Міжнародний гуманітарний університет
Факультет кібербезпеки, програмної інженерії та комп'ютерних наук

Кафедра комп'ютерної інженерії та інноваційних технологій

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
Комп'ютерні мережі

Галузь знань 12 Інформаційні технології
Спеціальність 125 Кібербезпека та захист інформації
Назва освітньої програми Кібербезпека
Рівень вищої освіти перший (бакалаврський) рівень

Розробники і викладачі	Контактний тел.	E-mail
доцент кафедри комп'ютерної інженерії та інноваційних технологій, кандидат технічних наук, доцент, **Педяш Володимир Віталійович**	+38067-37 87 003	vpedyash@gmail.com

1. АНОТАЦІЯ ДО КУРСУ

Комп'ютерні мережі — це фундаментальна дисципліна професійного циклу, спрямована на формування системного розуміння організації, архітектури та функціонування сучасних інформаційно-комунікаційних систем. Курс охоплює універсальні концепції, реалізовані в різних типах мереж — від локальних (LAN) до глобальних (WAN), незалежно від конкретних виробників обладнання. Основна увага приділяється еталонним моделям взаємодії (OSI, TCP/IP), механізмам IP-адресації, маршрутизації, сегментації трафіку, базовим методам захисту мережевої інфраструктури та засобам централізованого моніторингу.

Знання, отримані в рамках дисципліни, є необхідною основою для майбутніх фахівців з кібербезпеки, оскільки розуміння принципів побудови та функціонування мереж дає змогу ефективно виявляти, аналізувати та протидіяти кіберзагрозам. Навички моделювання, налаштування та діагностики мережевих систем забезпечують підготовку до виконання професійних завдань, пов'язаних із захистом інформаційних ресурсів у складних мережевих середовищах.

Метою дисципліни є формування у студентів цілісного уявлення про мережеві технології та розвиток практичних навичок проектування, налаштування й аналізу безпечних мереж. Курс спрямований на досягнення програмних результатів навчання, передбачених стандартом вищої освіти за спеціальністю 125 "Кібербезпека та захист інформації", зокрема таких, як здатність аналізувати інфраструктурні ризики, застосовувати механізми сегментації та фільтрації трафіку, а також використовувати інструменти моніторингу для виявлення інцидентів безпеки. Зміст дисципліни узгоджено з освітньо-професійною програмою підготовки фахівців з кібербезпеки та забезпечує необхідну теоретичну й практичну базу для подальшого вивчення дисциплін із захисту інформації, аналізу кіберзагроз та реагування на інциденти.

ПРЕРЕКВІЗИТИ. Передумовами є базові знання з програмування («Основи програмування», ОК 8), архітектурних принципів («Комп'ютерна схемотехніка та архітектура комп'ютерів», ОК 15, паралельно), а також знання з фізики (ОК 7) та математики (ОК 5).

ПОСТРЕКВІЗИТИ. Знання принципів побудови та функціонування комп'ютерних мереж є основою для вивчення «Захисту інформації в інфокомунікаційних системах та мережах» (ОК 12), «Основ Web-безпеки» (ОК 22), «Web-технологій» (ОК 14), «Комплексних систем захисту інформації» (ОК 24), «Управління інформаційною та кібербезпекою» (ОК 30), «Безпеки бездротових мереж Інтернету речей (IoT)» (ОК 27) та «Етичного хакінгу та тестування на проникнення» (ОК 18).

2. ОЧІКУВАНІ КОМПЕТЕНТНОСТІ, ЯКІ ПЛАНУЄТЬСЯ СФОРМУВАТИ ТА ДОСЯГНЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ

У процесі реалізації програми дисципліни «Комп'ютерні мережі» формуються наступні компетентності із передбачених освітньою програмою:

Інтегральна компетентність

ІК. Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі кібербезпеки та захисту інформації.

Загальні компетентності (ЗК)

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності

Спеціальні (фахові, предметні) компетентності

СК 3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.

СК 4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

СК 5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.

СК 10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

СК 11. Здатність здійснювати проєктування, адміністрування та керування інформаційно-комунікаційними системами, забезпечуючи їхню надійність, безпеку та ефективність функціонування.

