КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра інформаційних систем та технологій

«ЗАТВЕРДЖУЮ»
Заступник декана з навчально-виховної роботи
_____ Наталія ТМЄНОВА
«___»_____2024 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Захист інформації в Інтернеті речей»

для здобувачів освіти

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	**6**
Кількість кредитів ECTS	**4**
Мова викладання, навчання та оцінювання	**українська**
Форма заключного контролю	**залік**

Викладачі: доцент кафедри, к.т.н. Олена СІПКО

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

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

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

КИЇВ – 2024

Розробник: 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 №18_____ від «27» червня 2024 року

Схвалено науково-методичною комісією факультету інформаційних технологій

Протокол №__ від «27» червня 2024 року

Голова науково-методичної комісії _____ (Ганна КРАСОВСЬКА)

«_____» _____ 2024 року

Програму перевірено

1. Метою дисципліни «Захист інформації в інтернеті речей» (ВК.1.08) є формування у студентів здатностей:

Метою дисципліни «Захист інформації в інтернеті речей» є формування у студентів наступних здатностей до:

- ідентифікації та аналізу загроз і вразливостей – визначення потенційних загроз та вразливостей інформаційних систем в Інтернеті речей (IoT), проведення аналізу ризиків та оцінки можливих наслідків для безпеки інформації;
- моніторингу та виявлення інцидентів безпеки – налаштування систем моніторингу для виявлення інцидентів безпеки в реальному часі, аналіз та розслідування інцидентів інформаційної безпеки;
- реагування та відновлення після інцидентів – розробка та впровадження планів реагування на інциденти, здійснення заходів з відновлення функціональності інформаційних систем після інцидентів;
- застосування сучасних технологій та методів захисту – використання криптографічних методів для захисту даних в IoT, застосування методів аутентифікації та авторизації для забезпечення контролю доступу;
- проведення аудиту та тестування на проникнення – здійснення аудиту безпеки інформаційних систем та мереж, проведення тестування на проникнення для виявлення та усунення вразливостей.

2. Попередні вимоги до опанування або вибору навчальної дисципліни:

1) успішне опанування дисциплін «Операційні системи», «Технології програмування», «Основи програмування», «Вступ до мереж»;
2) базові знання у сфері інформаційних технологій: розуміння основ комп'ютерних мереж, включаючи протоколи передачі даних, топології мереж та принципи їх функціонування.
3) вміння проводити дослідження та аналіз: навички проведення досліджень, збору, аналізу та інтерпретації інформації, вміння використовувати наукові та технічні джерела для знаходження інформації, необхідної для вирішення завдань у сфері захисту інформації.

3. Анотація навчальної дисципліни:

Навчальна дисципліна «Захист інформації в інтернеті речей» спрямована на підготовку фахівців, здатних забезпечити ефективний захист інформації в умовах стрімкого розвитку технологій IoT. Курс охоплює основні принципи, методи та засоби забезпечення інформаційної безпеки в IoT-системах, враховуючи специфічні виклики та загрози, що виникають в цій сфері.

4. Завдання (навчальні цілі): полягають у тому, щоб надати студентам всебічне розуміння принципів та методів забезпечення інформаційної безпеки в середовищі IoT. Перш за все, курс має на меті ознайомити студентів з основними концепціями та архітектурою IoT, що включає вивчення ключових компонентів таких систем, як сенсори, актуатори та мережеві елементи. Це дозволить студентам зрозуміти, як функціонують пристрої IoT і як вони взаємодіють в мережі.

Далі, значна увага приділяється ідентифікації та аналізу загроз і вразливостей, притаманних IoT-середовищу. Студенти навчаться виявляти основні загрози та оцінювати можливі ризики, що дозволить їм зрозуміти, які саме аспекти безпеки потребують особливої уваги. Це включає вивчення методів аналізу ризиків та оцінки наслідків для інформаційної безпеки в контексті IoT.

Курс також охоплює опанування методів захисту інформації. Студенти дізнаються про принципи забезпечення конфіденційності, цілісності та доступності даних в IoT-системах. Особливу увагу буде приділено криптографічним методам захисту інформації, їх застосуванню в IoT та специфічним викликам, пов'язаним із цим.

