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

Кафедра обчислювальної техніки

Мережні технології

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	***Другий (магістерський)***
Галузь знань	12 Інформаційні технології
Спеціальність	123 Комп'ютерна інженерія
Освітня програма	Комп'ютерні системи та мережі
Статус дисципліни	Нормативна
Форма навчання	очна(денна)
Рік підготовки, семестр	1 курс, осінній семестр
Обсяг дисципліни	120 годин (36 годин – лекції, 18 годин – лабораторні, 66 години – СРС)
Семестровий контроль/ контрольні заходи	Залік
Розклад занять	http://rozklad.kpi.ua
Мова викладання	Українська
Інформація про керівника курсу / викладачів	Лектор: к.т.н, Роковий Олександр Петрович, rokovyi@comsys.kpi.ua Лабораторні: ст. викладач, Алєнін Олег Ігорович, oleg.alenin@gmail.com
Розміщення курсу	https://cloud.comsys.kpi.ua/s/q9aP9a5RwDi55AB

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Сучасні інформаційні технології тісно зв'язані з комп'ютерними мережами. Від ефективності роботи останніх залежить ефективність роботи багатьох елементів різноманітних комп'ютерних систем. Розробка якісного програмного забезпечення не можлива без врахування особливостей передачі даних в комп'ютерних мережах. Правильний вибір технологій, проколів, сервісів дозволить забезпечити надійне та безпечне функціонування комп'ютерних систем. Дисципліна «Мережні технології» окрім теоретичних питань архітектури та принципів побудови комп'ютерних мереж також приділяє багато уваги практичним аспектам їх застосування. Ось чому ця дисципліна може бути корисною майбутнім фахівцям в сфері інформаційних технологій.

Мета навчальної дисципліни – підготовка фахівців, які мають знання з архітектури та принципів побудови комп'ютерних мереж на базі стеку протоколів TCP/IP, а також практичні навички застосування мережних технологій для вирішення різноманітних завдань.

Предмет дисципліни – теоретичні та практичні основи передачі даних в комп'ютерних мережах, які забезпечують необхідний рівень швидкості, надійності та безпеки.

Дисципліна «Мережні технології» забезпечує наступні програмні компетентності і програмні результати освітньо-професійної програми: ФК1, ФК3, ФК6, ФК7, ФК8, ФК10, ПРН1, ПРН3, ПРН5, ПРН7, ПРН8, ПРН11, ПРН16:

- здатність до визначення технічних характеристик, конструктивних особливостей, застосування і експлуатації програмних, програмно-технічних засобів, комп'ютерних систем та мереж різного призначення;

- здатність проектувати комп’ютерні системи та мережі з урахуванням цілей, обмежень, технічних, економічних та правових аспектів;

- здатність використовувати та впроваджувати нові технології, включаючи технології розумних, мобільних, зелених і безпечних обчислень, брати участь в модернізації та реконструкції комп’ютерних систем та мереж, різноманітних вбудованих і розподілених додатків, зокрема з метою підвищення їх ефективності;

- здатність досліджувати, розробляти та обирати технології створення великих і надвеликих систем;

- здатність забезпечувати якість продуктів і сервісів інформаційних технологій протягом їх життєвого циклу;

- здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп’ютерних систем, мереж та їхніх компонентів.

Згідно програми навчальної дисципліни студенти після засвоєння дисципліни мають продемонструвати такі програмні результати навчання.

Знання:

- призначення та функції рівнів еталонної моделі взаємодії відкритих систем;

- функції та властивості основних протоколів стеку TCP/IP;

- механізми безпечної передачі даних в комп’ютерних мережах;

- механізмів автентифікації користувачів в комп’ютерних мережах;

- принципів побудови віртуальних приватних мереж;

- механізмів функціонування інфраструктури відкритих ключів.

Уміння:

- налаштовувати параметри мережних інтерфейсів в операційній системі GNU/Linux;

- встановлювати та налагоджувати мережні сервіси в операційній системі GNU/Linux;

- виконувати пошук та виправлення помилок в роботі мережних сервісів;

- забезпечувати необхідний рівень безпеки при передачі даних в комп’ютерних мережах;

- виконувати розрахунки параметрів мережі, побудованої на базі стеку протоколів TCP/IP.

Досвід:

- роботи з аналізаторами та генераторами мережного трафіку;

- роботи в командному рядку операційної системи GNU/Linux;

- керування режимами обробки мережного трафіку ядром операційної системи GNU/Linux.

