

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ПЕРВОМАЙСЬКИЙ ІНДУСТРІАЛЬНО-ПЕДАГОГІЧНИЙ ФАХОВИЙ КОЛЕДЖ  
(ППФК)  
Циклова комісія професійної освіти

**ЗАТВЕРДЖЕНО**

Наказ в. о. директора ППФК  
01.09.2025 № 88

**КОМП'ЮТЕРНІ МЕРЕЖІ ТА ЗАХИСТ ДАНИХ**

**Програма навчальної дисципліни**

підготовки	<i>фахових молодших бакалаврів</i>
галузі знань	<i>01 Освіта/Педагогіка</i>
спеціальності	<i>015 Професійна освіта (за спеціалізаціями)</i>
спеціалізації	<i>015.39 Цифрові технології</i>
освітньо-професійної програми	<i>Професійна освіта (Цифрові технології) (зі змінами, 2024)</i>
код ОК в ОПП	<b>ОК 20</b>

Програма навчальної дисципліни «Комп'ютерні мережі та захист даних» освітньо-професійної програми «Професійна освіта (Цифрові технології)» (зі змінами, 2024) спеціальності 015 Професійна освіта (за спеціалізаціями), спеціалізація 015.39 Цифрові технології, для здобувачів освіти II курсу денної форми навчання.

Розробник: *Максименко Володимир Геннадійович*, викладач комп'ютерних дисциплін, спеціаліст I категорії.

Програма розглянута і схвалена на засіданні циклової комісії професійної освіти 29.08.2025, протокол № 1, та затверджена рішенням методичної ради 29.08.2025, протокол № 1.

### 1. Опис освітнього компоненту (навчальної дисципліни)

Найменування показників	Характеристика навчальної дисципліни
<b>Форма навчання</b>	денна
<b>Рік підготовки</b>	II (другий)
<b>Семестр</b>	4-й
<b>Мова навчання</b>	українська
<b>Статус дисципліни</b>	обов'язкова
<b>Інформаційний обсяг навчальної дисципліни</b>	
<b>кількість кредитів ECTS</b>	4
<b>загальна кількість годин, в т.ч.:</b>	120
– аудиторних	56
– самостійної роботи здобувачів освіти	34
– підготовка до екзамену	30
<b>Модулів</b>	1
<b>Змістових модулів</b>	3
<b>Лекції</b>	40 год.
<b>Семінарські</b>	–
<b>Практичні</b>	–
<b>Лабораторні</b>	16 год.
<b>Самостійна робота</b>	34 год.
<b>Індивідуальні завдання</b>	–
<b>Вид контролю</b>	екзамен

## 2. Предмет, мета та завдання навчальної дисципліни

**Предметом** навчальної дисципліни «Комп'ютерні мережі та захист даних» є принципи побудови, функціонування та захисту комп'ютерних мереж, включаючи моделі OSI та TCP/IP, протоколи передачі даних, методи шифрування, а також технології забезпечення кібербезпеки.

**Метою викладання** навчальної дисципліни «Комп'ютерні мережі та захист даних» є формування у здобувачів освіти теоретичних знань і практичних навичок із проектування, налаштування та захисту комп'ютерних мереж як частини цифрових технологій, а також підготовка до роботи з сучасними мережевими системами та їх безпека.

**Основними завданнями** навчальної дисципліни «Комп'ютерні мережі та захист даних» є:

- формування базових знань про структуру та принципи роботи комп'ютерних мереж;
- оволодіння навичками налаштування локальних і бездротових мереж;
- набуття практичних умінь із аналізу мережевого трафіку та маршрутизації;
- освоєння методів шифрування даних і захисту мереж від кіберзагроз;
- розвиток умінь застосовувати інструменти моніторингу та виявлення вторгнень;
- підготовка до самостійного створення захищених мережеских проєктів.

**Передумови вивчення навчальної дисципліни.** Для вивчення дисципліни «Комп'ютерні мережі та захист даних» необхідними є знання та вміння, отримані здобувачами освіти при вивченні предметів «Операційні системи», «Архітектура комп'ютера», «Мови і технології програмування» на I курсі навчання.

