Міністерство освіти і науки України
Дніпровський національний університет залізничного транспорту імені академіка В. Лазаряна

Факультет «Комп'ютерні технології і системи»
Кафедра «Електронні обчислювальні машини»

ЗАТВЕРДЖУЮ
Перший проректор
професор _____ Б. Є. Боднар
«__» _____ 2021 р.

РОБОЧА ПРОГРАМА
навчальної дисципліни

ВВЕДЕННЯ В «ІНТЕРНЕТ РЕЧЕЙ» ТА КІБЕРБЕЗПЕКУ

Рівень вищої освіти – **другий (магістерський)**

Статус дисципліни – **вибіркова**

Обсяг – **3 кредита ЄКТС**

Дисципліна є компонентою освітньої програми:

Шифр галузі	Код і назва спеціальності	Назва ОП	Код навчальної дисципліни
03 Гуманітарні науки	035 Філологія	Германські мови та літератури (переклад включно)	ВБ 12.2

Форма підсумкового контролю – **залік**

м. Дніпро – 2021

Розробник робочої програми  доцент О.Й. Сторов

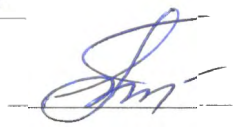
Робочу програму розглянуто та схвалено на засіданні кафедри «Електронні обчислювальні машини»

«24» 06 2021 р. протокол № 12

Завідувач кафедри, д. т. н., професор  І. В. Жуковицький

Розглянуто та схвалено вченою радою економіко-гуманітарного факультету

«29» 06 2021 р. протокол № 8

Голова вченої ради, доцент  Т. В. Полішко

ПОГОДЖЕННЯ:

Робоча програма дисципліни відповідає нормативам навчального плану

Начальник навчального відділу  Л. С. Андрашко

«01» 09 2021 р.

Робоча програма дисципліни відповідає вимогам нормативно-методичних документів

Начальник навчально-методичного відділу  С.М Гончаренко

«06» 09 2021 р.

1. Мета навчальної дисципліни

Предметом вивчення навчальної дисципліни є теоретичні та практичні основ «Інтернет речей» та їх кіберзахисту.

Метою дисципліни є досягнення компетентностей, які основані на зазначених в освітньо-професійній програмі (ОП):

1. Здатність до пошуку, опрацювання та аналізу інформації з різних джерел (загальна компетентність, ЗК3).
2. Уміння виявляти, ставити та вирішувати проблеми (загальна компетентність, ЗК4).
3. Здатність працювати в команді та автономно (загальна компетентність, ЗК5).
4. Навички використання інформаційних і комунікаційних технологій (загальна компетентність, ЗК9).
5. Усвідомлення ролі інтелектуальної власності у інноваційному розвитку суспільства (загальна компетентність, ЗК13).
6. Здатність генерувати нові ідеї (креативність) (загальна компетентність, ЗК15).
7. Усвідомлення методологічного, організаційного та правового підґрунтя, необхідного для досліджень та/або інноваційних розробок у галузі філології, презентації їх результатів професійній спільноті та захисту інтелектуальної власності на результати досліджень та інновацій (професійна компетентність, ФК5).

У процесі вивчення дисципліни у студентів формуються наступні «соціальні навички» Soft skills:

1. Особистісні: здатність приймати рішення та чітко формулювати цілі при виникнення неполадок в роботі комп'ютерних систем і мереж (ОН2, ОН3).
2. Комунікаційні: зрозуміло формулювати думки при формулюванні теоретичних та практичних питань (КН1), вислуховувати усі точки зору про прийняття рішення що до організації робіт виправлення аварійних ситуацій в роботі комп'ютерних систем (КН4).
3. Управлінські: мотивувати та розвивати членів команди для дотримання правил роботи з комп'ютерними системами і в мережі (УН2, УН3).