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Для успішного засвоєння дисципліни «Мережні технології» відповідно до освітньої програми необхідно попередньо оволодіти знаннями з дисциплін: «Вступ до операційної системи Linux», «Комп'ютерні мережі», «Захист інформації в комп’ютерних системах та мережах».

Компетентності, знання та вміння, отримані в рамках вивчення дисципліни «Мережні технології», можуть бути застосовані для створення нових та вдосконалювати існуючих технологій передачі

даних в комп'ютерних мережах, розробки програмного забезпечення з врахуванням особливостей функціонування мережних сервісів Інтернет.

3. Зміст навчальної дисципліни

Розділ 1. Мережний рівень стеку протоколів TCP/IP.

Тема 1.1. Еталонна модель взаємодії відкритих систем (ISO/OSI).

Тема 1.2. Протокол IP.

Тема 1.3. IP-адресація.

Тема 1.4. Допоміжні протоколи мережного рівня.

Тема 1.5. Протокол DHCP.

Розділ 2. Транспортний рівень стеку протоколів TCP/IP.

Тема 2.1. Транспортний рівень стеку TCP/IP.

Тема 2.2. Протокол UDP.

Тема 2.3. Протокол TCP.

Тема 2.4. Трансляція мережних адрес.

Розділ 3. Кібербезпека.

Тема 3.1. Основні відомості про кібербезпеку.

Тема 3.2. Фільтрація пакетів за допомогою iptables.

Тема 3.3. Віртуальні приватні мережі - VPN.

Тема 3.4. Захист віртуальних каналів на мережному рівні.

Тема 3.5. Інфраструктура відкритих ключів.

Тема 3.6. Автентифікація користувачів в комп’ютерних мережах.

Тема 3.7. Протоколи OAuth та OpenID.

Тема 3.8. Протоколи SSL і TLS.

4. Навчальні матеріали та ресурси

Базова література.

1. Evi Nemeth, Garth Snyder, Trent Hein, Ben Whaley, Dan Mackin. UNIX and Linux System Administration Handbook, 5th Edition. Addison-Wesley Professional, 2017. – 1232 p.
2. James Kurose, Keith Ross. Computer Networking: A Top-Down Approach, Global Edition, 8th Edition. Pearson Education, 2021.

Допоміжна література.

1. Tanenbaum, A. S., Bos, H. J. Modern Operating Systems, 4th Edition. Pearson Higher Education, 2015. – 1137 p.
2. Larry Peterson, Bruce Davie. Computer Networks: A Systems Approach, 2019. – 489 p. URL: https://github.com/SystemsApproach/book/releases/download/v6.1/book.pdf
3. Peter L Dordal. An Introduction to Computer Networks, 2021. – 947 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

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

5.1. Лекційні заняття

№ лекції	Назва теми лекції та перелік основних питань	Кількість ауд. годин
1	**Еталонна модель взаємодії відкритих систем (ISO/OSI).** Структура курсу. Проблеми побудови мереж. Протокол. Інтерфейс. Інкапсуляція. Рівні моделі OSI. Функції рівнів моделі OSI. Протокольний блок даних. Стек протоколів TCP/IP. Порівняння OSI та TCP/IP. **СРС:** Познайомитись з альтернативними стеку TCP/IP реалізаціями еталонної моделі взаємодії відкритих систем.	2
2	**Протокол IP.** Місце протоколу IP в моделях OSI і TCP/IP. Сервіси протоколу IP. Формат IP-пакета для 4-ї та 6-ї версій протоколу. Маршрутизація. Структура таблиці маршрутизації. **СРС:** Познайомитись з реалізаціями механізмів якості обслуговування (QoS) в протоколі IP.	2
3	**IP-адресація.** Глобальні і локальні адреси. Структура IP-адреси. Класи IP-адрес. Безкласова маршрутизація (Classless Inter-Domain Routing, CIDR). Маска підмережі. Спеціальні IP-адреси. **СРС:** Познайомитись з взаємодією мережного і канального рівнів під час передачі пакетів.	2
4	**Допоміжні протоколи мережного рівня.** Протокол ICMP. Формат заголовку ICMP. Типи ICMP-повідомлень. Утиліти ping та traceroute. Протокол ARP. Формат ARP-повідомлення. ARP-таблиця. **СРС:** Познайомитись з мережними атаками, які використовують протоколи ARP та ICMP.	2
5	**Протокол DHCP.** Способи конфігурації параметрів мережних інтерфейсів.	2