## 3. Компетентності та заплановані результати навчання

Компетентності, які мають бути сформовані в результаті опанування освітнього компоненту (дисципліни), та очікувані результати навчання:

<b>Компетентності</b>	
<b>Загальні компетентності (ЗК)</b>	ЗК4 Здатність використовувати інформаційні та комунікаційні технології. ЗК5 Знання та розуміння предметної області та розуміння професійної діяльності. ЗК8 Здатність застосовувати знання у практичних ситуаціях.
<b>Спеціальні компетентності (СК)</b>	СК5 Здатність застосовувати інноваційні педагогічні та цифрові технології, інформаційне та програмне забезпечення для вирішення професійних завдань у галузі цифрових технологій. СК17 Здатність застосовувати принципи і методи побудови та використання мережеских технологій, методи та засоби захисту програмного забезпечення та даних від несанкціонованого доступу.
<b>Зміст підготовки здобувачів фахової передвищої освіти, сформульований у термінах результатів навчання (РН)</b>	
РН15 Використовувати технічну термінологію галузі цифрових технологій. РН26 Експлуатувати комп'ютерні мережі, планувати та здійснювати заходи щодо захисту інформації та програмного забезпечення.	

*У результаті вивчення навчальної дисципліни здобувач освіти повинен:*

**знати:**

- основні поняття комп'ютерних мереж і моделі OSI та TCP/IP;
- принципи роботи протоколів (IP, TCP, UDP, HTTP тощо);
- методи шифрування та аутентифікації;
- основи кібербезпеки та типи мережевих атак;
- інструменти аналізу та захисту мереж.

**вміти:**

- налаштовувати локальні та бездротові мережі;
- аналізувати мережевий трафік за допомогою інструментів (наприклад, Wireshark);
- застосовувати методи шифрування (AES, RSA) і налаштовувати VPN;
- виявляти та захищати мережу від атак;
- розгортати захищені мережеві проекти;
- працювати з термінологією дисципліни та джерелами знань для самостійного навчання;
- використовувати цифрові інструменти для навчання: ефективно працювати в Google Workspace For Education (Google Клас, Google Meet, Google Форми) для виконання завдань і проходження оцінювання.

**Формат навчання**

Навчання здійснюється у дистанційному форматі з використанням платформи Google Workspace for Education за допомогою основних інструментів Google:

Google Клас — для розміщення навчальних матеріалів, завдань і тестів, забезпечення зворотного зв'язку;

Google Meet — для проведення лекцій, семінарів, консультацій у режимі реального часу;

Google Документи, Таблиці — для виконання завдань;

Google Форми — для оцінювання знань (тести), проведення опитувань.

## 4. Структура навчальної дисципліни

Назви змістових модулів і тем програми	Кількість годин			
	Усього	У тому числі		
		лекцій	лабора- торних	самос- тійної роботи
<b>Змістовий модуль 1. Основи комп'ютерних мереж</b>				
<i>Тема 1.</i> Вступ до комп'ютерних мереж	4	2	–	2
<i>Тема 2.</i> Модель OSI та TCP/IP	5	2	–	3
<i>Тема 3.</i> Фізичний рівень: передача даних	5	2	–	3
<i>Тема 4.</i> Канальний рівень: протоколи та технології	4	2	2	–
<i>Тема 5.</i> Мережевий рівень: IP-протокол	4	2	2	–
<i>Тема 6.</i> Локальні мережі (LAN)	8	2	2	4
<b>Разом за ЗМ 1</b>	<b>30</b>	<b>12</b>	<b>6</b>	<b>12</b>
<b>Змістовий модуль 2. Протоколи та маршрутизація</b>				
<i>Тема 7.</i> Маршрутизація в мережах	8	2	2	4
<i>Тема 8.</i> Транспортний рівень: TCP та UDP	7	2	2	2
<i>Тема 9.</i> Прикладний рівень: основні протоколи	7	2	2	3
<i>Тема 10.</i> Глобальні мережі (WAN)	5	2	–	3
<i>Тема 11.</i> Бездротові мережі	2	2	–	–
<b>Разом за ЗМ 2</b>	<b>29</b>	<b>10</b>	<b>6</b>	<b>12</b>
<i>Тематичне оцінювання</i>				
<b>Змістовий модуль 3. Захист даних у мережах</b>				
<i>Тема 12.</i> Вступ до захисту даних у мережах	4	2	–	2
<i>Тема 13.</i> Криптографія в мережах	2	2	–	–
<i>Тема 14.</i> Аутентифікація та контроль доступу	4	2	2	–
<i>Тема 15.</i> Мережеві атаки та їх класифікація	5	2	–	3
<i>Тема 16.</i> Захист мережевої інфраструктури	5	2	–	3
<i>Тема 17.</i> Безпека бездротових мереж	2	2	–	–
<i>Тема 18.</i> Моніторинг та аналіз мережевого трафіку	4	2	2	–
<i>Тема 19.</i> Хмарні технології та їх безпека	4	2	–	2
<i>Тема 20.</i> Тенденції розвитку мереж та кібербезпеки	2	2	–	–
<b>Разом за ЗМ 3</b>	<b>32</b>	<b>18</b>	<b>4</b>	<b>10</b>
<i>Тематичне оцінювання</i>				
<b>Підготовка до екзамену</b>	<b>30</b>			<b>30</b>
<b>Усього</b>	<b>120</b>	<b>40</b>	<b>16</b>	<b>64</b>

