Міжнародний гуманітарний університет
Факультет кібербезпеки, програмної інженерії
та комп'ютерних наук
Кафедра комп'ютерної інженерії та інноваційних
технологій

«ЗАТВЕРДЖУЮ»
Ректор Міжнародного
гуманітарного університету
д.ю.н., професор
_____ Костянтин ГРОМОВЕНКО
«29» серпня 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

КОМП'ЮТЕРНІ МЕРЕЖІ

Галузь знань — 12 Інформаційні технології

Спеціальність — 121 Інженерія програмного забезпечення

Назва освітньої програми — Інженерія програмного забезпечення

Рівень вищої освіти — перший (бакалаврський)

Одеса – 2025 рік

Робоча програма затверджена на засіданні кафедри комп'ютерної інженерії та інноваційних технологій.

Протокол № 1 від 28 серпня 2025 року.

Розробники і викладачі	Контактний тел.	E-mail
доцент кафедри комп'ютерної інженерії та інноваційних технологій, кандидат технічних наук, доцент, **Педяш Володимир Віталійович**	+380673787003	vpedyash@gmail.com

Завідувач кафедри комп'ютерної інженерії
та інноваційних технологій
к.т.н., доцент _____ Лариса ЙОНА

Гарант освітньої програми
к.т.н., доцент _____ Олександр РУСУ

Узгоджено
Начальник навчального відділу _____ Лілія САЄНКО

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td rowspan="2">Кількість кредитів – 6,
загальна кількість
годин – 180</td><td rowspan="2">Галузь –
12 Інформаційні технології

Спеціальність –
121 Інженерія програмного забезпечення</td><td>Денна форма</td><td>Заочна форма</td></tr>
<tr><td colspan="2">обов’язкова</td></tr>
<tr><td rowspan="14">Мова навчання – українська</td><td rowspan="14">Рівень вищої освіти –
перший (бакалаврський)</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td colspan="2">3</td></tr>
<tr><td colspan="2">Семестр:</td></tr>
<tr><td colspan="2">5</td></tr>
<tr><td colspan="2">Лекційні заняття:</td></tr>
<tr><td>40</td><td>12</td></tr>
<tr><td colspan="2">Практичні заняття:</td></tr>
<tr><td>26</td><td>6</td></tr>
<tr><td colspan="2">Лабораторні роботи</td></tr>
<tr><td>12</td><td>6</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>102</td><td>156</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td colspan="2">екзамен</td></tr>
</table>

Навчальна дисципліна «Комп’ютерні мережі» є складовою професійної підготовки здобувачів спеціальності 121 Інженерія програмного забезпечення та спрямована на формування системного розуміння принципів організації, архітектури та функціонування сучасних інформаційно-комунікаційних систем. Курс охоплює базові концепції побудови комп’ютерних мереж, що застосовуються у різних типах мережевих середовищ – від локальних (LAN) до глобальних (WAN), незалежно від конкретних виробників обладнання. Особлива увага приділяється еталонним моделям взаємодії (OSI, TCP/IP), механізмам IP-адресації, маршрутизації, сегментації трафіку, а також базовим підходам до забезпечення безпеки інфраструктури комп’ютерних мереж та засобам моніторингу мереж.

Знання, отримані під час вивчення дисципліни, є важливою основою для майбутніх фахівців з інженерії програмного забезпечення, оскільки розуміння принципів побудови та функціонування комп’ютерних мереж дає змогу ефективно розробляти програмні компоненти, що працюють у розподіленому середовищі, створювати розподілені програмні системи та забезпечувати взаємодію програмних модулів через комп’ютерні мережі. Практичні навички моделювання, налаштування та діагностики комп’ютерних мереж сприяють підготовці здобувачів до виконання професійних завдань, пов’язаних із розробкою, тестуванням і супроводженням програмних продуктів, що функціонують у розподілених інформаційних системах. Дисципліна також формує розуміння інформаційних моделей передавання даних у комп’ютерних мережах, зокрема структури мережевих пакетів і протоколів, що використовуються для організації обміну даними між програмними системами у розподіленому середовищі.

МЕТА ДИСЦИПЛІНИ. Метою викладання навчальної дисципліни є формування у здобувачів цілісного уявлення про архітектуру та принципи функціонування комп’ютерних мереж, а також розвиток практичних умінь проєктування, налаштування та аналізу систем передавання даних у контексті створення та експлуатації програмного забезпечення.

