КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

Кафедра інформаційних систем та технологій

«ЗАТВЕРДЖУЮ»
Заступник декана з навчально-виховної роботи
_____ Наталія ТМЄНОВА
(підпис)
«___» _____ 2024 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Захист інформації в інтернеті речей»

для студентів

галузь знань **12 «Інформаційні технології»**

спеціальність **126 «Інформаційні системи та технології»**

освітній рівень **бакалавр**

освітня програма **«Програмні технології інтернет речей»**

вид дисципліни **вибіркова**

Форма навчання **денна**

Навчальний рік	**2024/2025**
Семестр	**8**
Кількість кредитів ECTS	**4**
Мова викладання, навчання та оцінювання	**українська**
Форма заключного контролю	**залік**

Викладачі: Ірина БОРИСЕНКО к.т.н., доцент, Олена СІПКО к.т.н., доцент

Пролонговано: на 20__/20__ н.р. _____(_____) «__»___ 20__р.
(підпис, ПІБ, дата)

на 20__/20__ н.р. _____(_____) «__»___ 20__р.
(підпис, ПІБ, дата)

КИЇВ – 2024

Розробник: Максим ДЕЛЕМБОВСЬКИЙ., к.т.н., доцент, Ірина БОРИСЕНКО к.т.н., доцент кафедри інформаційних систем та технологій, Олена СІПКО к.т.н., доцент кафедри інформаційних систем та технологій

«ЗАТВЕРДЖЕНО»

Завідувач кафедри інформаційних систем та технологій

_____ д.т.н., проф. Володимир ДРУЖИНІН

Протокол №10-23/24 від «27» червня 2024 року

Схвалено науково - методичною комісією факультету інформаційних технологій

Протокол від «27» червня 2024 року №9

Голова науково-методичної комісії _____ (Ганна КРАСОВСЬКА)

Програму перевірено

«_____» _____ 20___ року

1. Мета дисципліни – полягає в навчанні студентів забезпечувати безпеку та конфіденційність даних у світі швидкого розвитку IoT, а також усвідомлення важливості цих аспектів для сталого функціонування сучасних технологічних рішень.

2. Попередні вимоги до опанування або вибору навчальної дисципліни:

1) успішне опанування дисципліни «Основи побудови інфокомунікаційних мереж», «Технології та протоколи мультисервісних мереж», «Сучасні інформаційні системи і технології», «Основи інформаційної безпеки»;
2) володіння навичками користування комп'ютером на рівні досвідченого (просунутого) користувача.

3. Анотація навчальної дисципліни:
Дисципліна "Захист інформації в Інтернеті речей" пропонує студентам глибше розібратися у викликах і можливостях, пов'язаних з безпекою інформації в світі Інтернету речей. Вона охоплює основні аспекти захисту даних, аутентифікації, шифрування та виявлення загроз у мережах IoT. Студенти отримають навички оцінювання ризиків і розробки стратегій захисту для пристроїв та даних у цьому сучасному і динамічному середовищі. Дисципліна також розглядає практичні застосування захисту даних у різних сферах, де IoT грає ключову роль, зокрема в медицині, транспорті та побуті.
Курс дисципліни розроблено на базі курсу Академії Cisco IoT Fundamentals: IoT Security.

4. Завдання (навчальні цілі): Основними завданнями полягає в навчанні студентів засобам та методам захисту даних та пристроїв у сучасних мережах IoT, оцінці ризиків та розробці стратегій захисту, а також в розгляді практичних застосувань та адаптації до змін в цій області.

5. Результати навчання за дисципліною:

Результат навчання (1. знати; 2. вміти; 3. комунікація; 4. автономність та відповідальність)		Форми (та/або методи і технології) викладання і навчання	Методи оцінювання та пороговий критерій оцінювання (за необхідності)	Відсоток у підсумковій оцінці з дисципліни
Код	**Результат навчання**			
1.1	Знати класифікацію типів мережевих атак IoT.	лекції	Опитування, тестування	20%
1.2	Знати способи визначення вразливостей IoT і атаки на них.	лекції	Опитування, тестування	20%
1.3	Знати моделі реагування для усунення інцидентів безпеки IoT	лекції	Опитування, тестування	20%
2.1	Вміти аналізувати роботу мережевих протоколів і служб.	Практичні роботи	Звіт по практичній роботі	10%
2.2	Вміти використовувати засоби мережевого моніторингу для визначення атак на мережеві протоколи і служби.	Практичні роботи	Звіт по практичній роботі	10%
2.3	Вміти застосовувати різні способи запобігання несанкціонованому доступу до IoT	Практичні роботи	Звіт по практичній роботі	10%
3.1	Працювати в команді при налагодженні інформаційних систем і визначенню вразливостей IoT.	Практичні роботи	Командна робота	10%

6. Співвідношення результатів навчання дисципліни із програмними результатами навчання

Результати навчання дисципліни / **Програмні результати навчання**	**1.1**	**1.2**	**1.3**	**2.1**	**2.2**	**2.3**	**3.1**
ПР 2 Застосовувати знання фундаментальних і природничих наук, системного аналізу та технологій моделювання, стандартних алгоритмів та дискретного аналізу при розв'язанні задач проектування і використання інформаційних систем та технологій.	+					+	+
ПР 4 Проводити системний аналіз об'єктів проектування та обґрунтовувати вибір структури, алгоритмів та способів передачі інформації в інформаційних системах та технологіях.	+	+	+	+	+	+	+
ПР 10 Розуміти і враховувати соціальні, екологічні, етичні, економічні аспекти, вимоги охорони праці,	+	+					+

виробничої санітарії, пожежної безпеки та існуючих державних і закордонних стандартів під час формування технічних завдань та рішень							
ПР 19 Використовувати можливості апаратного забезпечення, використовувати можливості операційних систем, використовувати можливості мережевих програмних систем, забезпечувати захищеність програм і даних від несанкціонованих дій.				+	+		

7. Схема формування оцінки.

