МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний економічний університет

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
_____ Задорожний З.-М. В.
"24" 09 2019 р.

РОБОЧА ПРОГРАМА
з дисципліни
«БЕЗПЕКА ІНТЕРНЕТ-РЕЧЕЙ»

рівень вищої освіти – третій (освітньо-науковий)
галузь знань – 12 Інформаційні технології
спеціальність – 121 Інженерія програмного забезпечення
освітньо-наукова програма – «Інженерія програмного забезпечення»

Тернопіль – ТНЕУ
2019

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ “Безпека Інтернет-речей”

1. Опис дисципліни “Безпека Інтернет-речей”

Дисципліна “Безпека Інтернет-речей”	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів – 5	галузь знань – 12 Інформаційні технології	**Статус дисципліни** вибіркова **Мова навчання** українська
Кількість залікових модулів – 1	спеціальність 121 Інженерія програмного забезпечення	Рік підготовки: *Денна – 1* *Заочна – 1* Семестр: *Денна – 2* *Заочна – 2,3*
Кількість змістових модулів – 2	рівень вищої освіти – третій (освітньо-науковий)	Аудиторні години: *Денна – 30* *Заочна – 12*
Загальна кількість годин – 150		Самостійна робота: *Денна – 120* *Заочна – 138*
Тижневих годин – 10, з них аудиторних – 2		Вид підсумкового контролю – *залік*

2. Мета і завдання дисципліни «Безпека Інтернет-речей»

2.1. Мета вивчення дисципліни.

Метою дисципліни «**Безпека Інтернет-речей**» є отримання знань та умінь, які необхідні для розробки та дослідження безпеки Інтернет-речей.

2.2. Завдання вивчення дисципліни

Основне завдання дисципліни дати студентам теоретичну та практичну підготовку з безпеки Інтернет-речей.

2.3. Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни.

Здатність виявляти, ставити та вирішувати проблеми дослідницького характеру в сфері інженерії програмного забезпечення, оцінювати та забезпечувати якість виконуваних досліджень.

2.4. Передумови для вивчення дисципліни.

Перелік знань, які мають бути вивчені раніше: засоби та технології програмування; дослідження і проектування систем захисту інформації; моніторинг мережевої безпеки, тестування комп'ютерних систем на проникнення.

2.5. Результати навчання.

Розробляти та реалізовувати наукові та/або інноваційні інженерні проекти, які дають можливість переосмислити наявне та створити нове цілісне знання та/або професійну практику і розв'язувати значущі наукові та технологічні проблеми інженерії програмного забезпечення з дотриманням норм академічної етики і врахуванням соціальних, економічних, екологічних та правових аспектів.

3. Програма навчальної дисципліни: «Безпека Інтернет-речей»

Змістовий модуль 1. Концепції та моделі IoT

Тема 1. Концепції гарантоздатності та безпеки для IoT.

1. Таксономія вимог надійності та безпеки.
2. Гарантоздатність, надійність та безпека визначає таксономію.
3. Основи аналізу ризиків.

Література: 1, 2, 4.

Тема 2.Моделі гарантоздатності та надійності IoT.

1. Довідкові архітектури Індустріальних IoT.
2. Заходи щодо надійності та безпеки.
3. Режим відмов, аналіз ефектів та критичності (FMECA) систем IoT.

Література: 1, 2, 3.

Тема 3. Моделі безпеки для IoT.

1. Архітектури систем IoT з точки зору безпеки.

2. Заходи безпеки.
3. Моделювання загроз та атак для систем IoT.
Література: 1, 2, 5.

Тема 4. Вимоги управління безпекою до IoT.
1. План управління безпекою та безпекою.
2. Управління людськими ресурсами.
3. Управління конфігурацією.
4. Підбір та оцінка інструментів.
5. Управління документацією.
6. Оцінка безпеки та безпеки.
Література: 1, 2, 10.

Тема 5. Життєвий цикл безпеки та безпеки для IoT.
1. Загальний життєвий цикл.
2. Життєвий цикл безпеки та безпеки: дизайнерський обід зверху вниз.
3. Життєвий цикл безпеки та безпеки: інтеграція вгорі.
4. Відстеження вимог.
Література: 1, 2, 6.

