 5th Edition. Addison-Wesley Professional, 2017. – 1232 p.

3. James Kurose, Keith Ross. Computer Networking: A Top-Down Approach, Global Edition, 8th Edition. Pearson Education, 2021.

4. Andrew S. Tanenbaum, Nick Feamster, David J. Wetherall. Computer Networks, 6th edition, 2021. – 946 p.

Supplementary literature.

1. Olivier Bonaventure. Computer Networking: Principles, Protocols and Practice, Release 2021. – 413 p. URL: https://www.computer-networking.info/_downloads/CNP3-2021.pdf

2. Tanenbaum, A. S., Bos, H. J. Modern Operating Systems, 4th Edition. Pearson Higher Education, 2015. – 1137 p.

3. Peter L Dordal. An Introduction to Computer Networks, 2022. – 963 p. URL: http://intronetworks.cs.luc.edu/current/ComputerNetworks.pdf

4. Paul Cobbaut. Linux Networking, 2015. – 294 p. URL: http://linux-training.be/linuxnet.pdf

5. William Shotts. The Linux Command Line. Fifth Internet Edition, 2019. – 555 p. URL: https://sourceforge.net/projects/linuxcommand/files/TLCL/19.01/TLCL-19.01.pdf/download

6. Paul Cobbaut. Linux System Administration, 2015. – 385 p. URL: http://linux-training.be/linuxsys.pdf

7. Paul Cobbaut. Linux Security, 2015. – 129 p. URL: http://linux-training.be/linuxsec.pdf

8. Paul Cobbaut. Linux Storage, 2015. – 278 p. URL: http://linux-training.be/linuxsto.pdf

9. Linux Administration I System and Users. Version 4, 2015 – 238 p. URL: https://www.tuxcademy.org/download/en/adm1/adm1-en-manual.pdf

10. Linux Administration II Linux as a Network Client. Version 4, 2015 – 217 p. URL: https://www.tuxcademy.org/download/en/adm2/adm2-en-manual.pdf

Educational content

5. Methodology

5.1. Lectures.

№	Lecture topic and list of main issues	Number of hours
1	**Structure and Namespace of DNS.** Functions of the DNS name system. DNS namespace. Types of resource records. **Self-study**: familiarize yourself with DNS transport protocols.	2
2	**Operating modes and format of DNS messages.** Resolving names to addresses. DNS operating modes. DNS message format. **Self-study**: familiarize yourself with secure version of DNSSEC.	2
3	**SMTP protocol.** Email architecture. SMTP protocol. Email format. SMTP commands. SMTP response codes. **Self-study**: familiarize yourself with the implementation of spam filtering based on SpamAssassin.	2
4	**Security in the SMTP protocol.** SMTP extension. Authentication of messages using DKIM. SPF Sender Policy Infrastructure. DMARC. **Self-study**: familiarize yourself with the implementation of the DMARC mechanism in exim or postfix.	2
5	**IMAP and POP3 protocols.** POP3 protocol. POP3 states. POP3 commands. IMAP protocol. Folders and flags in IMAP. IMAP states. **Self-study**: familiarize yourself with the authentication mechanisms in the IMAP and POP3 protocols.	2
6	**Network data storage.** Architectures of network data storage. FTP protocol. Active and passive FTP modes. **Self-study**: familiarize yourself with the TFTP protocol.	2
7	**FTP protocol.** FTP commands. FTPS protocol. SCP protocol. SFTP protocol. **Self-study**: familiarize yourself with the implementation of the FTP protocol based on FileZilla.	2
8	**NFS network file system.** The goals of creating NFS. NFS compliance with the ISO OSI model. NFS architecture. NFS protocol. Mounting a remote file system. Configuring the NFS server. Options for exporting directory hierarchies. **Self-study**: familiarize yourself with Kerberos authentication in NFS	2
9	**SMB/CIFS protocols.** SMB/CIFS services. SMB service ports. NetBIOS protocol. Name service. NetBIOS computer types. Name registration.	2

