МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ І. МЕЧНИКОВА
Кафедра математичного забезпечення комп'ютерних систем

"ЗАТВЕРДЖУЮ"
Проректор з науково-педагогічної роботи
"____" _____ 2024 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ВВ06 Захист інформації в комп'ютерних мережах
(назва навчальної дисципліни)

Рівень вищої освіти: *Перший (бакалаврський)*

Галузь знань: *12 – Інформаційні технології*

Спеціальність *123 – Комп'ютерна інженерія*
(код і назва спеціальності(тей)

Освітньо-професійна/наукова програма: *Комп'ютерна інженерія*
(назва ОПП/ОНП)

ОНУ – 2024

Робоча програма навчальної дисципліни «Захист інформації в комп'ютерних мережах» – Одеса:ОНУ, 2024. – 11 с.

Розробники: Шпінарева І.М., к.фіз.-матем. наук, доцент кафедри МЗКС

Робоча програма затверджена на засіданні кафедри математичного забезпечення комп'ютерних систем

Протокол № 1 від. 28 серпня 2024 р.

Завідувач кафедри _____ (Євгеній МАЛАХОВ)
(підпис) (Ім'я ПРІЗВИЩЕ)

Погоджено із гарантом ОПП/ОНП _____

_____ (Людмила ВОЛОЩУК)
(Ім'я ПРІЗВИЩЕ)

Схвалено навчально-методичною комісією (НМК) з ІТ факультету МФІТ

Протокол № 1 від. "30" серпня 2024р.

Голова НМК _____ (Лариса МАРТИНОВИЧ)
(підпис) (Ім'я ПРІЗВИЩЕ)

Переглянуто та затверджено на засіданні кафедри _____

Протокол № ___ від. "____"_____20__ р.

Завідувач кафедри _____ (_____)
(підпис) (Ім'я ПРІЗВИЩЕ)

Переглянуто та затверджено на засіданні кафедри _____

Протокол № ___ від. "____"_____20__ р.

Завідувач кафедри _____ (_____)
(підпис) (Ім'я ПРІЗВИЩЕ)

1. **Опис навчальної дисципліни**

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, спеціалізація, рівень вищої освіти</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td rowspan="15">Загальна кількість:
кредитів – 3

годин – 90

змістових модулів –2</td><td rowspan="15">Галузь знань
<u>12 – Інформаційні технології</u>

Спеціальність
<u>123 – Комп’ютерна інженерія</u>

Рівень вищої освіти:
Перший (бакалаврський)</td><td colspan="2">Нормативна / за вибором (ВНЗ/студента)</td></tr>
<tr><td colspan="2">Рік підготовки:</td></tr>
<tr><td>4-й</td><td>5-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td>7-й</td><td>10-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td>18 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>год.</td><td>год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>36 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>36 год.</td><td>78 год.</td></tr>
<tr><td colspan="2">у т.ч. ІНДЗ*: 20 год</td></tr>
<tr><td colspan="2">Форма підсумкового контролю:
іспит</td></tr>
</table>

* – за наявності

2. Мета дисципліни

Дисципліна призначена для формування знань про комплексні підходи захисту інформації корпоративних інформаційних систем.

Метою є вивчення основних засобів та методів захисту інформації в комп'ютерних мережах .

Основними задачами дисципліни:

– ознайомлення з основами теорії захисту інформації в комп'ютерних мережах;
– вивчення протоколів захищених каналів;
– вивчення програмних і апаратних засобів захисту інформації в комп'ютерних мережах;
– підготовка до виконання дипломних проектів, тематика яких пов’язана з безпекою інформації.

Процес вивчення дисципліни спрямований на формування елементів наступних **компетентностей**:

а) загальних (ЗК): -

б) спеціальних фахових:

КС4. Здатність забезпечувати захист інформації, що обробляється в комп’ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.

КС5. Здатність використовувати засоби і системи автоматизації проектування до розроблення компонентів комп’ютерних систем та мереж, Інтернет додатків, кіберфізичних систем тощо.

КС10. Здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації.

Програмні результати навчання:

ПР1. Знати і розуміти наукові положення, що лежать в основі функціонування комп’ютерних засобів, систем та мереж.

ПР2. Мати навички проведення експериментів, збирання даних та моделювання в комп’ютерних системах.

ПР6. Вміти застосовувати знання для ідентифікації, формулювання і розв’язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей.