Дисципліна спрямована на формування здатності застосовувати мережеві протоколи та технології взаємодії комп'ютерних систем під час розроблення програмних продуктів, що функціонують у розподіленому середовищі, а також аналізувати роботу програмних систем, які використовують мережеві сервіси та інфраструктуру комп'ютерних мереж.

ПРЕРЕКВІЗИТИ. Необхідною умовою для опанування дисципліни є знання, отримані під час вивчення навчальних компонент «Фізика», «Теорія інформації та кодування», «Операційні системи».

ПОСТРЕКВІЗИТИ. Знання та вміння, набуті під час вивчення дисципліни «Комп'ютерні мережі», є основою для подальшого опанування навчальних компонент «Безпека даних та програм», «Програмування інфокомунікаційних сервісів та систем», а також можуть використовуватися під час виконання кваліфікаційної роботи.

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

У процесі реалізації програми дисципліни формуються наступні компетентності із передбачених освітньою програмою:

Інтегральна компетентність

Здатність розв'язувати складні спеціалізовані завдання або практичні проблеми інженерії програмного забезпечення, що характеризуються комплексністю та невизначеністю умов, із застосуванням теорій та методів інформаційних технологій.

Спеціальні (фахові, предметні) компетентності

К18. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).

К19. Володіння знаннями про інформаційні моделі даних, здатність створювати програмне забезпечення для зберігання, видобування та опрацювання даних.

К20. Здатність застосовувати фундаментальні і міждисциплінарні знання для успішного розв'язання завдань інженерії програмного забезпечення.

К25. Здатність обґрунтовано обирати та освоювати інструментарій з розробки та супроводження програмного забезпечення.

Результати навчання

ПР07. Знати і застосовувати на практиці фундаментальні концепції, парадигми і основні принципи функціонування мовних, інструментальних і обчислювальних засобів інженерії програмного забезпечення.

ПР18. Знати та вміти застосовувати інформаційні технології обробки, зберігання та передачі даних.

ПР21. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.

Заплановані результати навчання за навчальною дисципліною

Знання:

– основні поняття, класифікації та архітектурні принципи побудови сучасних комп'ютерних мереж, включаючи типи мереж (LAN, MAN, WAN, PAN), топології, функції мережевого обладнання та роль комп'ютерних мереж у функціонуванні інформаційних систем;

– структуру та функції еталонних моделей OSI та TCP/IP, механізми інкапсуляції даних, призначення рівнів моделі та принципи передавання даних у мережевому середовищі;

– принципи функціонування протоколів фізичного, канального, мережного, транспортного та прикладного рівнів, зокрема Ethernet, IPv4/IPv6, TCP/UDP, DNS, DHCP, HTTP(S), а також особливості їх використання в сучасних програмних та інформаційних системах.

Уміння:

– аналізувати інфраструктуру комп'ютерної мережі за рівнями моделі OSI/TCP/IP, визначати призначення її компонентів та оцінювати особливості передавання даних у різних сегментах мережі;

– застосовувати знання мережевих протоколів для аналізу взаємодії програмних і апаратних компонентів у мережевому середовищі;

– обґрунтовано вибирати способи організації та налаштування комп'ютерних мереж, зокрема сегментацію, адресацію, маршрутизацію та базові засоби керування доступом;

– оцінювати ефективність функціонування комп'ютерної мережі, виявляти типові проблеми передавання даних і пропонувати способи їх усунення.

Навички:

– ефективно використовувати інструменти моделювання комп'ютерних мереж (зокрема Cisco Packet Tracer) для проєктування, налаштування та тестування мережевих топологій;

– виконувати базову діагностику та моніторинг мережі за допомогою механізмів Syslog, SNMP, аналізу журналів подій, інтерфейсів та таблиць маршрутизації;

– налаштовувати та перевіряти працездатність комп'ютерних мереж з урахуванням принципів сегментації, централізованого контролю та надійного функціонування мережевих сервісів.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Основи комп'ютерних мереж

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. Роль комп'ютерних мереж у функціонуванні сучасних інформаційних систем та програмного забезпечення. Зв'язок архітектури мережі з організацією захисту інформації.