Тема 6. Огляд, аналіз та методи тестування IoT.
1. Огляд документів.
2. Статичний аналіз коду.
3. Функціональне тестування.
4. Структурне тестування коду.
Література: 1, 4, 9.

Змістовий модуль 2. **Прийоми та заходи безпеки для IoT.**
Тема 7. Забезпечення Case основи.
1. Концепція та історія Case основи.
2. Стандарти щодо забезпечення Case.
Література: 1, 2, 9, 10.

Тема 8. Прийоми та заходи безпеки для IoT.
1. Позначення претензій, аргументів та доказів (CAE).
2. Оновлення та застосування записів про претензії, аргументи та докази (CAE)
3. Позначення про структурування цілей (GSN).
Література: 1, 2, 4.

Тема 9. Інформація про безпеку та інформування про енергетичну ефективність
1. Інструменти для розробки випадку впевненості.
2. Структура випадку впевненості для систем IoT.
Література: 1, 2, 7.

Тема 10. Основи технології blockchain та приклади застосування
1 Принцип технології blockchain
2 Структура блоку та дерево Меркле
3 Криптографія в блокчейні
Література: 1, 2, 10.

Тема 11. Алгоритми консенсусу в технології Blockchain
1 Алгоритм підтвердження роботи
2 Доведення алгоритмів консенсусу
3 Технологія Blockchain для безпеки IoT
Література: 1, 2, 5

Тема 12. Технологія Blockchain для безпеки IoT
1 Blockchain та IoT
2 Переваги інтеграції Blockchain з IoT
3 Основні проблеми Blockchain в IoT
4 Рішення безпеки IoT на основі Blockchain
Література: 1, 2, 8.

4. Структура залікового кредиту з дисципліни "Безпека Інтернет-речей"

(денна форма навчання)

	Кількість годин	
	Аудиторні години	Самостійна робота
Змістовий модуль 1. *Концепції та моделі IoT*		
Тема 1. Концепції гарантоздатності та безпеки для IoT.	2	8
Тема 2. Моделі гарантоздатності та надійності IoT	2	8
Тема 3. Моделі безпеки для IoT.	2	8
Тема 4. Вимоги управління безпекою до IoT.	2	8
Тема 5. Життєвий цикл безпеки та безпеки для IoT.	2	10
Тема 6. Огляд, аналіз та методи тестування IoT.	2	10
Змістовий модуль 2 Прийоми та заходи безпеки для IoT		
Тема 7. Забезпечення Case основи	4	8
Тема 8. Прийоми та заходи безпеки для IoT	4	10
Тема 9. Інформація про безпеку та інформування про енергетичну ефективність	2	10
Тема 10. Основи технології blockchain та приклади застосування	2	12
Тема 11. Алгоритми консенсусу в технології Blockchain	4	14
Тема 12. Технологія Blockchain для безпеки IoT	2	14
Разом	**30**	**120**

(заочна форма навчання)

	Кількість годин	
	Аудиторні години	Самостійна робота
Змістовий модуль 1. *Концепції та моделі IoT*		
Тема 1. Концепції гарантоздатності та безпеки для IoT.	1	10
Тема 2. Моделі гарантоздатності та надійності IoT	1	10
Тема 3. Моделі безпеки для IoT.	1	10
Тема 4. Вимоги управління безпекою до IoT.	1	10
Тема 5. Життєвий цикл безпеки та безпеки для IoT.	1	12
Тема 6. Огляд, аналіз та методи тестування IoT.	1	12
Змістовий модуль 2 Прийоми та заходи безпеки для IoT		
Тема 7. Забезпечення Case основи	1	12
Тема 8. Прийоми та заходи безпеки для IoT	1	12
Тема 9. Інформація про безпеку та інформування про енергетичну ефективність	1	10
Тема 10. Основи технології blockchain та приклади застосування	1	12
Тема 11. Алгоритми консенсусу в технології Blockchain	1	14
Тема 12. Технологія Blockchain для безпеки IoT	1	14
Разом	**12**	**138**