2. Міждисциплінарні зв'язки

Перелік дисциплін, які потрібні для вивчення дисципліни «Введення в «Інтернет речей» та кібербезпеку» (ВБ 12.2):

ВБ 11.1	Охорона праці в галузі та цивільний захист
ВБ 11.2	Профілактика та локалізація техногенних аварій і катастроф
ВБ 11.3	Небезпеки сучасного світу

Дисципліни, вивчення яких спираються на дисципліні «Введення в «Інтернет речей» та кібербезпеку» (ВБ 12.2):

ОК1	Інтелектуальна власність
ОК2	Сучасні інформаційні технології при перекладі
ОК9	Науково-виробнича практика

3. Очікувані результати навчання

Дисципліна «Введення в «Інтернет речей» та кібербезпеку» відповідно до ОПП другого (магістерського) рівня вищої освіти спеціальності 035 Філологія, що затверджено головою вченої ради проф. Пшінько О.М. від 10.09.2020р., повинна забезпечити такі результати навчання (ПР):

Знання і розуміння:	
ПРН1	Оцінювати власну навчальну та науково-професійну діяльність, будувати і втілювати ефективну стратегію саморозвитку та професійного самовдосконалення
Застосування знань і розумінь:	
ПРН3	Застосовувати сучасні методики і технології, зокрема інформаційні, для успішного й ефективного здійснення професійної діяльності та забезпечення якості дослідження в конкретній філологічній галузі
Формування суджень:	
ПРН24	Володіти новими інформаційними та мультимедійними технологіями й орієнтуватися в інформаційному просторі: здатність знаходити та систематизувати джерела інформації за певним критерієм; використовувати різноманітні шляхи отримання, перетворення та збереження інформації, актуалізувати її в ситуаціях інтелектуально-пізнавальної діяльності з метою застосування в процесі перекладу

Очікуванні результати навчання (ОРН), які повинні бути досягнуті після опанування дисципліни «Введення в «Інтернет речей» та кібербезпеку».

№	ОРН	Рівень	Шифр ПРН
1	Оволодіти загальними знаннями побудови комп'ютерних мереж, операційних систем та мережевого обладнання	IV	ПРН3, ПРН24
2	Оволодіти загальними знаннями про способи захисту даних і конфіденційність в Інтернеті	III, IV	ПРН3, ПРН24
3	Зрозуміти освітні та ділові можливості в цифровому світі	II, III	ПРН3
4	Зрозуміти основи побудови IoT	II, III	ПРН3
5	Зрозуміти сучасні види кіберугроз та технології протидії їм	II, III	ПРН3
6	Мати базові поняття про Big Data та Google Drive	I, II	ПРН1, ПРН3
7	Мати базові поняття безпеки в цифровому світі	I	ПРН1
8	Мати знання про інформацію та засоби її зберігання	I	ПРН1

4. Критерії оцінювання результатів навчання

Шкала ЄКТС	ОРН
A	Знати основи побудови комп'ютерних мереж. операційних систем та мережевого обладнання
B	Мати знання про способи та засоби автоматизації в сучасному світі
C	Знати сучасні види кіберугроз та технології протидії їм
D	Маті знання про інформацію в сучасному світі
E	Знати базові поняття безпеки в цифровому світі
Fx	Мати основні представлення про IoT
F	Окреслити коло вирішуваних задач

Досягнення вищих оцінок за шкалою ЄКТС базується на досягнутих нижчих.

5. Види діагностування результатів навчання

Семестр	Вид контролю	Бал
Перший	ПК 1	100

Співставлення шкал оцінювання

Бал	Оцінка ECTS	Оцінка за чотирибальною шкалою	
90-100	A	відмінно	відмінно
82-89	B	добре	дуже добре
75-81	C		добре
67-74	D	задовільно	задовільно
60-66	E		достатньо
35-59	Fx	незадовільно	незадовільно з повторним складанням контрольного заходу
1-34	F		незадовільно з повторним вивченням дисципліни

6. Розподіл навчального часу для денної форми навчання на 2021 / 2022 навчальний рік

Види навчання	Третій семестр	
	І половина	
	кр год.	кр ECTS
Загальний обсяг за навчальним планом	90	3
Навчальні заняття:		
- лекції		
- лабораторні заняття		
- практичні заняття	32	
- семінарські заняття		
Самостійна робота:	58	
- підготовка до лекцій		
- підготовка до практичних робіт	16	
- підготовка до лабораторних робіт		
- виконання і захист курсового проекту		
- виконання і захист курсового завдання		
- опрацювання розділів програми, які не викладаються на лекціях	24	
- підготовка до контрольних заходів	18	
підсумковий контроль	ПК1	