Тема 2. Моделі мережевої взаємодії OSI та TCP/IP

Семирівнева модель OSI та чотирирівнева модель TCP/IP, їх функції та відповідність. Інкапсуляція даних у стеку протоколів. Уразливості на різних рівнях моделі. Протоколи з низьким рівнем захисту: Telnet, HTTP, SNMPv1. Роль моделей у діагностиці мережевих інцидентів та аналізі взаємодії програмних і мережевих компонентів.

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.

Тема 4. Мережевий рівень – IP-адресація, маршрутизація

Структура IPv4-пакета, підмережування, VLSM. Основи IPv6: формати адрес, типи, особливості використання. Таблиця маршрутизації та типи маршрутів. Загрози мережевого рівня: IP-спуфінг, маршрутизаційні атаки. Значення правильної адресації та маршрутизації для забезпечення надійної передачі даних та стабільного функціонування інформаційних систем.

Тема 5. Транспортний та прикладний рівні

Протоколи TCP та UDP: надійність, порти, структура сегментів. Прикладні протоколи: DNS, DHCP, HTTP(S), SMTP, FTP. Особливості взаємодії прикладного програмного забезпечення з мережевими сервісами. Типові загрози: DoS-атаки, підміна DNS, перехоплення трафіку. Засоби захисту: шифрування, використання TLS/SSL, фільтрація трафіку.

Тема 6. Базові механізми безпеки мережевої інфраструктури

Безпечний доступ до обладнання через SSH. Налаштування 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 та підвищення надійності функціонування мережевих сервісів.

Тема 7. Проєктування, моделювання та моніторинг мереж

Етапи проєктування мережі: аналіз вимог, сегментація, IP-планування, вибір обладнання. Принципи забезпечення надійності та безпеки мережевої інфраструктури при проєктуванні. Моделювання мереж у Cisco Packet Tracer. Використання програмних інструментів для тестування мережевих конфігурацій та аналізу взаємодії програмних компонентів у мережевому середовищі. Основи централізованого моніторингу: Syslog, SNMP. Аналіз стану мережі та виявлення аномалій у її функціонуванні.

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин									
	Денна форма					Заочна форма				
	Заг.	у тому числі				Заг.	у тому числі			
		Лек.	Прак.	Лаб.	Сам. роб.		Лек.	Прак.	Лаб.	Сам. роб.
Тема 1. Основи комп'ютерних мереж	18	2	2	2	12	18	2	0	0	16
Тема 2. Моделі мережевої взаємодії OSI та TCP/IP	22	4	2	4	12	22	2	0	0	20
Тема 3. Фізичний та канальний рівні – технології, протоколи, вразливості та засоби захисту	30	6	4	2	18	30	2	0	0	24
Тема 4. Мережевий рівень – IP-адресація, маршрутизація	30	6	4	2	18	30	2	0	2	24
Тема 5. Транспортний та прикладний рівні	24	6	4	2	12	24	2	0	0	24
Тема 6. Базові механізми безпеки мережевої інфраструктури	28	8	4	0	16	28	0	2	2	24
Тема 7. Проєктування, моделювання та моніторинг мереж	28	8	4	0	14	28	2	4	2	24
Загалом	**180**	**40**	**26**	**12**	**102**	**180**	**12**	**6**	**6**	**156**
Підсумковий контроль – екзамен										

5. ПИТАННЯ ДО ПРАКТИЧНИХ ЗАНЯТЬ

Назва теми	Кількість годин	
	Денна форма	Заочна форма
Тема 1. Основи комп'ютерних мереж 1. Поняття комп'ютерної мережі та її роль у сучасній інформаційно-комунікаційній інфраструктурі. 2. Класифікація мереж за географічним охопленням: особливості LAN, MAN, WAN, PAN та їх безпекові наслідки. 3. Відмінність фізичної та логічної топологій мережі та їх вплив на проєктування мережевої інфраструктури та захисту інформації. 4. Основні типи мережевого обладнання (комутатор, маршрутизатор, точка доступу, міжмережевий екран) та їх функції з погляду безпеки. 5. Зв'язок між архітектурою мережі та організацією захисту інформаційних ресурсів у кібербезпечному середовищі.	2	0
Тема 2. Моделі мережевої взаємодії OSI та TCP/IP 1. Структура семирівневої моделі OSI та призначення кожного рівня у процесі передачі даних. 2. Чотирирівнева модель TCP/IP та її відповідність рівням моделі OSI. 3. Механізм інкапсуляції та декапсуляції даних у стеку протоколів. 4. Типові уразливості на різних рівнях моделі OSI (наприклад, фізичний, канальний, мережевий) та їх наслідки. 5. Роль моделей OSI і TCP/IP у діагностиці мережевих інцидентів та аналізі кіберзагроз. 6. Приклади небезпечних протоколів (Telnet, HTTP, SNMPv1) та їх місце в моделях взаємодії.	2	0
Тема 3. Фізичний та канальний рівні – технології, протоколи, вразливості та засоби захисту 1. Середовища передачі на фізичному рівні: вита пара, коаксіальний кабель, оптичне волокно, бездротові технології — порівняння за надійністю та стійкістю до	4	0

