Форма № Н - 3.04

Національний університет біоресурсів і природокористування України
Кафедра комп'ютерних систем, мереж та кібербезпеки

"ЗАТВЕРДЖУЮ"
Декан факультету інформаційних технологій
_____ проф. О.Г. Глазунова
"__" _____ 2023 р.

СХВАЛЕНО
на засіданні кафедри
комп'ютерних систем, мереж та кібербезпеки
Протокол №10 від "17" травня 2023 р.
Завідувач кафедри
(доц. Касаткін Д.Ю.)

РОЗГЛЯНУТО
Гарант ОП
«Кібербезпека»
_____
Гарант ОП
_____ (проф. Лахно В.А.)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
"СИСТЕМИ МОНІТОРИНГУ ЗАГРОЗ ТА АТАК"

зі спеціальності 125 – «Кібербезпека»
(шифр і назва напряму підготовки)
Освітня програма «Кібербезпека»

факультет інформаційних технологій
(назва факультету)

Київ – 2023 р.

Опис навчальної дисципліни
СИСТЕМИ МОНІТОРИНГУ ЗАГРОЗ ТА АТАК
(назва)

Галузь знань, напрям підготовки, спеціальність, освітньо-кваліфікаційний рівень		
Галузь знань	Інформаційні технології	
Спеціальність	125 – «Кібербезпека»	
другий (магістерський) рівень	Бакалавр	
Характеристика навчальної дисципліни		
Вид	Вибіркова	
Загальна кількість годин	120	
Кількість кредитів ECTS	4	
Кількість змістових модулів	2	
Курсовий проект (робота) (якщо є в робочому навчальному плані)	-	
Форма контролю	Іспит	
Показники навчальної дисципліни для денної та заочної форм навчання		
	денна форма навчання	заочна форма навчання
Рік підготовки	2023-2024	
Семестр	2	
Лекційні заняття	30 год.	
Практичні, семінарські заняття		
Лабораторні заняття	30 год.	
Самостійна робота	60 год.	
Індивідуальні завдання		
Кількість тижневих годин для денної форми навчання: аудиторних	4 год.	

1. Мета та завдання навчальної дисципліни

Дана навчальна дисципліна є теоретичною основою сукупності знань та вмінь, що формують профіль фахівця в області мережевої безпеки. На базі здобутих знань та умінь фахівець зможе вирішувати професійні задачі, що базуються на сучасних технологіях та методах захисту інформації у сучасних інформаційно-комунікаційних систем та мереж.

Метою викладання дисципліни є розкриття сучасних методів захисту інформації в комп'ютерних системах та мережах і ознайомлення з особливостями їх апаратної та програмної реалізацій.

У результаті вивчення даної навчальної дисципліни студент повинен:

Знати:

- види загроз інформації в комп'ютерних системах та мережах;
- основні протоколи безпеки;
- принципи функціонування систем захисту;
- основні програмні і апаратні засоби захисту інформації в комп'ютерних системах та мережах;
- засоби організації розмежування доступу комп'ютерних мережах.

Вміти:

- виконати аналіз безпеки комп'ютерної системи або мережі та усунути можливі шляхи несанкціонованого доступу;
- здійснити організаційні та програмні заходи щодо підвищення рівня безпеки зберігання інформації;
- виконати адміністрування прав доступу до комп′ютерної системи та мережі з метою перешкоди призначення невиправданих привілеїв;
- перевірити надійність захисту інформації та стійкості його щодо хакерських атак шляхом моделювання загроз;

- підібрати тип та структуру локальної комп'ютерної мережі;

- підібрати комплекс необхідних апаратно-програмних засобів для захисту комп'ютерної системи та мережі.

Набуття компетентностей:

Відповідно до освітньої програми підготовки фахівців за спеціальністю 125 «Кібербезпека» навчальна дисципліна забезпечує формування загальних і фахових компетентностей:

Загальні компетентності:

КЗ1. Здатність застосовувати знання у практичних ситуаціях.

КЗ2. Знання та розуміння предметної області та розуміння професії.

КЗ8. Здатність до абстрактного і системного мислення, аналізу та синтезу.

Спеціальні (фахові) компетентності:

СК6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

СК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)..

В результаті вивчення навчальної дисципліни студент набуде певні програмні результати, а саме:

ПРН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.

ПРН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

Навчальна програма розрахована на здобувачів вищої освіти, які навчаються за освітньою програмою підготовки бакалаврів за спеціальністю 125 «Кібербезпека».

Робоча програма побудована за вимогами кредитно-модульної системи організації навчального процесу у закладах вищої освіти і використанням академічної системи оцінювання досягнень студентів та шкали оцінок Європейської кредитно-трансферної системи (ECTS).