№ лекції	Назва теми лекції та перелік основних питань	Кількість ауд. годин
	Повідомлення протоколу DHCP. Конфігураційна інформація DHCP. Схема роботи протоколу DHCP. Ретранслятор DHCP. Часові параметри оренди IP-адреси. **СРС:** Познайомитись з мережними атаками, які використовують протокол DHCP.	
6	**Транспортний рівень стеку TCP/IP.** Призначення транспортного рівня. Надійність передачі даних. Типи портів. Перегляд з'єднань і портів. Транспортні протоколи стеку TCP/IP. **СРС:** Познайомитись з протоколами SCTP, DCCP.	2
7	**Протокол UDP.** Призначення протоколу UDP. Формат заголовку UDP. Мережні сервіси, які використовують UDP. **СРС:** Познайомитись з мережними атаками, які використовують протокол UDP.	2
8	**Протокол TCP.** Призначення протоколу TCP. Формат заголовку TCP. Встановлення та завершення з'єднання в TCP. Вікно підтвердження TCP. Керування потоком в TCP. Контроль перевантаження в TCP. **СРС:** Познайомитись з механізмами контролю перевантаження: cubic, vegas, veno, westwood, illinois, hybla, reno.	2
9	**Трансляція мережних адрес.** Причини використання NAT. Статичний NAT. Динамічний NAT. Перевантажений NAT. Схема роботи NAPT. Переваги та недоліки використання NAT. **СРС:** Познайомитись з механізмом обходу NAT (NAT traversal).	2
10	**Основні відомості про кібербезпеку.** Терміни і визначення. Трикутник інформаційної безпеки. Загрози інформаційної безпеки. Типи атак. Механізми захисту від атак. Протоколи захищеного каналу. **СРС:** Познайомитись з системою виявлення вторгнень (IDS).	2
11	**Фільтрація пакетів за допомогою iptables.** Типи брандмауерів. Архітектура iptables. Таблиці, ланцюжки та правила в iptables. Шлях перевірки пакета в iptables. **СРС:** Фільтрація на прикладному рівні в iptables.	2
12	**Фільтрація пакетів за допомогою iptables.** Призначення та дії в таблицях mangle, nat, filter, security, raw. Критерії відповідності пакету правилу. **СРС:** Познайомитись з інструментами регулювання пропускної здатності каналів у Linux (Traffic shaping).	2
13	**Віртуальні приватні мережі - VPN.**	2

№ лекції	Назва теми лекції та перелік основних питань	Кількість ауд. годин
	Поняття про віртуальні приватні мережі (VPN). Види віртуальних приватних мереж. Сервіси VPN. Способи утворення захищених тунелів. Рівні реалізації VPN. Протоколи: IPSec, PPTP, L2F, L2TF. **СРС:** Познайомитись з реалізацією VPN на базі пакету openvpn (https://openvpn.net/).	
14	**Захист віртуальних каналів на мережному рівні.** Архітектура засобів захисту IPSec. Транспортний та тунельний режими IPSec. Протокол AH. Протокол ESP. Протокол IKE. Асоціації захисту (SA). **СРС:** Познайомитись з реалізацією IPSec в ОС GNU/Linux на базі пакету strongSwan (https://www.strongswan.org/).	2
15	**Інфраструктура відкритих ключів.** Можливості PKI. Основні компоненти інфраструктури відкритих ключів та їх функції. Формат сертифікатів відкритих ключів X.509. Електронний цифровий підпис. Автентифікація за допомогою сертифікатів. **СРС:** Створити за допомогою утиліти openssl власний центр сертифікації (CA), створити сертифікати вузла та користувача.	2
16	**Автентифікація користувачів в комп'ютерних мережах.** Типи протоколів автентифікації. Протокол Kerberos. Протокол LDAP. Протокол RADIUS. Способи багатофакторної автентифікації. **СРС:** Познайомитись з реалізацією протоколу RADIUS (https://freeradius.org/).	2
17	**Протоколи OAuth та OpenID.** Основні компоненти протоколу OAuth та їх функції. Схема авторизації в OAuth. Основні компоненти протоколу OpenID та їх функції. Протокол OpenID Connect. Переваги та недоліки протоколів OAuth та OpenID. **СРС:** Познайомитись з технологією єдиного входу (Single sign-on).	2
18	**Протоколи SSL і TLS.** Версії протоколів SSL і TLS. Протокол встановлення з'єднання. Автентифікація, хешування, режими шифрування. Генерація ключа сесії. Протокол передачі записів. Цілі створення TLS 1.3. **СРС:** Познайомитись з механізмами автентифікації в TLS.	2
	Разом:	36

5.2. Лабораторні заняття (комп'ютерний практикум).