перехоплення. 2. Структура кадру Ethernet та принципи MAC-адресації. 3. Принцип роботи комутатора L2, формування CAM-таблиці та її вразливості. 4. Загрози канального рівня: ARP-спуфінг, MAC-флудінг, перехоплення трафіку у бездротових мережах. 5. Механізми захисту: Port Security, STP Guard, захист проти несанкціонованого підключення. 6. Роль VLAN у сегментації трафіку та зменшенні поверхні атаки на канальному рівні.		
Тема 4. Мережевий рівень – IP-адресація, маршрутизація 1. Структура IPv4-пакета та формат IP-адреси, особливе значення полів TTL, Protocol, Source/Destination IP. 2. Принципи підмережування, VLSM та їх застосування для організації безпечної адресації. 3. Основи IPv6: формати адрес, типи (unicast, multicast, anycast), відмінності у безпеці порівняно з IPv4. 4. Призначення таблиці маршрутизації та типи маршрутів: прямі, статичні, динамічні. 5. Загрози мережевого рівня: IP-спуфінг, маршрутизаційні петлі, атаки на протоколи динамічної маршрутизації. 6. Вплив правильної IP-адресації та маршрутизації на виявлення та ізоляцію інцидентів безпеки.	4	0
Тема 5. Транспортний та прикладний рівні 1. Порівняння протоколів TCP і UDP: надійність, встановлення з'єднання, порти, типові сценарії використання. 2. Структура сегментів TCP/UDP та роль номерів портів у мультиплексуванні та демультиплексуванні. 3. Основні прикладні протоколи: DNS, DHCP, HTTP(S), SMTP, FTP — їх функції та безпечні альтернативи. 4. Загрози транспортного та прикладного рівнів: SYN-флуд, DoS/DDoS, підміна DNS, перехоплення незашифрованого трафіку. 5. Механізми захисту: шифрування (TLS/SSL), використання безпечних протоколів (HTTPS, DNSSEC, SFTP). 6. Роль фільтрації трафіку за портами та протоколами у запобіганні несанкціонованому доступу.	4	0
Тема 6. Базові механізми безпеки мережевої інфраструктури 1. Принципи безпечного доступу до мережевого обладнання: порівняння Telnet і SSH з погляду конфіденційності. 2. Настройка автентифікації, шифрування паролів (enable secret), рівнів привілеїв на маршрутизаторі чи комутаторі. 3. Структура та типи списків контролю доступу (ACL): стандартні, розширені, часові. 4. Застосування ACL для фільтрації вхідного та вихідного трафіку за IP-адресами, портами, протоколами. 5. Роль VLAN у логічній сегментації мережі та обмеженні поширення інцидентів безпеки. 6. Комбіноване використання ACL, VLAN та безпечного управління для створення захищеної мережевої інфраструктури.	4	2
Тема 7. Проєктування, моделювання та моніторинг мереж 1. Етапи проектування безпечної мережі: аналіз вимог, визначення масштабу, вибір топології, сегментація. 2. Принципи безпеки при проектуванні: мінімізація поверхні атаки, сегментація, надмірність, відмовостійкість. 3. Використання Cisco Packet Tracer для моделювання, налаштування та тестування мережевих топологій. 4. Основи централізованого моніторингу: роль Syslog та SNMP у зборі подій безпеки. 5. Налаштування маршрутизатора або комутатора як джерела подій для систем моніторингу. 6. Практичні підходи до виявлення аномалій: аналіз журналів, змін стану інтерфейсів, помилок автентифікації.	4	4
Загалом	**26**	**6**

6. САМОСТІЙНА РОБОТА

До самостійної роботи здобувачів відносяться наступні види діяльності:

1. Опрацювання лекційного матеріалу.
2. Підготовка до практичних занять.
3. Консультації з викладачем впродовж семестру.
4. Ознайомлення з додатковою літературою відповідно до зазначених у програмі тем.
5. Самостійне опрацювання окремих питань навчальної дисципліни.
6. Підготовка індивідуальних завдань у вигляді презентацій або рефератів.
7. Підготовка до підсумкового контролю.