Навчальна програма розроблена на підставі наступних документів:

-освітньо-професійна програма підготовки фахівців за спеціальністю «Кібербезпека»;

-навчальний план підготовки бакалаврів за спеціальністю «Кібербезпека».

Навчальна програма характеризує шляхи перетворення інформації, що одержується студентом впродовж вивчання курсу, і відбиває зміст курсу, розподілення його на розділи та їх обсяги, дані про форми вивчення та контролю знань.

Теоретичною базою для вивчення є курс «Комп'ютерні системи».

2. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	денна форма						Заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Змістовий модуль 1. Моніторинг мережевої безпеки.												
Тема №1. Основні поняття та концепції моніторингу. Компоненти та рівні систем моніторингу.	7	2		0		5						
Тема №2. Побудова схеми управлінського моніторингу конкретного об'єкту.	11	2		4		5						
Тема №3. Сутність моніторингу в окремих сферах діяльності. Класифікаціясистем моніторингу.	11	2		4		5						
Тема №4. Функції, задачі та принципиорганізації моніторингу.	9	2		2		5						
Тема №5. Датчики,як джерело збору інформації у автоматизованих системах моніторингу.	9	2		2		5						
Тема №6. Дослідження принципів роботидатчиків.	9	2		2		5						
Разом за змістовим модулем 1	**56**	**12**		**14**		**30**						
Змістовий модуль 2. Практичне застосування систем моніторингу загроз та атак.												
Тема № 7. Організація систем моніторингу загроз та атак підприємства.	9	2		2		5						
Тема №8. Системи моніторингу загроз підприємства АПК.	7	2		0		5						
Тема № 9. Системи моніторингу комп'ютерних мереж, системи виявлення атак (СВА), сканери мережі SIEM, HP Operations Manager, ManageEngine OpManager, SolarWinds, IBM Tivoli, WhatsUp Gold.	13	2		6		5						
Тема № 10. Кібергігієна - як основа захистувідзагроз в інформаційномусуспільстві.	11	4		2		5						
Тема № 11. IDS.	13	4		4		5						
Тема № 12. IPS.	11	4		2		5						
Разом за змістовим модулем 2	**64**	**18**		**16**		**30**						
Усього годин за курс	**120**	**30**		**30**		**60**						

4. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
	Не передбачено робочим навчальним планом	

5. Теми практичних занять

№ з/п	Назва теми	Кількість годин
	Не передбачено робочим навчальним планом	

6. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1.	Побудова схеми управлінського моніторингу конкретного об'єкту.	4
2.	Функції, задачі та принципиорганізації моніторингу.	4
3.	Налагодження зору інформації з датчиків систем моніторингу загроз та атак.	4
4.	Організація систем моніторингу загроз та атак підприємства.	4
5.	Системимоніторингу комп'ютерних мереж, системи виявлення атак (СВА), сканери мережі SIEM, HP Operations Manager,ManageEngine OpManager, SolarWinds, IBM Tivoli, WhatsUp Gold.	6
6.	IDS.	4
7.	IPS.	4
	Разом	**30**

7. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Функції, задачі та принципи організації моніторингу (На основі аналізу моніторингових онлайн ресурсів)	5
2	Поняття, структура, алгоритм розробки Паспорта загрози національнійбезпеці	5
3	Датчики, як джерело збору інформації у автоматизованих системах моніторингу. Дослідження принципів роботи датчиків	5
4	Організація відеонагляду як засобу моніторингу периметру, онлайн камери як засіб моніторингу загроз суспільній безпеці	5
5	Організація політики та систем моніторингу інформаційної безпекипідприємств	5
6	Засоби запобігання загрозам інформаційній безпеці при роботі з мережею"Інтернет"	5
7	Загрози інформаційної безпеки держави в соціальних мережах та месенджерах	5
8	Системи моніторингу комп'ютерних мереж, системи виявлення атак (СВА),сканери мережі: SIEM, HP Operations Manager, ManageEngine OpManager, SolarWinds, IBM Tivoli, WhatsUp Gold.	5
9	Механізми моніторингу загроз інформаційній безпеці Українисоціально-економічного характеру.	5
10	Автоматизовані системи моніторингу. Пристрої управління датчиками, на прикладі Arduino Mega 2560.	5
11	Автоматизовані системи моніторингу, на прикладі систем Smart house та професійної системи безпеки Ajkc.	5
12	Інформаційно-аналітична технологія моніторингу засобами Micro Strategy Platform.	5
	Разом	**60**

8. Контрольні питання для перевірки знань студентів (приклади питань)

1. Основні поняття: “моніторинг”, “системи моніторингу”.
2. Схема управлінського моніторингу конкретного об'єкту.
3. Складові системи моніторингу.
4. Рівні забезпечення моніторингу.
5. Загрози інформаційній безпеці як об’єкт моніторингу.
6. Сутність моніторингу в окремих сферах діяльності.
7. Класифікація систем моніторингу.
8. Функції та задачі моніторингу.
9. Принципи організації моніторингу.
10. Поняття, структура, алгоритм розробки Паспорта загрози інформаційній безпеці
11. Роль державних органів у організації системи моніторингу загроз інформаційній безпеці.