№	Lecture topic and list of main issues	Number of hours
	Self-study: familiarize yourself with implementation of the CIFS/SMB3 server in the Linux kernel.	
10	**SMB/CIFS protocols.** NetBIOS resource types. Session service. Datagram service. CIFS protocol. CIFS package structure. **Self-study**: familiarize yourself with implementation of the CIFS/SMB3 server in the Linux kernel.	2
11	**HTTP protocol.** Resource identifiers. HTTP request structure. HTTP response structure. Methods of the HTTP protocol. HTTP statuses. **Self-study**: familiarize yourself with the HTTP/3 protocol	2
12	**Sessions in the HTTP protocol.** Client identification methods in HTTP. Keep state through Cookies. Attributes of Cookies. Use of cookies in the session. **Self-study**: Session ID in the URL.	2
13	**Caching in the HTTP protocol.** Types of caching. Header Cache-Control. GET request with a condition. Web proxy server. Reverse proxy server. **Self-study**: familiarize yourself with the possibilities of controlling caching by the Web server.	2
14	**HTTP performance improvement mechanisms.** Persistent connection in HTTP. HTTP pipeline processing. **Self-study**: familiarize yourself with the possibilities of monitoring a permanent connection by a Web server.	2
15	**Load balancing for Web services.** Purpose and functions of the load balancer. Load balancer traffic types. Load balancing algorithms. Keep state during load balancing. High availability of the load balancer. **Self-study**: familiarize yourself with balancing mechanisms at the transport level.	2
16	**SSL/TLS protocols.** Handshake protocol in TLS. Server authentication using digital certificates. Key exchange algorithms, encryption and hashing in TLS. **Self-study**: familiarize yourself with the public key infrastructure.	2
17	**Instant messaging (IM) services.** Purpose and functions of IM. Instant messaging networks and their protocols. XMPP protocol. XMPP architecture. **Self-study**: familiarize yourself with implementation of the XMPP protocol based on ejabberd.	2
18	**Matrix instant messaging services.** The purpose and capabilities of the Matrix specification. Services provided to customers in Matrix. Matrix architecture. Rooms in the Matrix. User identification.	2

№	Lecture topic and list of main issues	Number of hours
	Self-study: familiarize yourself with implementation of the Matrix server based on Synapse and the client based on Element.	
	Total:	36

5.2. Laboratory classes (computer workshop).

The main task of laboratory classes (computer workshop) is to provide students with the necessary practical skills for working with the TCP/IP protocol suite.

To successfully master the course, each student needs to prepare a workplace with two virtual machines. It is recommended to use VirtualBox virtualization system (https://www.virtualbox.org/wiki/Downloads)

For laboratory work, it is recommended to use latest stable release of Debian operating system (https://www.debian.org/download). To reduce the resource requirements for the hardware platform, you can use the operating system without a graphical user interface.

For full performance of all laboratory work, each virtual machine must be connected to the Internet.

№	Topic of laboratory work (computer workshop)	Number of hours
1	**TCP/IP protocol suite diagnostic tools.** Familiarity with tools used for debugging in the TCP/IP protocol suite: ping, traceroute, nslookup, dig, netstat, nmap, tcpdump, telnet, nc, scapy.	2
2	**Domain name system - DNS.** Setting up a DNS server based on the GNU/Linux OS.	2
3	**SMTP, POP3 and IMAP email services.** Setting up an email server that implements SMTP, POP3 and IMAP protocols based on the GNU/Linux OS.	5
4	**File transfer service.** Setting up an FTP server based on the GNU/Linux OS.	2
5	**Network file system - NFS.** Setting up an NFS server based on the GNU/Linux OS. Familiarity with the utilities used to diagnose the NFS server: nfsstat, showmount, mount, tcpdump.	2
6	**SMB/CIFS file access service.** Setting up an SMB server based on the GNU/Linux OS. Familiarity with the utilities used to diagnose the SMB server: nbtscan, nmblookup, smbtree, nmap.	2
7	**Web service.** Setting up a Web server based on the GNU/Linux OS. Familiarity with the utilities used to diagnose the Web server: telnet, netcat, openssl, curl.	3
	Total:	18

6. Self-study

6.1. Topics that are submitted for self-study.

№	Topic submitted for self-study	Number of hours
1	Utility for scanning computer network nmap.	4
2	Security mechanisms in instant messaging services.	4
3	Implementation of bridges between instant messaging services.	4
	Total:	12

Before each class, the student performs self-study training in accordance with the topic of the lecture or laboratory work for at least two hours.
Thus, the student's self-study work during the semester should be: 36 + 18 + 12 = 66 hours.