Назва теми	Кількість годин	
	Денна форма	**Заочна форма**
Тема 1. Основи комп'ютерних мереж 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.	12	16
Тема 2. Моделі мережевої взаємодії OSI та TCP/IP 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.	12	20
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.	18	24
Тема 4. Мережевий рівень – IP-адресація, маршрутизація Структура IPv4-пакета, підмережування, VLSM. Основи IPv6: формати адрес, типи, особливості безпеки. Таблиця маршрутизації та типи маршрутів. Загрози мережевого рівня: IP-спуфінг, маршрутизаційні атаки. Значення правильної адресації та маршрутизації для запобігання інцидентам.	18	24
Тема 5. Транспортний та прикладний рівні 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.	12	24
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.	16	24
Тема 7. Проєктування, моделювання та моніторинг 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.	14	24
Загалом	**102**	**156**

7. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Види контролю	Складові оцінювання
Поточний контроль, який здійснюється під час проведення практичних (лабораторних) занять, виконання самостійної роботи, індивідуальних завдань, дослідної роботи здобувача тощо	50%
Підсумковий контроль, який здійснюється у ході проведення екзамену	50%

Методи діагностики знань (контролю)	Фронтальне опитування, розв'язання практичних завдань, тестування здобувачів, наукові доповіді, реферати, усні повідомлення, екзамен

Питання для підсумкового контролю

1. Поняття комп'ютерної мережі та її роль у сучасній інформаційно-комунікаційній інфраструктурі.
2. Класифікація мереж за географічним охопленням: особливості LAN, MAN, WAN, PAN та їх безпекові наслідки.
3. Відмінність фізичної та логічної топологій мережі та їх вплив на проєктування мережевої інфраструктури та захисту інформації.
4. Основні типи мережевого обладнання (комутатор, маршрутизатор, точка доступу, міжмережевий екран) та їх функції з погляду безпеки.
5. Зв'язок між архітектурою комп'ютерної мережі та організацією захисту інформаційних ресурсів.
6. Структура семирівневої моделі OSI та призначення кожного рівня у процесі передачі даних.
7. Чотирирівнева модель TCP/IP та її відповідність рівням моделі OSI.
8. Механізм інкапсуляції та декапсуляції даних у стеку протоколів.
9. Типові уразливості на різних рівнях моделі OSI (наприклад, фізичний, канальний, мережевий) та їх наслідки.
10. Роль моделей OSI і TCP/IP у діагностиці мережевих проблем та аналізі мережевого трафіку.
11. Приклади небезпечних протоколів (Telnet, HTTP, SNMPv1) та їх місце в моделях взаємодії.
12. Середовища передачі на фізичному рівні: вита пара, коаксіальний кабель, оптичне волокно, бездротові технології — порівняння за надійністю та стійкістю до перехоплення.
13. Структура кадру Ethernet та принципи MAC-адресації.
14. Принцип роботи комутатора L2, формування CAM-таблиці та її вразливості.
15. Загрози канального рівня: ARP-спуфінг, MAC-флудінг, перехоплення трафіку у бездротових мережах.
16. Механізми захисту: Port Security, STP Guard, захист проти несанкціонованого підключення.
17. Роль VLAN у сегментації трафіку та організації логічної структури комп'ютерної мережі.
18. Структура IPv4-пакета та формат IP-адреси, особливе значення полів TTL, Protocol, Source/Destination IP.
19. Принципи підмережування, VLSM та їх застосування для організації безпечної адресації.

20. Основи IPv6: формати адрес, типи (unicast, multicast, anycast), відмінності у безпеці порівняно з IPv4.

21. Призначення таблиці маршрутизації та типи маршрутів: прямі, статичні, динамічні.

22. Загрози мережевого рівня: IP-спуфінг, маршрутизаційні петлі, атаки на протоколи динамічної маршрутизації.