## 5. Програма навчальної дисципліни

### Змістовий модуль 1. Основи комп'ютерних мереж

#### **Тема 1. Вступ до комп'ютерних мереж**

Огляд комп'ютерних мереж: визначення, історія розвитку, класифікація (LAN, WAN, MAN, PAN). Основні компоненти мереж (пристрої, канали зв'язку, протоколи). Приклади мереж у повсякденному житті (домашній Wi-Fi, офісні мережі, інтернет). Значення мереж для сучасного суспільства (комунікація, бізнес, освіта). Вступ до понять пропускної здатності, затримки, топології.

#### **Тема 2. Модель OSI та TCP/IP**

Опис моделі OSI: 7 рівнів (фізичний, канальний, мережевий, транспортний, сеансовий, представлення, прикладний), функції кожного рівня, приклади протоколів. Порівняння з моделлю TCP/IP: 4 рівні (мережевий доступ, інтернет, транспортний, прикладний), відповідність OSI. Переваги та недоліки моделей. Роль інкапсуляції й деінкапсуляції в передачі даних.

#### **Тема 3. Фізичний рівень: передача даних**

Основи фізичного рівня: передача сигналів (аналогові, цифрові), типи носіїв (кручена пара, оптоволокно, радіохвилі). Кодування даних (NRZ, Manchester). Шум, перешкоди, пропускна здатність каналу (теорема Шеннона). Обладнання: кабелі, конектори, підсилювачі, повторювачі. Ethernet-кабелі, Wi-Fi-частоти. Ключові поняття: Сигнал, носій, кодування, пропускна здатність, шум.

#### **Тема 4. Канальний рівень: протоколи та технології**

Завдання канального рівня: кадркування, контроль доступу до середовища (MAC), виявлення помилок. Протоколи: Ethernet (IEEE 802.3), PPP, HDLC. Структура кадру Ethernet (преамбула, MAC-адреси, дані, CRC). Технології: комутатори, мости, ARP. Приклади: передача кадру в LAN, таблиця MAC-адрес.

#### **Тема 5. Мережевий рівень: IP-протокол**

Функції мережевого рівня: адресація, маршрутизація, фрагментація. IP-протокол: IPv4 (структура адреси, класи, підмережі), IPv6 (переваги, формат). Заголовок IP-пакета. Протоколи: ICMP (ping, traceroute), NAT. Підмережа 192.168.1.0/24, ping до сервера.

#### **Тема 6. Локальні мережі (LAN)**

Визначення LAN, характеристики (висока швидкість, мала затримка). Топології: зірка, шина, кільце. Обладнання: комутатори, роутери, кабелі (кручена пара, Cat5e/Cat6). Стандарти: IEEE 802.3 (Ethernet), IEEE 802.11 (Wi-Fi). Домашня мережа, офісна LAN.

### Змістовий модуль 2. Протоколи та маршрутизація

#### **Тема 7. Маршрутизація в мережах**

Поняття маршрутизації: вибір шляху для пакетів. Типи: статична (ручна), динамічна (автоматична). Таблиці маршрутизації: структура (мережа, шлюз, метрика). Протоколи: RIP (стрибки), OSPF (найкоротший шлях). Статичний маршрут до провайдера, OSPF у корпоративній мережі. Детальний аналіз метрик у таблицях маршрутизації

### ***Тема 8. Транспортний рівень: TCP та UDP***

Завдання транспортного рівня: доставка до програм, порти. TCP: з'єднання (триходове рукоштовування), надійність (контроль помилок, порядок). UDP: без з'єднання, швидкість, без гарантій. Порівняння: TCP (веб, пошта), UDP (стрімінг, ігри). TCP для HTTPS, UDP для DNS.

