НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Кафедра комп'ютерних систем, мереж та кібербезпеки

ЗАТВЕРДЖЕНО

Факультет інформаційних технологій

«02» червня 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «КОМП'ЮТЕРНІ МЕРЕЖІ»

(частина 2)

Галузь знань 12 «Інформаційні технології»

Спеціальність 125 «Кібербезпека та захист інформації»

Освітня програма «Кібербезпека»

Факультет інформаційних технологій

Розробники: Матієвський В. В. старший викладач

(посада, науковий ступінь, вчене звання)

Київ – 2025 р.

Опис навчальної дисципліни «Комп’ютерні мережі»

Навчальна дисципліна «Комп’ютерні мережі» є обов’язковим компонентом освітньої програми «Кібербезпека». Вивчення дисципліни забезпечує базову підготовку здобувачів вищої освіти в галузі принципів функціонування, архітектури та технологій сучасних комп'ютерних мереж. Вона знайомить студентів з основними моделями взаємодії мереж (OSI/TCP/IP), протоколами різних рівнів, а також з апаратними та програмними засобами, що використовуються для побудови та адміністрування мережевої інфраструктури. Курс охоплює такі теми, як топології мереж, передача даних, маршрутизація, комутація, мережева безпека, бездротові мережі. Особлива увага приділяється практичним навичкам налаштування та діагностики мережевого обладнання, а також аналізу мережевого трафіку, та забезпечення безпечного функціонування мережі.

Галузь знань, спеціальність, освітня програма, освітній ступінь		
Освітній ступінь	бакалавр	
Спеціальність	125 Кібербезпека та захист інформації	
Освітня програма	«Кібербезпека»	
Характеристика навчальної дисципліни		
Вид	обов’язкова	
Загальна кількість годин	180	
Кількість кредитів ECTS	6	
Кількість змістових модулів	3	
Курсовий проект (робота) (за наявності)	+	
Форма контролю	іспит	
Показники навчальної дисципліни для денної та заочної форм здобуття вищої освіти		
	Форма здобуття вищої освіти	
	денна	**заочна**
Курс (рік підготовки)	4	
Семестр	7	
Лекційні заняття	*30 год.*	
Практичні, семінарські заняття	-	
Лабораторні заняття	*45 год.*	
Самостійна робота	*105 год.*	
Кількість тижневих аудиторних годин для денної форми здобуття вищої освіти	*5 год.*	

1. Мета, компетентності та програмні результати навчальної дисципліни

Мета: теоретична та практична підготовка здобувачів вищої освіти до аналізу функціонування та розробки комп'ютерних мереж та забезпечення їх захисту

Набуття компетентностей:

інтегральна компетентність (ІК):

Здатність розв'язувати складні спеціалізовані- задачі і практичні завдання у галузі кібербезпеки та захисту інформації.

загальні компетентності (ЗК):

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

спеціальні (фахові) компетентності (СК):

СК4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

СК5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.

СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки

Програмні результати навчання (ПРН):

ПРН4. 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.

ПРН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

ПРН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

ПРН13. 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.

ПРН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.

2. Програма та структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин						
	денна форма						
	тижні	усього	у тому числі				
			л	п	лаб	інд	с.р.
Модуль 1. Резервування мереж							
Тема 1. Базові налаштування пристрою. Принципи комутації		13	2		2		9
Тема 2. Віртуальні локальні мережі		20	4		6		10
Тема 3 Протоколи STP, EtherChannel		18	4		4		10
Разом за модулем 1		51	10	0	12	0	29
Модуль 2 Інтернет протокол							
Тема 1. DHCPv4, SLAAC, DHCPv6 Протокол FHRP		24	4		4		16
Тема 2. Безпека рівня 2 та WLAN.		22	2		4		16
Разом за модулем 2		46	6	0	8	0	32
Модуль 3 Маршрутизація. Мережна безпека							
Тема 1. Принципи маршрутизації. Статична та динамічна маршрутизації RIPv2, OSPF		32	4		12		16
Тема 2. Мережна безпека.		28	4		8		16
Тема 3 Функціонування WAN		23	6		5		12
Разом за модулем 3		83	14	0	25	0	44
Усього годин		180	30	0	45	0	105
Курсовий проект (робота) з Комп'ютерних мереж							
Усього годин		180	30	0	45	0	105