Навчальна дисципліна «Комп'ютерні мережі» забезпечує досягнення програмних результатів навчання (РН), передбачених освітньою програмою:

РН 4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність

РН 5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення

РН 7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності

РН 10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

РН 11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.

РН 12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

РН 13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому.

РН 14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.

РН 21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

РН 22. Вміти застосовувати методи та інструменти проєктування й адміністрування мереж і систем, виконувати налаштування, моніторинг та підтримку їхньої працездатності з урахуванням вимог інформаційної безпеки.

3. ОБСЯГ ТА ОЗНАКИ КУРСУ

Загалом		**Вид заняття** (денне відділення / заочне відділення)				**Ознаки курсу**		
ЄКТС	**годин**	**Лекційні заняття**	**Лабораторні заняття**	**Практичні заняття**	**Самостійна робота**	**Курс, (рік навчання)**	**Семестр**	**Обов'язкова / вибіркова**
4	120	26/4	12/4	14/2	68/110	2	3	**Обов'язкова**

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин									
	денна форма					Заочна форма				
	усього	у тому числі				усього	у тому числі			
		лекц.	лаб.	прак.	сам. роб.		лекц.	лаб.	прак.	сам. роб.
Тема 1. Основи комп'ютерних мереж та їх роль у забезпеченні інформаційної безпеки	14	2		2	10	17	2			15
Тема 2. Моделі мережної взаємодії OSI та TCP/IP у контексті безпеки	16	4	2	2	8	15				15
Тема 3. Фізичний та канальний рівні – технології, протоколи, вразливості та засоби захисту	18	4	2	2	10	15				15
Тема 4. Мережний рівень – IP-адресація, маршрутизація та їх роль у безпеці мереж	18	4	2	2	10	19	2	2		15
Тема 5. Транспортний та прикладний рівні – протоколи, уразливості та механізми захисту	18	4	2	2	10	15				15
Тема 6. Базові механізми безпеки мережевої інфраструктури	18	4	2	2	10	17		2		15
Тема 7. Проектування, моделювання та моніторинг безпечних мереж	18	4	2	2	10	22			2	20
Усього годин	**120**	**26**	**12**	**14**	**68**	**120**	**4**	**4**	**2**	**110**
ПІДСУМКОВИЙ КОНТРОЛЬ – ЕКЗАМЕН										

5. ТЕХНІЧНЕ Й ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ / ОБЛАДНАННЯ

Студенти отримують теми та питання курсу, основну і додаткову літературу, рекомендації, завдання та оцінки за їх виконання як традиційним шляхом, так і з використанням університетської платформи он-лайн навчання на базі Moodle. Окрім того, практичні навички у пошуку та аналізу інформації за курсом, з оформлення індивідуальних завдань, тощо, студенти отримують, користуючись університетськими комп'ютерними класами та бібліотекою.

6. САМОСТІЙНА РОБОТА

До самостійної роботи студентів щодо вивчення дисципліни «Комп'ютерні мережі» включаються:

1. Знайомство з науковою та навчальною літературою відповідно зазначених у програмі тем.
2. Опрацювання лекційного матеріалу.
3. Підготовка до практичних занять.
4. Консультації з викладачем протягом семестру.
5. Самостійне опрацювання окремих питань навчальної дисципліни.
6. Підготовка та виконання індивідуальних завдань у вигляді есе, рефератів тощо.
7. Підготовка до підсумкового контролю.