12. Датчики, як джерело збору інформації у автоматизованих системах моніторингу
13. Принципи роботи датчиків
14. Засоби збору та зберігання інформації у системах моніторингу загроз.
15. Бази даних у системах моніторингу загроз.
16. Штучний інтелект у системах моніторингу загроз
17. Організація відеонагляду та онлайн камери як засіб моніторингу
18. Організація систем моніторингу загроз підприємства
19. Спеціалізовані системи моніторингу: банківський моніторинг.
20. Системи моніторингу загроз інформаційній безпеці
21. Системи моніторингу комп'ютерних мереж, системи виявлення атак (СВА), сканери мережі
22. Кібергігієна - як основа захисту від загроз в інформаційному суспільстві
23. Класифікація загроз національній безпеці.
24. Види загроз інформаційній безпеці.
25. Загрози інформаційної безпеки держави в соціальних мережах.
26. Система моніторингу загроз соціальній безпеці.
27. Система моніторингу загроз економічній безпеці.
28. Система моніторингу загроз інформаційній безпеці.
29. Системи моніторингу загроз оборонно-військової галузі
30. Моніторингові функції Головного центру спеціального контролю
31. Діяльність Спеціальної моніторингової місії ОБСЄ в Україні
32. Безпілотні літаючі апарати як засіб моніторингу
33. Автоматизовані системи моніторингу, на прикладі систем Smart house та Професійна система безпеки Ауах.

9. Методи навчання

Проведення лекцій з використанням технічних засобів навчання.

Виконання лабораторних робіт з використанням наочних технічних засобів навчання у вигляді систем моделювання за допомогою інженерних пакетів проектування цифрових пристроїв.

Проведення самостійної роботи засобами інформаційно-комунікаційних технологій в освіті.

Використовується електронний навчальний курс на платформі Moodle.

10. Форми контролю

Захист результатів виконання лабораторних робіт.

Контрольне тестування відповідно до кожного змістовного модуля, що створений у комп'ютерному навчальному середовищі.

Підсумкова атестація: іспит.

11. Розподіл балів, які отримують студенти

Оцінювання знань студента відбувається за 100-бальною шкалою і переводиться в національні оцінки згідно з табл. 1 «ПОЛОЖЕННЯ про екзамени та заліки у НУБіП України» (наказ про уведення в дію від «26» квітня 2023 р. протокол № 10):

Рейтинг здобувача вищої освіти, бали	**Оцінка національна за результати складання екзаменів заліків**	
	Екзамен	**Залік**
90-100	Відмінно	зараховано
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	не зараховано

Для визначення рейтингу студента із засвоєння дисципліни $R_{дис}$ (до 100 балів) одержаний рейтинг з атестації $R_{АТ}$ (до 30 балів) додається до рейтингу студента з навчальної роботи $R_{НР}$ (до 70 балів): $R_{дис}=R_{НР}+R_{АТ}$.

12. Методичне забезпечення

Електронний навчальний курс на платформі Moodle вміщує методичне забезпечення включаючи: лекції, презентації до лекцій, методичні вказівки до виконання лабораторних робіт, глосарій термінів тощо.

13. Рекомендована література

Базова

1. Анна Корченко, Методи ідентифікації аномальних станів для систем виявлення вторгнень. Монографія, Київ, ЦП «Компринт», 2019 – 361 с.

2. Методи та засоби захисту інформації [Навчальний посібник] / В.А. Лахно, Є.В. Василіу, В.М. Гладких, В.М. Домрачев, Н.М. Сивкова. – К. : ЦП «Компринт» О.В., 2020. – 444 с.

Допоміжна

1. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. – Х.: Вид. ХНЕУ, 2010. – 316 с.

2. Браіловський М.М. Захист інформації у банківській діяльності / М.М. Браіловський, Г.П. Лазарєв, В.О. Хорошко. – К.: ТОВ “ПоліграфКонсалтинг”, 2010. – 216 с.

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.

14. Інформаційні ресурси

1. ДСТУ ISO/IEC 11770-3:2002 «Інформаційні технології. Методи захисту».

2. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

3. НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в автоматизованій системі.