3. Теми лекцій

№ з/п	Назва теми	Кількість годин
1	Налаштування комутаторів та маршрутизаторів	2
2	Основи віртуальній мережі	2
3	Маршрутизація між VLAN	2
4	Принцип роботи протоколу STP	2
5	EtherChannel	2
6	DHCPv4	2
7	SLAAC та DHCPv6	2
8	Принципи безпеки LAN	2
9	Статична та динамічна маршрутизації RIPv2	2
10	Основи протоколу OSPFv2 для однієї зони	2
11	Принципи роботи ACL Налаштування ACL для IPv4	4
12	NAT для IPv4	2
13	Функціонування VPN	4

4. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Налаштування проміжних пристроїв	2
2	Впровадження VLAN та транкових каналів	2
3	Маршрутизація між VLAN	4
4	Дослідження принципів роботи STP для уникнення петель	2
5	Впровадження EtherChannel	2
6	Впровадження DHCPv4	2
7	Налаштування HSRP	2
8	Налаштування безпеки на комутаторі	2
9	Налаштування базової WLAN з WLC	2
10	Статична маршрутизація усунення неполадок	2
11	Визначення DR і BDR. Зміна OSPFv2 для однієї зони	4
12	Налаштування OSPFv2 для однієї зони. Усунення неполадок	6
13	Налаштування нумерованих стандартних ACL для IPv4. Налаштування іменованих стандартних ACL для IPv4	4
14	Комплексне завдання щодо розгортання ACL для IPv4	4
15	Налаштування NAT для IPv4	3
16	Налаштування VPN	2

5. Теми самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Захищений віддалений доступ	9
2	Принципи комутації. Виявлення та усунення несправностей із маршрутизацією між VLAN.	10
3	Виявлення та усунення несправностей STP. Виявлення та усунення несправностей EtherChannel.	10
4	Принципи роботи протоколу FHRP	16
5	Налаштування безпеки на комутаторі. Принципи WLAN. Налаштування WLAN	16
6	Налаштування OSPFv2 для однієї зони	16
7	Поняття мережної безпеки IPsec	16
8	Організація WAN. Призначення WAN. Традиційне WAN з'єднання. Сучасні WAN з'єднання	12

Самостійна робота студентів передбачає:
- систематичне вивчення лекційного матеріалу і навчальної літератури, що рекомендуються;
- сумлінну підготовку до лабораторних занять;
- вчасне і якісне оформлення звітів про лабораторні роботи.

Систематичний контроль за самостійною роботою студентів і якістю засвоєння ними поточного навчального матеріалу передбачає:
- перевірку на лабораторних роботах підготовки до виконання роботи;
- вивчення літератури, що рекомендувалася, та конспекту лекцій;
- оформлення звітів з лабораторних робіт.

6. Методи та засоби діагностики результатів навчання:

– усне або письмове опитування;
– співбесіда;

– тестування;
– захист лабораторних/практичних, розрахункових/графічних робіт, проектів;
– пірінгове оцінювання, самооцінювання.

7. Методи навчання *:*

– метод проблемно-орієнтованого навчання;
– метод практико-орієнтованого навчання;
– метод навчальних дискусій;
– метод командної роботи, мозкового штурму

8. Оцінювання результатів навчання.