Тематика та питання до самостійної підготовки та індивідуальних завдань

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Тема 1. Основи комп'ютерних мереж та їх роль у забезпеченні інформаційної безпеки** Поняття комп'ютерної мережі. Класифікація мереж за географічним охопленням: LAN, MAN, WAN, PAN. Фізична та логічна топології. Основні типи мережевого обладнання: комутатори, маршрутизатори, точки доступу, міжмережеві екрани. Зв'язок архітектури мережі з організацією захисту інформації.	10	15
2	**Тема 2. Моделі мережної взаємодії OSI та TCP/IP у контексті безпеки** Семирівнева модель OSI та чотирирівнева модель TCP/IP, їх функції та відповідність. Інкапсуляція даних у стеку протоколів. Уразливості на різних рівнях моделі. Небезпечні протоколи: Telnet, HTTP, SNMPv1. Роль моделей у діагностиці мережевих інцидентів.	8	15
3	**Тема 3. Фізичний та канальний рівні – технології, протоколи, вразливості та засоби захисту** Середовища передачі: вита пара, оптичне волокно, бездротові технології. Протокол Ethernet, структура кадру, MAC-адресація. Принципи роботи комутаторів та формування CAM-таблиць. Загрози канального рівня: ARP-спуфінг, MAC-флудінг. Методи захисту: Port Security, STP Guard, сегментація VLAN.	10	15
4	**Тема 4. Мережний рівень – IP-адресація, маршрутизація та їх роль у безпеці мереж** Структура IPv4-пакета, підмережування, VLSM. Основи IPv6: формати адрес, типи, особливості безпеки. Таблиця маршрутизації та типи маршрутів. Загрози мережного рівня: IP-спуфінг, маршрутизаційні атаки. Значення правильної адресації та маршрутизації для запобігання інцидентам.	10	15
5	**Тема 5. Транспортний та прикладний рівні – протоколи, уразливості та механізми захисту** Протоколи TCP та UDP: надійність, порти, структура сегментів. Прикладні протоколи: DNS, DHCP, HTTP(S), SMTP, FTP. Типові загрози: DoS-атаки, підміна DNS, перехоплення трафіку. Засоби захисту: шифрування, використання TLS/SSL, фільтрація трафіку.	10	15
6	**Тема 6. Базові механізми безпеки мережевої інфраструктури** Безпечний доступ до обладнання через SSH. Настройка автентифікації, шифрування паролів, рівнів привілеїв. Списки контролю доступу (ACL): типи, синтаксис, застосування для фільтрації трафіку. Сегментація мережі за допомогою VLAN та ACL для обмеження поширення інцидентів.	10	15

7	**Тема 7. Проектування, моделювання та моніторинг безпечних мереж** Етапи проектування безпечної мережі: аналіз вимог, сегментація, IP-планування, вибір обладнання. Принципи безпеки при проектуванні. Моделювання мереж у Cisco Packet Tracer. Основи централізованого моніторингу: Syslog, SNMP. Виявлення та реагування на мережеві аномалії.	10	20
	Всього	**68**	**110**

7. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Види контролю	**Складові оцінювання**	
	Для екзамену	**Для заліку**
поточний контроль, який здійснюється у ході: проведення практичних (лабораторних) занять, виконання самостійної роботи, індивідуальних завдань, дослідна робота здобувача тощо.	**50%**	**100%**
підсумковий контроль	**50%**	

Методи діагностики знань (контролю)	фронтальне опитування; наукова доповідь, реферати, усне повідомлення, індивідуальне опитування; робота у групах; ділова гра, розв`язання ситуаційних завдань, кейсів, практичних завдань, екзамен

8. ОЦІНЮВАННЯ ЗДОБУВАЧІВ ВИЩОЇ ТА ФАХОВОЇ ПЕРДВИЩОЇ ОСВІТИ ЗА НАВЧАЛЬНУ ДИСЦИПЛІНУ У МІЖНАРОДНОМУ ГУМАНІТАРНОМУ УНІВЕРСИТЕТІ

(*поточний контроль, підсумковий контроль, загальний результат оцінювання)*

ЕКЗАМЕН

Поточний контроль			
Види роботи	**Планові терміни виконання**	**Форми контролю та звітності**	**Максимальний відсоток оцінювання**
Систематичність і активність роботи на практичних (лабораторних) заняттях			
1.1. Підготовка до практичних (лабораторних) занять	Відповідно до робочої програми та розкладу занять	Перевірка обсягу та якості засвоєного матеріалу під час практичних (лабораторних) занять	**30**
Виконання завдань для самостійного опрацювання			