Policy and Assessment

7. Course policy

Course policy:
- for successful study of the course it is desirable to be present at all lectures;
- in lectures it is allowed to use any technique only for the purpose related to the lesson, without disturbing other students and teachers;
- during the lecture you can ask questions to the teacher, for this you need to raise your hand and get permission;
- it is forbidden to speak at lectures without the permission of the teacher;
- in lectures it is forbidden to engage in activities that do not directly relate to the course;
- laboratory work takes place in the form of a computer workshop;
- only students who are ready to defend their work should be present at laboratory classes;
- during the defense of the laboratory work the student must demonstrate the completed task and answer the teacher's questions (questions from the theory, practical task, etc.);
- options (if the division into options is provided in the task) for laboratory work are selected as follows: the first 15 students receive options according to the number in the group list, the student with number 16 in the list receives option 1, etc.
- penalty points for late protection of laboratory work are not accrued;
- it is possible to defend laboratory works in any sequence;
- repeated protection of laboratory works is prohibited;
- it is forbidden to use outside help during the defense of laboratory work.

8. Monitoring and grading policy

The final rating of a student in the course "Networks and network information technologies" consists of points that he receives:
- for academic work during the semester (starting scores);
- for exam.

8.1. Getting of starting scores.
During the semester the student performs 7 laboratory works.
For each laboratory work the student receives:
- 8 scores for completed in full and without significant errors task for laboratory work;

- from 0 to 4 scores for the defense of laboratory work, which consists of theoretical questions, practical tasks.
1 modular test is planned, for which the student can receive from 0 to 16 points.
The student's starting scores are calculated as the sum of scores for all laboratory works and modular test multiplied by a coefficient of 0.6.

8.2. Conditions for admission to the exam.
To obtain admission to the exam student must defend 7 laboratory works.

8.3. Scoring for the exam.
In the exam, students must answer three theoretical questions. Each theoretical question is evaluated in 20 score.
Theoretical evaluation system:
18-20 score - complete answer (not less than 90% of the required information);
15-17 score - a fairly complete answer (at least 75% of the required information, or minor inaccuracies);
12-14 score - incomplete answer (at least 60% of the required information and some errors);
0 score - unsatisfactory answer (less than 60% of the required information or significant errors).

The sum of starting score and score for the exam are adopted by university grading system as follows:

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

During lectures, in addition to presentations, it is necessary to use software to demonstrate the operation of network services. This will give the student the opportunity to learn the lecture material more deeply.

9.1. List of theoretical questions for the exam.

- Types of DNS servers and their purpose.
- Types of resource records in DNS and their purpose.
- Server operation in iterative and recursive modes.
- The general procedure for resolving domain name into an IP address.
- Caching in DNS.
- Email architecture.
- Purpose and architecture of SMTP, POP3 and IMAP protocols.
- Email message format.
- Routing of email messages.

- DKIM and SPF mail authentication methods.
- DMARC technology.
- Purpose and features of FTP protocol.
- Passive and active modes of FTP server.
- FTP protocol commands.
- FTPS protocol (FTP over SSL/TLS).
- SFTP protocol.
- Compliance of NFS with the ISO/OSI model.
- NFS architecture.
- Purpose and functions of NFS components: mountd, nfsd, rpcbind (portmapper).
- Procedure for mounting a file system in NFS.
- NetBIOS/SMB stack.
- NetBIOS resource names and types.
- NetBIOS name service. Registering and viewing NetBIOS names. NetBIOS computer types.
- Election of master browser.
- Datagram and session services in NetBIOS/SMB.
- HTTP protocol.
- URIs and URLs.
- Structure of HTTP messages.
- HTTP methods.
- Sessions in the HTTP protocol.
- Caching in the HTTP protocol.
- Persistent HTTP connection.
- Web server load balancing algorithms.
- Saving the state when balancing the load of the Web server.
- Open systems interaction reference model (ISO/OSI).
- The multi-level structure of the TCP/IP suite.
- Application layer.
- Transport layer.
- Network layer.
- Network interfaces layer.
- Compliance of the TCP/IP suite layers with the ISO/OSI model.
- The main protocols of the TCP/IP suite, their purpose.
- Purpose and functions of IM.
- Instant messaging networks and their protocols.
- XMPP protocol.
- Security mechanisms in instant messaging services.

- Purpose and capabilities of the Matrix specification.
- Services provided to clients in Matrix.
- Matrix architecture.
- Rooms and user identification in Matrix.

9.2. Additional Information Resources

https://www.cs.vu.nl/~ast/CN5/

Syllabus of the course

Is designed by teacher Associate Professor, Ph.D, Oleksandr Rokovyi

Adopted by Department of Computing Engineering (protocol № 13, 10 May 2023)

Approved by the Faculty Board of Methodology (protocol № 11, 29 June 2023)