### ***Тема 9. Прикладний рівень: основні протоколи***

Роль прикладного рівня: взаємодія з користувачем. Протоколи: HTTP/HTTPS (веб), FTP (файли), SMTP/POP3/IMAP (пошта), DNS (імена). Структура запитів і відповідей (наприклад, HTTP GET). Завантаження сайту, надсилання листа.

### ***Тема 10. Глобальні мережі (WAN)***

Визначення WAN, відмінності від LAN (масштаб, швидкість). Технології: MPLS, VPN, Frame Relay. Обладнання: маршрутизатори, модеми. Протоколи: PPPoE, BGP. Підключення до провайдера, корпоративна WAN.

### ***Тема 11. Бездротові мережі***

Основи бездротових мереж: радіохвилі, частоти (2.4 ГГц, 5 ГГц). Стандарти: IEEE 802.11 (Wi-Fi a/b/g/n/ac/ax). Обладнання: точки доступу, антени. Безпека: WEP, WPA, WPA2/3. Домашній Wi-Fi, hotspot у кафе.

## **Змістовий модуль 3. Захист даних у мережах**

### ***Тема 12. Вступ до захисту даних у мережах***

Значення безпеки мереж: захист даних, конфіденційність. Типи загроз: віруси, хакери, перехоплення. Основи: аутентифікація, шифрування, контроль доступу. Регуляції (GDPR). Витік паролів, атака на Wi-Fi.

### ***Тема 13. Криптографія в мережах***

Основи криптографії: симетричне (AES) і асиметричне (RSA) шифрування. Хеш-функції (SHA). Протоколи: SSL/TLS, IPsec. HTTPS-сертифікат, шифрування VPN.

### ***Тема 14. Аутентифікація та контроль доступу***

Аутентифікація: паролі, біометрія, двофакторна (2FA). Контроль доступу: ACL, ролі. Протоколи: RADIUS, Kerberos. Логін у мережу, блокування IP через ACL.

### ***Тема 15. Мережеві атаки та їх класифікація***

Типи атак: DoS/DDoS, фішинг, MITM, SQL-ін'єкція. Механізми: перехоплення пакетів, спуфінг. Інструменти атак: Metasploit.

### ***Тема 16. Захист мережевої інфраструктури***

Методи захисту: фаєрволи, IDS/IPS, антивіруси. Налаштування: VPN, DMZ. Блокування портів фаєрволом, виявлення вторгнень IDS.

### ***Тема 17. Безпека бездротових мереж***

Уразливості Wi-Fi: слабкі паролі, WEP. Захист: WPA2/3, прихований SSID. Атаки: злочинний AP, deauthentication. Злам Wi-Fi, захист корпоративного Wi-Fi.

### **Тема 18. Моніторинг та аналіз мережевого трафіку**

Інструменти: Wireshark, Nmap. Аналіз: виявлення аномалій, підозрілих пакетів. Метрики: пропускна здатність, затримка. Приклади: захоплення трафіку, пошук сканування портів.

### **Тема 19. Хмарні технології та їх безпека**

Основи хмар: IaaS, PaaS, SaaS. Безпека: шифрування, резервування, доступ. Загрози: витік даних, слабкі API. AWS, Google Drive, атака на хмару.

### **Тема 20. Тенденції розвитку мереж та кібербезпеки**

Сучасні тренди: IoT, 5G, SD-WAN. Нові загрози: AI-атаки, квантові обчислення. Майбутнє: автоматизація безпеки, zero trust. IoT у розумному домі, 5G у мережах.

### **Основні поняття дисципліни**

Мережа, Протокол, Модель OSI, TCP/IP, Фізичний рівень, Канальний рівень, MAC-адреса, IP-адреса, Підмережа, LAN, Маршрутизація, Маршрутизатор, Таблиця маршрутизації, RIP, OSPF, Транспортний рівень, TCP, UDP, Порт, Прикладний рівень, WAN, Wi-Fi, Безпека мереж, Шифрування, Аутентифікація, Контроль доступу, Мережева атака, DoS, MITM, Фаєрвол, VPN, WPA, Трафік, Хмарні технології