1.2. Індивідуальне тестування, завдання, підготовка реферату (есе) за заданою тематикою	Відповідно до робочої програми та розкладу занять	Розгляд відповідного матеріалу під час аудиторних занять або ІКР[1], перевірка конспектів навчальних текстів тощо	**10**
Виконання індивідуальних завдань, дослідна робота здобувача			
1.3. Інші види індивідуальних завдань, в т.ч. підготовка наукових публікацій, участь у роботі круглих столів, конференцій тощо.	Відповідно до робочої програми та розкладу занять	Обговорення результатів проведеної роботи під час аудиторних занять, наукових конференцій та круглих столів.	**10**
Разом балів за поточний контроль			**50**
Підсумковий контроль екзамен			**50**
Загальний результат оцінювання			**100**

Поточний контроль знань здобувачів освіти при формі контролю **екзамен** (максимум 50 балів) оцінюється за шкалою *(«2», «3», «4», «5»)*, з обов'язковим переведенням балів за кожний вид роботи таким чином:

- за підготовку до аудиторних занять (максимум 30 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості практичних (лабораторних) занять, для переводу балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 6;
- за виконання завдань для самостійного опрацювання (тестування, завдання, підготовка реферату (есе) за заданою тематикою) (максимум 10 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості програмного матеріалу, що виноситься на самостійне вивчення, для переводу зазначених балів середньоарифметична оцінка множиться на коефіцієнт 2;
- за інші види індивідуальних завдань, в т.ч. підготовку наукових публікацій, участь у роботі круглих столів, конференцій тощо (максимум 10- балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості інших видів індивідуальних завдань, для переводу балів за пдготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 2.

КРИТЕРІЇ ОЦІНЮВАННЯ ЗА ПОТОЧНИЙ КОНТРОЛЬ

- «2»- виставляється за неправильну відповідь (письмову роботу), яка не відповідає змісту теми та свідчить про нерозуміння її основних положень;
- «3» -виставляється за відповідь (письмову роботу), яка відповідає змісту теми, але є неповною і неточною у визначенні понять, свідчить про неповне розуміння основних положень навчального матеріалу, свідчить про те, що знання студента мають фрагментарний, поверховий характер;
- «4» - оцінюється правильна і обґрунтована відповідь (письмова робота), з якої видно, що студент знає й розуміє теоретичний матеріал в обсязі навчальної теми, володіє необхідними навичками, не допускає суттєвих помилок.
- «5» - оцінюється повна, правильна, ґрунтовна відповідь (письмова робота) на запитання теми, що передбачає логічність і послідовність викладу матеріалу, володіння термінологією, показує вміння повно й глибоко використовувати теоретичні знання в практичній площині.

[1] Індивідуально-консультативна робота викладача зі здобувачами

КРИТЕРІЇ ОЦІНЮВАННЯ ПІДСУМКОВОГО КОНТРОЛЮ ЗНАНЬ ЗДОБУВАЧІВ ЗА ІСПИТ
(максимум 50 балів)

Рівень знань оцінюється:

- від 40 до 50 балів - студент виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки;
- 30 до 40 балів - студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді;
- 20 - 30 балів - студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки.
- 10 - 20 балів - володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих;
- 0 10 балів - володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки.

9. КРИТЕРІЇ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗДОБУВАЧІВ
(для екзамену / заліку)

Рівень знань оцінюється:

- «відмінно» / «зараховано» A - від 90 до 100 балів. Студент виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки. Був присутній на лекціях та семінарських заняттях, під час яких давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;
- «добре» / «зараховано» B - від 82 до 89 балів. Студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді. Був присутній на лекціях та семінарських заняттях, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;
- «добре» / «зараховано» C - від 74 до 81 балів. Студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, реферату та активність у науково-дослідній роботі;
- «задовільно» / «зараховано» D - від 64 до 73 балів. Студент був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, рефератів (есе);
- «задовільно» / «зараховано» E - від 60 до 63 балів. Студент був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки, має неповний конспект з завданнями до самостійної роботи.
- «незадовільно з можливістю повторного складання» / «не зараховано» FX – від 35 до 59 балів. Студент володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу.