23. Вплив правильної IP-адресації та маршрутизації на виявлення та ізоляцію інцидентів безпеки.

24. Порівняння протоколів TCP і UDP: надійність, встановлення з'єднання, порти, типові сценарії використання.

25. Структура сегментів TCP/UDP та роль номерів портів у мультиплексуванні та демультиплексуванні.

26. Основні прикладні протоколи: DNS, DHCP, HTTP(S), SMTP, FTP — їх функції та безпечні альтернативи.

27. Загрози транспортного та прикладного рівнів: SYN-флуд, DoS/DDoS, підміна DNS, перехоплення незашифрованого трафіку.

28. Механізми захисту: шифрування (TLS/SSL), використання безпечних протоколів (HTTPS, DNSSEC, SFTP).

29. Роль фільтрації трафіку за портами та протоколами у запобіганні несанкціонованому доступу.

30. Принципи безпечного доступу до мережевого обладнання: порівняння Telnet і SSH з погляду конфіденційності.

31. Настройка автентифікації, шифрування паролів (enable secret), рівнів привілеїв на маршрутизаторі чи комутаторі.

32. Структура та типи списків контролю доступу (ACL): стандартні, розширені, часові.

33. Застосування ACL для фільтрації вхідного та вихідного трафіку за IP-адресами, портами, протоколами.

34. Використання VLAN разом із ACL для обмеження поширення інцидентів безпеки в комп'ютерній мережі.

35. Комбіноване використання ACL, VLAN та безпечного управління для створення захищеної мережевої інфраструктури.

36. Етапи проєктування безпечної мережі: аналіз вимог, визначення масштабу, вибір топології, сегментація.

37. Принципи безпеки при проєктуванні: мінімізація поверхні атаки, сегментація, надмірність, відмовостійкість.

38. Використання Cisco Packet Tracer для моделювання, налаштування та тестування мережевих топологій.

39. Основи централізованого моніторингу: роль Syslog та SNMP у зборі подій безпеки.

40. Налаштування маршрутизатора або комутатора як джерела подій для систем моніторингу.

41. Практичні підходи до виявлення аномалій: аналіз журналів, змін стану інтерфейсів, помилок автентифікації.

42. Використання моделювання та моніторингу для верифікації проєктних рішень та підвищення надійності мережі.

8. ОЦІНЮВАННЯ ПОТОЧНОЇ, САМОСТІЙНОЇ ТА ІНДИВІДУАЛЬНОЇ РОБОТИ ЗДОБУВАЧІВ

Види роботи	Планові терміни виконання	Форми контролю та звітності	Максимальний відсоток оцінювання
Систематичність і активність роботи на практичних заняттях			
1.1. Підготовка до практичних занять	Відповідно до робочої програми та розкладу занять	Перевірка обсягу та якості засвоєного матеріалу під час практичних занять	**30**
Виконання завдань для самостійного опрацювання			
1.2. Індивідуальне тестування	Відповідно до робочої програми та розкладу занять	Перевірка результатів індивідуального тестування, перевірка конспектів лекцій, перевірка рефератів	**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**
Загалом балів			**100**

Поточний контроль знань здобувачів при підсумковому контролі у формі екзамену (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 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 підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 2.

Критерії оцінювання поточного контролю

– **«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 здобувача мають фрагментарний, поверховий характер;

– **«4»** – оцінюється правильна і обґрунтована відповідь (письмова робота), з якої видно, що здобувач 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.

Критерії оцінювання підсумкового контролю у формі екзамену

Максимальна оцінка підсумкового контролю у формі екзамену не може перевищувати 50 балів. При цьому рівень знань оцінюється:

– **від 40 до 50 балів** – здобувач виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки;

– **від 30 до 40 балів** – здобувач володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді;

– **від 20 до 30 балів** – здобувач 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.

– **від 10 до 20 балів** – здобувач володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих;

– від 0 до 10 балів – здобувач 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. ОЦІНЮВАННЯ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ЗНАНЬ ЗДОБУВАЧІВ

Загальні результати знань здобувачів по даній дисципліні оцінюються наступним чином:

– **«Відмінно»/«зараховано» (А)** – від 90 до 100 балів. Здобувач виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки. Був присутній на лекціях та практичних заняттях, під час яких давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, має конспект з виконаними завданнями до самостійної роботи, презентував реферат за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;

– **«Добре»/«зараховано» (В)** – від 82 до 89 балів. Здобувач 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 практичних заняттях, має конспект з виконаними завданнями до самостійної

роботи, презентував реферат за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;

– **«Добре»/«зараховано» (C)** – від 74 до 81 балів. Здобувач 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. Здобувач був присутній не на всіх лекціях та практичних 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 та рефератів;

– **«Задовільно»/«зараховано» (E)** – від 60 до 63 балів. Здобувач був присутній не на всіх лекціях та практичних 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. Здобувач 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. Здобувач не володіє навчальним матеріалом.