## **6. Теми лекцій**

№ з/п	Назва теми	Кількість годин
	<b>ЗМ 1. Основи комп'ютерних мереж</b>	<b>12</b>
1.	Вступ до комп'ютерних мереж	2
2.	Модель OSI та TCP/IP	2
3.	Фізичний рівень: передача даних	2
4.	Канальний рівень: протоколи та технології	2
5.	Мережевий рівень: IP-протокол	2
6.	Локальні мережі (LAN)	2
	<b>ЗМ 2. Протоколи та маршрутизація</b>	<b>10</b>
7.	Маршрутизація в мережах	2
8.	Транспортний рівень: TCP та UDP	2
9.	Прикладний рівень: основні протоколи	2
10.	Глобальні мережі (WAN)	2
11.	Бездротові мережі	2
	<b>ЗМ 3. Захист даних у мережах</b>	<b>18</b>
12.	Вступ до захисту даних у мережах	2
13.	Криптографія в мережах	2
14.	Аутентифікація та контроль доступу	2
15.	Мережеві атаки та їх класифікація	2
16.	Захист мережевої інфраструктури	2
17.	Безпека бездротових мереж	2
18.	Моніторинг та аналіз мережевого трафіку	2
19.	Хмарні технології та їх безпека	2
20.	Тенденції розвитку мереж та кібербезпеки	2
	<b>Усього</b>	<b>40</b>

## 7. Теми лабораторних робіт

№ з/п	Назва теми	Кількість годин
	<b>ЗМ 1. Основи комп'ютерних мереж</b>	<b>6</b>
1.	<i>Лабораторна робота № 1.</i> Побудова простої локальної мережі (LAN)	2
2.	<i>Лабораторна робота № 2.</i> Аналіз роботи канального рівня	2
3.	<i>Лабораторна робота № 3.</i> Налаштування IP-адресації	2
	<b>ЗМ 2. Протоколи та маршрутизація</b>	<b>6</b>
5.	<i>Лабораторна робота № 4.</i> Налаштування статичної маршрутизації	2
6.	<i>Лабораторна робота № 5.</i> Використання протоколу OSPF	2
7.	<i>Лабораторна робота № 6.</i> Аналіз TCP і UDP трафіку	2
	<b>ЗМ 3. Протоколи та маршрутизація</b>	<b>4</b>
9.	<i>Лабораторна робота № 7.</i> Налаштування базового захисту мережі	2
10.	<i>Лабораторна робота № 8.</i> Моніторинг мережевого трафіку	2
	<b>Усього</b>	<b>16</b>

## 8. Теми практичних робіт

Практичні роботи навчальним планом не передбачено.

## 9. Теми семінарських занять

Семінарські заняття навчальним планом не передбачено

## 10. Самостійна робота

№ з/п	Назва теми	Кількість годин
	<b>ЗМ 1. Основи комп'ютерних мереж</b>	<b>12</b>
1.	<i>Тема 1.</i> Історія розвитку комп'ютерних мереж.	2
2.	<i>Тема 2.</i> Переваги та недоліки моделей OSI і TCP/IP	3
3.	<i>Тема 3.</i> Типи кодування даних (NRZ, Manchester)	3
4.	<i>Тема 6.</i> Топології мереж: шина, кільце (порівняння із зіркою)	4
	<b>ЗМ 2. Протоколи та маршрутизація</b>	<b>12</b>
5.	<i>Тема 7.</i> Детальний аналіз метрик у таблицях маршрутизації	4
6.	<i>Тема 9.</i> Протоколи POP3 та IMAP (другорядні порівняно з SMTP)	2
7.	<i>Тема 10.</i> Технології Frame Relay і MPLS (менш актуальні сьогодні)	3
8.	<i>Тема 11.</i> Історія стандартів IEEE 802.11 (a/b/g)	3
	<b>ЗМ 3. Захист даних у мережах</b>	<b>10</b>
9.	<i>Тема 12.</i> Регуляції безпеки (наприклад, GDPR)	2
10.	<i>Тема 13.</i> Хеш-функції (SHA) у деталях.	3
11.	<i>Тема 15.</i> Інструменти атак (наприклад, Metasploit).	3
12.	<i>Тема 19.</i> Типи хмарних моделей: PaaS, SaaS (порівняно з IaaS)	2
	<b>Усього</b>	<b>34</b>
	<b>Підготовка до екзамену</b>	<b>30</b>
	<b>Усього</b>	<b>64</b>

## 11. Засоби та форми контролю

Оцінювання навчальної діяльності здобувачів освіти здійснюється шляхом **поточного контролю, тематичної атестації та підсумкового контролю** із застосуванням цифрових інструментів Google Workspace for Education.