- «незадовільно з обов'язковим повторним вивченням дисципліни» / «не зараховано» F – від 0 до 34 балів. Студент не володіє навчальним матеріалом.

ТАБЛИЦЯ ВІДПОВІДНОСТІ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗА РІЗНИМИ ШКАЛАМИ

100-бальною шкалою	Шкала за ECTS	За національною шкалою	
		екзамен	залік
90-100	A	Відмінно	Зараховано
82-89	B	Добре	
74-81	C		
64-73	D	Задовільно	
60-63	E		
35-59	Fx	Незадовільно	Не зараховано
1-34	F		

10. ДОТРИМАННЯ ВИМОГ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ

Викладання та засвоєння навчальної дисципліни передбачає неухильне дотримання вимог академічної доброчесності, яка регулюється Законом України "Про освіту" (Відомості Верховної Ради (ВВР), 2014, № 37-38, ст.2004), «Методичними рекомендаціями для закладів вищої освіти з підтримки принципів академічної доброчесності» (Лист МОН № 1/9-650 від 23.10.18 року), іншими нормативними документами. Зокрема, основні засади дотримання академічної доброчесності визначено у «Положенні про академічну доброчесність у Міжнародному гуманітарному університеті», «Кодексі академічної доброчесності Міжнародного гуманітарного університету» та «Інструкції щодо процедури технічної перевірки на наявність текстових запозичень (академічного плагіату)», затвердженої наказом МГУ від 03.05.2024 р., № 708а.

Відповідно до ст.42 Закону України "Про освіту" академічна доброчесність - це сукупність етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання та/або наукових (творчих) досягнень.

Дотримання академічної доброчесності передбачає:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);
- посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;
- дотримання норм законодавства про авторське право і суміжні права;
- надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

11. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Жураковський Б. Ю. Комп'ютерні мережі. Частина 1. [навчальний посібник] / Б. Ю. Жураковський, І.О. Зенів. – Київ : КПІ ім. Ігоря Сікорського, 2020. – 336 с.
2. Педяш В. В. Комп'ютерні мережі : методичні рекомендації для практичних та лабораторних занять (частина 1) [Електронне видання] / В. В. Педяш, Л. Г. Йона, Г. Д. Мазур ; Кафедра комп'ютерної інженерії та інноваційних технологій Міжнародного гуманітарного університету. — Одеса, 2025. — 123 с. — Режим доступу: https://hdl.handle.net/11300/32280
3. Педяш В. В. Комп'ютерні мережі : метод. реком. для практичних та лабораторних занять (частина 2) [Електронне видання] / В. В. Педяш, Л. Г. Йона, Г. Д. Мазур ; Кафедра комп'ютерної інженерії та інноваційних технологій Міжнародного гуманітарного університету. — Одеса, 2025. — 142 с. — Режим доступу: https://hdl.handle.net/11300/32281
4. Педяш В.В. Збірник методичних вказівок для виконання індивідуального завдання з дисципліни "Комп'ютерні мережі". Кафедра комп'ютерних наук Міжнар. гуманітар. ун-ту. 2024, МГУ, Одеса. - 40 с.

5. Б. Ю. Жураковський. Комп'ютерні мережі. Частина 2. [навчальний посібник] / Б. Ю. Жураковський, І.О. Зенів. – Електронні текстові дані. – Київ : КПІ ім. Ігоря Сікорського, 2020. – 372 с.
6. Азаров О. Д. Комп'ютерні мережі : підручник / О. Д. Азаров, С. М. Захарченко, О. В. Кадук та ін. − Вінниця : ВНТУ, 2020. − 378 с.
7. Карпенко М. Ю. Конспект лекцій з курсу «Комп'ютерні мережі» / М. Ю. Карпенко, Н. В. Макогон; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Харків : ХНУМГ ім. О. М. Бекетова, 2019. – 99 с.
8. Блозва А.І. Комп'ютерні мережі [навчальний посібник] / А.І.Блозва, Ю.В.Матус, В.В.Смолій, Б.С.Гусєв, Д.Ю.Касаткін, Т.Ю.Осипова, Я.А.Савицька // - К.: Компрінт, 2017.- 821с.
9. Тарбаєв С.І. Проектування інфокомунікаційних мереж. Навчальний посібник. – Київ: ННІТІ ДУТ, 2019. – 186 ст.
10. Задерейко О. В. Комп'ютерні мережі : навчальний посібник [Електронне видання] / О. В. Задерейко, Н. І. Логінова, А. А. Толокнов. – Одеса : Фенікс, 2022. – 249 с.