ПР9. Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп’ютерних систем та мереж для вирішення технічних задач спеціальності.

ПР10. Вміти розробляти програмне забезпечення для вбудованих і розподілених застосувань, мобільних і гібридних систем, розраховувати, експлуатувати, типове для спеціальності обладнання.

ПР11. Вміти здійснювати пошук інформації в різних джерелах для розв’язання задач комп’ютерної інженерії.

ПР12. Вміти ефективно працювати як індивідуально, так і у складі команди.

ПР13. Вміти ідентифікувати, класифікувати та описувати роботу комп'ютерних систем та їх компонентів.
ПР19. Здатність адаптуватись до нових ситуацій, обґрунтовувати, приймати та реалізовувати у межах компетенції рішення.
ПР20. Усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення.
ПР21. Якісно виконувати роботу та досягати поставленої мети з дотриманням вимог професійної етики.

Очікувані результати навчання. У результаті вивчення навчальної дисципліни студент повинен
знати*: основні поняття і методи захисту інформації в комп'ютерних мережах, моделі захисту мережі, криптографічні протоколи захисту інформації, програмні та апаратні засоби захисту інформації в комп'ютерних мережах.*
вміти*: розробляти політику безпеки мережі, виконувати захист мережі, застосовуючи сучасні інструменти безпеки.*

3. Зміст навчальної дисципліни

Змістовний модуль 1. ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Тема 1. Класифікація мережевих атак і методи протидії атакам. Етапи мережевої атаки. Загрози та вразливості дротових корпоративних мереж. Способи забезпечення інформаційної безпеки (Частковий і комплексний підхід). Шляхи вирішення проблем захисту інформації в мережах. Дослідження мережевої топології. Методи сканування портів.
Література: [1, 2, 3, 4, 5].
Тема 2. Захист комп'ютерної мережі з використанням міжмережевих екранів. Поняття брандмауера (МЕ). Функції МЕ. Політика міжмережевого екранування. Архітектура брандмауера. Основні схеми підключення брандмауера. Проблеми безпеки брандмауера.
Література: [3, 4, 5, 6].
Тема 3. Адаптивна безпека мережі: технології виявлення атак, технології управління ризиками. Компоненти моделі адаптивного управління безпекою: адаптивний і керуючий.
Література: [3, 4, 5, 6, 7].
Тема 4. Технологія аналізу захищеності. Рівні моделі OSI, на яких функціонують сканери безпеки. Механізми роботи сканерів безпеки: сканування і зондування. Методи, що реалізують механізми сканування: перевірка. Схема проведення аналізу захищеності (системи Internet Scanner).
Література: [3, 4, 5, 6, 8].
Тема 5. Системи виявлення атак (IDS). Класифікація систем виявлення атак IDS. Компоненти та архітектура IDS. Сигнатурний аналіз і виявлення аномалій. Розподілені системи виявлення атак. Методи реагування. Система виявлення атак Snort. Література: [3, 4, 5, 6, 7 , 8]

Змістовний модуль 2. ОРГАНІЗАЦІЯ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ та БЕЗПЕКА WI-FI

Тема 6. Організація віртуальних приватних мереж (VPN). Задачі, які вирішуються VPN. Туннелірованіє VPN. Варіанти побудови віртуальних захищених каналів. Класифікація VPN за рівнем моделі OSI. Класифікація VPN з архітектури технічного рішення: внутрішньо корпоративні мережі VPN, VPN з віддаленим доступом, міжкорпоративні мережі VPN. Класифікація VPN за способом технічної реалізації.

Література: [3, 4, 5, 6, 7 , 8]

Тема 7. Методи організації захисту мережі WI-FI. Атаки на WI-FI мережу. Протоколи захисту WEP, WPA, WPA2.

Література: [4, 5, 6, 7].

Тема 8. Сервери аутентифікації : RADIUS, TACACS+, DIAMETR.

Література: [3, 4, 5, 6, 8].