Основне завдання циклу лабораторних занять (комп'ютерного практикуму) - отримання студентами необхідних практичних навиків роботи зі стеком протоколів TCP/IP.

Для успішного засвоєння дисципліни кожному студенту необхідно підготувати робоче місце у вигляді чотирьох віртуальних машин. Рекомендується використовувати систему віртуалізації VirtualBox (https://www.virtualbox.org/wiki/Downloads)

Для проведення лабораторних робіт у якості дистрибутива рекомендується використовувати Debian (https://www.debian.org/download) однієї з останніх стабільних версій. Для зменшення вимог по ресурсам до апаратної платформи можна використовувати варіант встановлення операційної системи без графічного інтерфейсу.

Для повноцінного виконання всіх лабораторних робіт кожна віртуальна машина повинна мати підключення до мережі Інтернет.

№ з/п	Назва лабораторної роботи (комп'ютерного практикуму)	Кількість ауд. годин
1	**Діагностичні утиліті стеку протоколів TCP/IP.** Знайомство з утилітами, які використовуються для діагностики та пошуку помилок в роботі стеку протоколів TCP/IP: ping, traceroute, nslookup, dig, netstat, nmap, tcpdump, telnet, nc, scapy.	5
2	**Динамічне конфігурування мережних інтерфейсів за допомогою протоколу DHCP.** Налаштування серверу DHCP на базі ОС GNU/Linux.	4
3	**Маршрутизація в IP-мережах.** Налаштування програмного маршрутизатора на базі ОС GNU/Linux, який реалізує статичну та динамічну маршрутизацію (RIP, OSPF).	4
4	**Засоби фільтрації IP-пакетів. Технологія трансляція мережних адрес (NAT).** Налаштування мережного фільтру та сервісу трансляції адрес і портів за допомогою iptables у ОС GNU/Linux.	5
	Разом:	18

6. Самостійна робота студента/аспіранта

6.1. Теми, які виносяться на самостійне опрацювання.

№ з/п	Назва теми, що виноситься на самостійне опрацювання	Кількість годин СРС
1	Генератор мережного трафіку scapy	2
2	Протокол маршрутизації BGP.	2
3	Механізми керування перевантаженням в протоколі TCP.	2
	Разом:	6

Перед кожним аудиторним заняттям студент виконує самостійну підготовку відповідно до теми лекції або лабораторної роботи не менше двох годин. Підготовка до заліку має складати не менше 8 годин.

Таким чином самостійна робота студента протягом семестру має складати: 36 + 16 + 8 + 6 = 66 годин.

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Система вимог, які ставляться перед студентом:
- для успішного вивчення дисципліни бажана присутність на всіх лекціях;
- на лекціях дозволяється використовувати будь-яку техніку тільки з метою, яка стосується заняття, не заважаючи іншим студентам та викладачу;
- під час лекції можна ставити питання викладачу, для цього необхідно підняти руку і отримати дозвіл;
- на лекціях забороняється розмовляти без дозволу викладача;
- на лекціях забороняється займатися діяльністю, яка прямо не стосується навчальної дисципліни;
- лабораторні роботи проходять у формі комп'ютерного практикуму;
- на лабораторних заняттях мають бути присутніми тільки студенти, які готові до захисту роботи;
- під час захисту лабораторної роботи студент має продемонструвати виконане за варіантом завдання та відповісти на запитання викладача (запитання з теорії, практична задача, тощо);
- варіанти (якщо поділ на варіанти передбачено у завданні) на лабораторні роботи обираються таким чином: перші 15 студентів отримують варіанти відповідно номеру у списку групи, студент з номером 16 у списку отримує варіант 1 і т.д.
- штрафні бали за несвоєчасний захист лабораторних робіт не нараховуються;
- захищати лабораторні роботи можна в довільній послідовності;
- повторний захист лабораторних робіт заборонений;
- забороняється використовувати сторонню допомогу під час захисту лабораторних робіт.

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Підсумкова рейтингова оцінка студента з дисципліни «Мережні технології» складається з балів, які він отримує:
– за навчальну роботу впродовж семестру;
– за залікову співбесіду.

8.1. Нарахування балів .
Протягом семестру студент виконує 4 лабораторні роботи.
За кожну лабораторну роботу студент отримує:
- 15 балів за виконане в повному обсязі та без суттєвих помилок завдання на лабораторну роботу;
- від 0 до 10-ти балів за захист лабораторної роботи, який складається з теоретичних запитань, практичних завдань, короткої доповіді на тему (на вибір студента).

8.2. Умови допуску до заліку.
Щоб отримати допуск до заліку необхідно захистити 4 лабораторні роботи.