Допоміжна

1. Comer D. E. Computer Networks and Internets. Global Edition : textbook / D. E. Comer. – 6th ed. – Boston : Pearson Education, 2016. – 672 p.
2. Kurose J. F. Computer Networking: A Top-Down Approach : textbook / J. F. Kurose, K. W. Ross. – 8th ed. – Boston : Pearson Education, 2021. – 864 p.
3. Peterson L. L. Computer Networks: A Systems Approach : textbook / L. L. Peterson, B. S. Davie. – 6th ed. – Amsterdam : Morgan Kaufmann, 2021. – 896 p.
4. Goralski W. The Illustrated Network: How TCP/IP Works in a Modern Network : textbook / W. Goralski. – 2nd ed. – Amsterdam : Morgan Kaufmann, 2017. – 936 p.
5. Odom W. CCNA 200-301 Official Cert Guide. Volume 1 / W. Odom. – 2nd ed. – Indianapolis : Cisco Press, 2024. – 1024 p.

6. Odom W. CCNA 200-301 Official Cert Guide. Volume 2 / W. Odom. – 2nd ed. – Indianapolis : Cisco Press, 2024. – 992 p.
7. Sequeira A. J. CCNA 200-301 Hands-on Mastery with Packet Tracer : practical guide / A. J. Sequeira, R. Wong. – 2nd ed. – Indianapolis : Cisco Press, 2024. – 704 p.
8. Sanders C. Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems : textbook / C. Sanders. – 3rd ed. – San Francisco : No Starch Press, 2021. – 432 p.
9. Limoncelli T. A. The Practice of Network and System Administration : textbook / T. A. Limoncelli, C. J. Hogan, S. R. Chalup. – 2nd ed. – Boston : Addison-Wesley, 2020. – 1040 p.
10. Hucaby D. CCNA 200-301 Portable Command Guide : reference guide / D. Hucaby, W. Odom. – 2nd ed. – Indianapolis : Cisco Press, 2024. – 352 p.

Інформаційні ресурси

1. Національна бібліотека України ім. В.І. Вернадського : веб-сайт. URL: http://www.nbuv.gov.ua.
2. Он-лайн бібліотека. URL: http://www.lib.com.ua
3. MIT OpenCourseWare (OCW). URL: https://ocw.mit.edu/
4. Dive into Systems. URL: https://diveintosystems.org/
5. Open Textbook Library. URL: https://open.umn.edu/opentextbooks
6. Directory of Open Access Books (DOAB). URL: https://www.doabooks.org/
7. Cisco Networking Academy : educational portal. URL: https://www.netacad.com/.
8. Internet Engineering Task Force (IETF) : official web-site. URL: https://www.ietf.org/.
9. RFC Editor : Request for Comments (RFC) archive. URL: https://www.rfc-editor.org/.
10. Internet Assigned Numbers Authority (IANA) : protocol parameters registry. URL: https://www.iana.org/.
11. IEEE Standards Association : official standards portal. URL: https://standards.ieee.org/.
12. IEEE 802 LAN/MAN Standards Committee : networking standards. URL: https://www.ieee802.org/.
13. World Wide Web Consortium (W3C) : web standards specifications. URL: https://www.w3.org/.
14. Wireshark Documentation : protocol analysis reference. URL: https://www.wireshark.org/docs/.
15. Cisco Documentation : technical documentation and configuration guides. URL: https://www.cisco.com/c/en/us/support/index.html.
16. Juniper Networks TechLibrary : networking protocols and configuration guides. URL: https://www.juniper.net/documentation/.