5. Самостійна робота

№ п/п	Тематика	К-сть годин ДФН	К-сть годин ЗФН
1	Концепція Інтернет речей (IoT)	6	8
2	Як працює Інтернет речей?	6	6
3	Архітектури Інтернет речей (IoT)	6	8
4	Моделі комунікації IoT	6	8
5	Модель пристрою до пристрою	6	6
4	Режим "Пристрій до пристрою"	6	8
5	Модель пристрою до шлюзу	6	6
6	Резервний режим обміну даними	6	8
7	Розуміння нападів IoT	6	6
8	Проблеми перед IoT	6	6
9	OWASP Топ-10 вразливостей IoT	6	8
10	Ланшафт атаки IoT	6	6
11	DDoS атака	6	8
12	Rolling Gode атака	6	6
13	BlueBorne атака	6	6
14	Атака заклинювання	6	8
15	Backdoor	6	6
16	Методологія злому IoT	6	8

17	Збір інформації	6	6
18	Сканування вразливості	6	6
19	Контрзаходи	6	6
20	Розумні контракти	6	6
Разом:		**120**	**138**

6. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни "**Безпека Інтернет-речей**" використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

- стандартизовані тести;
- поточне опитування;
- залікове модульне тестування та опитування;
- наскрізні проекти;
- командні проекти;
- аналітичні звіти, реферати, есе;
- розрахункові та розрахунково-графічні роботи;
- студентські презентації та виступи на наукових заходах;
- завдання на лабораторному обладнанні, тренажерах, реальних об'єктах тощо;
- залік.

7. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100-бальною шкалою) з дисципліни "**Безпека Інтернет-речей**" визначається за шкалою оцінювання:

За шкалою ТНЕУ	**За національною шкалою**	**За шкалою ECTS**
90–100	відмінно	A (відмінно)
85–89	добре	B (дуже добре)
75-84		C (добре)
65-74	задовільно	D (задовільно)
60-64		E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов'язковим повторним курсом)

8. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№	**Найменування**	**Номер теми**
1.	Мультимедійний проектор	1 – 12
2.	Комп'ютерна лабораторія. Доступ до Інтернету.	1 – 12
3.	Одноплатні комп'ютери Raspberry Pi	2 – 12

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Інтернет речей для індустріальних і гуманітарних застосунків. У трьох томах. Том 1. Основи і технології / За ред. В. С. Харченка. - Міністерство освіти і науки України, Національний аерокосмічний університет ХАІ, 2019. -547 с.

2. Sklyar V.V., Yatskiv V.V., Yatskiv N.G. Dependability and Security of IoT: Practicum / Kharchenko V.S. and Sklyar V.V. (Eds.) – Ministry of Education and Science of Ukraine, National Aerospace University “KhAI”, Ternopil National Economic University, 2019. – 98 p.

3. Hanssen G., Stålhane T, Myklebust T. SafeScrum® – Agile Development of Safety-Critical Software. Springler, 2018.

4. NISTIR 8200, Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT). –National Institute of Standards and Technologies, 2018.

5. NIST SP 1500-201, Framework for Cyber-Physical Systems. National Institute of Standards and Technologies, 2017.

6. Martins B., Laranjeiro N., Vieira M. INTENSE: INteroperability TEstiNg as a Service // Proceedings of 2017 IEEE International Conference on Web Services (ICWS 2017).

7. Nunes P., Medeiros I., Fonseca J. at all. Benchmarking Static Analysis Tools for Web Security. IEEE Transactions on Reliability (2018), 67(3): 1159-1175

8. Sklyar V., Kharchenko V. Green Assurance Case: Applications for Internet of Things. Green IT Engineering: Social, Business and Industrial Applications. Studies in Systems, Decision and Control, vol 171. Springer, Cham, 2019.

9.Haddon-Cave C. The Nimrod Review. An independent review into the broader issues surrounding the loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006. Crown Copyright, 2009.

10. Kelly T. Are Safety Cases Working? Safety Critical Systems Club Newsletter, Vol. 17, n. 2, 2008.