8.3. Студенти, які виконали всі умови допуску до заліку та мають суму балів за навчальну роботу впродовж семестру 60 і більше, отримують відповідну до набраної суми балів оцінку без додаткових випробувань.

8.4. Для студентів, які виконали всі умови допуску до заліку та мають суму балів за навчальну роботу впродовж семестру менше 60, а також студентів, які бажають підвищити свою оцінку на останньому за розкладом занятті в семестрі проводиться залікова співбесіда. При цьому до суми балів за навчальну роботу впродовж семестру застосовується коефіцієнт 0,6.

8.5. Нарахування балів за залікову співбесіду.
На заліковій співбесіді студенти мають відповісти на три теоретичних питання. Кожне теоретичне питання оцінюється у 20 балів.
Система оцінювання теоретичних питань:
18-20 балів – повна відповідь (не менше 90% потрібної інформації);
15-17 балів – достатньо повна відповідь (не менше 75% потрібної інформації, або незначні неточності);
12-14 балів – неповна відповідь (не менше 60% потрібної інформації та деякі помилки);
0 балів – незадовільна відповідь (менше 60% потрібної інформації або суттєві помилки).

Сума балів за навчальну роботу впродовж семестру та балів за залікову співбесіду, якщо вона проводилась, переводиться до залікової оцінки згідно з таблицею:

Кількість балів	Оцінка
100-95	Відмінно
94-85	Дуже добре
84-75	Добре
74-65	Задовільно
64-60	Достатньо
Менше 60	Незадовільно
Не виконані умови допуску	Не допущено

9. Додаткова інформація з дисципліни (освітнього компонента)

Під час проведення лекційних занять необхідно окрім презентацій використовувати термінал для демонстрації живих прикладів. Це дасть можливість студенту глибше засвоїти матеріал лекції.

9.1. Перелік теоретичних питань на залікову співбесіду.

- Еталонна модель взаємодії відкритих систем (ISO/OSI).
- Багаторівнева структура стеку TCP/IP.
- Прикладний рівень.
- Транспортний рівень.
- Мережний рівень.
- Рівень мережних інтерфейсів.
- Відповідність рівнів стеку TCP/IP моделі ISO/OSI.
- Основні протоколи стеку TCP/IP, їх призначення.
- Основні функції протоколу IP.
- Загальний сценарій роботи модуля IP.
- Формат заголовку IPv4.
- Формат заголовку IPv6.
- Адресація в IP-мережах.
- Особливі IP-адреси.
- Використання масок в IP-адресації.

- Поняття про маршрутизацію. Основні принципи маршрутизації.
- Структура таблиць маршрутизації в IP-мережах.
- Динамічна маршрутизація.
- Протокол RIP.
- Протокол OSPF.
- Протокол BGP.
- Протокол DHCP.
- Агент ретрансляції DHCP.
- Трансляція мережних адрес (NAT). Причини підміни адрес.
- Трансляція мережних адрес і номерів портів.
- Обмеження NAT. NAT і ICMP.
- Протокол перетворення адрес ARP.
- Протокол зворотного перетворення адрес RARP.
- Міжмережний протокол керуючих повідомлень ICMP.
- Утиліта Traceroute. Способи визначення маршруту просування IP-пакетів.
- Протокол UDP.
- Протокол TCP.
- Встановлення та завершення TCP-з'єднання.
- Послідовний номер і номер підтвердження в TCP.
- Вікно прийому TCP.
- Основні відомості про кібербезпеку.
- Особливості безпеки комп'ютерних мереж.
- Класифікація віддалених атак на розподілені обчислювальні системи.
- Механізми захисту від атак.
- Принципи роботи і види мережних фільтрів.
- Шлях перевірки пакета в iptables.
- Ланцюжки та таблиці в iptables, їх призначення.
- Правила iptables.
- Поняття про віртуальні приватні мережі VPN.
- Види віртуальних приватних мереж.
- Архітектура засобів захисту IPSec.
- Інфраструктура відкритих ключів PKI.
- Структура сертифікату X.509.
- Електронний цифровий підпис.
- Протоколи TLS/SSL.
- Протокол встановлення з'єднання TLS/SSL.

9.2. Додаткові Інформаційні ресурси

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

Робочу програму навчальної дисципліни (силабус):

Склав доцент кафедри обчислювальної техніки, к.т.н. Роковий Олександр Петрович.

Ухвалено кафедрою обчислювальної техніки (протокол № 10 від 25.05.2022)

Погоджено Методичною комісією факультету інформатики та обчислювальної техніки (протокол № 10 від 09.06.2022)