7. Зміст дисципліни

Модуль	Тема лекцій (заняття)	Обсяг годин	СН
ПК1	**Поточний контроль 1 (1 половина третього семестру): Introduction to IoT, Introduction to Cybersecurity**		
	Практичні заняття Практичне заняття 1. Все підключено	4	УН3
	Практичне заняття 2. Всі речі можна програмувати	4	УН2
	Практичне заняття 3. Все навколо створює дані	4	УН3, УН2
	Практичне заняття 4. Все може бути автоматизованим	4	ОН2
	Практичне заняття 5. Все повинно бути захищеним	4	ОН2, КН1
	Практичне заняття 6. Освітні та ділові можливості	4	УН3
	Практичне заняття 7. Потреба в кібербезпеці	2	ОН3
	Практичне заняття 8. Атаки, поняття та методи	2	
	Практичне заняття 9. Захист даних і конфіденційність	2	КН4
	Практичне заняття 10. Захист організації	2	ОН2, КН4
	Самостійна робота Підготовка до аудиторних занять (практичних, практичних занятій)	16	УН3
	Опрацювання розділів програми, які не викладаються на лекціях	24	ОН2
	Підготовка до контрольних заходів та їх складання	18	
		90 3 кр ECTS	

ПРАКТИЧНІ ЗАНЯТТЯ

№№ робіт	Зміст роботи	Обсяг, години	Тестове завдання			
			кількість	просте	середнє	складне
1	2	3	4	5	6	7
1	**Все підключено** 1.1: Цифрова трансформація 1.2: Вплив цифрової трансформації на бізнес 1.3: Визначте своє покоління	4	15	8	4	3

2	**Всі речі можна програмувати** 2.1: Застосувати базове програмування для підтримки пристроїв IoT 2.2: Прототипування вашої ідеї	4	15	8	4	3
3	**Все навколо створює дані** 3.1: Великі дані 3.2: Джерела інформації 3.3: Візуалізація даних	4	15	8	4	3
4	**Все може бути автоматизованим** 4.1: Що може бути автоматизованим? 4.2: Як використовують автоматизацію	4	15	8	4	3
5	**Все повинно бути захищеним** 5.1: Безпека в цифровому світі 5.2: Виклики захисту пристроїв IoT 5.3 Фізична безпека	4	15	8	4	3
6	**Освітні та ділові можливості** 6.1: Виклики та можливості в цифровому світі 6.2: Ринок ділової активності 6.3: Навчання протягом всього життя	4	15	8	4	3
7	**Потреба у кібербезпеці** 7.1: Персональні дані 7.2: Корпоративні дані 7.3: Зловмисники та експерти з кібербезпеки 7.4: Кібервійни	2	9	4	3	2
8	**Атаки, поняття та методи** 8.1: Аналіз кібератаки 8.2: Ландшафт кібербезпеки	2	6	2	2	2
9	**Захист даних і конфіденційність** 9.1: Захист ваших даних 9.2: Захист конфіденційності в Інтернеті	2	5	1	2	2
10	**Захист організації** 10.1: Міжмережні екрани 10.2: Підхід до кібербезпеки на основі поведінки 10.3: Підхід Cisco до кібербезпеки	2	5	1	2	2

ОПРАЦЮВАННЯ РОЗДІЛІВ ПРОГРАМИ, ЯКІ НЕ ВИКЛАДАЮТЬСЯ НА ЛЕКЦІЯХ

№№	Назва теми	Обсяг, години	Тестове завдання			
			кількість			
				просте	середнє	складне
1	Поняття Big Data	6	10	5	3	2
2	Робота з Google Drive	6	10	5	3	2
3	Операційна система Windows	12	10	5	3	2

8. Методи навчання

Практичні заняття починаються з пояснення з використанням електронних дидактичних демонстраційних матеріалів. Далі виконуються тренувальні вправи за певним зразком.