**Поточний контроль передбачає** фронтальне та індивідуальне опитування, тестування (Google Форми), виконання практичних завдань з використанням Google Документів, Таблиць, Презентацій; перевірку результатів виконання лабораторних робіт та звітів до них

**Контроль самостійної роботи** здійснюється за допомогою усного та письмового опитування, підготовки повідомлень, виконання практичних та тестових завдань.

**Тематична атестація** проводиться після завершення кожного змістового модуля як результат узагальнення результатів поточного оцінювання.

**Підсумковий (семестровий) контроль** — *екзамен*, який складається з теоретичної частини (комп'ютерне тестування із використанням Google Форм) та практичного завдання.

## 12. Критерії оцінювання результатів навчання

Оцінювання результатів навчальної діяльності здобувачів освіти здійснюється за **національною чотирибальною шкалою** з урахуванням цифрового формату навчання і рівня сформованості компетентностей. Для відповідності стандартам ECTS у програмі подається довідкова таблиця переведення без фактичного застосування цього переведення при виставленні балів.

**Таблиця відповідності результатів контролю знань здобувачів освіти, рівень знань яких оцінюється за 4-бальною шкалою, у системі ECTS**

За 4-бальною шкалою	Оцінка в ECTS	Критерії оцінювання
5 (відмінно)	A	Здобувач освіти виявляє особливі творчі здібності, вміє самостійно здобувати знання, без допомоги викладача знаходить та опрацьовує необхідну інформацію, вміє використовувати набуті знання і вміння для прийняття рішень у нестандартних ситуаціях, переконливо аргументує відповіді, самостійно розкриває власні обдарування і нахили
4 (добре)	B	Здобувач освіти вільно володіє вивченим обсягом матеріалу, застосовує його на практиці, вільно розв'язує вправи і задачі у стандартних ситуаціях, самостійно виправляє допущені помилки, кількість яких незначна
	C	Здобувач освіти вміє зіставляти, узагальнювати, систематизувати інформацію під керівництвом викладача; в цілому самостійно застосовувати її на практиці; контролювати власну діяльність; виправляти помилки, серед яких є суттєві, добирати аргументи для підтвердження думок

3 (задовільно)	D	Здобувач освіти відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень; з допомогою викладача може аналізувати навчальний матеріал, виправляти помилки, серед яких є значна кількість суттєвих
	E	Здобувач освіти володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні
2 (незадовільно)	FX	Здобувач освіти володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу
	F	Здобувач освіти володіє матеріалом на рівні елементарного розпізнання і відтворення окремих фактів, елементів, об'єктів

**Оцінка «5» (відмінно) / А.** Здобувач освіти логічно та усвідомлено відтворює навчальний матеріал у межах програми: чітко пояснює принципи роботи мереж (LAN, WAN), маршрутизації (RIP, OSPF), транспортних протоколів (TCP, UDP), основи безпеки (шифрування, аутентифікація); робить висновки щодо їх застосування. Може структурувати знання, порівнювати різні протоколи чи методи захисту, стисло узагальнювати інформацію з кількох джерел.

Вільно користується термінологією дисципліни (мережа, IP-адреса, порт, фаєрвол), демонструє міцні знання принципів створення й захисту мереж, пояснює взаємодію рівнів OSI/TCP-IP і компонентів безпеки.

При виконанні лабораторних робіт самостійно налаштовує мережі: будує LAN у Cisco Packet Tracer, налаштовує статичну й динамічну маршрутизацію (OSPF), аналізує TCP/UDP-трафік, застосовує ACL для захисту. Інтерпретує отримані результати, надає аргументовані пояснення щодо конфігурації чи безпеки. Звіти оформлені чітко, із дотриманням вимог, здаються своєчасно.

Виконано 100% обсягу самостійної роботи: аналіз таблиць маршрутизації, порівняння протоколів, дослідження мережеских атак із документацією.

За результатами тестування — **90-100% правильних відповідей.**

**Оцінка «4» (добре) / В–С.** Здобувач освіти відтворює основний навчальний матеріал із незначними невідповідностями. Застосовує необхідну термінологію (LAN, маршрутизатор, TCP, WPA), дає визначення основних понять дисципліни.

Має знання та може пояснити принципи роботи мереж: структуру LAN, маршрутизацію через OSPF, базову різницю між TCP і UDP, основи шифрування. Розуміє принципи безпеки мереж, але може потребувати уточнень у деталях (наприклад, як працює MITM).