У процесі навчання студенти засвоять технології аутентифікації та авторизації, необхідні для забезпечення безпеки в IoT. Вони дізнаються про різні методи контролю доступу та управління правами користувачів, що дозволить їм ефективно захищати дані від несанкціонованого доступу.

Крім того, курс має на меті навчити студентів використовувати сучасні системи моніторингу та виявлення аномалій для своєчасного виявлення інцидентів безпеки. Студенти навчаться аналізувати та реагувати на інциденти, розробляти та впроваджувати плани реагування та відновлення.

Окремо розглядаються питання розробки та впровадження політик безпеки для IoT-систем, а також їх інтеграції в загальні бізнес-процеси організацій. Студенти дізнаються про важливість створення ефективних політик безпеки та способи їх реалізації.

Завершальним етапом курсу є навчання проведенню аудиту безпеки та тестування на проникнення в IoT-системах. Це допоможе студентам виявляти та усувати вразливості до того, як вони можуть бути використані зловмисниками.

Таким чином, курс «Захист інформації в інтернеті речей» має на меті забезпечити студентів комплексними знаннями та навичками, необхідними для ефективного захисту інформації в умовах зростаючої кількості IoT-пристроїв та технологій.

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	*Основні концепції та архітектуру Інтернету речей*	*Лекції курсу лабораторні роботи курсу, самостійна робота, дискус, аналітична доповідь*	*Опитування, тестування, залік*	30%
1.2	*Основні загрози та вразливості, характерні для IoT-середовища*			
1.3	*Принципи забезпечення конфіденційності, цілісності та доступності даних.*			
1.4	*Методи криптографічного захисту інформації та їх застосування в IoT*			
1.5	*Сучасні методи, технології та засоби захисту інформації в IoT*			
2.1	*Ідентифікувати та аналізувати загрози та вразливості в IoT-системах*		*Звіт з лабораторних робіт, тестування, залік*	10%
2.2	*Розробляти та впроваджувати плани реагування на інциденти та відновлення систем*			25%
2.3	*Використовувати криптографічні методи для захисту даних*			15%

3	*Ефективно спілкуватися з командою, пояснюючи складні технічні концепції доступною мовою*		*Виконання групових досліджень за додатковою тематикою курсу*	20%

6. Співвідношення результатів навчання дисципліни із програмними результатами навчання

Програмні результати навчання (код)	Результати навчання дисципліни (код)								
	1.1	**1.2**	**1.3**	**1.4**	**1.5**	**2.1**	**2.2**	**2.3**	**3**
ПР 3. Використовувати базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології розроблення алгоритмів і комп'ютерних програм мовами високого рівня із застосуванням об'єктно-орієнтованого програмування для розв'язання задач проектування і використання інформаційних систем та технологій.	+	+	+	+	+	+	+	+	
ПР 5. Аргументувати вибір програмних та технічних засобів для створення інформаційних систем та технологій на основі аналізу їх властивостей, призначення і технічних характеристик з урахуванням вимог до системи і експлуатаційних умов; мати навички налагодження та тестування програмних і технічних засобів інформаційних систем та технологій.						+	+	+	+
ПР 6. Демонструвати знання сучасного рівня технологій інформаційних систем, практичні навички програмування та використання прикладних і спеціалізованих комп'ютерних систем та середовищ з метою їх запровадження у професійній діяльності.	+	+	+	+	+	+	+	+	
ПР 15. Демонструвати знання основних методів та технологій об'єктно-орієнтованого програмування, а також основ інших парадигм програмування, основ конструювання програмного забезпечення, раціональні алгоритми вирішення задач оптимізації та оптимального керування, уміння ставити конкретну прикладну задачу, знаходити оптимальні рішення за допомогою методів прийняття рішень.	+	+	+	+	+				+
ПР 18. Розробляти та проводити тестування для кожного програмного модуля проекту, кваліфіковане тестування всього програмного комплексу відповідно до існуючих або сформульованих вимог, подальша інсталяція програмного продукту та його обслуговування.					+	+	+	+	+
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: рівень досягнення усіх запланованих результатів навчання визначається за результатами вивчення відеолекцій розміщених в Teams, проміжного тестування за двома модулями, захисту результатів лабораторних робіт, опитування та реферативної доповіді в рамках дисципліни. Дисципліна закінчується **заліком**.