Оцінювання знань здобувача вищої освіти відбувається за 100-бальною шкалою і переводиться в національну оцінку згідно чинного «Положення про екзамени та заліки у НУБіП України»

8.1. Розподіл балів за видами навчальної діяльності

Вид навчальної діяльності	**Результати навчання**	**Оцінювання**
Модуль 1. Резервування мереж		
Лабораторна робота 1.	. 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. ПРН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.	**12**
Самостійна робота		
Лабораторна робота 2.		**12**
Самостійна робота		
Лабораторна робота 3.		**22**
Самостійна робота		
Лабораторна робота 4.		**12**
Самостійна робота		
Лабораторна робота 5.		**12**
Самостійна робота		
Модульна контрольна робота 1.		**30**
Всього за модулем 1		**100**
Модуль 2 Інтернет протокол		
Лабораторна робота 6.	. 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. ПРН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.	**18**
Самостійна робота		
Лабораторна робота 7.		**17**
Самостійна робота		
Лабораторна робота 8.		**18**
Самостійна робота		
Лабораторна робота 9.		**17**
Самостійна робота		
Модульна контрольна робота 2.		**30**
Всього за модулем 2		**100**

Модуль 3 Маршрутизація. Мережна безпека		
Лабораторна робота 10.	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. ПРН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.	**10**
Самостійна робота		
Лабораторна робота 11.		**10**
Самостійна робота		
Лабораторна робота 12.		**10**
Самостійна робота		
Лабораторна робота 13.		**10**
Самостійна робота		
Лабораторна робота 14.		**10**
Самостійна робота		
Лабораторна робота 15.		**10**
Самостійна робота		
Лабораторна робота 16.		**10**
Самостійна робота		
Модульна контрольна робота 3.		**10**
Всього за модулем 3		**30**
Навчальна робота	**(М1 + М2 + М3)/3*0,7 ≤ 70**	
Екзамен/залік	**30**	
Всього за курс	**(Навчальна робота + екзамен) ≤ 100**	

8.2. Шкала оцінювання знань здобувача вищої освіти

Рейтинг здобувача вищої освіти, бали	Оцінка за національною системою (екзамени/заліки)
90-100	відмінно
74-89	добре
60-73	задовільно
0-59	незадовільно

8.3. Політика оцінювання

Політика щодо дедлайнів та перескладання	роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний).
Політика щодо академічної доброчесності	списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних девайсів). реферати повинні мати коректні текстові посилання на використану літературу
Політика щодо відвідування	відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись індивідуально (в он-лайн формі за погодженням із деканатом)

9. Навчально-методичне забезпечення:

- електронний навчальний курс навчальної дисципліни https://elearn.nubip.edu.ua/course/view.php?id=3485;
- Блозва А.І., Матус Ю.В., Касаткін Д.Ю. Комп'ютерній мережі підручник том.1 К.: Компрінт, 2019 – 483 с.

).

10 Рекомендовані джерела інформації

1. Кулаков, Ю. О. Комп'ютерні мережі [Електронний ресурс] : навчальний посібник/ Кулаков Ю. О. ; КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, 2022. – 247 с.
2. КОМП'ЮТЕРНІ МЕРЕЖІ. Навч. посіб./ Б. Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, 2020. – 336 с.
3. Адміністрування комп'ютерних систем і мереж. Хомуляк М.О. – К.: Магнолія, 2023. – 154 с.
4. Коробейнікова Т. І., Захарченко С. М. Комп'ютерні мережі. Видавництво: Львівська політехніка, 2022, 228 с.
5. Городецька, О. С. Комп'ютерні мережі : навчальний посібник / О. С. Городецька, В. А. Гикавий, О. В. Онищук. - Вінниця : ВНТУ, 2017. - 129 с.
6. Hacha B. Switching, Routing, and Wireless Essentials Companion Guide (CCNAv7). Hoboken : Cisco Press, 2020. 1669 p.
7. Lammle T. CompTIA Network+ Study Guide: Exam N10-008 (Sybex Study Guide). Sybex, 2021. 1008 p.
8. Jernigan S. CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008) / ed. by M. Meyers. eBook : McGraw Hill, 2022. 1255 p.