4. Структура навчальної дисципліни

Назви тем	Кількість годин									
	Денна форма					Заочна форма				
	Усього	у тому числі				Усього	у тому числі			
		л	п/с	лаб	ср		л	п/с	лаб	ср
1	2	3	4	5	6	7	8	9	10	11
Змістовий модуль 1. Захист інформації в комп'ютерних мережах.										
Тема 1.	6	2		2	2	11	1			10
Тема 2.	6	2		2	2	13	1		2	10
Тема 3.	8	2		2	2	10.5	0.5			10
Тема 4.	8	2		2	2	11.5	0.5		1	10
Тема 5.	8	2		4	2	11	1			10
Разом за змістовим модулем 1	**36**	**10**		**12**	**10**	**57**	**4**		**3**	**50**
Змістовий модуль 2. Організація віртуальних приватних мереж та безпека wi-fi.										
Тема 1.	11	3		8	2	12	1		1	10
Тема 2.	10	2		8	2	11.5	0.5		1	10
Тема 3.	13	3		8	2	9.5	0.5		1	8
Разом за змістовим модулем 2	**34**	**8**		**24**	**6**	**33**	**2**		**3**	**28**
ІНДЗ	20				**20**					
Усього годин	**90**	**18**		**36**	**36**	**90**	**6**		**6**	**78**

Форма контролю: **КО** –контрольне опитування (поточне)

ІЗ –індивідуальне завдання (домашнє)

КР – контрольна робота

КМ – контроль модуля за тестовою системою

5. Теми семінарських занять

Семінарські заняття не передбачені.

6. Теми практичних занять

Практичні заняття не передбачені.

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
		Денна форма	Заочна форма
1	Налаштування мережевих сервісів в програмі Packet Tracer. Сервер DHCP, WEB,FTP	2	
2	Приховування внутрішню структуру локальної мережі за допомогою NAT і обмеження доступу до мережі.	4	2
3	Списки управління доступом ACL	6	2
4	Cisco ASA 5505. Firewall Appliance. Побудова захисту КМ Firewall.	4	
5	Побудова демілітаризованої зони	4	
6	Побудова VPN за допомогою CiscoASA.	4	2
7	Протокол AAA	4	
8	Захист мережі WI-FI	4	
9	Протокол SYSLOG I NTP	4	
	Разом	**36**	**6**

8. Самостійна робота

№ з/п	Назва теми	Кількість годин	
		Денна форма	Заочна форма
1	Аналіз безпеки мережі за допомогою сніферу Wireshark [1].	4	14
2	Технологія аналізу захищеності.Рівні моделі OSI, на яких функціонують сканери безпеки. Механізми роботи сканерів безпеки: сканування і зондування. Методи, що реалізують механізми сканування: перевірка.Схема проведення аналізу захищеності (системи Internet Scanner) [1].	4	14
3	Системи виявлення атак. (IDS).Методи аналізу мережевої інформації. Класифікація систем виявлення атак IDS: за способом реагування, за способом виявлення атаки (виявлення зловживань і виявлення аномалій), за	4	14

	способом збору інформації про атаку (на рівні мережі (network-based), на рівні хоста (host-based), на рівні додатку (application-based). Компоненти та архітектура IDS.ПЗ SNORT [1]		
4	Розробка ACCESS LIST [1].	4	16
Разом без ІНДЗ		**16**	**58**
ІНДЗ		**20**	**20**
Усього		**36**	**78**

До самостійної роботи відноситься:
[1] – підготовка до лекцій, лабораторних занять.

8.1. **Індивідуальне навчально-дослідне завдання**

Розрахунково-графічна робота полягає в налаштуванні захисту комп'ютерної мережі предметної області проекту організації/підприємства та аналізу безпеки даної мережі. Комп'ютерна мережа спроектована та налаштована в середовищі візуального моделювання мереж.
Студент повинен:
– розробити політику безпеки КМ організації/ підприємства;
– виконати приховування внутрішньої структури локальної мережі та обмеження доступу до мережі з Інтернету;
– виконати обмеження доступу легітимних користувачів КМ;
– виконати захист бездротової мережі;
– вибрати антивірусну програму, firewall, систему виявлення атак на сервери та вузли мережі;
– виконати аналіз безпеки комп'ютерної мережі.

9. **Методи навчання**

Лекції з використанням мультимедійного презентаційного матеріалу.

10. **Методи контролю**

Під час **захисту індивідуального завдання** студент повинен:
– роз'яснити створену політику безпеки мережі;
– продемонструвати та роз'яснити методи захисту мережі.
Під час **підсумкового контролю** студент повинен відповісти на 2 запитання екзаменатора з переліку, наведеному у п. 11.
Критерії оцінювання на підсумковому модульному контролі:
1. Відповідь повинна бути повною і короткою. Вона не повинна мати в собі матеріал, що не відноситься до сутті питання.
2. Чітко формулювати твердження, вправно застосовувати необхідні формули і знання основних питань програми.
3. Відповіді, що мають помилкові твердження оцінюються виходячи з близькості відповіді до правильної.