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

• результати навчання 1-(знання) РН 1.1., РН 1.2., РН 1.3., РН 1.4., РН 1.5. - до 30% ;

• результати навчання 2-(вміння) РН 2.1., РН 2.2., РН 2.3.- до 50% ;

• результати навчання 3-(комунікація) РН 3 - до 20%.

7.2 Організація оцінювання.

Семестрове оцінювання: 60 балів (100%)

Оцінка за семестр формується шляхом успішного виконання та обов'язкового захисту лабораторних робіт, а також реферативних виступів та відповідей при дискусіях на лекційних заняттях.

Поточне оцінювання проводиться у формі опитування студентів за темами попередніх лекцій, темами лабораторних робіт чи темами домашнього завдання, проміжного тестування. Здобувач виконує та захищає 9 лабораторних робіт, що оцінюються від 2 до 3 балів за кожну роботу (всього від 16 до 24 балів).

Якщо здобувач не вчасно виконує лабораторну роботу, то оцінка знижується на 0,5 бали за кожен тиждень протермінування. Робота вважається зданою вчасно, коли захист відбувається на наступній парі після видачі завдання, якщо викладачем не повідомлено інші терміни. Терміни здачі викладач оголошує та викладає окремим повідомленням в команді системи Microsoft Teams (чи інших затверджених кафедрою системах навчання).

Протягом семестру проводиться проміжний контроль у формі тестування за тематикою лекційних занять. Студенти приймають активну участь у дискусах на лекційних заняттях. Оцінюється від 8 до 16 балів.

Для студентів, які набрали сумарно меншу кількість балів ніж критично-розрахунковий мінімум (48 балів), для допуску до заліку не допускаються. Обов'язковими є виконання та захист запланованих індивідуальних лабораторних, практичних робіт та проміжного тестування на бали від 60%.

Підсумкове оцінювання *у* формі заліку: складає *20 модульних балів (20% від загального рейтингу).*

На останньому занятті проводиться залікова робота у формі тестування.

Оцінка за залік не може бути меншою 12 балів для отримання позитивної оцінки за предмет.

Підсумкова оцінка визначається шляхом підсумовування балів семестрової роботи та залікового тестування. Якщо у підсумку студент набрав більше 60 балів, йому ставиться оцінка «зараховано».

При простому розрахунку отримаємо:

	Лабораторні роботи	Проміжне тестування	Залікове тестування	Підсумкова оцінка
Мінімум	16	8	12	60
Максимум	24	36	40	100

7.3 Шкала відповідності оцінок

Зараховано / Passed	60-100
Не зараховано / Fail	0-59

8. Структура навчальної дисципліни.

№ п/п	Назва лекції	Кількість годин		
		Лекції	Лабораторні	СР
1	Тема 1. Основи інформаційної безпеки	2	2	4
2	Тема 2. Загрози та вразливості в IoT-середовищі	2	4	6
3	Тема 3. Принципи захисту інформації в IoT	2	4	6
4	Тема 4. Аутентифікація та авторизація в IoT	2	4	6
5	Тема 5. Захист мережевих з'єднань в IoT	2	4	8
6	Тема 6. Моніторинг та виявлення інцидентів в IoT	2	4	8
7	Тема 7. Реагування на інциденти та відновлення після атак	2	4	6
8	Тема 8. Політики безпеки для IoT	2	4	6
9	Тема 9. Аудит та тестування на проникнення в IoT-системах	2	4	6
10	Тема 10. Нормативні вимоги та стандарти в сфері інформаційної безпеки IoT	2	4	8
	ВСЬОГО ЗА СЕМЕСТР	**20**	**34**	**64**

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

9. Рекомендовані джерела:

Основна: *(Базова)*

1. Sen, J., & Mishra, S. (Eds.). (рік видання). Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations. – 2016.
2. Simon, M-Sh. Building the Internet of Things: Implement New Business Models, Disrupt Competitors, Transform Your Industry. – 2018.
3. Russel, B. Practical Internet of Things Security. – 2018.
4. Jessu, Sh. Securing the Internet of Things. – 2021.
5. Johnson, B.K. IoT Security: A Guide for IT and Security Professionals. – 2019.