Підготовка до практичних занять передбачає опрацювання теоретичного матеріалу та виконання тесту для в главах курсів Introduction to IoT, Introduction та to Cybersecurity.

Підготовка до поточного контролю передбачає опрацювання питань глав курсів Introduction to IoT, Introduction та to Cybersecurity та виконання тестів для самоконтролю.

Здатність приймати рішення (ОН2) розвивається та реалізується студентами на практичних заняттях, під час яких пропонуються при різноваріантності рішень не штатних ситуацій в роботі комп'ютерної техніки.

Здатність чітко формулювати цілі (ОН3) розвивається у студентів під час підготовки та захисту практичних робіт з дослідженням.

Розвивати здатність мотивувати команду (УН2) під час тих навчальних занять студенти висловлюють мотиви зміцнення і розвитку комп'ютерних систем.

Розвивати членів команди (УН3) під час тих навчальних занять студентам необхідно надавати допомогу один одному для успішного оволодіння необхідними знаннями.

Здатність зрозуміло формулювати думки (КН1) усно і письмово формується на аудиторних заняттях під час спілкування з викладачем та студентами.

Вміння вислуховувати усі точки зору (КН4) набувається студентами для подальшого прийняття рішення в невизначеній обстановці з точки зору не штатних ситуацій в комп'ютерних системах і мережах.

9. Методи оцінювання

Вид контролю	Метод демонстрування результатів навчання	Бал
ПК1(перший семестр)	Згідно виконання практичних робіт № 1-10 та проведення тестування кожного з курсів.	**60..100**
	Всього	**60..100**

Несуть відповідальність студенти, які під час будь-якого методу оцінювання порушують принципи академічної доброчесності, тобто: списують, - виконують аудиторну письмову роботу із залученням зовнішніх джерел інформації, крім дозволених для використання; обманюють – видають роботи (курсове завдання), які виконані третіми особами, як власні. За порушення академічної доброчесності із результату, який отримав студент, вираховується 30 % від максимального балу за той захід оцінювання, в якому було виявлено порушення.

10. Методичне забезпечення

1. Introduction to IoT. Інтернет-ресурс Академії CISCO, netacad.com
2. Introduction to CyberSecurity. Інтернет-ресурс Академії CISCO, netacad.com.

11. Рекомендована література

Основна

1. Kimberly Graves. CEH: Official Certified Ethical Hacker Review Guide [Текст] / USA: ECCouncil, 2007. – 264 с.
2. Jonathan LeBlanc. Identity and Data Security for Web Development: Best Practices [Текст] / UK.: O'Reilly Media. 2016. 204 с.
3. Гарасимчук О.І., Дудикевич В.Б., Ромака В.А. Комплексні системи санкціонованого доступу: навч. посібник [Текст] / О.І. Гарасимчук, В.Б. Дудикевич, В.А. Ромака – Л. : Вид-во Львів. політехніки, 2010. –212 с.
4. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. НД ТЗІ 2.5-005-99 [Текст] / ДСТСЗІ СБ України. – К., 1999. 25 с.
5. Основи інформаційної безпеки [Текст]: навч. пос. / Дудикевич В. Б., Хорошко В.О., Яремчук Ю.С. – Вінниця : ВНТУ, 2018. - 316 с.

Додаткова

6. Антонюк А.О. Основи захисту інформації в автоматизованих системах: Навч. посібник [Текст] / К. : Видавничий дім "КМ Академія", 2003. - 244 с.
7. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1-002-99 [Текст] / ДСТСЗІ СБ України. – К., 1999. – 31 с.
8. Кулаков Ю. А., Омелянский С. В. Компьютерные сети [Текст] / Киев: Юниор, 1999. – 544 с.
9. Забезпечення інформаційної безпеки держави [Текст] : Навчальний посібник / В. Б. Дудикевич, І. Р. Опірський, П. І. Гаранюк, В. С. Зачепило, А. І. Партика. Львів : Видавництво Львівської політехніки, 2017.— 204 с.

11. Інформаційні ресурси

Бібліотека університету та її депозитарій www.library.diit.edu.ua