4. Пропуски в обґрунтуванні тверджень враховуються і це призводить до зменшення кількості балів.
5. Малі недоліки, неточності при викладенні матеріалу, зменшують кількість балів.
6. Незнання і нерозуміння основної ідеї теоретичного питання або задачі призводить до зняття до 90 % балів.
7. Якщо відповідь на питання відсутня то виставляється нуль балів.

11. **Питання для підсумкового контролю**

1. Поясніть загальні поняття захисту інформації.
2. Описати атаки на комп'ютерні мережі.
3. Описати роботу служби DNS.
4. Описати роботу служби DHCP.
5. Описати як налаштовується клієнт DHCP.
6. Вкажіть розташування папки з контентом Web вузла і FTP сервера.
7. Описати всі можливі схеми роботи служби NAT.
8. Поясніть які приватні IP адреси використовуються службою NAT в кожному класі адрес.
9. Перелічіть переваги і недоліки служби NAT. Перерахуйте етапи настройки служби NAT.
10. Описати основні проблеми в роботі сервера NAT
11. Описати які параметри контролює розширені списки доступу?
12. Наведіть приклад команди, роздільною передачу пакетів від хоста на все веб-сервера.
13. Описати основні типи списків доступу.
14. Описати функції Firewall.
15. Особливості функціонування ME Firewall на різних рівнях моделі OSI.
16. Назвіть основні схеми підключення міжмережевих екранів. Опишіть функціонування схеми з закритою підмережою, що захищається, і з відкритою підмережою, що не захищається.
17. Поясніть поняття системи виявлення атак.
18. Описати методи виявлення атак.
19. Описати IPS, IDS, HIDS, NIDS.
20. Поясніть поняття Virtual Private Network.
21. Описати на яких уровнях моделі OSI працює VPN.

12. **Розподіл балів, які отримують студенти**

Поточний та періодичний контроль								Підсумковий контроль (іспит)	Сума балів
Змістовий модуль №1					Змістовий модуль № 2			ІНДЗ		
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8			
5	5	5	5	5	5	5	5	20	40	100

Т1, Т2 ... – теми змістових модулів

Шкала оцінювання: національна та ECTS

Загальна сума балів	Оцінка ECTS	Національна шкала	
90 — 100	A – «відмінно»	5 «відмінно»	«залік»
85 — 89	B – «дуже добре»	4 «добре»	
75 — 84	C – «добре»		
70 — 74	D – «задовільно»	3 «задовільно»	
60 — 69	E – «допустимо»		
35 — 59	F – «незадовільно з можливістю повторного складання»	2 «незадовільно»	«незалік»
0 — 34	FX – «незадовільно з обов'язковим повторним курсом»		

13. Навчально-методичне забезпечення

Конспект лекцій у електронному форматі; методичні вказівки для виконання лабораторних робіт; нормативні документи; презентаційні матеріали.

14. Рекомендована література

Основна

1. НД ТЗІ 1.6-004-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що становить державну таємницю.
2. НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.
3. Проєктування комплексних систем захисту інформації / Підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць. Львів : Видавництво Львівської політехніки, 2020. 320 с.
4. Захист інформації в комп'ютерних системах та мережах : навч. посіб. / С.Г.Семенов, А.О.Подорожняк, О.І.Баленко, С.Ю.Гавриленко – Х.: НТУ «ХПІ», 2014.– 251 с.
5. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с.

Додаткова

6. Комплексні системи захисту інформації : навчальний посібник / Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2018. – 118 с.
7. Комплексні системи захисту інформації: проектування, впровадження, супровід. Збірник лекцій [Електронний ресурс] / Гребенніков В.В. // 2015 - Режим доступу: http://www.cryptohistory.ru/for students/ 03-KSZ
8. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін. – К. : ДУТ-КНУ, 2016. – 178 с.

15. **Електронні інформаційні ресурси**

1. Cisco Networking Academy Курси:Cybersecurity Essentials, Cisco Cyber Ops – Режим доступу: http://www.cisco.com/web/learning/netacad/index.html
2. Whireshark Режим доступу: https://www.wireshark.org/