Таблиця відповідності результатів контролю знань за різними шкалами

100-бальна шкала	Шкала за ECTS	Національна шкала	
		Екзамен	Залік
90-100	A	Відмінно	Зараховано
82-89	B	Добре	Зараховано
74-81	C		
64-73	D	Задовільно	Зараховано
60-63	E		
35-59	FX	Незадовільно	Не зараховано
0-34	F		

10. 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. 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.
3. Азаров О. Д. Комп'ютерні мережі : підручник / О. Д. Азаров, С. М. Захарченко, О. В. Кадук та ін. − Вінниця : ВНТУ, 2020. − 378 с.

4. 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.

5. 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.

6. Тарбаєв С.І. Проектування інфокомунікаційних мереж. Навчальний посібник. – Київ: ННІТІ ДУТ, 2019. – 186 ст.

7. 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

8. Comer D. E. Computer Networks and Internets. Global Edition : textbook / D. E. Comer. – 6th ed. – Boston : Pearson Education, 2016. – 672 p.

9. Kurose J. F. Computer Networking: A Top-Down Approach : textbook / J. F. Kurose, K. W. Ross. – 8th ed. – Boston : Pearson Education, 2021. – 864 p.

10. Peterson L. L. Computer Networks: A Systems Approach : textbook / L. L. Peterson, B. S. Davie. – 6th ed. – Amsterdam : Morgan Kaufmann, 2021. – 896 p.

11. Goralski W. The Illustrated Network: How TCP/IP Works in a Modern Network : textbook / W. Goralski. – 2nd ed. – Amsterdam : Morgan Kaufmann, 2017. – 936 p.

12. Odom W. CCNA 200-301 Official Cert Guide. Volume 1 / W. Odom. – 2nd ed. – Indianapolis : Cisco Press, 2024. – 1024 p.

13. Odom W. CCNA 200-301 Official Cert Guide. Volume 2 / W. Odom. – 2nd ed. – Indianapolis : Cisco Press, 2024. – 992 p.

14. 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.

15. 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.

16. 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.

17. Hucaby D. CCNA 200-301 Portable Command Guide : reference guide / D. Hucaby, W. Odom. – 2nd ed. – Indianapolis : Cisco Press, 2024. – 352 p.

Інформаційні ресурси

18. Національна бібліотека України ім. В.І. Вернадського : веб-сайт. URL: http://www.nbuv.gov.ua

19. Он-лайн бібліотека. URL: http://www.lib.com.ua

20. MIT OpenCourseWare (OCW). URL: https://ocw.mit.edu/

21. Dive into Systems. URL: https://diveintosystems.org/

22. Open Textbook Library. URL: https://open.umn.edu/opentextbooks

23. Directory of Open Access Books (DOAB). URL: https://www.doabooks.org/

24. Cisco Networking Academy : educational portal. URL: https://www.netacad.com/

25. Internet Engineering Task Force (IETF) : official web-site. URL: https://www.ietf.org/

26. RFC Editor : Request for Comments (RFC) archive. URL: https://www.rfc-editor.org/

27. Internet Assigned Numbers Authority (IANA) : protocol parameters registry. URL: https://www.iana.org/

28. IEEE Standards Association : official standards portal. URL: https://standards.ieee.org/
29. IEEE 802 LAN/MAN Standards Committee : networking standards. URL: https://www.ieee802.org/
30. World Wide Web Consortium (W3C) : web standards specifications. URL: https://www.w3.org/
31. Wireshark Documentation : protocol analysis reference. URL: https://www.wireshark.org/docs/
32. Cisco Documentation : technical documentation and configuration guides. URL: https://www.cisco.com/c/en/us/support/index.html .
33. Juniper Networks TechLibrary : networking protocols and configuration guides. URL: https://www.juniper.net/documentation/