7.1. Форми оцінювання студентів:

- семестрове оцінювання:

Максимальна кількість балів яку може отримати студент протягом семестру - 100 балів (100%).

1. Практичні роботи: 36 (мінімум) -80 (максимум) балів.

2. Підсумкова модульна контрольна робота: 12 (мінімум) -20 (максимум) балів.

Питома вага результатів навчання у підсумковій оцінці за умови опанування дисципліни на належному рівні така:

1. Результати навчання 1 (знання): РН 1.1-1.3 – до 25%;

2. Результати навчання 2 (вміння): РН 2.1-2.3 – до 65%;

3. Результати навчання 3 (комунікація): РН 3.1 – до 10%.

- підсумкове оцінювання (у формі заліку):

Залік виставляється студенту за результатами поточної роботи впродовж семестру. При отриманні результуючої підсумкової кількості балів від 60 (60% від максимальної кількості) і вище студенту виставляється «зараховано». Студенти, які набрали сумарно меншу кількість балів ніж критично-розрахунковий мінімум — 48 балів отримають оцінку «не зараховано» і мають право на перескладання згідно порядку перескладання, який встановлюється Положенням про організацію освітнього процесу, а терміни перескладання графіком складання сесії.

При бажанні студента, за наявності залікових балів покращити свій результат, він має право здавати залік, на який виноситься 20 балів, але сумарна кількість балів при цьому не може перевищувати 100 балів.

7.2 Організація оцінювання:

Студент допускається до підсумкової модульної контрольної роботи при наявності всіх зданих і захищених лабораторних робіт з оцінкою не нижче 36 балів

Проведення підсумкової модульної контрольної роботи здійснюється шляхом тестування в середовищі netacad.com (Cisco) або https://moodle.fit.knu.ua (LMS Moodle).

Підсумкове оцінювання: складає максимально **20** модульних балів (**20%** від загального рейтингу).

Здобувач допускається до підсумкового оцінювання за умови здачі та захисту всіх передбачених планом лабораторних робіт.

Підсумкова оцінка визначається шляхом підсумовування балів **семестрової роботи** та **підсумкової модульної контрольної роботи**.

При описаному вище розрахунку отримаємо:

	Лабораторні роботи	Тести по лекціях, дискус, аналітична доповідь	МКР	Підсумкова оцінка
Min. – балів	36	12	12	60
Max. –балів	60	20	20	100

7.3 Шкала відповідності оцінок

Зараховано	60-100
Незараховано	0-59

8. Структура навчальної дисципліни.

№ п/п	Назва лекції	Кількість годин		
		Лекції	Лабораторні	СР
1	Тема 1. IoT під атакою.	2	4	6
2	Тема 2. Системи та архітектури IoT	2	6	12
3	Тема 3. Поверхня атаки рівня пристроїв Інтернету речей.	4	6	12
4	Тема 4. Поверхня атаки рівня зв'язку Інтернету речей.	4	6	12
5	Тема 5. Поверхня атаки рівня додатків IoT.	4	6	12
6	Тема 6. Оцінка вразливості та ризиків у системі IoT.	4	6	10
	Всього годин	20	34	64

Загальний обсяг 120 *год.,* в тому числі:
Консультації – 2 ***год***
Лекцій **– 20** *год.*
Лабораторні заняття **- 34** *год.*
Самостійна робота **- 64** *год.*

9. Рекомендовані джерела:

Основна: *(Базова)*

2. Practical IoT Hacking: The Definitive Guide to Attacking the Internet of Things. Чанціс Ф., Стаіс І. - ISBN: 978-5-97060-974-3 – 2022
3. Остапов С.Е., Євсеєв С.П., Король О.Г. Кібербезпека: сучасні технології захисту. / Навчальний посібник для студентів вищих навчальних закладів – Львів: «Новий Світ - 2000», 2021. – 678 с.
4. Бабак В.П. Теоретичні основи захисту інформації / В. П. Бабак: Підручник. – Книжкове видавництво НАУ, 2008. – 752 с.
5. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп'ютерні мережі [навчальний посібник] – Львів, «Магнолія 2006», 2013. – 256 с.

Додаткова:

1. IoT Fundamentals: IoT Security Cisco / [Електронний ресурс]. - Режим доступу: https://www.netacad.com/courses/cybersecurity/iot-security

10. Додаткові ресурси:

Інформаційні ресурси

https://moodle.fit.knu.ua/ - Захист інформації в інтернеті речей Moodle Київського національного університету імені Тараса Шевченка.

https://netacad.com/ - мережева академія Cisco.