Самостійно виконує лабораторні роботи: налаштовує прості мережі, однак допускає дрібні помилки (наприклад, неправильна маска підмережі чи конфігурація портів), які оперативно виправляє. Може частково аргументувати вибір протоколу чи методу захисту, аналізувати результати.

Виконано 90-100% обсягу самостійної роботи: аналіз маршрутизації виконаний, але звіт може бути менш детальним; дослідження атак виконані з незначними недоліками.

За результатами тестування — **75-89% правильних відповідей.**

**Оцінка «3» (задовільно) / D–E.** Здобувач освіти відтворює частину навчального матеріалу: знає базові поняття (IP-адреса, порт, DoS), кілька протоколів (RIP, TCP), але допускає помилки при поясненні складніших концепцій (OSPF, VPN). Ілюструє розуміння прикладів із лекцій чи підручника.

Має початкові знання про мережі: може описати структуру LAN, налаштувати простий маршрут, але не повністю розуміє динамічну маршрутизацію чи принципи безпеки. Володіє базовою термінологією, але плутає деталі (наприклад, TCP із UDP).

Лабораторні роботи виконує лише за детальними інструкціями: будує прості LAN, але допускає помилки (наприклад, неправильний шлюз чи слабкий захист Wi-Fi), які виправляє з допомогою викладача. Звіти оформлені з помилками чи неповні, здаються із запізненням.

Виконано не менше 70% обсягу самостійної роботи: аналіз протоколів поверхневий, дослідження частково завершені.

За результатами тестування — **50-74% правильних відповідей.**

**Оцінка «2» (незадовільно) / FX–F.** Здобувач освіти засвоїв знання у формі окремих фактів: може назвати кілька понять (мережа, IP, фаєрвол), але не пояснює їх використання. Відповідає лише на прості запитання, не володіє термінологією.

Має поверхневі уявлення про мережі: не розуміє, як працюють маршрутизація чи транспортний рівень, не може пояснити принципи безпеки чи захисту. Не розрізняє основні протоколи чи методи.

Не здатен застосовувати теоретичні знання на практиці: лабораторні роботи виконує фрагментарно або не виконує (наприклад, не може налаштувати LAN чи ACL). Звіти не здаються або оформлені з суттєвими порушеннями, здаються несвоєчасно.

Виконано менше 50% обсягу самостійної роботи: аналіз мереж чи безпеки відсутній або не відповідає темі.

За результатами тестування — **менше 50% правильних відповідей.**

### 13. Методичне забезпечення

1. Програма навчальної дисципліни.
2. Силабус навчальної дисципліни.
3. Конспекти лекцій.
4. Інструктивно-методичні матеріали до проведення лабораторних робіт.
5. Тестові завдання для контролю знань за темами програми та підсумкового контролю.
6. Мультимедійні презентації до тем програми.
7. Методичні рекомендації до самостійного вивчення.
8. Екзаменаційний матеріал.
9. Програмне забезпечення: симулятор мережевої інфраструктури Cisco Packet Tracer.

### 14. Рекомендована література

#### Основна

1. [Азаров О. Д., Захарченко С. М., Кадук О. В. та ін. Комп'ютерні мережі: підручник. Вінниця : ВНТУ, 2020. 378 с.](#) (у вільному доступі, репозиторій ВНТУ).
2. [Жураковський Б. Ю., Зенів І. О. Комп'ютерні мережі. Частина 1: навчальний посібник. Київ : КПІ ім. Ігоря Сікорського, 2020. 336 с.](#) (у вільному доступі, репозиторій КПІ)

3. Буров Є. В., Митник М. М. Комп'ютерні мережі. Підручник. Том 2. Львів : Магнолія 2006, 2024. 204 с.

### *Допоміжна*

1. Євсєєв С. П., Дженюк Н. В. Комп'ютерні мережі. Книга 1: Технології комп'ютерних мереж. Київ : Новий світ-2000, 2024. 471 с.

### **15. Інформаційні ресурси**

1. Онлайн-ресурс: Cisco Networking Academy. URL: <https://www.netacad.com>
2. Онлайн-ресурс: Wireshark Documentation. URL: <https://www.wireshark.org/docs>
3. Онлайн-ресурс: RFC Editor. URL: <https://www.rfc-editor.org>
4. Онлайн-ресурс: OWASP. URL: <https://owasp.org>